Naciones Unidas A/HRC/62/45*

Asamblea General

Distr. general
21 de abril de 2026
Español
Original: inglés

Consejo de Derechos Humanos
62º período de sesiones
15 de junio a 10 de julio de 2026
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Los efectos disuasorios del ecosistema de vigilancia digital al descubierto: la erosión de los derechos de reunión y asociación

Informe de la Relatora Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Gina Romero**

Resumen

En el presente informe, la Relatora Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Gina Romero, examina las amenazas que la vigilancia digital supone para estos derechos. Partiendo de la labor realizada anteriormente en el marco del mandato, el informe documenta y pone de manifiesto los efectos disuasorios asociados a dicha vigilancia, y detalla las importantes injerencias en el ejercicio efectivo de los derechos de reunión y de asociación. En él se expone cómo deben integrarse tales efectos disuasorios en un análisis de este fenómeno desde la perspectiva del derecho de los derechos humanos, centrado en el reconocimiento de los daños acumulados y en el ecosistema de vigilancia imperante.

* Publicado nuevamente por razones técnicas el 21 de mayo de 2026.
** Los anexos del presente documento se distribuyen tal como se recibieron, únicamente en el idioma en que se presentaron.

Se ruega reciclar

I. Introducción

1. En el presente informe, la Relatora Especial sobre los derechos a la libertad de reunión pacífica y de asociación destaca las graves repercusiones de la vigilancia digital[1] en los derechos a la libertad de reunión pacífica y de asociación, centrándose específicamente en los efectos disuasorios relacionados con la vigilancia. Al detallar estas repercusiones, el informe va más allá de las perspectivas centradas en el derecho a la intimidad y/o la libertad de expresión que predominan en los estudios actuales. Este planteamiento no desdeña el impacto que sufren dichos derechos, sino que pone de manifiesto que los efectos disuasorios sobre el ejercicio de las libertades públicas afectan simultáneamente a una serie de derechos interconectados e interdependientes, lo cual provoca un daño acumulado. Resulta fundamental situar en primer plano los efectos concretos en la libertad de reunión, de asociación y de participación, dada su importancia fundamental para el buen funcionamiento de las sociedades democráticas[2].

2. La información para el presente informe se ha extraído de un estudio de alcance mundial[3] para el cual se realizaron entrevistas y consultas con diversos participantes de distintos contextos y jurisdicciones. Se entrevistó a un total de 152 activistas, defensores de los derechos humanos, defensores públicos, abogados, periodistas y representantes de la sociedad civil de todas las regiones[4] con el fin de recabar experiencias comunes o transversales en materia de vigilancia digital. Se organizó 1 consulta en la región de Oriente Medio y Norte de África, 2 en América Latina, 3 en Asia Sudoriental y 2 en África, además de 1 evento mundial en línea. Este método se diseñó para obtener datos fiables con el fin de rebatir las opiniones escépticas según las cuales los efectos disuasorios son excesivamente subjetivos o difíciles de medir de manera eficaz. El informe se alimenta además de 62 contribuciones escritas —49 procedentes de la sociedad civil, el mundo académico, organismos internacionales y una importante empresa tecnológica mundial, y 13 de los Estados— y de los datos recabados en reuniones con la sociedad civil y las víctimas, durante visitas académicas y en el marco de una visita oficial a un país. En conjunto, estos datos se refieren a 84 Estados y entidades, lo que pone de manifiesto lo extendido que está el fenómeno de los efectos disuasorios.

[1] Aunque este no es un inventario exhaustivo de las capacidades actuales y emergentes, la Relatora Especial ha constatado un uso cada vez mayor de las siguientes prácticas de vigilancia: a) los dispositivos infiltrados —en los que se han instalado herramientas comerciales de ciberintrusión (programas espía o *spyware*), como Novispy, Pegasus y Predator— y el uso de herramientas de ciencia forense digital, como Cellebrite, e interceptores de identidad internacional de abonado móvil (IMSI) para monitorear los dispositivos móviles y las actividades de sus propietarios; b) las intrusiones mediante *software* y en redes, que incluyen la intromisión e infiltración en plataformas de comunicación como WhatsApp y Signal, así como de cuentas de correo electrónico y líneas de comunicación; el ciberpatrullaje en medios sociales; y la manipulación de redes, incluida la intromisión en el sistema de nombres de dominio (DNS) de Google; c) tecnologías de identificación biométrica —como las de reconocimiento facial y la biometría conductual y de la marcha—, que a menudo se combinan con otros conjuntos de datos para la identificación y el monitoreo de personas y actividades; d) la adaptación de infraestructuras de vigilancia existentes —como sería la propagación sigilosa de las redes urbanas de videovigilancia y la reconversión de las iniciativas de "ciudad inteligente" (ambas gestionadas a menudo mediante alianzas público-privadas), el uso de vehículos aéreos (drones), el recurso al rastreo geoespacial de dispositivos y la instrumentalización de datos administrativos con fines de vigilancia; y e) las plataformas digitales gestionadas por el Estado, incluidas las aplicaciones de prestación de servicios que, en algunos casos, facilitan la delación entre particulares o sirven de mecanismos digitales para inducir a la comisión de un delito.

[2] La Relatora Especial agradece el apoyo prestado por el Centro de Derecho Internacional de la Universidad Queen Mary de Londres; el Departamento de Sociología, Política Social y Criminología de la Universidad de Southampton; y el programa Future Leaders Fellowship de UK Research and Innovation (MR/T042133/2). También agradece el apoyo prestado por auxiliares de investigación, voluntarios y pasantes.

[3] "Pushed into the shadows: evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", disponible en https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

[4] En el anexo II se describen en detalle los métodos empleados.

3. El anexo I del presente informe contiene una descripción general de las actividades clave realizadas por el mandato desde enero de 2025.

II. Normalización de la vigilancia

4. La creciente preocupación por la seguridad se ha esgrimido para justificar los avances en los sistemas de vigilancia, incluidos aquellos con doble finalidad civil y militar[5]. Unidas a la creciente securitización y militarización en todo el mundo de las fuerzas del orden y la labor policial, estas tecnologías aumentan la complejidad y la gravedad de la amenaza que se cierne sobre las libertades públicas.

5. Los sistemas digitales intrusivos, de gran alcance y de alto riesgo, que a menudo son intrínsecamente incompatibles con las obligaciones en materia de derechos humanos, suelen justificarse inadecuadamente mediante discursos que se centran en la seguridad[6] y la prevención de la delincuencia, esgrimiendo argumentos de carácter general sobre la seguridad nacional, la soberanía, el terrorismo, la seguridad pública, la delincuencia transnacional, la ciberseguridad, los delitos de odio, los "delitos morales", la desinformación y otros temas similares. El activismo cívico y político son un pretexto cada vez más frecuente para recurrir a la vigilancia. A menudo se cuelga a asociaciones y concentraciones la etiqueta de "amenaza para la seguridad nacional", "agente extranjero", "delincuente" o "terrorista"[7]. Las autoridades recurren a una combinación de estrategias de monitoreo encubierto, oculto y en línea (incluida la extracción de datos), junto con métodos más evidentes y visibles (como los drones de vigilancia).

6. Esto normaliza el desarrollo de infraestructuras de vigilancia intrusivas (incluso en las democracias), las cuales son susceptibles de ser desviadas de su finalidad original y de prestarse a una propagación encubierta de la vigilancia.

7. La normalización de la vigilancia digital suele justificarse con argumentos relacionados con la seguridad y la prevención de la delincuencia sin datos que permitan determinar su necesidad o eficacia. Los Estados han adoptado medidas excesivamente amplias que extienden la vigilancia al tiempo que evitan la transparencia, el control público y las garantías de los derechos humanos. Este giro hacia un paradigma preventivo erosiona de manera fundamental la presunción de inocencia y las debidas garantías procesales; al obligar a las personas a demostrar que no suponen ninguna amenaza, el Estado invierte, en la práctica, la carga de la prueba. Este marco facilita la criminalización a gran escala de los activistas, convirtiendo el entorno digital en un espacio de sospecha permanente.

8. La normalización de una vigilancia indiscriminada y ubicua atenta contra los requisitos fundamentales de necesidad y proporcionalidad aplicables a las restricciones de la libertad de reunión pacífica y de asociación[8].

9. Los marcos internacionales de lucha contra el terrorismo y la ciberdelincuencia que carecen de garantías en materia de derechos humanos contribuyen a la expansión y al posible uso indebido de la vigilancia digital, lo que facilita la represión transnacional[9]. En lugar de reforzar los marcos jurídicos compatibles con los derechos humanos, la tendencia a recurrir al derecho no vinculante *(soft law)* para regular a nivel multilateral y nacional las potentes herramientas de vigilancia (como los programas espía comerciales) contribuye a la normalización de dichas herramientas.

[5] Véase https://shorturl.at/0vEby y https://shorturl.at/68IL2.
[6] Véase A/HRC/52/39.
[7] A/HRC/56/49, párr. 23: "También se observa una tendencia a la designación de grupos LGBT como entidades extremistas o como amenaza para la seguridad nacional".
[8] Véase A/HRC/55/60.
[9] Véanse A/HRC/52/39 y https://tinyurl.com/2fs6frur.

III. Los ecosistemas de vigilancia en la era digital

10. La vigilancia a nivel de toda la sociedad constituye una amenaza omnipresente que es consustancial al entorno digital contemporáneo. Las herramientas digitales y los procesos alojados en línea son hoy en día fundamentales para actividades humanas básicas de tipo social, profesional y económico. Al mismo tiempo, los procesos sociales y económicos dependen del tratamiento de datos digitales. Estos factores aumentan la vulnerabilidad de todas las personas al monitoreo digital. El entorno digital contemporáneo supone un cambio cualitativo en la capacidad de vigilancia de los actores estatales y no estatales, e incluso la de entidades malintencionadas, y propicia el "autoritarismo digital".

11. La vigilancia digital se lleva a cabo de forma remota, es en gran medida invisible, implica múltiples fuentes y se caracteriza por una opacidad y una falta de transparencia inherentes. Esto significa que, aunque las personas puedan ser conscientes de la posibilidad de que se las vigile, no saben —y a menudo no pueden saber— si se las está vigilando, cuándo y cómo, ni quién lo hace. Esto da lugar a nuevas asimetrías de poder, lo que merma la capacidad de oponerse a esta vigilancia mediante la exigencia de responsabilidades ante la opinión pública o por vías políticas o jurídicas.

12. Dada la importancia fundamental de la infraestructura digital en la vida de hoy, no resulta factible sustraerse voluntariamente a la vigilancia; esto genera una situación inevitable de cercamiento digital, presentada como si la vigilancia fuera una nueva normalidad aceptada.

13. Los dispositivos digitales de uso cotidiano pueden convertirse en potentes herramientas de vigilancia: los dispositivos portátiles de seguimiento de la actividad física pueden utilizarse para mostrar la frecuencia cardíaca (o el nivel de estrés) de una persona en un momento determinado; las tarjetas electrónicas permiten rastrear los desplazamientos en transporte público; y el acceso a redes wifi o de telecomunicaciones permite determinar con precisión la presencia de una persona en un lugar concreto a una hora determinada.

14. La infraestructura de vigilancia está incorporada a la mayoría de los entornos urbanos, incluidas las escuelas y los lugares de trabajo. Muchas herramientas de vigilancia avanzadas funcionan mediante *software* y pueden integrarse en las infraestructuras de vigilancia existentes, y servir para ampliarlas. Aunque a menudo se introducen con fines legítimos, resulta sencillo desviar estas herramientas de su propósito original, por ejemplo, para reprimir el activismo de base, las asociaciones y las reuniones pacíficas.

15. Las herramientas y prácticas de vigilancia presentan una interoperabilidad cada vez mayor. En lugar de ser elementos independientes, actúan de forma conjunta para potenciar sus capacidades. Por ejemplo, la identificación biométrica puede utilizarse con imágenes de video, conectarse a arquitecturas de datos complejas (incluida la inteligencia obtenida de los medios sociales, los registros administrativos y los perfiles de los proveedores de datos comerciales) y analizarse mediante inteligencia artificial (IA). Esto supone un cambio decisivo, pues se pasa de la "minimización de datos", que consiste en extraer únicamente la información estrictamente necesaria, a la "maximización de datos", que consiste en recopilar, analizar y aprovechar toda la información disponible.

16. La vigilancia digital facilita el análisis algorítmico y basado en la IA, desencadenando así su considerable potencial. Este análisis basado en la vigilancia puede utilizarse, por ejemplo, para rastrear o monitorear a (un número casi infinito de) personas, para elaborar perfiles sobre sus hábitos de vida, para detectar actividades "sospechosas" o para ejercer control sobre personas y poblaciones. Estas herramientas pueden generar alertas cuando una persona entra o sale de una zona concreta (el denominado "geovallado") o se reúne con determinadas personas. Estas alertas se convierten en nuevos datos que propician seguir investigando o justifican una intervención física en tiempo real.

17. Esto aumenta el grado de intrusión y facilita la tarea de deducir información —por ejemplo, sobre las opiniones políticas de una persona, su afiliación a asociaciones, su participación en actividades, su orientación sexual y su estado de salud—, así como la localización y la persecución de personas.

18. La vigilancia digital también se extiende al ámbito privado. Los programas espía son un ejemplo destacado. Otras formas de vigilancia invasiva incluyen el acceso a los registros de comunicaciones por Internet o a los metadatos de las comunicaciones.

19. En conjunto, esto convierte la participación legítima en asociaciones, e incluso en grupos de la sociedad civil, o la asistencia a reuniones, en actividades de alto riesgo, especialmente para las poblaciones marginadas.

20. En lugar de centrarse en herramientas y prácticas concretas, resulta más acertado ver estos avances como elementos constituyentes de un ecosistema de vigilancia.

21. Los ecosistemas de vigilancia están compuestos por infraestructuras digitales y de datos gestionadas tanto por actores estatales como no estatales. Los actores no estatales, incluidas las entidades comerciales, disponen de datos personales detallados que resulta posible utilizar con fines de vigilancia. Además, la recopilación y la venta de datos se han convertido en sí mismas en un producto. El acceso del Estado a los datos digitales y de telecomunicaciones en manos de empresas privadas amplía considerablemente el poder y el alcance de las autoridades. Este acceso suele producirse mediante acuerdos de intercambio (formales o informales) o por mandato de las fuerzas del orden, a veces aprovechando vacíos legales o excepciones por motivos de seguridad nacional. Esta interacción entre el Estado y los actores no estatales carece de transparencia, lo que da lugar a una falta de previsibilidad que atenta contra el principio de legalidad.

22. La expansión de la vigilancia digital también viene impulsada por la falta de control sobre el poder que tienen las plataformas y los proveedores de servicios digitales, cuyos modelos de negocio suelen basarse en la extracción de datos personales a gran escala. Al diseñar arquitecturas que dan prioridad a la recolección de datos, las empresas tecnológicas privadas han creado precisamente la infraestructura que los Estados aprovechan ahora para la vigilancia. Esta coordinación entre el sector público y el privado facilita una transición fluida desde la recopilación de datos con fines comerciales hasta el monitoreo a manos del Estado. Cuando estas empresas anteponen el lucro o la obediencia a las exigencias del Estado a la protección de los usuarios se convierten en cómplices de los efectos disuasorios que erosionan el espacio cívico.

IV. Marco normativo internacional en materia de tecnología y vigilancia

23. La Asamblea General y el Consejo de Derechos Humanos han instado repetidamente a los Estados a que se abstengan de toda práctica de vigilancia ilegal o arbitraria[10], y a que velen por el respeto y la efectividad de los derechos humanos a lo largo de todo el ciclo de vida de las tecnologías digitales, incluida la IA. Esto incluye las fases de prediseño, diseño, desarrollo, evaluación, puesta a prueba, despliegue, uso, venta, adquisición, funcionamiento y retirada. Los Estados deben adoptar medidas eficaces para prevenir, mitigar y remediar los efectos negativos de estas tecnologías sobre los derechos humanos[11] mediante una supervisión adecuada[12]. Estas obligaciones dimanan del derecho internacional de los derechos humanos, incluidos el Pacto Internacional de Derechos Civiles y Políticos y los Principios Rectores sobre las Empresas y los Derechos Humanos.

24. El estricto cumplimiento de las disposiciones del derecho internacional de los derechos humanos, incluido el establecimiento de garantías adecuadas, es un requisito previo para el uso o la transferencia de tecnologías digitales. El Consejo de Derechos Humanos ha afirmado que no deben introducirse tecnologías que no respeten la legislación en materia de derechos humanos o que entrañen riesgos indebidos, y que las tecnologías de reconocimiento biométrico no deben utilizarse para la vigilancia a gran escala[13]. Estas exigencias son reflejo

[10] Resolución 78/213 de la Asamblea General y resolución 59/4 del Consejo de Derechos Humanos.
[11] Resolución 78/213 de la Asamblea General.
[12] Resoluciones de la Asamblea General 77/211, 78/213 y 80/215.
[13] Resolución 58/23 del Consejo de Derechos Humanos.

de las recomendaciones formuladas desde hace tiempo por este mandato y por los órganos regionales[14].

25. Cualquier tecnología de vigilancia digital que interfiera con los derechos debe ajustarse a los principios de legalidad, necesidad y proporcionalidad. Su uso debe basarse en un marco jurídico accesible y preciso que defina claramente los fines autorizados y las categorías de personas objeto de vigilancia. La injerencia en los derechos a la libertad de reunión pacífica y de asociación solo es admisible en casos excepcionales y limitados, cuando esté estrictamente justificada para alcanzar los fines legítimos establecidos en los artículos 21 y 22 del Pacto Internacional de Derechos Civiles y Políticos. La vigilancia debe tener un alcance y una duración limitados —incluso cuando se realice por motivos de seguridad nacional— y debe recurrirse a ella únicamente cuando sea "necesaria en una sociedad democrática". Cualquier restricción debe ser excepcional, lo menos intrusiva posible y preservar la esencia de estos derechos. Las medidas de vigilancia requieren una autorización previa, una supervisión adecuada e independiente de principio a fin (en cuyo marco se evalúe la necesidad y la proporcionalidad de la medida en cada etapa) y un examen independiente *a posteriori*[15]. La Relatora Especial sostiene que debe ser obligatorio realizar una evaluación holística de los daños acumulados que se deriven de la vigilancia.

26. Una supervisión humana eficaz de los sistemas de IA es esencial para prevenir o mitigar los riesgos para los derechos humanos y para asegurarse de que los sistemas sigan siendo seguros y éticos y estén sujetos a la rendición de cuentas[16].

27. Sin embargo, estas normas a menudo se ven menoscabadas por medidas de lucha contra el terrorismo y la ciberdelincuencia demasiado amplias, así como por las excepciones previstas para la seguridad nacional en los marcos mundiales, regionales y nacionales, a lo que se suma la falta de voluntad política para regular las tecnologías de vigilancia que presentan riesgos elevados, algunas de las cuales podrían ser intrínsecamente incompatibles con las obligaciones de los Estados en materia de derechos humanos[17]. El motor de todo ello suele ser, por un lado, unas relaciones de colaboración opacas entre los Estados y las empresas que pasan por alto las obligaciones en materia de derechos humanos, y, por el otro, la presión coercitiva ejercida tanto por los Estados como por las empresas para eliminar las salvaguardias que impiden los abusos o el uso indebido[18].

28. De conformidad con el derecho internacional de los derechos humanos, los Estados deben velar por que la vigilancia, incluida la vigilancia digital, no interfiera indebidamente en la libertad de reunión pacífica y de asociación. Estas obligaciones legales siguen estando vigentes durante las situaciones de emergencia pública, en las que las medidas de vigilancia no deben interferir nunca de manera indebida en las libertades públicas[19]. Del mismo modo, la vigilancia digital y el desarrollo y uso de tecnologías nuevas y emergentes en el ámbito militar deben respetar el derecho internacional de los derechos humanos y el derecho internacional humanitario a lo largo de todo su ciclo de vida[20].

[14] Véase https://shorturl.at/Xb3cW.

[15] Tribunal Europeo de Derechos Humanos, *Ekimdzhiev and Others v. Bulgaria*, demanda núm. 70078/12, sentencia, 11 de abril de 2022; *Green Alliance v. Bulgaria*, demanda núm. 6580/22, sentencia, 17 de febrero de 2026; *Big Brother Watch and Others v. the United Kingdom*, demandas núms. 58170/13, 62322/14 y 24960/15, sentencia, 25 de mayo de 2021; y Corte Interamericana de Derechos Humanos, *Integrantes del Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, sentencia, 18 de octubre de 2023.

[16] Resoluciones de la Asamblea General 79/175 y 78/265; y Reglamento de Inteligencia Artificial de la Unión Europea.

[17] Fionnuala Ní Aoláin, "One step forward? Agreement on spyware regulation in the Pall Mall Process", 9 de mayo de 2025.

[18] Véanse https://tinyurl.com/4jmf86aa, https://tinyurl.com/ycxxhkjm, https://tinyurl.com/e6mu9x9u y https://tinyurl.com/rtch62xu.

[19] Véanse A/HRC/50/42 y https://shorturl.at/BYrPy.

[20] Resolución 79/239 de la Asamblea General y documento A/C.1/80/L.46.

V. Elementos fundamentales de los derechos de reunión y asociación en el contexto de la vigilancia digital

29. Goza de amplia aceptación la idea de que la libertad de asociación y de reunión es imprescindible en una democracia dinámica[21]. La sociedad civil[22] —y los medios de comunicación[23]— ejercen de "guardianes públicos", esenciales para los procesos democráticos; por lo tanto, cualquier injerencia en estos derechos afecta también directamente al derecho a participar en los asuntos públicos[24]. Dado el carácter facilitador e interrelacionado de los derechos a la libertad de reunión pacífica y de asociación, cualquier injerencia indebida merma la capacidad de abogar por todos los derechos humanos. Esto atenta contra la dignidad humana, coarta la capacidad de acción democrática y limita la construcción de sociedades justas y pacíficas, lo que, en última instancia, frena el progreso en ámbitos fundamentales como el desarrollo sostenible, la justicia climática, la seguridad y la paz[25].

30. En el presente informe, la Relatora Especial examina los elementos fundamentales de los derechos a la libertad de reunión pacífica y de asociación, haciendo hincapié en su protección efectiva en la práctica. La Relatora Especial se centra en aquellos elementos que permiten a las personas, las asociaciones, los movimientos sociales y las congregaciones actuar libremente en la consecución de sus objetivos. En concreto, se centra en la capacidad de organización y de movilización, y en la capacidad de acceder a los recursos y gestionarlos (incluida la financiación extranjera), así como en otras actividades esenciales y legítimas, como la planificación, la elección de estrategias y objetivos, la difusión de información, la comunicación y la expresión, la libre circulación y el acceso a la solidaridad[26].

31. La organización y la movilización para el activismo cívico o político dependen de una implicación sostenida a nivel individual y colectivo[27]. La facilidad de comunicación es esencial para difundir información, acceder a recursos, movilizar a participantes y simpatizantes, y obtener protección y justicia. En este caso, la resiliencia y la confianza son fundamentales[28]. Cualquier factor que menoscabe la resiliencia merma la capacidad de generar y mantener la acción colectiva, así como de crear y compartir conocimientos o de preservar la memoria colectiva y la solidaridad. Del mismo modo, la erosión de la confianza interpersonal da lugar a la desocialización, lo que limita la capacidad de las personas y los grupos para comunicarse libremente y actuar con eficacia[29]. Esto refuerza el aislamiento y aumenta la vulnerabilidad ante la estigmatización, la represión o el cierre arbitrario de organizaciones[30]. La confianza y el tejido social se ven profundamente afectados también

[21] Comité de Derechos Humanos, observación general núm. 37 (2020), párrs. 1 y 12. A/HRC/20/27, párrs. 24 y 51; A/77/171, párrs. 5, 8 y 36; A/HRC/31/66, párr. 5; Principios de Yogyakarta sobre la Aplicación de la Legislación Internacional de Derechos Humanos en relación con la Orientación Sexual y la Identidad de Género, principio 20; Comité de los Derechos del Niño, observación general núm. 25 (2021), párr. 64; y Tribunal Europeo de Derechos Humanos, *Gorzelik and Others v. Poland*, demanda núm. 44158/98, sentencia, 17 de febrero de 2004, párr. 93.

[22] Tribunal Europeo de Derechos Humanos, *Magyar Helsinki Bizottság v. Hungary*, demanda núm. 18030/11, sentencia, 8 de noviembre de 2016, párr. 167; y *Szabo and Vissy v. Hungary*, demanda núm. 37138/14, sentencia, 6 de junio de 2016, párr. 38.

[23] Tribunal Europeo de Derechos Humanos, *Jersild v. Denmark*, demanda núm. 15890/89, sentencia, 23 de septiembre de 1994, párr. 31.

[24] A/HRC/59/44, párr. 1; y Comité de Derechos Humanos, observación general núm. 25 (1996).

[25] Véanse A/HRC/59/44 y A/78/246.

[26] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 33; A/HRC/53/38/Add.4, párr. 7; y A/77/171, párr. 4.

[27] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 33.

[28] A/77/171, párr. 52; y Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki y Amy Stevens, "The chilling effects of surveillance and human rights: insights from qualitative research in Zimbabwe and Uganda", *Journal of Human Rights Practice*, vol. 16, núm. 1 (febrero de 2024).

[29] A/77/171, párr. 52.

[30] A/80/219, párr. 86.

cuando las aplicaciones móviles de prestación de servicios fomentan la delación entre particulares, como ocurre en China y en Venezuela (República Bolivariana de)[31].

32. Los derechos a la libertad de reunión pacífica y de asociación se aplican sin discriminación a todas las personas —incluidos los ciudadanos, los no ciudadanos[32] y los niños[33]— y las obligaciones del Estado de facilitar el ejercicio de estos derechos son "neutrales en cuanto al contenido"[34]. La independencia de las asociaciones debe estar protegida.

33. El derecho de los derechos humanos reconoce claramente la importancia de un espacio cívico (tanto físico como digital) carente de obstáculos para el ejercicio de dichos derechos[35]. Dentro de ese espacio, la posibilidad de actuar de forma anónima o de revelar selectivamente ciertos aspectos de la propia identidad es fundamental para que las personas puedan participar en la vida pública[36] y perseguir los objetivos que hayan escogido. Además, tanto la importancia de la espontaneidad a la hora de responder a las necesidades urgentes de la comunidad, como el carácter intrínsecamente perturbador de las reuniones pacíficas son objeto de reconocimiento y protección[37].

34. El acceso a la justicia es fundamental para el ejercicio efectivo de estas libertades. La falta de transparencia en torno a la vigilancia digital y la insuficiencia de las garantías jurídicas impiden la rendición de cuentas, lo cual obstaculiza el ejercicio efectivo de estos derechos[38].

A. Daños interseccionales

35. La vigilancia digital, y sus efectos disuasorios, dan lugar a claros daños interseccionales. Estos perjuicios multiplican el efecto de las vulnerabilidades sociopolíticas ya existentes y de la discriminación histórica.

36. Tal y como ha señalado este mandato, la estigmatización[39] se dirige habitualmente contra las mujeres y los activistas marginados mediante técnicas de vigilancia digital que incluyen el uso de programas espía, el monitoreo en los medios sociales o la difusión o publicación de información privada e identificable en Internet con fines maliciosos *(doxing)*. Estas acciones, destinadas a dañar la reputación y forzar un desistimiento, suelen incluir ataques de carácter sexual, como las ultrafalsificaciones *(deepfakes)*, o la divulgación no consentida de la orientación o identidad de activistas LGBTQI+. Esas tácticas utilizan la tecnología como arma con la que silenciar las voces diversas en el espacio cívico.

37. La vigilancia de los espacios públicos erosiona la vida sociocultural. El miedo a que se les tache de "agentes extranjeros", "delincuentes", "terroristas" o "agitadoras", o a que se les aplique cualquier otra etiqueta, disuade a las personas de aparecer en público. Las repercusiones se acentúan en contextos represivos, especialmente en el caso de las asociaciones a las que se ha criminalizado, los grupos de protesta y las personas en situación migratoria precaria. Además, la vigilancia que se lleva a cabo en las inmediaciones de los proveedores de servicios limita el acceso a los servicios sociales, incluida la atención de la salud, mientras que la vigilancia en las instituciones académicas perjudica a los niños y jóvenes, ya que interfiere en su educación, su autoestima, su identidad y el desarrollo de sus perspectivas de carrera. Del mismo modo, los efectos disuasorios derivados de la vigilancia inciden de manera desproporcionada en las comunidades marginadas y racializadas, así como

[31] Véase https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29302.
[32] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 5.
[33] Convención sobre los Derechos del Niño, art. 15.
[34] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 21.
[35] *Ibid*., párrs. 1 y 53; CCPR/C/108/D/1948/2010 y CCPR/C/108/D/1948/2010/Corr.1, párr. 7.4; y A/77/171, párr. 53.
[36] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 60; y A/HRC/44/24, párr. 24.
[37] Comité de Derechos Humanos, observación general núm. 37 (2020), párr. 47.
[38] Véanse A/HRC/47/24 y A/HRC/53/38/Add.4.
[39] Véase A/79/263.

en las personas o grupos que cuestionan el *statu quo*, denuncian los abusos de poder, exigen justicia y rendición de cuentas por las violaciones de los derechos humanos o lideran iniciativas contra la corrupción.

38. Los efectos discriminatorios de las herramientas de vigilancia basadas en la IA, como el reconocimiento facial y los algoritmos predictivos, están ampliamente documentados[40]. Dichos efectos se han corroborado mediante datos que ponen de manifiesto la forma en que los sesgos de los sistemas de IA afectan de manera desproporcionada, entre otros grupos, a los afrodescendientes, a las minorías étnicas y religiosas y a los niños.

B. La diligencia debida en materia de derechos humanos y las tecnologías de vigilancia digital

39. Para cumplir sus obligaciones en materia de derechos humanos, los Estados y las empresas deben llevar a cabo un riguroso proceso de diligencia debida para evaluar las repercusiones de la vigilancia digital. Un análisis riguroso de la "necesidad" requiere una evaluación holística de la utilidad y los daños. Este enfoque holístico del "daño acumulado" es esencial, ya que las evaluaciones se limitan con demasiada frecuencia a la privacidad o a la libertad de expresión y, aunque son fundamentales, estos aspectos solo representan una parte del panorama. Una evaluación completa del impacto sobre los derechos humanos debe incluir explícitamente la libertad de reunión y de asociación, junto con cualquier otro derecho afectado. La evaluación de la utilidad y el daño causado debe basarse en datos empíricos, ser específica para cada contexto y/o herramienta, tener en cuenta los daños interseccionales y adoptar métodos interdisciplinarios[41].

40. Las evaluaciones del impacto en los derechos humanos son fundamentales en el caso de las tecnologías emergentes, pues a menudo no es posible prever de inmediato la verdadera magnitud de sus consecuencias para los derechos humanos, las cuales tienden a ir acumulándose con el tiempo.

VI. Introducción a los efectos disuasorios

41. Los efectos disuasorios derivados de la vigilancia se producen cuando las personas modifican su comportamiento por temor a las consecuencias de un monitoreo real, insinuado o percibido. Los efectos disuasorios son diversos e influyen en la participación en los medios sociales, las visitas a sitios web, las búsquedas en Internet y la asistencia a reuniones (incluidas las celebradas en línea). Influyen en con quién hablan las personas, en qué dicen, en qué actividades sociales públicas o privadas participan y en si (o cómo) toman parte en los procesos democráticos y en las actividades políticas, entre otras cosas. Los efectos disuasorios pueden hacer que personas o colectivos se inhiban de organizarse o participar en reuniones, de relacionarse o colaborar con determinados actores (por ejemplo, autoridades, donantes, socios, comunidades, víctimas, periodistas, abogados y otros) o de llevar a cabo actividades.

42. Los efectos disuasorios no son exclusivamente binarios. Son variados y matizados, también en cuanto a su intensidad y repercusión. Sus repercusiones no se limitan a inducir las prácticas habituales destinadas a preservar la privacidad y el anonimato, como el uso de redes privadas virtuales o la implantación de culturas de seguridad estrictas en las organizaciones. Pueden provocar cambios en la intención de realizar ciertas actividades. Por ejemplo, pueden llevar a las agrupaciones o asociaciones a optar por estilos de comunicación más "moderados" o más "aceptables", o por actuar de forma menos visible.

43. En el presente informe, la Relatora Especial detalla cómo las personas sometidas a vigilancia y a la amenaza de ser vigiladas suelen sufrir consecuencias graves y altos niveles

[40] Véase, por ejemplo, Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

[41] A/HRC/55/60, párr. 24.

de represión, mediante prácticas como la estigmatización, la intimidación, la criminalización, las detenciones arbitrarias o las amenazas contra la vida.

44. Los efectos disuasorios van mucho más allá de las personas que son blanco de la vigilancia (real o supuesta) y afectan a sus familiares, a sus comunidades, a los movimientos sociales y a la sociedad en general. Los efectos disuasorios de la vigilancia son duraderos y se propagan más allá de cualquier actividad de monitoreo real o insinuada, a veces durante generaciones.

45. Los efectos disuasorios tienen múltiples orígenes y se alimentan tanto de las consecuencias de las manifestaciones directas y visibles de la vigilancia como de insinuaciones más indirectas y ambiguas de que está teniendo lugar.

46. En algunos casos, las actividades de vigilancia digital son clandestinas, mientras que en otros se llevan a cabo abiertamente y se instrumentalizan con la intención explícita de desalentar e inhibir el activismo y la disidencia. En ambos casos, sus efectos disuasorios tienen gran calado.

47. La vigilancia digital remota e invisible genera una ambigüedad constante en torno a si la vigilancia está teniendo lugar. A esto se suma la falta de transparencia en lo que respecta a las actividades de vigilancia, el tratamiento y la conservación de datos, las restricciones opacas al acceso a la información recopilada y la naturaleza compleja (y a menudo no declarada) de quién posee, opera y gestiona los sistemas de vigilancia y recaba los datos. La legislación en vigor suele ser insuficiente, ya que otorga facultades amplias y poco restrictivas, carece de garantías suficientes y no prevé mecanismos adecuados de rendición de cuentas. A menudo, las personas no tienen más remedio que vivir suponiéndose vigiladas de manera constante.

48. Aunque los órganos de derechos humanos y la jurisprudencia[42] reconocen sobradamente la existencia de los efectos disuasorios, aquellos que se derivan de la vigilancia digital de hoy en día aún no se han incorporado a un análisis eficaz desde la perspectiva del derecho de los derechos humanos. Hasta la fecha, la jurisprudencia en materia de derechos humanos se ha centrado principalmente en formas de vigilancia más tradicionales[43] o en los efectos disuasorios de estas[44]. Al no tener en cuenta las especificidades de la vigilancia digital, los marcos jurídicos actuales no acaban de hacerse cargo plenamente del daño general que esta supone para los derechos humanos y las libertades.

VII. Interferencia en los derechos a la libertad de reunión y de asociación derivada de los efectos intimidatorios

49. Las tendencias que aquí se detallan reflejan las experiencias de quienes han contribuido al presente informe con su testimonio (152 actores diversos de todo el mundo; 62 contribuciones escritas[45]): las citas escogidas son representativas de experiencias ampliamente compartidas y observables en los datos. Por lo tanto, cada referencia no constituye una lista exhaustiva de las personas afectadas por el problema en cuestión. En función del consentimiento de los participantes y por motivos de seguridad, algunas

[42] Comité de Derechos Humanos, observaciones generales núm. 37 (2020) y núm. 34 (2011); A/HRC/27/37; A/HRC/56/50; A/HRC/23/40; Corte Interamericana de Derechos Humanos, *Integrantes del Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, sentencia, 18 de octubre de 2023; y Tribunal Europeo de Derechos Humanos, *Glukhin v. Russia*, demanda núm. 11519/20, sentencia, 4 de octubre de 2023.

[43] Pete Fussey y Daragh Murray, *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence* (Oxford University Press, 2025); y el Tribunal Europeo de Derechos Humanos, *Catt v. the United Kingdom*, demanda núm. 43514/15, sentencia, 24 de abril de 2019, párr. 123.

[44] Tribunal Europeo de Derechos Humanos, *Navalnyy v. Russia*, demandas núms. 29580/12, 36847/12, 11252/13, 12317/13 y 43746/14, sentencia, 15 de noviembre de 2018, párr. 103; y *Baka v. Hungary*, demanda núm. 20261/12, sentencia, 23 de junio de 2016, párr. 173.

[45] Véase el anexo II.

aportaciones o citas se atribuyen a un país o región, en lugar de a una organización u otro identificador directo, con el fin de preservar el anonimato[46].

50. La vigilancia digital ha redefinido la capacidad de mantener el anonimato en público. Las tecnologías, en particular la tecnología de reconocimiento facial, permiten identificar y rastrear de forma rápida y precisa a las personas que participan en concentraciones públicas y en las actividades de las asociaciones. Los activistas de todas las regiones consultadas documentaron cómo el monitoreo de multitudes en tiempo real y la identificación retrospectiva de personas a partir de imágenes captadas intensificaban el efecto disuasorio, erosionaban el anonimato, daban lugar a detenciones arbitrarias, preventivas y masivas, y reducían la participación ciudadana en las concentraciones[47]. La expansión de las capacidades de vigilancia afecta de manera decisiva a la capacidad de participar en el espacio cívico, incluidas las acciones en defensa de los derechos laborales, ya que la vigilancia digital se ha utilizado para perseguir a las organizaciones sindicales y a sus miembros.

51. El uso cada vez mayor de la vigilancia encubierta por parte de actores estatales y no estatales para controlar las reuniones pacíficas altera de manera fundamental la presunción de inocencia y la capacidad de participar sin injerencias. Los participantes en los movimientos universitarios de solidaridad con Palestina de todo el mundo denunciaron un aumento de la vigilancia en los campus, incluida la instalación de nuevas cámaras, sistemas de reconocimiento facial y un mayor monitoreo de los medios sociales[48]. Un académico que fue objeto de vigilancia encubierta antes de impartir una conferencia en una universidad del Reino Unido de Gran Bretaña e Irlanda del Norte explicó: “Se supone que uno es inocente hasta que se demuestre lo contrario [...] Pero empezaron a investigarme [...] por mi labor académica. Me dedico al estudio de Palestina. ¿Qué se supone que debo estudiar y enseñar para evitar este control y esta vigilancia injustificados, discriminatorios e injustos?”[49] Esto concuerda con la práctica generalizada de las universidades británicas y las de los Estados Unidos de América de contratar a empresas privadas dedicadas a la obtención de información para investigar a activistas propalestinos antes de las manifestaciones, a menudo por presiones empresariales[50].

52. El aumento del monitoreo de los espacios físicos ha contribuido al auge de las reuniones en línea, que se han convertido en un salvavidas indispensable, especialmente para los activistas exiliados. Sin embargo, esta transición plantea un nuevo dilema: en algunos casos, pasar al entorno digital permite eludir las consecuencias de la vigilancia ejercida en la calle, pero, a cambio, permite un aumento de la vulnerabilidad, la visibilidad y la exposición debido a una vigilancia digital menos perceptible. Los participantes se enfrentan a una censura generalizada, a una vigilancia intrusiva, a acoso selectivo y a detenciones. Las autoridades utilizan los espacios digitales como herramientas de vigilancia y control, rastreando la actividad en línea de las personas para identificar, localizar y detener a quienes se dedican al activismo. Una activista afgana describió haber vivido una situación de “instrumentalización del espacio digital a manos de las autoridades en contra de estas personas; los funcionarios talibanes localizan a los activistas a través de su actividad en Internet y los detienen”[51].

53. Las asociaciones y reuniones en línea también corren un riesgo desproporcionado de sufrir cortes generales del acceso a Internet. Se aplican a fases concretas de las protestas, como se ha visto a lo largo de 2026 en la República Islámica del Irán, y de forma habitual en eventos clave, como el Día de los Derechos Humanos, el Cinco de Mayo y otros[52].

[46] El estudio mundial puede consultarse en https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

[47] Entrevistas segunda, tercera y decimocuarta, primera consulta en Asia Sudoriental, primera consulta en África y aportaciones escritas de la sociedad civil procedentes del Reino Unido de Gran Bretaña e Irlanda del Norte, Serbia y Georgia.

[48] Véase https://tinyurl.com/mrbdx9ku.

[49] Comunicación de Liberty Investigates.

[50] Véanse https://tinyurl.com/5ayc7yz7 y https://tinyurl.com/mrbdx9ku.

[51] Contribución escrita de la sociedad civil procedente del Afganistán; decimosexta entrevista (Nigeria); y primera consulta en África.

[52] Primera consulta en América Latina (Cuba). Véase también A/HRC/47/24/Add.2.

A. Implicación restringida y “desocialización”

54. La vigilancia digital está vinculada a la restricción de los contactos que personas y organizaciones mantienen entre ellas. Entre las medidas que al parecer se están adoptando en respuesta a esta situación figuran evitar las reuniones que requieran tecnologías digitales; limitar las comunicaciones relativas a la estrategia, la organización o la defensa de causas; y el abandono general de las relaciones personales y profesionales. Esto afecta a las personas que son objeto de vigilancia y, de forma indirecta, a quienes temen ser acusados u objeto de mayor vigilancia debido a su asociación con esas personas. Este aislamiento autoimpuesto restringe inevitablemente el acceso a los canales de defensa de causas, a la financiación y a las medidas de protección, lo cual acentúa el repliegue y merma la capacidad para alcanzar los objetivos estratégicos.

55. La vigilancia ejerce un claro efecto disuasorio, lo que dificulta la movilización de participantes y simpatizantes (incluidos los voluntarios), la contratación de personal y, entre otras cosas, disuade a las personas de unirse a grupos sociopolíticos o de mantener su compromiso con ellos[53]. Esto da lugar a un proceso de desocialización y reducción de la actividad colectiva en el que los efectos disuasorios “equivalen a una disolución *de facto* de los espacios asociativos”[54] y a la eliminación del compromiso político[55].

56. Los efectos disuasorios de la vigilancia impulsan una tendencia hacia la descentralización con el fin de contrarrestar la exposición y evitar poner en peligro a los colaboradores, lo que hace que la acción colectiva unificada resulte menos viable[56]. Muchas organizaciones se mostraban reacias a comunicarse con personas u organizaciones que no contaran con suficientes garantías de seguridad digital[57], mientras que otras habían suspendido su participación en movimientos solidarios que eran objeto de un elevado nivel de atención por parte del Estado[58]. Los efectos disuasorios imponen limitaciones a las organizaciones; y estas erosionan un elemento fundamental de la construcción de movimientos sociales[59].

57. Los efectos disuasorios de la vigilancia son duraderos y persisten mucho tiempo después de que hayan concluido las actividades de monitoreo en cuestión. Este impacto duradero se hace especialmente patente entre quienes han sido víctimas de ataques con programas espía. Unos periodistas de los Balcanes relataron cómo un compañero cuyo dispositivo había sido “infectado con Pegasus” fue marginado y tratado como si estuviera “literalmente infectado”[60]. Por lo común, las víctimas de ataques con programas espía describieron efectos intimidatorios a varios niveles, como una exclusión de larga duración, el fin de su trayectoria profesional y la autocensura para proteger a otras personas, incluidos los beneficiarios[61].

B. Injerencias en la función de “guardián público”

58. Los efectos disuasorios de la vigilancia limitan el acceso a las fuentes necesarias para sacar a la luz las violaciones de los derechos humanos, lo que altera de manera fundamental las relaciones con los denunciantes de irregularidades[62], los defensores de las comunidades

[53] Comunicaciones escritas de la sociedad civil procedentes de Italia, el Pakistán, España y los Estados Unidos de América; primera consulta en África; segunda consulta en Asia Sudoriental; y consultas segunda y tercera en América Latina.

[54] Contribución escrita de la sociedad civil presentada por el Centro para Defensores y la Justicia, República Bolivariana de Venezuela.

[55] Consultas primera y tercera en Asia Sudoriental.

[56] Segunda consulta en América Latina (República Bolivariana de Venezuela); y novena entrevista (Estados Unidos).

[57] Entrevistas duodécima y decimotercera.

[58] Novena entrevista (Estados Unidos) sobre los movimientos propalestinos; y décima entrevista.

[59] Primera consulta en Asia Sudoriental.

[60] Octava entrevista.

[61] Entrevistas séptima y octava.

[62] Cuarta entrevista (Serbia).

marginadas[63], los movimientos sindicales[64] y los periodistas que tratan de dar a conocer las violaciones de los derechos humanos[65]. La labor informativa en el contexto de la vigilancia se ha vuelto considerablemente más compleja[66], ya que cuenta con menos fuentes[67] y algunos periodistas y observadores de las protestas han optado por no informar sobre las manifestaciones[68].

C. Miedo a poner a otros en peligro

59. La rotura de vínculos profesionales para proteger a los demás es una consecuencia directa de la vigilancia digital. Activistas de la sociedad civil de Argelia expresaron su temor a exponer a sus compañeros a los niveles de vigilancia que el Estado reserva a los riesgos de seguridad nacional[69]. Activistas de Myanmar explicaron que los efectos disuasorios de la vigilancia los habían obligado a limitar sus interacciones y a mantenerlas de formas sumamente peligrosas y clandestinas[70]. Activistas de Australia, el Brasil y los Estados Unidos, así como de Europa y de toda África, explicaron que se veían obligados a filtrar constantemente la información para reducir el riesgo de perjudicar a otras personas o de exponerlas a la criminalización[71]. En palabras de un activista de los derechos indígenas: "Resulta más difícil, y menos ético, convencer a las comunidades de que alcen la voz"[72].

60. La preocupación por los familiares era una constante en todas las regiones donde se realizaron consultas y en numerosos países, lo que pone de relieve que los efectos disuasorios se propagan sistemáticamente más allá de quienes son objeto de vigilancia directa y afectan a personas ajenas a la situación. Los efectos disuasorios colaterales contra las familias disuadían a muchos activistas de participar en concentraciones pacíficas[73], sobre todo tras la incautación de dispositivos y la consiguiente exposición de sus redes de contactos personales[74].

61. Las inquietudes por la familia ponen de manifiesto la dimensión transnacional de los efectos disuasorios. Esta dinámica se hace sentir a escala mundial y queda patente, por ejemplo, en las experiencias de los activistas tibetanos exiliados, que de manera asidua han restringido sus actividades en los países de acogida en reacción a las amenazas de que son objeto sus familias en su lugar de origen[75]. A medida que se ha extendido la vigilancia digital, también lo ha hecho el impacto de este fenómeno. Numerosos testimonios de primera mano describieron con detalle la represión transnacional ejercida contra los chinos exiliados y las comunidades de la diáspora en el extranjero, lo cual repercutía en el derecho de reunión pacífica en terceros países, independientemente de las garantías de derechos humanos existentes en ellos[76]. Activistas de Bahrein, Etiopía, Georgia, Uganda, Belarús, Rusia y la República Unida de Tanzanía, entre muchos otros países, relataron experiencias similares vividas en primera persona[77]. Un activista afgano describió esta experiencia como algo que había "destrozado todo en mi vida"[78], mientras que activistas de la región de Oriente Medio y Norte de África afirmaron que, si los exiliados participaban en actividades de defensa de

[63] Primera consulta en América Latina.
[64] Consultas segunda y tercera en América Latina.
[65] Consulta en Oriente Medio y Norte de África; y cuarta consulta en América Latina.
[66] Cuarta consulta en América Latina.
[67] Séptima entrevista; y segunda consulta en África.
[68] Segunda consulta en América Latina (Argentina).
[69] Consulta en Oriente Medio y Norte de África.
[70] Primera consulta en Asia Sudoriental.
[71] Segunda consulta en América Latina; cuarta consulta en Asia Sudoriental (Australia); tercera entrevista (Alemania); novena entrevista; y primera consulta en África.
[72] Primera consulta en América Latina.
[73] Novena entrevista; consultas primera y tercera en Asia Sudoriental; primera consulta en África; Consulta en Oriente Medio y Norte de África; y segunda consulta en América Latina.
[74] Undécima entrevista.
[75] Consultas segunda y tercera en Asia Sudoriental.
[76] Segunda consulta en Asia Sudoriental; y véanse https://shorturl.at/fZD5X y https://shorturl.at/OuZ85.
[77] Entrevistas quinta, decimocuarta, decimosexta y decimoséptima. Comunicaciones escritas de la sociedad civil.
[78] Contribución escrita de la sociedad civil procedente del Afganistán, testimonios 31 y 32.

los derechos humanos en el extranjero, sus progenitores, familiares y amistades eran detenidos o desaparecían[79].

62. La vertiente familiar de los efectos intimidatorios afecta a las personas de maneras profundas. Entre ellas figuran el aislamiento forzoso y la ruptura intencionada de los lazos con los seres queridos —incluidos los hijos— con el fin de protegerlos[80], así como la renuncia al contacto en momentos de enfermedad y duelo[81].

D. (Des)confianza y estigmatización

63. La vigilancia fomenta un clima de desconfianza y erosiona la solidaridad. Esto implica un proceso mental constante de recalibrado de los niveles de confianza. Como explicó un representante de la sociedad civil: "La confianza ya no es algo automático. Hay que negociarla cada día"[82]. La vigilancia digital ha transformado la cultura de seguridad de la sociedad civil, generando sospechas injustificadas hacia algunos grupos[83] y obligando a otros a recurrir a formas de comunicación más complejas y onerosas para demostrar que son merecedores de confianza[84].

64. La desconfianza provocada por el efecto disuasorio de la vigilancia tiene un gran impacto en las relaciones personales[85] y "ha quebrado la capacidad de socializar y mantener relaciones humanas normales, ya que uno no puede ser del todo quien es"[86]. En casos más extremos, la confianza se vuelve muy condicional, y depende, por ejemplo, de la voluntad compartida de afrontar una pena de prisión[87]. La desconfianza provocada por los efectos disuasorios también afecta a las relaciones de pareja[88].

65. Las campañas de estigmatización merman la capacidad de organizarse y movilizarse[89]. La vigilancia cumple una doble función: recopila información que nutre una estigmatización inicial y, a continuación, instrumentaliza la estigmatización para justificar una mayor vigilancia. Entre las tácticas utilizadas se encuentra la filtración de información privada recopilada mediante vigilancia ilegal —incluido el monitoreo de espacios domésticos íntimos— con el fin de amenazar y desacreditar a los activistas mediante campañas de desprestigio[90].

66. Ha habido víctimas de la violencia policial que han sufrido campañas de estigmatización[91]. Esas tácticas sirven para desacreditar futuras protestas y tienen un efecto disuasorio notable sobre quienes están a punto de organizar o de sumarse a un movimiento[92].

67. La estigmatización en Internet suele tener una dimensión de género, e incluye insultos y amenazas de violencia sexual contra las mujeres activistas. El uso de los medios sociales para empañar la reputación de figuras destacadas de la sociedad civil es algo habitual[93]. El daño se acentúa en entornos marcadamente conservadores y discriminatorios. En el Afganistán, diversos actores de la sociedad civil han denunciado que, con frecuencia, se

[79] Consulta en Oriente Medio y Norte de África.
[80] Contribución escrita de la sociedad civil procedente del Afganistán; consultas primera y tercera en Asia Sudoriental; decimoquinta entrevista (África Occidental); y primera consulta en África.
[81] Contribución escrita de la sociedad civil procedente del Afganistán; y primera consulta en África.
[82] Consulta en Oriente Medio y Norte de África.
[83] Decimocuarta entrevista.
[84] Entrevistas cuarta y decimoquinta; y segunda consulta en América Latina.
[85] Decimoquinta entrevista; y primera consulta en Asia Sudoriental.
[86] Entrevistas novena y decimocuarta.
[87] Decimocuarta entrevista.
[88] Entrevistas primera, decimoprimera y decimocuarta.
[89] Cuarta consulta en Asia Sudoriental; sexta consulta en América Latina; y primera consulta en África.
[90] Amy Stevens, Pete Fussey, Daragh Murray y otros, "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe", *Big Data and Society*, vol. 10, núm. 1 (2023).
[91] Consultas primera y segunda en América Latina.
[92] *Ibid*.
[93] Segunda consulta en Asia Sudoriental; decimosexta entrevista; y consultas segunda y sexta en América Latina.

amenaza a las activistas detenidas con difundir en Internet fotos o vídeos de abusos y humillaciones captados durante su detención si siguen manifestándose públicamente[94].

68. Haber experimentado una infiltración de las redes y asociaciones profesionales o sociales, consumada o en grado de tentativa, suele ser un factor que provoca efectos disuasorios. En muchos países, la coacción física y la digital van de la mano, ya que la incautación física de teléfonos facilita la infiltración en redes digitales a través de dispositivos intervenidos. Esto, a su vez, afecta al grado de confianza entre los activistas, lo que merma su capacidad para comunicarse libremente y organizarse[95].

69. Activistas de Sudán del Sur describieron una infiltración generalizada y deliberada, diseñada con el propósito explícito de intimidar. Esto minó su capacidad de organizarse, movilizarse y actuar. En Asia Sudoriental, la infiltración en grupos de chat digitales era tan habitual que los activistas calificaban las conversaciones privadas de "esfera semipública", donde la infiltración tenía por objetivo acallar el debate, es decir, que se trataba de un "acto de perturbación"[96]. En el Togo se denuncian prácticas similares.

70. A veces, la infiltración se lleva a cabo íntegramente en línea, a menudo mediante una suplantación o usurpación de identidad[97]. Varias organizaciones de la sociedad civil africanas sospechaban que el Estado y las empresas colaboraban a través de la reasignación de números de teléfono móvil y el posterior acceso a ellos, así como de la clonación de tarjetas SIM, lo que permitía la vigilancia o el envío de mensajes amenazantes o sospechosos[98]. Por ejemplo, activistas de Kenya denunciaron el uso de tarjetas SIM clonadas para enviar mensajes destinados a fomentar la desconfianza entre personas cercanas o a enviar a personas hacia lugares donde serían objeto de acoso policial[99]. Las víctimas de la piratería informática y de la suplantación de identidad denuncian consecuencias similares a las de las personas afectadas por programas espía, en particular un ostracismo prolongado y la imposibilidad de mantener sus redes profesionales[100]. Las tácticas deliberadas de intimidación ponen de manifiesto que quienes llevan a cabo la vigilancia son conscientes de que los efectos disuasorios existen y de que tienen un impacto devastador en quienes los sufren.

71. Ciertos organismos encargados de hacer cumplir la ley, por ejemplo en la Argentina, Bangladesh y Tailandia, recurren al ciberpatrullaje para monitorear los medios sociales e inmiscuirse arbitrariamente en reuniones, incluso en aquellas celebradas en espacios privados.

E. Límites a la conservación y el intercambio de información

72. El temor a la vigilancia supone un escollo considerable a la circulación de información. Activistas de zonas en conflicto y militarizadas, como Darfur (Sudán) y Sudán del Sur, describieron cómo los registros, el acoso y la persecución a que se veían sometidos en los frecuentes puestos de control tenían un efecto disuasorio sobre su implicación y su capacidad para compartir información[101].

73. En el Sudán, transportar consigo según qué material acarreaba un riesgo de confiscación de dispositivos, especialmente en los puestos de control, donde a menudo se obligaba a las personas a desbloquear sus dispositivos para inspeccionarlos. Al parecer los periodistas y los defensores de los derechos humanos eran blanco selectivo de tales prácticas[102].

[94] Comunicaciones escritas de la sociedad civil procedentes del Afganistán.
[95] Primera consulta en África; Amy Stevens, Pete Fussey, Daragh Murray y otros, "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe"; y segunda consulta en América Latina.
[96] Primera consulta en Asia Sudoriental.
[97] Primera consulta en África.
[98] *Ibid*.
[99] Segunda consulta en África.
[100] Primera consulta en África; y contribución escrita de la sociedad civil procedente del Pakistán;
[101] Primera consulta en África.
[102] *Ibid*.

74. Activistas tibetanos describieron cómo los efectos disuasorios de la vigilancia ralentizaban el tránsito de información a través de las fronteras nacionales, lo cual limitaba gravemente la capacidad de las organizaciones de la sociedad civil en el exilio y de la diáspora[103]. En casos extremos, el efecto disuasorio de la vigilancia limitaba el acceso a herramientas básicas de comunicación. Esto incluía la renuncia de algunos activistas a utilizar el teléfono a raíz de una detención[104] y la práctica habitual de bloquear todos los contactos tras la incautación de dispositivos móviles[105].

75. Estas limitaciones de la capacidad de comunicación, provocadas por los efectos disuasorios, tienen un impacto a largo plazo, ya que erosionan la memoria colectiva necesaria para sostener una organización o un movimiento.

76. Las alternativas más trabajosas —como desplazarse a las reuniones en lugar de comunicarse en línea, o el transporte físico de datos, en lugar de enviarlos— dan lugar a un menor intercambio de información, a demoras y a una pérdida de vigencia de la información compartida[106]. También puede ser necesario un esfuerzo adicional para recomponer información fragmentaria, lo que a menudo ocurre a expensas de la exactitud. En zonas de conflicto como Darfur, donde la información puede ser una cuestión de vida o muerte y la verificación implica tomar decisiones que pueden poner en peligro a personas, las organizaciones de la sociedad civil señalaron que, aunque el acceso a la información es complejo, resulta necesario para alejar del peligro a las personas que se desplazan; sin embargo, la difusión de información fragmentaria puede suponer riesgos mayores[107].

F. La reducción de la visibilidad y sus consecuencias

77. El aumento de la vigilancia y la estigmatización afectan a la visibilidad pública de los actores de la sociedad civil, las asociaciones, las agrupaciones y los periodistas, lo que limita directamente su capacidad para relacionarse, actuar y comunicarse libremente. Muchos actores redujeron su presencia en los medios sociales y en la esfera pública, lo cual mermó fuertemente su capacidad de llegar al público, su capacidad de movilización y su acceso a los recursos; en suma, redujo su impacto y el alcance de sus objetivos[108]. Como explicaron los representantes de la sociedad civil de América Latina y África: "¿Quién va a financiar una organización que no es visible?"[109]. En Túnez, actores de la sociedad civil describieron la "necesidad de trabajar más sigilosamente" y señalaron dificultades similares a la hora de acceder a la financiación. Estos efectos disuasorios suponen una doble desventaja: la menor utilidad de las herramientas digitales y del espacio cívico, y la percepción de que es necesario autocensurarse para eludir la criminalización: "La visibilidad conlleva un riesgo enorme… Nos comunicamos menos en público y más en la sombra"[110].

78. Organizaciones de Kenya y Venezuela (República Bolivariana de) se vieron obligadas a trasladarse en múltiples ocasiones y a alejarse lo más posible de la atención del Estado, lo que a su vez aumentó su distanciamiento con respecto a sus redes profesionales[111].

79. Muchas organizaciones eliminaron sus perfiles públicos y se retiraron de los medios sociales. En la República Bolivariana de Venezuela, algunas organizaciones han eliminado sus propios sitios web y sus repositorios de información en línea ante el acoso del Gobierno, una medida de autoprotección que tiene como consecuencia la pérdida de la memoria institucional del sector[112]. En la Argentina, muchas personas que trabajan para organizaciones

[103] Tercera consulta en Asia Sudoriental.
[104] Primera consulta en África; y contribución escrita de la sociedad civil procedente del Afganistán.
[105] Primera entrevista.
[106] Consultas segunda y cuarta en América Latina.
[107] Primera consulta en África.
[108] Comunicaciones escritas de la sociedad civil procedentes de la Argentina, España, los Estados Unidos, la India, Indonesia, Italia, Myanmar, la República Unida de Tanzanía, Uganda y Venezuela (República Bolivariana de).
[109] Tercera consulta en América Latina; y segunda consulta en África.
[110] Consulta en Oriente Medio y Norte de África.
[111] Tercera consulta en América Latina; y segunda consulta en África.
[112] Tercera consulta en América Latina.

no gubernamentales de defensa de los derechos humanos optaban por mantener en secreto su labor en este ámbito[113]. Es habitual verse obligado a borrar toda presencia propia en los medios sociales, lo que a veces supone perder cientos de miles de seguidores que se han ido ganando a lo largo de los años[114].

G. Consecuencias para los recursos y las operaciones

80. Los efectos disuasorios de la vigilancia digital reducen los recursos económicos y, por lo tanto, la capacidad de las organizaciones de la sociedad civil. En un sector donde la financiación es limitada[115], destinar recursos a mitigar la amenaza y el impacto de la vigilancia coarta necesariamente la capacidad de las personas, los movimientos y las organizaciones (incluidos los donantes) para perseguir libremente sus objetivos estratégicos.

81. Los siguientes testimonios describen una experiencia habitual: “El efecto disuasorio afecta a […] todas las medidas de protección. [...] requiere mucho esfuerzo, tiempo, recursos y fondos”[116]. “Este nivel de vigilancia no es normal [...] Ha afectado, tanto en el plano estratégico como en el operacional, a nuestra forma de trabajar. Se dedican muchos recursos, tiempo y energía a […] mitigar la vigilancia”[117].

82. Otras consecuencias financieras directas incluyen la necesidad de organizar procesos alternativos para el envío de remesas y formas clandestinas de financiación para pagar al personal que se encuentra vigilado, con el fin de mantener el secreto y reducir la vulnerabilidad[118].

83. A menudo es necesario incurrir en gastos más elevados en desplazamientos y logística para generar confianza y eludir la vigilancia[119]. Una persona que defiende los derechos de los pueblos indígenas señaló que, en la Amazonía, “debido a la política del miedo, hoy en día el 50 % de nuestro presupuesto debe destinarse a la movilización; a viajar para convencer a la gente de que no hay peligro”[120].

84. En todas las regiones se señaló el problema que supone tener que desviar recursos para mitigar las vulnerabilidades frente a la vigilancia digital, lo cual interfiere de forma notable en la capacidad de actuar con miras al logro de objetivos estratégicos. A nivel orgánico, reforzar la seguridad ante la vigilancia digital supone una inversión estratégica importante[121]. El desvío de fondos a este propósito exige un esfuerzo adicional para justificar el cambio de prioridades ante los donantes.

85. Los recursos de las organizaciones también se ven sometidos a una gran presión como consecuencia de los ataques con programas espía. Esto implica la laboriosa tarea de analizar las redes y los contactos de las víctimas para determinar quiénes son los “vigilados colaterales”[122] de dichos ataques, lo que implica identificar quiénes pueden haber quedado expuestos a raíz de las infecciones[123].

86. Agentes de la sociedad civil de toda África y Asia Sudoriental señalaron que el tamaño de las organizaciones determinaba su capacidad para invertir en medidas de seguridad digital, y que los grupos de base y los de menor tamaño se enfrentaban a las decisiones más difíciles y al mayor grado de vulnerabilidad[124], una situación agravada por los cambios en el

[113] Segunda consulta en América Latina (Argentina).
[114] Primera entrevista.
[115] Véase A/80/219.
[116] Tercera consulta en Asia Sudoriental.
[117] Sexta entrevista.
[118] Segunda consulta en América Latina.
[119] Cuarta entrevista.
[120] Primera consulta en América Latina (Brasil).
[121] Cuarta entrevista.
[122] Daragh Murray y Pete Fussey, “Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data”, *Israel Law Review*, vol. 52, núm. 1 (2019).
[123] Tercera consulta en Asia Sudoriental.
[124] Segunda consulta en Asia Sudoriental.

ecosistema financiero, incluida la suspensión de la financiación procedente del Gobierno de los Estados Unidos[125].

87. Por lo tanto, existen diferencias en materia de seguridad digital entre las distintas organizaciones de la sociedad civil. Por ejemplo, los grupos más pequeños y remotos suelen verse más expuestos y se ven obligados a destinar un mayor porcentaje de su presupuesto a esta actividad en comparación con los grandes grupos internacionales de la sociedad civil[126].

H. Repercusiones de los efectos disuasorios en las personas

88. Los efectos disuasorios de la vigilancia que afectan a la libertad de asociación y de reunión tienen profundas repercusiones en las personas que se manifiestan de formas diversas y cruciales, y afectan a los ámbitos más íntimos de la vida. Más allá de las consecuencias económicas, culturales y sociales, estas afectan a la capacidad de las personas para desenvolverse en la sociedad y acceder a servicios esenciales.

89. Numerosos agentes de la sociedad civil describieron cómo la sensación de estar bajo vigilancia mina la confianza interpersonal y las relaciones sociales[127]. La desconfianza, el aislamiento y la fractura de las relaciones sociales generan un profundo estrés psicológico que afecta a "todos los aspectos de la vida de un activista". Esta intromisión "transforma radicalmente la vida de los activistas: cada conversación se vuelve sospechosa, cada relación puede estar comprometida y cada momento del ámbito privado es tal vez objeto de observación"[128].

1. Psicología individual e hipervigilancia

90. Una experiencia común entre las personas consultadas era un estado de hipervigilancia constante como respuesta a la sensación de estar siendo vigiladas, algo que minaba considerablemente la resiliencia y la capacidad de la persona de mantenerse implicada de forma duradera.

91. Muchos participantes tenían motivos de peso para ese estado de alerta constante. En Sudán del Sur, los activistas creen que se recurrió a la vigilancia biométrica para identificar y asesinar a personas que habían participado en las protestas[129]. En Etiopía, la hipervigilancia fue consecuencia de maniobras directas de intimidación, por ejemplo el descubrimiento de que alguien había entrado a robar en un refugio cuya ubicación se suponía secreta[130]. El costo psicológico que supone saber que a uno lo siguen físicamente, agravado por la vigilancia digital, era una experiencia habitual en todas las regiones del mundo. Los niveles de alerta también aumentaban a raíz de presiones para actuar "con normalidad" ante los demás.

92. Muchos activistas tenían la sensación de que la vigilancia era constante y ubicua: "Todos sienten que están siendo vigilados, que alguien los sigue"[131].

93. Era habitual que el panorama mental de los activistas presentara niveles elevados e intrusivos de hipervigilancia. Entre los testimonios más representativos figuran los siguientes: "Me volví un poco paranoico, pero creo que es una paranoia positiva"[132] y "Fue muy extraño[...] No soy paranoico, pero tenía esa intuición intensa de que algo iba mal"[133]; también se aludió a la práctica de hacer luz de gas hasta el punto en que la persona afectada cuestionaba su propia cordura: "Siempre te encuentras en una situación en la que no sabes

[125] Primera consulta en África.
[126] Cuarta entrevista.
[127] Comunicaciones escritas de la sociedad civil procedentes de Tailandia, los Estados Unidos y Uganda. Esto concuerda con los estudios académicos sobre el impacto de los efectos disuasorios causados por la vigilancia en la confianza interpersonal: véase Amy Stevens, Pete Fussey, Daragh Murray et al., "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe".
[128] Contribución escrita de la sociedad civil procedente del Pakistán.
[129] Primera consulta en África.
[130] Entrevistas duodécima y decimocuarta.
[131] Quinta entrevista.
[132] Primera entrevista.
[133] Octava entrevista.

cuándo estás solo y cuándo no lo estás... ¿o estás siendo paranoico sin más?[134]" Un activista etíope describió cómo esa hipervigilancia acabó normalizándose hasta convertirse en un estado de ansiedad habitual: "No puedo salir a la calle[...] porque estás paranoico todo el tiempo, sobre todo si tienes hijos[...] siempre estás paranoico"[135]. Otros describieron la imposibilidad de encontrar un respiro en casa: "Intento controlarlo hasta cierto punto, pero esos pensamientos intrusivos, esos sentimientos negativos ¿me explico? ese miedo a que pueda pasar algo, siguen ahí, así que es difícil lidiar con ello"[136].

94. Hay varias razones que explican el carácter persistente de la hipervigilancia. Una de ellas es la convicción de que la vigilancia se llevará a cabo independientemente de cualquier medida personal que se adopte para mitigarla. En alusión a la rápida expansión de la tecnología de reconocimiento facial en el Brasil, algunos participantes señalaron que "São Paulo es una ciudad marcada por la ansiedad y la hipervigilancia"[137]. A esto se suma la sensación de que la vigilancia es ubicua e ineludible, así como la incertidumbre de no saber nunca con certeza si se está siendo objeto de ella. Esto es especialmente cierto en redes cuyos miembros han sido víctimas de programas espía: "Esto te hace cuestionarte dos veces todo lo que haces"[138].

2. Salud física y mental

95. Los efectos de la vigilancia constante sobre la salud mental están ampliamente documentados en psicología, epidemiología y otros ámbitos de la medicina[139]. Aunque muchos de estos estudios se centran en el impacto de formas de vigilancia claras y visibles, como el exceso de presencia policial en los barrios, la era de la tecnología digital y el auge de herramientas de monitoreo a distancia intrusivas y apenas detectables amplifican los efectos de la vigilancia en la salud mental.

96. El agotamiento mental y el agotamiento profesional eran un fenómeno constante en todas las regiones estudiadas, tal y como se desprende de los testimonios de los propios activistas y de las observaciones del personal de los servicios de salud mental. Una organización señaló que más del 60 % de los activistas sufrían depresión, agotamiento y otros problemas, y añadió que "por supuesto, hay otros factores que contribuyen a estos problemas de salud mental, pero la represión constituye un factor importante"[140]. En la salud mental repercuten otros muchos factores que habitualmente afectan a la sociedad civil, entre ellos el ser blanco de constantes "campañas de desprestigio, día tras día. Te agota mental, física y socialmente que te vigilen tanto en Internet como otros espacios, las 24 horas del día", lo que ha llevado a muchos a abandonar el activismo[141].

97. Casi todos los activistas de la región de Oriente Medio y Norte de África mencionaron el agotamiento psicológico y emocional[142], asociado a menudo con una sensación de derrota ante la vigilancia autoritaria[143]. Una víctima de programas espía describió "una pérdida total, una sensación de impotencia"[144], mientras que activistas del Afganistán explicaron que "es difícil exagerar el grado de desesperanza que la vigilancia en línea […] ha provocado. Está teniendo un efecto auténticamente disuasorio"[145].

98. Otros describieron la imposibilidad de encontrar un espacio seguro[146], incluida la sensación de que ningún lugar ofrece resguardo, a medida que los efectos disuasorios van

[134] Cuarta entrevista.
[135] Decimocuarta entrevista.
[136] Segunda entrevista.
[137] Primera consulta en América Latina.
[138] Segunda entrevista.
[139] Véase https://shorturl.at/25MEV.
[140] Primera consulta en Asia Sudoriental.
[141] *Ibid*.; y cuarta entrevista.
[142] Consulta en Oriente Medio y Norte de África.
[143] Cuarta entrevista.
[144] Entrevistas cuarta y decimotercera.
[145] Contribución escrita de la sociedad civil procedente del Afganistán.
[146] Primera consulta en Asia Sudoriental; y consulta en Oriente Medio y Norte de África.

invadiendo las esferas más íntimas de la experiencia humana[147]. Un simple comentario espontáneo puede dar lugar a horas de reevaluación psicológica[148]. En este caso, los efectos intimidatorios van más allá de la autocensura: provocan un malestar persistente causado por el cuestionamiento de uno mismo[149].

99. Numerosas tácticas avanzadas de vigilancia tienen efectos psicológicos de gran alcance e indiscriminados y, además, agravan las desigualdades interseccionales. Por ejemplo, el estado de excepción constitucional de emergencia vigente en la Región de la Araucanía (Chile), ha hecho que las comunidades mapuches sean objeto de extensivas medidas de vigilancia desde 2021. La vigilancia constante mediante aeronaves tripuladas y no tripuladas (drones) ha provocado un alarmante "aumento de los casos de ansiedad, insomnio, depresión y estrés postraumático" entre los miembros de la comunidad, especialmente entre los niños[150]. De manera similar a las vivencias de los escolares de zonas sometidas a vigilancia aérea en las favelas brasileñas[151], se han documentado casos de niños que pierden la concentración, muestran signos de ansiedad y buscan refugio en el interior de sus casas al oír un dron.

100. Los casos de vigilancia suelen describirse como un trauma genuino y profundo[152], y muchas de las personas afectadas presentan diagnósticos médicos de afecciones derivadas del trauma[153]. Muchas personas dedican una parte considerable de sus ingresos a paliar estos efectos mediante terapia[154]. Este es un fenómeno tan habitual que la terapia desarrollada expresamente para atender este problema se ha convertido en una especialidad aparte y en expansión[155].

101. Jóvenes manifestantes de todo el mundo ven limitado su acceso a la justicia ante las violaciones de sus derechos, lo cual agrava el trauma que sufren. La vigilancia omnipresente instrumentaliza a su vez dicho padecimiento, con el objetivo de acallar el apoyo de esos manifestantes a las víctimas y su legítima búsqueda de responsabilidades.

VIII. Los efectos disuasorios y el ecosistema de vigilancia

102. Para las personas sometidas a vigilancia, las medidas de vigilancia no son actos puntuales y aislados. Por ejemplo, el uso del reconocimiento facial en las concentraciones, la utilización de programas espía contra los activistas, las infraestructuras de videovigilancia pública, el despliegue de sistemas de reconocimiento automático de matrículas, la presencia policial en las inmediaciones de un evento o la infiltración en grupos de WhatsApp, entre otras cosas, no se consideran hechos aislados, aunque estén dirigidos a grupos diferentes. En realidad, forman un ecosistema de vigilancia. Las incertidumbres que rodean la relación entre los actores estatales y no estatales, especialmente en lo que respecta al intercambio de datos, agravan aún más los perjuicios derivados de un entorno de vigilancia interconectado.

103. Las actividades de vigilancia, aunque sean discretas, se inscriben en un continuo y perduran en el tiempo, dejando huellas profundas y duraderas en toda la sociedad. Menoscaban la confianza fundamental en las instituciones democráticas, en particular respecto de las labores de gobernanza y policía de proximidad —para cuyo desempeño la confianza es esencial— y acentúan los efectos disuasorios. Este impacto de origen ecosistémico es decisivo en el grado en que cada persona y grupo experimenta los efectos disuasorios. Este impacto es aún más grave para las comunidades marginadas y vulnerables, así como para quienes participan en actividades sociopolíticas que cuestionan el *statu quo*.

147 Cuarta consulta en Asia Sudoriental.
148 Primera consulta en África.
149 Undécima entrevista.
150 Véase A/HRC/62/45/Add.1.
151 Segunda consulta en América Latina.
152 Tercera consulta en América Latina.
153 Primera entrevista; y tercera consulta en América Latina.
154 Primera consulta en África.
155 Decimotercera entrevista.

104. Esto supone un problema para los análisis tradicionales efectuados desde la perspectiva del derecho de los derechos humanos, ya que los efectos disuasorios de origen ecosistémico no son los típicos daños de "causa y efecto", en los que un incidente concreto da lugar a un daño determinado. A menos que se haga algo al respecto de este ecosistema de vigilancia, su impacto en el conjunto del espacio cívico será ignorado o subestimado, lo que distorsionará la evaluación de si una restricción cumple el criterio de "necesaria en una sociedad democrática". Esto dará lugar a un sesgo que favorecerá las actividades y herramientas de vigilancia perjudiciales, lo que, a su vez, agravará aún más los efectos disuasorios.

IX. El daño acumulado

105. Los efectos disuasorios afectan al derecho a la intimidad, y también al derecho a la libertad de expresión, y también al derecho a la libertad de reunión pacífica, y también al derecho a la libertad de asociación, y también al derecho a la no discriminación, y también a otros derechos conexos[156]. Los efectos disuasorios afectan a estos derechos de forma simultánea e interfieren en su relación de interconexión e interdependencia. En este sentido, causan un daño acumulado a los derechos humanos. Hasta la fecha, las repercusiones de los efectos disuasorios no se han estudiado[157], o se analizan de forma restrictiva, derecho por derecho. Por ejemplo, las repercusiones sobre la libertad de expresión se analizan separadamente de las repercusiones sobre otros derechos[158].

106. Es importante destacar que el concepto de daño acumulado no se refiere únicamente al daño simultáneo causado a varios derechos humanos. Al interferir en la relación de interconexión e interdependencia de los derechos afectados, el daño en sí mismo se acumula y se intensifica. Por ejemplo, en su conjunto, la libertad de reunión pacífica, de asociación y de expresión y el derecho a la vida privada protegen tanto el desarrollo de la identidad de las personas como el funcionamiento de una sociedad democrática[159]. Por lo tanto, los efectos disuasorios no solo vulneran los derechos subyacentes, sino que también merman la capacidad de las personas y los colectivos para desarrollar y expresar libremente su identidad y para participar en la vida social, cultural y política. La gravedad del daño se acentúa si se tiene en cuenta la "función facilitadora" que tiene la libertad de reunión pacífica y de asociación. Por lo tanto, los efectos disuasorios menoscaban la capacidad misma de abogar por los derechos y de defenderlos. Por daño acumulado se entiende la totalidad del daño derivado de los efectos disuasorios de la vigilancia.

107. Este daño acumulado debe tenerse en cuenta en cualquier proceso de diligencia debida y en las evaluaciones del impacto en los derechos humanos.

X. Conclusión

108. **En el presente informe, la Relatora Especial destaca los efectos disuasorios de la vigilancia digital, los cuales son complejos y poliédricos, y pone de manifiesto que dichos efectos existen y se hacen sentir de manera habitual, independientemente del país o el contexto. Los efectos disuasorios tienen un profundo impacto sociopolítico e interfieren directamente en la capacidad de las personas, los grupos, las asociaciones y las congregaciones para ejercer eficazmente las libertades fundamentales, ejercer la acción política y participar en la vida pública. La vigilancia omnipresente agudiza los efectos disuasorios de la estigmatización y la criminalización.**

[156] Véase https://committees.parliament.uk/writtenevidence/148179/pdf.

[157] Tribunal Europeo de Derechos Humanos, *Glukhin v. Russia*, demanda núm. 11519/20, sentencia, 4 de octubre de 2023, párr. 88.

[158] Tribunal Europeo de Derechos Humanos, *Catt v. the United Kingdom*, demanda núm. 43514/15, sentencia, 24 de abril de 2019, párr. 123.

[159] Ronit Matar y Daragh Murray, "Rethinking international human rights law's approach to identity in light of surveillance and AI", *Human Rights Law Review*, vol. 25, núm. 3 (junio de 2025).

109. **Los efectos disuasorios tienen repercusiones tangibles en la vida real de las personas afectadas directa e indirectamente. Cuando los espacios públicos se vacían o las acciones se "suavizan" por motivos de seguridad, cuando desaparecen palabras de las campañas de reivindicación, de los informes y los proyectos de los donantes, cuando la labor dedicada a los derechos humanos pasa a denominarse "ayuda", cuando los recursos se destinan a la seguridad digital en lugar de a la defensa de los derechos —todo ello para eludir la vigilancia y evitar repercusiones mayores—, las consecuencias son graves. Estos factores merman la resiliencia y la posibilidad de participar de forma continuada en el activismo cívico y político. La normalización de la vigilancia da lugar a violaciones institucionales de las libertades fundamentales. En efecto, reprime el activismo y la participación democrática inclusiva.**

110. **La gravedad y el carácter sistemático de los efectos disuasorios que se han puesto de manifiesto, amplificados por técnicas de vigilancia facilitadas por la tecnología digital y propulsadas por la IA, constituyen una clara señal de alarma que exige una respuesta mundial concertada. Ya no es posible seguir soslayando el impacto que tienen los efectos disuasorios, a raíz de estas técnicas de vigilancia, en el espacio cívico. Si bien los Estados tienen la responsabilidad de velar por la seguridad nacional y la seguridad pública, deben hacerlo protegiendo las libertades fundamentales y propiciando su ejercicio. Por lo tanto, los efectos disuasorios y la injerencia que estos suponen en los derechos a la libertad de reunión pacífica y de asociación deben convertirse en un elemento fundamental de las evaluaciones realizadas desde la perspectiva del derecho de los derechos humanos, las acciones judiciales, la legislación y la formulación de políticas. Esto es extensivo también al diseño, el despliegue y la venta de herramientas digitales.**

111. **La seguridad y la prevención y mitigación de los efectos disuasorios deben incorporarse en la fase de diseño para evitar posibles usos indebidos y abusos que busquen atacar y silenciar la participación democrática, el control público y el activismo político. La participación ciudadana sin obstáculos, tanto en Internet como en los demás entornos, es fundamental para el desarrollo democrático y para una participación inclusiva que valore a todos los miembros, incluidos los niños.**

XI. Recomendaciones

112. **Los Estados, las Naciones Unidas y todas las partes interesadas deberían velar por un entorno propicio para el ejercicio de los derechos y proteger el espacio cívico frente a los efectos disuasorios. Deberían:**

a) Abstenerse de estigmatizar y criminalizar el activismo cívico legítimo, así como de utilizar la vigilancia y las tecnologías digitales para reprimir la disidencia política y las acciones de la sociedad civil. Debe prohibirse el uso de la tecnología digital para estos fines;

b) Proteger el espacio cívico mediante la promoción y la protección de un cifrado de alta seguridad, que incluya la integridad del cifrado de extremo a extremo, y abstenerse de criminalizar las medidas legítimas destinadas a preservar el anonimato;

c) Asegurarse de que haya un marco jurídico conforme con las normas de derechos humanos que regule todas las actividades de vigilancia facilitadas por medios digitales y de que ese marco se rija por los principios de legalidad, necesidad, proporcionalidad y no discriminación. Los efectos disuasorios deben tenerse en cuenta en el análisis del criterio de necesidad. Cualesquiera excepciones, incluidas las motivadas por la seguridad nacional, deben interpretarse de manera restrictiva y estar estrictamente limitadas. Teniendo en cuenta el ritmo de los avances tecnológicos, toda legislación debería limitar las facultades de vigilancia en lugar de ser permisiva, y debería ser objeto de un examen periódico. La venta, la transferencia y la intermediación en la provisión de herramientas de vigilancia digital, así como el correspondiente soporte técnico, deberían regirse por un marco jurídico similar;

d) Velar por que las medidas de vigilancia, incluidas las que se llevan a cabo mediante herramientas digitales e IA, estén sujetas a rigurosas garantías en materia de derechos humanos, las cuales exijan que dichas medidas tengan una duración estrictamente limitada, estén sujetas obligatoriamente a una autorización judicial previa y a una supervisión independiente y efectiva, y que se ofrezcan vías de recurso;

e) Hacer obligatorios los procesos de diligencia debida en materia de derechos humanos y las evaluaciones del impacto en los derechos humanos cuando se trate de toda actividad de vigilancia digital. Estos procesos deben basarse en datos empíricos, tener en cuenta los posibles efectos disuasorios y analizar el daño acumulado, teniendo en cuenta la gravedad interseccional. La diligencia debida debe ser, necesariamente, un proceso continuo;

f) Establecer un proceso de diligencia debida diferenciado e institucionalizado que se centre en la evaluación del ecosistema de vigilancia. Evaluar periódicamente la "necesidad" de la labor general de vigilancia realizada por el Estado, teniendo en cuenta los diversos riesgos e impactos interseccionales y acumulados. Este proceso debe ser obligatorio, especialmente antes del despliegue de nuevas tecnologías de vigilancia, cuando se produzca un cambio de contexto, y antes de los procesos democráticos (como las elecciones);

g) Asegurarse de que haya supervisión humana y mecanismos de rendición de cuentas:

i) Velar por la transparencia pública y por que se celebren consultas amplias e inclusivas en relación con la adquisición, la transferencia y el despliegue de sistemas de vigilancia, y cuando se trate de colaboraciones con empresas;

ii) Asegurarse de que haya mecanismos de supervisión independientes, eficaces y dotados de los recursos necesarios, con competencias para auditar los sistemas de vigilancia, su injerencia en los derechos y libertades y sus efectos disuasorios interseccionales, para investigar las denuncias y para suspender o sancionar a los actores estatales y no estatales en caso de incumplimiento;

iii) Asegurarse de que las fuerzas del orden y el poder judicial dispongan de la capacidad necesaria para investigar y enjuiciar a todos los responsables de la cadena decisoria asociada a la vigilancia ilegal, incluida la vinculada a violaciones de la libertad de reunión pacífica y de asociación, así como a los efectos disuasorios conexos;

iv) Asegurarse de la existencia de mecanismos de denuncia y reparación específicos, centrados en las víctimas y orientados a prestarles apoyo, que permitan a todas las personas, incluidos los niños y los grupos marginados, denunciar de forma segura los abusos en materia de vigilancia, y que permitan obtener e impugnar la información almacenada sobre ellas, incluso la que obre en poder de actores no estatales;

v) Ofrecer las medidas de reparación adecuadas que tengan en cuenta el daño interseccional, entre ellas la destrucción de los datos recopilados de forma ilícita;

h) Velar por la formulación de políticas que se hagan cargo de las cuestiones de género y la interseccionalidad, teniendo en cuenta el impacto diferenciado de la vigilancia digital y las tecnologías digitales. Se debería prestar especial atención al uso indebido de los datos personales, incluidos los datos sobre salud reproductiva, y a la violencia de género en Internet;

i) Prohibir terminantemente lo siguiente:

i) El uso y la transferencia de herramientas digitales intrusivas que no respeten las garantías de derechos humanos, incluidos los programas espía altamente invasivos (cuyas funciones no puedan limitarse o cuyo uso no pueda ser objeto de una auditoría independiente);

ii) La vigilancia arbitraria, indiscriminada y en masa para hacer cumplir la ley, incluidas las aplicaciones biométricas y de IA, como la tecnología de reconocimiento facial, los sistemas de IA que crean o amplían bases de datos de reconocimiento facial mediante la recopilación no selectiva de imágenes faciales de Internet o de grabaciones de cámaras de seguridad, y los sistemas de IA para la puntuación social *(social scoring)*;

iii) El uso de tecnologías de vigilancia y la recopilación de datos con fines predictivos y de perfilado que sean arbitrarios y discriminatorios, incluida la labor policial predictiva, así como para fines que no estén justificados;

iv) El uso de tecnologías y técnicas de vigilancia de carácter militar para hacer cumplir la ley, especialmente en el contexto de los derechos a la libertad de reunión pacífica y de asociación, y el uso de datos sobre el activismo civil con fines militares;

v) Prohibir de inmediato la transferencia y el uso de tecnologías y productos implicados en facilitar la comisión de violaciones graves de los derechos humanos, incluso cuando su utilización para tales fines sea un riesgo;

vi) Abstenerse de utilizar la vigilancia digital en el ámbito educativo y en los lugares de trabajo;

vii) En general, las tecnologías que presentan un mayor potencial coercitivo, incluida la posibilidad de destinarse a un uso militar, deben estar sujetas a requisitos más estrictos en cuanto a su autorización y uso, con el fin de evitar el daño acumulado.

113. **Las Naciones Unidas y la comunidad internacional deberían:**

a) Aprobar normas jurídicas vinculantes centradas en los derechos humanos y mecanismos de gobernanza global que regulen las tecnologías de vigilancia digital y la IA, buscando solución a los posibles efectos disuasorios;

b) Asegurarse de que los marcos mundiales de prevención de la delincuencia, incluidos los relativos a la lucha contra el terrorismo y la prevención de la ciberdelincuencia, no tengan un efecto disuasorio sobre el ejercicio de las libertades públicas. Abordar con carácter urgente estas cuestiones en el marco del proceso en curso de actualización del marco de lucha contra el terrorismo de las Naciones Unidas;

c) Respaldar la creación de una comisión mundial para la verdad y la justicia que se ocupe del impacto sistémico y generalizado de la vigilancia digital, incluidos los efectos disuasorios interseccionales;

d) Prohibir la venta, la transferencia y el uso de tecnologías comerciales que faciliten la vigilancia ilegal y las restricciones graves e indebidas de las libertades públicas, y sancionar eficazmente las infracciones;

e) Exigir a las empresas que rindan cuentas por las violaciones de los derechos humanos derivadas de la transferencia y el uso de sus productos, incluidos los efectos disuasorios.

114. **El sector empresarial (desarrolladores, medios sociales, proveedores de servicios, plataformas digitales, empresas de telecomunicaciones y otras entidades implicadas en la vigilancia, incluidas las grandes empresas tecnológicas) debe implementar rigurosos procesos de diligencia debida en materia de derechos humanos a lo largo de todo el ciclo de vida de las tecnologías de vigilancia. Esta evaluación de diligencia debida debería tener en cuenta los efectos disuasorios e implicar de manera auténtica a todo un abanico de actores de la sociedad civil. El sector empresarial debería:**

a) Asegurarse de que el diseño inclusivo y las funciones digitales no permitan un monitoreo ilegal (incluido el de carácter desproporcionado, indiscriminado y sesgado);

b) No ceder a las exigencias de los Estados que reclamen datos para fines de vigilancia, salvo que medie una orden judicial, y publicar periódicamente informes de

transparencia exhaustivos en los que se detallen las solicitudes procedentes de los órganos estatales;

c) Asegurarse de que los contratos con los Estados incluyan obligaciones claras en materia de derechos humanos, derechos de auditoría y procesos de diligencia debida;

d) Abstenerse de vender tecnologías de vigilancia cuando exista el riesgo de que acarreen efectos adversos para los derechos humanos.

115. **Los donantes deberían proporcionar un apoyo financiero sostenido a los activistas y las asociaciones para mejorar la seguridad, mitigar repercusiones y defenderse de la vigilancia mediante acciones judiciales, apoyo psicosocial, la documentación de incidentes a cargo de la comunidad y el fomento de la capacidad en materia de defensa jurídica.**

Annex I

I. Key activities conducted from 1 January 2025 to 31 May 2026

1. The period from 2025 through the first quarter of 2026 has been a pivotal era for the defence of the freedoms of association and peaceful assembly. Throughout this timeframe, the mandate faced significant global challenges, yet also witnessed important advances fuelled by the tireless action of civil society, social movements, community leaders, and international actors.

2. The Special Rapporteur expresses her sincere gratitude to: i) her supporting staff at the OHCHR; ii) her external advisors, specially Sonya Merkova, Felipe Caicedo and Luz Avendaño; iii) interns from the Master of Advanced Studies International Humanitarian Law and Human Rights, at the Geneva Academy; iv) all the volunteers that have supported her mandate extensively ; v) Prof. Pete Fussey and Dr. Daragh Murray, for their generosity and wisdom; vi) and all the other individuals, associations, including pro-bono groups, governments, international bodies and donors, among others, that have engaged with the mandate.

3. The Special Rapporteur shares a warm recognition in solidarity with: i) all civil society colleagues and friends who have experienced one of the toughest years on record, due to the deadly combination of funding cuts, a shifting financial landscape, the accelerated closing of civic space worldwide, a deep crisis in multilateralism, and the rise of conflicts, wars and genocides; and to ii) the victims of the violations of the right to freedom of peaceful assembly and of association worldwide, especially the youth that have been at the forefront of the defence of human dignity. For their courage, these two groups have been stigmatized, vilified, harassed, surveyed, detained, punished, harmed and even killed. My heart is with you, and my actions are for you.

4. The Special Rapporteur also wishes to acknowledge most of her fellow Special Procedures mandate holders, who even in the mist of reforms (including the disappearance of the Special Procedures Branch at the OHCHR), defunding, a lack of appropriate support, and constant attacks, remain deeply committed to advancing their mandates and protecting human rights. A special acknowledgment to Francesca Albanese, Special Rapporteur on the Occupied Palestinian Territories, who has been subjected to the most outrageous attacks and profound lack of protection from the organization and member States, despite her privileges and immunities.

5. The Special Rapporteur also expresses her appreciation to those Member States that supported the mandate – including its core group – and those that have actively engaged with and provided information in response to requests. She highlights that a global debate is most fruitful when all parties participate actively. For this new cycle, she expresses her hope that all governments will increase their commitments to human rights by transforming words into real actions, including the genuine protection of multilateralism. In a world that is losing its strongest advocates for human rights, we need new leadership – one deeply rooted in respect for human dignity and our shared human values.

6. The Special Rapporteur also expresses her appreciation to Switzerland for the provision of a Junior Professional Officer to support the mandate; and reiterates that greater contributions are required from member States to fulfil the objectives of her mandate.

II. On-the-ground activities and country visits

7. During this reporting period, the Special Rapporteur emphasized face-to-face connections and the prioritization of local realities in her actions. She conducted a total of 249 engagements, meeting with more than 1,753 people in person out of approximately 3,503 people reached across both physical and digital spaces.

8. The Rapporteur's mobility was central to the mandate's effectiveness, spending more than 100 days on the road across 17 different countries and 19 cities. These visits encompassed 1 official visit (to Chile), as well as 2 travels to present reports (New York and Geneva) and to 17 different countries to attend meetings and events organised by civil society organizations or within educational and research environments.

9. A significant focus of these engagements remained on victims and civil society, who constituted 73% of all interactions. Through over 100 dedicated meetings, the Rapporteur engaged with over 2,200 individuals from these groups to ensure their voices remained the primary focus of the mandate's work. These efforts were balanced with over 80 high-level meetings with government representatives and international organizations to share information, advocate for legislative and policy reforms, and to ask for accountability, justice and reparation.

III. Reports

10. The Special Rapporteur presented two thematic reports: one to the Human Rights Council addressing the lessons learned from the "super election" cycle and the resulting impact on civic space (A/HRC/59/44), and one to the General Assembly focused on the existential threats currently facing the rights to freedom of peaceful assembly and of association and the critical role of human solidarity in the current global context (A/80/219).

IV. Communications

11. Between 1 January 2025 and 31 March 2026, the Special Rapporteur joined or led over 300 communications. In terms of regional distribution, Asia accounted for the largest share with 73 communications. Africa and the Americas followed with a similar volume of 51 and 45 communications, respectively. Europe accounted for 35 communications, while Oceania recorded the lowest number with 2 communications. The Special Rapporteur led 37 of these communications. These interventions were primarily driven by a systematic pattern of repression against peaceful protesters, civil society activists, and human rights defenders. Key reasons for these communications included the excessive and disproportionate use of force by security forces, frequently leading to extrajudicial killings, widespread injuries, and the detention of peaceful demonstrators. A persistent pattern of arbitrary arrests and detentions used to criminalize dissent, which in some instances resulted in enforced disappearances. Finally, the implementation of restrictive laws and police and officials actions, such as internet shutdowns, the acquisition and deployment of "less lethal weapons" for crowd control or of surveillance tools and strategies, used to curtail the rights to assembly and expression.

12. The Special Rapporteur also sent letters to around 15 other stakeholders including universities, social media and tech companies.

13. The Special Rapporteur issued two special statements: i) Civic space must be protected and expanded in anti-corruption efforts: Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism,[1] and ii) Streets must be spaces of freedom, not of fear: A call to protect women's right to protest this March 8th.[2]

14. The Special Rapporteur published four newsletters with information of her action: May 2024 and January 2025–February–Apr 2025–May–July 2025–August–October 2025 – 2025 summary.

[1] United Nations, "Joint statement by a group of Special Procedures mandate holders:* Civic space must be protected and expanded in anti-corruption efforts: Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism" (22 August 2025), available at www.ohchr.org/sites/default/files/statements/20250822-stm-uncac-cop-sr-assembly.pdf.

[2] See https://us10.campaign-archive.com/?u=92a2c63767a801e0d97cf1568&id=a46cb60268.

V. Technical assistance and cooperations

15. The Special Rapporteur has been providing ongoing technical assistance to different actors involved in the mutual evaluations and other activities held in relation with the Financial Action Task Force (FATF). This collaboration, that includes governments and civil society, aims to ensure that the country recommendations provided by the Task Force are fully aligned with international human rights standards and do not inadvertently jeopardize citizens' rights to freedom of peaceful assembly and of association.

16. The Special Rapporteur provided comments in the following processes:

(a) Corte Interamericana de Derechos Humanos, Caso Ramos Durand y otros vs. Perú. – May 2025;

(b) Comisión Interamericana de Derechos Humanos, Peritaje caso Diego Lamagna y familia, Marcelo Gastón Riva y familia vs Argentina;

(c) United Kingdom of Great Britain and Northern Ireland Parliament's inquiry on Human rights and the regulation of AI.

17. The special Rapporteur coordinated different actions with regional bodies such as:

(a) Joint declaration about the prolonged detention of human rights defenders with the UN Special Rapporteur on the situation of human rights defenders; the UN Special Rapporteur on Environmental Defenders under the Aarhus Convention; the African Commission on Human and Peoples' Rights, Special Rapporteur on Human Rights Defenders, Focal Point on Reprisals and Focal Point on the Independence of the Judiciary in Africa; and the Inter-American Commission on Human Rights and Rapporteur on Human Rights Defenders and Justice Operators.

(b) Joint Declaration on Protecting the rights to freedom of peaceful assembly and of association from criminalization amid intensified existential threats, with the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), the Commissioner Rapporteur for Human Rights Defenders of the IACHR, and the Special Rapporteur on Human Rights Defenders and focal point for reprisals in Africa of the African Commission on Human and Peoples Rights (ACHPR).

(c) Joint Statement on the Recognition of the Right to Care and the Freedom of Association of Women Workers, 01 May 2025, with the Rapporteur on the Rights of Women of the Inter-American Commission on Human Rights (IACHR); and the Special Rapporteur on Economic, Social, Cultural and Environmental Rights (REDESCA) of the IACHR.

(d) Peer review of ODIHR opinions on:

(i) Cyprus: Urgent Opinion on the Law 151(I) of 2025 on Public Gatherings and Parades;

(ii) Urgent opinion on the amendments to the law on assemblies and demonstrations, the code of administrative offences and the criminal code of Georgia (as adopted on 6 February 2025);

(iii) Opinion on the draft act on the registration of foreign agents in Bulgaria (as of 11 November 2024).

Annex II

Methodology and sources

1. Evidence for this report was drawn from a global study,[1] that included interviews, consultations and focus groups with 152 activists, human rights defenders, public defenders and other lawyers, journalists and civil society actors across all regions of the world. Diverse participants, across distinct contexts and jurisdictions were interviewed to identify common and/or cross-cutting experiences of digital surveillance. These participants advocated across the spectrum of issues including indigenous rights, environmental activism, gender equality, LGBTQIA+ rights, racial justice and the range of concerns related to democratic participation. One consultation was convened in the MENA region, two in Latin America (composed by six different meetings), three in Southeast Asia, two in Africa and a further global event hosted online. This methodology was aimed at countering sceptical views that claim chilling effects are overly subjective, or difficult to measure effectively. Further informing the report are 63 written submissions: 49 from civil society, academics, international bodies, a major global tech company, and 13 State submissions. In addition, the Rapporteur included information she received during her term in victims' sub-missions, meetings with civil society, academic visits and an official country visits. Collectively, this data concerns 84 States and other entities, demonstrating the widespread nature of the chilling effects phenomenon.

2. Participants contributing to this report were from the following States and other entities: Afghanistan, Algeria, Argentina, Armenia, Australia, Azerbaijan, Bahrain, Bangladesh, Belarus, Bhutan, Brazil, Cambodia, Canada, Chile, China, Colombia, Côte d'Ivoire, Cuba, Czechia, Denmark, Ecuador, Egypt, El Salvador, Eritrea, Eswatini, Ethiopia, France, Georgia, Hungary, Honduras, India, Indonesia, Iran (Islamic Republic of), Iraq, Ireland, Israel, Italy, Jordan, Kenya, Kuwait, Lebanon, Libya, Malaysia, Mexico, Morocco, Myanmar, Nepal, Nicaragua, Niger, Nigeria, Oman, Pakistan, Paraguay, Peru, Philippines, Poland, Russian Federation, Saudi Arabia, Serbia, South Africa, South Sudan, Spain, Sri Lanka, Sudan, State of Palestine, Switzerland, Syrian Arab Republic, United Republic of Tanzania, Thailand, Tunisia, Türkiye, Uganda, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan, Venezuela (Bolivarian Republic of), Viet Nam, Yemen, Zambia, Zimbabwe.

[1] See the Global Study, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.