SALVAGUARDIAS PARA LAS ASOCIACIONES PÚBLICO-PRIVADAS DE VIGILANCIA

Diciembre 2021

privacyinternational.org

ACERCA DE PRIVACY INTERNATIONAL

Los Gobiernos y las empresas están usando la tecnología para explotarnos. Sus abusos de poder amenazan nuestras libertades y aquello que nos hace humanos. Esta es la razón por la que Privacy International promueve el progreso que todos nos merecemos. Actuamos para proteger la democracia, defender la dignidad de las personas y exigir la responsabilidad de las instituciones poderosas que violan la confianza pública. Al fin y al cabo, la privacidad es sumamente valiosa para cada uno de nosotros, sin importar si estamos pidiendo asilo, luchando contra la corrupción o buscando orientación médica.

Así que únase a nuestro movimiento mundial y luche por lo que realmente importa: nuestra libertad de ser humanos.

CONTENIDO

INTRODUCCIÓN 3

SALVAGUARDIAS

I. TRANSPARENCIA (SALVAGUARDIAS 1-5) 6

II. CONTRATACIÓN ADECUADA (SALVAGUARDIAS 6-10) 13

III. RENDICIÓN DE CUENTAS (SALVAGUARDIAS 11-15) 19

IV. LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD (SALVAGUARDIAS 16-18) 25

V. SUPERVISIÓN (SALVAGUARDIAS 19-21) 28

VI. REPARACIÓN (SALVAGUARDIAS 22-23) 32

INTRODUCCIÓN

A medida que los Estados del mundo buscan expandir su capacidad de vigilancia y aprovechar el poder de los datos para prestar servicios públicos, a menudo se ven tentados por la posibilidad de utilizar los servicios de empresas privadas de tecnología a través de asociaciones público-privadas (APP). La lucha contra la Covid-19, y la urgencia de encontrar respuestas y soluciones que genera, ha aumentado la necesidad que perciben los Estados de recurrir a tecnologías "innovadoras" y sistemas de inteligencia de datos desarrollados por empresas. Pero estas APP están adoptando una forma nueva, diferente de las relaciones de contratación pública tradicionales. Observamos que existe mucha más codependencia entre las partes, ya que es posible que el Estado desarrolle nuevos sistemas o procesos que dependen enteramente de los servicios de una empresa y que la empresa acceda a datos o información que puede utilizar para desarrollar sus propios servicios. Estas asociaciones no son simples relaciones comerciales aisladas y puntuales, sino que a menudo se construyen con base en cortejos, promesas de alcanzar la verdad perfecta y cada vez más acceso privado a los datos, con frecuencia eludiendo las normas de contratación pública e interfiriendo con los derechos fundamentales en el proceso.

La privatización de las responsabilidades públicas puede ser muy problemática si se realiza sin las salvaguardias adecuadas para garantizar que los derechos humanos no sean vulnerados silenciosamente. Esto es especialmente cierto cuando los sistemas son utilizados para la vigilancia y el tratamiento en masa de datos personales. Se sabe que existen empresas privadas que han manipulado los límites de lo que es posible hacer legal y éticamente con la identidad y los datos de las personas, sin que estén sujetas al mismo nivel de responsabilidad que se exige a las autoridades públicas, lo que es una grave afrenta a los derechos fundamentales cuando se utiliza para prestar un servicio público.

A través de nuestra labor de investigación y de la labor de nuestros aliados en todo el mundo, PI ha identificado una serie de problemas comunes a las APP que involucran tecnología de vigilancia y/o el tratamiento masivo de datos. Con el fin de abordar estos problemas, hemos definido las salvaguardias correspondientes que recomendamos que sean aplicadas por las autoridades públicas y las empresas que desean participar en este tipo de asociaciones. Clasificadas según los principios de transparencia, contratación pública adecuada, rendición de cuentas, legalidad, necesidad y proporcionalidad, supervisión y reparación, en conjunto buscan defender los derechos humanos y restablecer la confianza en las funciones públicas del Estado ante la creciente tercerización de las mismas al sector privado. Las salvaguardias han sido concebidas para ser independientes de la jurisdicción, de modo que puedan ser aplicadas con la mayor amplitud posible en todo el mundo. Son un documento vivo que actualizamos periódicamente con nuevos ejemplos de abusos ocurridos en diferentes partes del mundo y éxitos alcanzados en la lucha contra las asociaciones para la vigilancia.

Los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos ("Principios Rectores de la ONU"),[1] respaldados unánimemente por los Estados en la Asamblea General de la ONU en 2011,[2] constituyen un mandato claro para que tanto los Estados como las empresas refuercen las medidas encaminadas a respetar, proteger y cumplir los derechos humanos y las libertades fundamentales y, además, expandan sus responsabilidades en este sentido, incluso en la industria tecnológica.[3] Las siguientes salvaguardias representan lo que PI considera un marco de protección razonable para hacer cumplir estas responsabilidades y garantizar que las APP no generen abusos de los derechos humanos. PI espera que esta

[1] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Principios Rectores sobre las Empresas y los Derechos Humanos, 2011, disponible en https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[2] Resolución del Consejo de Derechos Humanos de la ONU sobre los derechos humanos y las empresas transnacionales y otras empresas comerciales, UN Doc A/HRC/RES/17/4, 6 de julio de 2011, disponible en https://undocs.org/en/A/HRC/RES/17/4.
[3] La aplicación de los Principios Rectores de la ONU a la industria tecnológica fue reafirmada por el Alto Comisionado de la ONU para los Derechos Humanos en el documento B-Tech Foundational Paper on The UN Guiding Principles in the Age of Technology, disponible en https://www.ohchr.org/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf.

síntesis ayude a la sociedad civil y a las comunidades a abogar por este tipo de esquema de cara al despliegue omnipresente de la tecnología.

I. TRANSPARENCIA

La transparencia es esencial y constituye un requisito previo para el ejercicio y la protección de los derechos humanos. Sin la transparencia apropiada no es posible someter el ejercicio de los poderes del Estado a un escrutinio público adecuado. El Relator Especial de la ONU sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo ha observado que "el principio de transparencia e integridad requiere la apertura y la comunicación de las prácticas de vigilancia". El Relator Especial también señaló que "un debate abierto y un examen minucioso son esenciales para comprender las ventajas y los límites de las técnicas de vigilancia, de forma que el público pueda comprender la necesidad y la legalidad de la vigilancia".[4]

A menudo, las APP, y la relación comercial que establecen, se caracterizan por una falta de transparencia. Las empresas tienen un interés comercial en preservar la confidencialidad de los sistemas y algoritmos de su propiedad, y con frecuencia hemos observado cómo los Estados utilizan esta justificación con liberalidad para abstenerse de revelar la mayor cantidad posible de información sobre los detalles de las tecnologías de vigilancia o la inteligencia de datos. Sin embargo, al igual que en cualquier proceso de contratación púbica, las APP exigen transparencia en todas las etapas que requiere su implementación, desde los procesos de licitación pública hasta las políticas relativas al despliegue de las tecnologías, pasando por el impacto y los resultados de su implementación. Esto es esencial para que el público y la sociedad civil puedan percibir el alcance y las modalidades de la vigilancia y el gobierno a través de los datos.

[4] Informe del Relator Especial de la ONU sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/HRC/13/37, 28 de diciembre de 2009 ("Informe de 2009 del Relator Especial de la ONU sobre la lucha contra el terrorismo"), párrafos 54 y 56, disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement; véase también *Escher y Otros vs. Brazil*, Corte Interamericana De Derechos Humanos, Sentencia (Excepciones Preliminares, Fondo, Reparaciones y Costas), Voto concurrente del Juez Sergio García Ramírez, Series C No. 200, 6 de julio de 2009, párrafo 6 ("Rechazamos el secreto en el que refugia el tirano su arbitrio insoportable. Condenamos el arcano que encierra las claves del autoritarismo. Reprobamos la opacidad en el ejercicio del poder público. Exigimos –y logramos, paso a paso, también con el argumento que ofrecen los derechos humanos– transparencia en los actos de gobierno y en la conducta de los gobernantes").

	Problema	Ejemplo(s)	Salvaguardia(s)
1	Existe muy poca información disponible públicamente: las OSC tienen que hacer grandes esfuerzos para obtener limitadas y restringidas respuestas a las solicitudes de información	Palantir y el Gobierno del Reino Unido: la información sobre la colaboración de Palantir con departamentos gubernamentales del RU es muy limitada. PI y otras OSC han intentado en repetidas ocasiones obtener más información, pero han recibido información adicional escasa y a veces contradictoria.[5]	**Toda la documentación de la APP debería estar disponible públicamente**, y si surgen inquietudes legítimas sobre la divulgación de información sensible (como secretos de Estado o información de seguridad nacional), debería estar disponible de manera confidencial para los organismos de supervisión independientes relevantes[6] (con los permisos/derechos de acceso apropiados) para que puedan evaluar su idoneidad y exigir cambios si es necesario.[7] Cualquier tachadura en los documento a disposición del público debe ser justificada estrictamente y ser revisada por un organismo de supervisión independiente si necesario o si es impugnada. Los contratos de las contrataciones públicas deberían ser puestos a disposición del público (esto ya es un requisito en muchas jurisdicciones). La documentación general de la APP debería ofrecer suficiente

[5] Véase informe de PI y No Tech for Tyrant, All Roads Lead to Palantir, 29 de octubre de 2020, disponible en https://privacyinternational.org/report/4271/all-roads-lead-palantir.
[6] Numerosas salvaguardias recomiendan encomendar algunas funciones a un organismo de supervisión independiente. El organismo de supervisión independiente adecuado para cada caso dependerá del contexto nacional pertinente y de la naturaleza de la asociación en cuestión. Por ejemplo, una asociación en la que el Estado contrata con una empresa el uso de tecnología para la vigilancia de las comunicaciones requerirá la supervisión de un regulador con la facultad de supervisar los poderes de investigación del Estado. Si la tecnología en cuestión implica el tratamiento en masa de datos personales, debería intervenir una autoridad de protección de datos.
[7] Para un ejemplo en Argentina de cómo el derecho de acceder a la información pública interactúa con las excepciones por causa de seguridad nacional, véanse las presentaciones realizadas por la Asociación por los Derechos Civiles (ADC) ante la Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH) (mayo de 2018), disponibles en https://adc.org.ar/wp-content/uploads/2019/06/039-acceso-a-la-informacion-publica-y-excepciones-de-seguridad-nacional-en-argentina-05-2018.pdf.

	Problema	Ejemplo(s)	Salvaguardia(s)
			información sobre los aspectos importantes de la asociación que permita comprender su impacto sobre el público y los derechos fundamentales de los ciudadanos. **La documentación de la APP usualmente debería incluir lo siguiente** (es posible que se requieran algunas evaluaciones dependiendo de la naturaleza de la tecnología y servicios suministrados): • Contratos, información de la contratación, memorandos de entendimiento (**MDE**) y cualquier otro documento que aporte detalles de la asociación • Acuerdos para el intercambio de datos (**AID**) o acuerdos para el tratamiento de datos (**ATD**) • Evaluación de impacto sobre los derechos humanos (**EIDH**) • Evaluación de impacto sobre la protección de los datos (**EIPD**) o evaluación de impacto sobre la privacidad (**EIP**) • Evaluación de impacto del algoritmo (**AIA**) • Registros del tratamiento de datos Las autoridades deberían mantener un **registro público actualizado de las tecnologías**

	Problema	Ejemplo(s)	Salvaguardia(s)
			de vigilancia utilizadas o desplegadas en su jurisdicción. El registro debería incluir los detalles y el propósito de las tecnologías, su cobertura (geográfica y temporal) y los riesgos identificados en relación con los derechos de las personas y las medidas adoptadas para mitigar tales riesgos.
2	Intereses comerciales o derechos de propiedad intelectual impiden revelar los detalles de una tecnología o un sistema	Amazon y el NHS del RU: gran parte del contrato obtenido tenía tachaduras por razones de interés comercial de Amazon.[8] Tras la impugnación de PI, la autoridad de protección de datos del Reino Unido ordenó su revelación parcial.[9] Voto electrónico en Paraguay: las máquinas pudieron ser auditadas, pero ni el código fuente ni el	Las empresas que participan en las APP deberían renunciar a la confidencialidad comercial y permitir que sus tecnologías puedan ser **auditadas completamente** por cualquier tercero, para permitir comprender (1) a qué datos tienen acceso la empresa y su tecnología, (2) cómo la tecnología analiza los datos y saca conclusiones (que incluya revelar los parámetros del algoritmo) y (3) qué papel desempeña la tecnología en el proceso de toma de decisiones de la autoridad pública. Debería permitirse el escrutinio público de esta información antes de realizarse la contratación. Si no es posible revelar los detalles del funcionamiento de una tecnología concreta por motivos válidos y especificados que impliquen un grave daño

[8] Privacy International, Alexa, what is hidden behind your contract with the NHS?, 6 de diciembre de 2019, disponible en https://privacyinternational.org/node/3298.
[9] Privacy International, Amazon Alexa/NHS contract: ICO allows partial disclosure, 27 de abril de 2021, disponible en https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure.

	Problema	Ejemplo(s)	Salvaguardia(s)
		hardware estaban disponibles para auditoría.[10]	comercial a la empresa, un **organismo de supervisión independiente** obligado a mantener la confidencialidad debería tener pleno acceso a toda la información que se necesite sobre la tecnología para establecer esos detalles.
3	Falta de claridad acerca de si los datos personales son tratados, y si lo son, falta de claridad sobre qué tipos de datos personales son procesados	Palantir y la Herramienta de Flujo Fronterizo del Cabinet Office del RU: PI tardó meses y tuvo que recurrir a múltiples solicitudes basadas en la Ley de Libertad de Información (**FOI**, por sus siglas en inglés) para entender la clase de datos personales que trataría Palantir – el contrato público solo mencionaba el tratamiento de datos de "miembros del público". [11]	Cuando una APP contemple el tratamiento de datos personales, cualquier documentación provisional o definitiva deberá incluir **detalles sobre las actividades de tratamiento de datos previstas y actuales**, incluido, por lo menos: • Las categorías de las personas a las que se refieren los datos (cabe señalar que el uso de términos amplios como "miembros del público" tiende a demostrar que las autoridades no han reflexionado adecuadamente sobre las repercusiones del tratamiento) • Clases de datos personales, junto con el fin que persigue el tratamiento de esta clase de datos • Fuentes de los datos personales (dónde se

[10] TEDIC, Voto electrónico: falta de claridad de parte del TSJE a pocos días hábiles del periodo de testeo, 9 de marzo de 2020, disponible en https://www.tedic.org/voto-electronico-falta-de-claridad-testeo-tsje/.
[11] Whatdotheyknow, Record of Privacy International FOI requests to the Cabinet Office, 18 de septiembre de 2020 a 3 de marzo de 2021, disponible en https://www.whatdotheyknow.com/request/contracts_with_palantir#incoming-1737614.

	Problema	Ejemplo(s)	Salvaguardia(s)
			obtendrán los datos) y fundamento jurídico para obtenerlos de cada una de esas fuentes La información debería ser publicada en políticas dirigidas a las poblaciones cuyos datos serán tratados.
4	Falta de claridad en cuanto a la clase y el nivel de acceso a la información concedido a la empresa	Palantir y el NHS: el contrato contradecía la EIPD realizada respecto al acceso a la información de Palantir.[12]	**Los contratos de las APP deberían detallar explícitamente el acceso de la empresa a los datos** (ya sea para el mantenimiento de los programas de software, la atención al cliente, los registros de auditoría o fines de emergencia) y estipular las salvaguardias correspondientes para garantizar la seguridad y el tratamiento adecuado de los datos. Las EIPD deberían evaluar el riesgo de que los datos de los ciudadanos (en algunos casos, datos muy sensibles) sean transferidos a manos privadas y debería considerar, además, la idoneidad de los correspondientes derechos al acceso, la seguridad y las medidas de retención y eliminación.
5	A menudo, el acceso público a la información sobre la	Cámaras de vigilancia de Huawei en	Es necesario que exista o se apruebe **legislación que garantice acceso adecuado a**

[12] Privacy International, The Corona Contracts: Public-Private Partnerships and the Need for Transparency, 26 de junio de 2020, disponible en https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency.

	Problema	Ejemplo(s)	Salvaguardia(s)
	APP es obstruido por la ausencia o la falta de idoneidad del marco jurídico o el procedimiento para acceder a la información (por ejemplo, la Ley de Libertad de Información FOIA)	Valenciennes, Francia: las numerosas solicitudes presentadas por PI a la ciudad de Valenciennes tardaron meses en ser respondidas porque ninguna entidad específica había sido designada con la responsabilidad de responder nuestras peticiones.[13]	**la información de interés público**. La documentación de la APP debería estar disponible para ser consultada por el público en virtud de dicha legislación. Al establecer una APP, se debería designar a **una persona o entidad de la autoridad pública relevante como responsable** de proveer acceso a la información sobre el despliegue de la tecnología y los servicios correspondientes. Sus datos de contacto deberían figurar en todos los sitios web públicos que notifiquen el despliegue de la tecnología o en la documentación pública de la APP.

[13] Privacy International, Huawei in Valenciennes: a bad romance (18 de noviembre de 2021), disponible en https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.

II. CONTRATACIÓN ADECUADA

Los Estados deben cumplir ciertos procesos formales para contratar y evaluar los servicios de las empresas privadas que desempeñen funciones públicas. Este es un principio fundamental de la contratación pública, que es esencial para preservar la integridad del gasto público y el cumplimiento de las funciones públicas. Mediante estos procesos de contratación, el Estado y la empresa deberían aplicar procesos de debida diligencia recíprocos para garantizar el cumplimiento de sus obligaciones en materia de derechos humanos. En virtud de los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, las empresas deben "abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación" y, además, "saber y hacer saber" que no infringen los derechos humanos a través de sus operaciones o relaciones comerciales.

En el contexto de las APP para el despliegue de tecnologías que podrían afectar el disfrute de los derechos humanos, los procesos de contratación deberían ser fortalecidos con ciertas salvaguardias y principios. Deberían garantizar que se realizaron evaluaciones de impacto adecuadas y que las tecnologías únicamente serán utilizadas para cumplir los objetivos declarados y aprobados públicamente (para evitar prácticas como la corrupción, los grupos de presión abusivos, el nepotismo, etc.). Cuando los Estados exigen que las empresas cumplan las obligaciones de debida diligencia en materia de derechos humanos (DDDH), se garantiza que la tecnología sea evaluada adecuadamente en las fases de diseño y desarrollo, y no solamente en la fase de implementación. En la fase posterior a la implementación, las relaciones cada vez más codependientes y duraderas entre Estados y empresas en el ámbito de la tecnología de vigilancia exigen que las evaluaciones y el escrutinio también sean constantes y acumulativos a lo largo de la totalidad del ciclo de vida de la asociación.

	Problema	Ejemplo(s)	Salvaguardia(s)
6	Ausencia de procesos formales de aprobación, o incumplimiento de los mismos, y/o excepciones a dichos procesos formales por razones de seguridad nacional	Perú En Tus Manos: en Perú, el Gobierno impulsó el uso de una aplicación de seguimiento de la Covid-19, a pesar de no haberse realizado ningún proceso de aprobación formal.[14] El contrato original entre Palantir y el NHS concluido por el valor de 1 libra esterlina para el almacenamiento de los datos de la Covid fue suscrito sin el escrutinio adecuado y sin cumplir los procesos de contratación.[15]	En la adjudicación de contratos a empresas, las autoridades públicas deben demostrar el cumplimiento de los **procesos formales de contratación pública** y deben tener **documentación formal** que regule la asociación. Cualquier excepción a estos procesos formales (por seguridad nacional u otros motivos) debe ser estrictamente delimitada, y no debe ser usada para introducir una nueva tecnología y luego volver a adaptarla a fines no incluidos en la excepción sin cumplir los procesos de aprobación o la documentación exigida. El nivel de escrutinio requerido para un proceso de contratación no debería depender del valor del contrato sino de los riesgos que supone el despliegue de la tecnología.
7	Ausencia de EIDH o EIPD, o falta de diligencia en el desarrollo de las mismas	Reconocimiento facial en Argentina: el RE de la ONU sobre privacidad expresó su preocupación	Los Estados y las empresas contratantes deben asegurarse de que existen procesos robustos de **debida diligencia en materia de derechos humanos**, que abarquen tanto las primeras fases de diseño y desarrollo de una tecnología como

[14] Hiperderecho, Liderazgo, estrategia, y donaciones privadas de tecnología frente al Covid-19, 6 de julio de 2020, disponible en https://hiperderecho.org/2020/07/liderazgo-estrategia-y-donaciones-privadas-de-tecnologia-frente-al-covid-19/. Para consultar el cubrimiento de PI, véase Public-Private Partnerships in Technology in Peru: A Government without horizon, 17 de septiembre de 2020, disponible en https://privacyinternational.org/case-study/4167/public-private-partnerships-technology-peru-government-without-horizon.
[15] The Bureau of Investigative Journalism, Revealed: Data giant given 'emergency' Covid contract had been wooing NHS for months, 24 de febrero de 2021, disponible en https://www.thebureauinvestigates.com/stories/2021-02-24/revealed-data-giant-given-emergency-covid-contract-had-been-wooing-nhs-for-months.

	Problema	Ejemplo(s)	Salvaguardia(s)
		porque dos ciudades implementaron programas de reconocimiento facial y otros programas de vigilancia sin realizar ninguna EIP, y nadie pudo explicar la necesidad o la proporcionalidad de los mismos.[16] Huawei en Como, Italia: la EIPD que realizó el municipio no abordó el impacto de la tecnología de	las fases de despliegue y uso.[18] [19] La información detallada de los procesos debe ser pública y estar disponible para ser examinada. Cuando se considere una APP, deben realizarse EIDH siempre que se despliegue de manera general o específica una tecnología.[20] Se debe efectuar una EIPD para implementar cualquier tecnología que implique el tratamiento de datos personales independientemente de si se considera que el tratamiento podría suponer un alto riesgo para las personas.[21] También se deben realizar EIA cuando se utilicen algoritmos para tomar decisiones automatizadas. [22]

[16] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Declaración a los medios de comunicación del Relator Especial de las Naciones Unidas sobre el derecho a la privacidad, al concluir su visita oficial a Argentina, 17 de mayo de 2019, disponible en https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E).

[18] El documento B-Tech Foundational Paper on Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect del Alto Comisionado de las Naciones Unidas para los Derechos Humanos establece la "expectativa de que las empresas realizarán la debida diligencia en materia de derechos humanos para "saber y hacer saber" cómo responden a los impactos adversos en los que participan, o puedan participar, incluido el diseño y uso de sus productos y servicios", disponible en https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

[19]La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha elaborado unas guías sobre cómo las empresas pueden desarrollar la debida diligencia en materia de derechos humanos, disponibles en https://www.ohchr.org/EN/Issues/Business/Pages/CorporateHRDueDiligence.aspx. La Guía de la OCDE sobre Debida Diligencia para una Conducta Empresarial Responsable también ofrece orientación práctica y operativa para efectuar la debida diligencia en materia de derechos humanos, disponible en https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm.

[20] Para orientación práctica sobre cómo realizar las EIDH, véase, por ejemplo, The Danish Institute for Human Rights, Human rights impact assessment guidance and toolbox, 25 de agosto de 2020, disponible en https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox.

[21] Para orientación práctica sobre la realización de las EIPD y un modelo de EIPD, véase, por ejemplo, Information Commissioner's Office, Data protection impact assessments, disponible en https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[22] Para orientación práctica sobre la realización de las EIA, véase, por ejemplo, AI Now Institute, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability, abril de 2018, disponible en https://ainowinstitute.org/aiareport2018.pdf.

	Problema	Ejemplo(s)	Salvaguardia(s)
		reconocimiento facial (**TRF**) y no evaluó la precisión de los algoritmos de TRF.[17]	
8	Las EIPD se realizan después de la adjudicación con el propósito de completar la lista de requisitos en vez de ser utilizadas antes de la adjudicación como herramientas para la toma de decisiones	Huawei en Como, Italia: La EIPD se realizó después de que se adjudicara la licitación a A2A Smart City.[23]	Se deben realizar EIPD individuales durante los procesos de contratación para evaluar las diferentes tecnologías y los servicios que prestan las empresas, y los resultados de las EIPD deben tenerse en cuenta en la decisión de adjudicar el contrato. **Las autoridades públicas solamente deben adjudicar los contratos de las APP *después* de que la EIPD haya sido realizada, publicada y puesta a disposición** de los organismos de supervisión independientes y del público para su revisión durante un plazo especificado.
9	Las empresas podrían estar contribuyendo a la vigilancia masiva y a las prácticas autoritarias de un Estado a cambio de desplegar sus tecnologías en el país	Huawei en Uganda: Según informes, Huawei impartió capacitación en vigilancia a funcionarios de los servicios de inteligencia, capacitación que luego se utilizó	Las autoridades deben evaluar las políticas y el historial de las empresas en materia de derechos humanos, y solo deben adjudicar contratos APP a empresas que, en sus políticas de derechos humanos u otros códigos éticos, **se comprometan a rechazar cualquier solicitud de los Estados de colaborar con iniciativas de vigilancia ilegal contra grupos específicos o cuando existan**

[17] Véase Wired, Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale, 9 de junio de 2020, disponible en https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/. Para conocer el cubrimiento de PI, véase How facial recognition is spreading in Italy: the case of Como, 17 de septiembre de 2020, disponible en https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como.

[23] Véase nota 17.

	Problema	Ejemplo(s)	Salvaguardia(s)
		para espiar a los opositores del Gobierno.[24] Una autoridad del Reino Unido concluyó que las políticas de RSE y prácticas de debida diligencia en materia de derechos humanos de Gamma International no son adecuadas.[25]	**amenazas graves a los derechos humanos.** El hecho de que una empresa concursante haya participado en abusos de los derechos humanos en otros países debe ser un factor para rechazar la oferta.
10	A veces, las autoridades públicas utilizan tecnologías que fueron desplegadas con fines privados para fines policiales, sin cumplir con los procesos de contratación pública y las salvaguardias exigidas	Amazon Ring ha suscrito acuerdos con organismos policiales en todo el mundo para concederles acceso a las redes de vigilancia privada.[26] Sistemas Facewatch utilizados para la vigilancia en los comercios fueron ofrecidos a las	Por principio, **las autoridades públicas no deben emplear de manera sistemática los sistemas de vigilancia y tratamiento en masa de datos instalados en espacios privados y/o los datos que se deriven de estos sistemas.** Estos sistemas solamente deben usarse, cuando sea estrictamente necesario, de acuerdo con el marco legal apropiado y conforme a las condiciones de transparencia y debido proceso que aplican a todas la APP. Esto significa, por ejemplo, que las autoridades no deben gozar de acceso general a dichos sistemas o datos, sino que deben solicitar

[24] The Wall Street Journal, Huawei Technicians Helped African Governments Spy on Political Opponents, 15 de agosto de 2019, disponible en https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
[25] UK National Contact Point, Decision in Privacy International complaint to UK NCP about Gamma International UK Ltd CHECK, 26 de febrero de 2016, disponible en https://www.gov.uk/government/publications/privacy-international-complaint-to-uk-ncp-about-gamma-international-uk-ltd.
[26] Privacy International, One Ring to watch them all, 25 de junio de 2020, disponible enhttps://privacyinternational.org/long-read/3971/one-ring-watch-them-all.

	Problema	Ejemplo(s)	Salvaguardia(s)
		fuerzas policiales.[27] Reconocimiento facial en la estación londinense de King's Cross: la TRF instalada con fines de seguridad privada se utilizó posteriormente para la vigilancia policial.[28]	información específica cuando la necesiten, siguiendo el marco legal apropiado y el procedimiento preestablecido.

[27] Véase PI letter to Mark Smith, CEO of Southern Co-Operative, 1 de diciembre de 2020, disponible en https://privacyinternational.org/sites/default/files/2020-12/PI%20Letter%20to%20Co-Op%20re%20Facewatch.pdf.
[28] Privacy International, King's Cross has been watching you – and the police helped, 25 de junio de 2020, disponible en https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped.

III. RENDICIÓN DE CUENTAS

La rendición de cuentas en el derecho de los derechos humanos "abarca la obligación de quienes ocupan cargos de autoridad a asumir la *responsabilidad* de sus acciones, a dar *justificaciones* ante las personas afectadas y a estar sujetos a *sanciones* cuando su actuación, o sus explicaciones, no resulten convincente".[29] Se trata de un principio medular que permite que todos los demás principios se hagan valer de manera efectiva contra los "titulares de deberes". En este sentido, los Estados deben proporcionar un amplio espacio para que la sociedad civil pueda observar, denunciar y cuestionar los usos de la tecnología que vulneren o amenacen con vulnerar los derechos humanos.[30]

En el contexto de las salvaguardias para el despliegue de las APP, definir la rendición de cuentas exige identificar las obligaciones, los deberes y las normas que se impondrán a cada actor de la relación; por ejemplo, mediante la inclusión de referencias a códigos ya existentes o políticas diseñadas a la medida. En las APP el reto es considerable porque el Estado confía en un agente privado, que no tiene la obligación de actuar en beneficio del interés público, para desempeñar una función pública. Por ello, los mecanismos de rendición de cuentas deben ser especialmente robustos y deben ser definidos *antes* de poner en marcha la APP.

	Problema	Ejemplo(s)	Salvaguardia(s)
11	Las autoridades públicas suelen	Thomson Reuters vendió datos a la	Cuando se acuerda una APP que podría afectar al goce de los

[29] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Who Will Be Accountable? Human Rights and the post-2015 Development Agenda, Summary, 2015, disponible en https://www.ohchr.org/Documents/Publications/WhoWillBeAccountable_summary_en.pdf.

[30] El documento del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, B-Tech Foundational Paper on Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect, señala que "es imperativo que los Estados no utilicen el hecho de sus obligaciones de proteger contra los daños a los derechos humanos como pretexto para moldear las prácticas, los productos y los servicios de las empresas de maneras que causen o contribuyan a las violaciones de los derechos humanos. En este sentido, todos los interesados –especialmente la sociedad civil y las organizaciones de derechos humanos– tienen un papel fundamental a la hora de detectar estos riesgos, denunciarlos y trabajar con ahínco para abordarlos". Disponible en https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

	Problema	Ejemplo(s)	Salvaguardia(s)
	estar sujetas a leyes o códigos especiales que establecen las obligaciones del Estado en materia de derechos humanos, mientras que las empresas privadas no siempre están sujetas a esas mismas leyes	Oficina de Inmigración y Control de Aduanas (ICE, por sus siglas en inglés), una agencia estadounidense que, según informes, separó a los niños de sus padres y los detuvo en condiciones espantosas. Thomson Reuters solo pudo remitirse a sus "Principios de Confianza" para demostrar su compromiso de no contribuir a violaciones de los derechos humanos, en vez un compromiso claro de cumplir con la legislación en materia de derechos humanos	derechos humanos, las obligaciones del Estado de proteger contra los abusos de los derechos humanos también deberían aplicar expresamente a la empresa. Debe existir un mecanismo para que la empresa rinda cuentas ante cualquier abuso de los derechos humanos propiciado por su tecnología y/o servicios. Por consiguiente, los Estados deben procurar que las empresas contratadas en el marco de una APP **adopten las disposiciones de cualquier ley, directriz o código pertinente que obligue a la autoridad pública contratante**.[32] Esto debe estipularse explícitamente en la documentación que rige la asociación.[33]

[32] En el Reino Unido, el Comisario de Cámaras de Vigilancia hizo esta recomendación para la implementación por las fuerzas policiales del sistema de reconocimiento facial en tiempo real Live Facial Recognition, en su informe Facing the Camera, Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales, noviembre de 2020, párrafo 4.73: "Si la operación de un sistema de cámaras de vigilancia por parte de terceros ha sido contratada con un proveedor de servicios del sector privado, la policía debe procurar que todos los contratos relacionados con la operación del sistema le impongan al proveedor la obligación de actuar conforme a lo dispuesto en el Código [de Cámaras de Vigilancia] y las normas relevantes en los casos en que tal sistema esté siendo operado en conjunto o a petición/solicitud de la policía". Disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.

[33] El Principio Rector 5 de la ONU establece que "es necesario que los contratos de prestación de servicios o la legislación que habilite esa prestación precisen que el Estado espera de esas empresas que respeten los derechos humanos. Los Estados deben asegurarse de su capacidad de supervisar efectivamente las actividades de las empresas, en particular mediante mecanismos adecuados e independientes de supervisión y de rendición de cuentas".

	Problema	Ejemplo(s)	Salvaguardia(s)
		al prestar sus servicios.[31]	
12	Las tecnologías desarrolladas en un país son suministradas a otro país que tiene normas de derechos humanos distintas	El Gobierno chino trabaja con empresas chinas de vigilancia para desarrollar normas de tecnología de reconocimiento facial que se consideran represivas (por ejemplo, incorporando el rastreo étnico); posteriormente, esas mismas tecnologías son exportadas.[34] Empresas de telecomunicaciones proveen infraestructura para la interceptación legal de telecomunicaciones desarrollada conforme a las normas de la UE a regímenes cuyas normas de derechos humanos	Los Estados deben **controlar la exportación** de tecnologías de vigilancia considerando la posibilidad de que sean utilizadas para cometer abusos contra los derechos humanos. La documentación de la APP debe anexar los **marcos de derechos humanos convenidos** por las partes, que regirán la asociación y servirán para verificar a lo largo del ciclo de vida de la APP que la tecnología, su uso por parte del Estado y los servicios complementarios prestados por la empresa respetan los derechos humanos. Las empresas deben abstenerse de suministrar sus productos o servicios a un Estado si saben que este no respeta las normas internacionales de derechos humanos.[36]

[31] Sam Biddle, Thomson Reuters Defends Its Work for ICE, Providing "Identification and Location of Aliens", The Intercept, 27 de junio de 2018, disponible en https://theintercept.com/2018/06/27/thomson-reuters-defends-its-work-for-ice/.
[34] Avi Asher-Schapiro, China found using surveillance firms to help write ethnic-tracking specs, Reuters, 30 de marzo de 2021, disponible en https://www.reuters.com/article/us-china-tech-surveillance-trfn-idUSKBN2BM1EE.
[36] Los Principios Rectores de la ONU exigen a las empresas que consideren el uso potencial de sus productos como parte de su debida diligencia en materia de derechos humanos.

	Problema	Ejemplo(s)	Salvaguardia(s)
		son distintas o inexistentes.[35]	
13	Expansión gradual de las funciones: el uso de la tecnología evoluciona con el tiempo sin nuevos procesos de aprobación y supervisión	Las cámaras CCTV son utilizadas durante la pandemia de Covid-19 para monitorear el uso de tapabocas y el distanciamiento social en los espacios públicos.[37]	Tras aprobarse el uso de una tecnología, se debería elaborar una **política para el uso de la tecnología** que rija su uso por la autoridad pública y que defina claramente los límites de su finalidad y uso, y que incluya una lista taxativa de usos autorizados y una lista no taxativa de usos prohibidos.[38] Cualquier uso de la tecnología que no se ajuste a esta política debe ser sometido a un nuevo proceso de aprobación para determinar su legalidad y si cumple las demás salvaguardias. Adicionalmente, la política de uso de la tecnología debe ser modificada para reflejar el nuevo uso aprobado. Debe rechazarse cualquier nuevo uso que sea totalmente incompatible con la finalidad original del despliegue de la tecnología.
14	Las empresas recurren a "consejos de derechos humanos"	Palantir creó el Consejo de Asesores sobre Privacidad y Libertades Civiles	Si las empresas contratadas mediante APP desean recurrir a consejos internos y privados para demostrar que ejercen la debida diligencia y tienen en cuenta los

[35] Véase, por ejemplo, Christopher Rhoads y Loretta Chao, Iran's Web Spying Aided By Western Technology, The Wall Street Journal, 22 de junio de 2009, disponible en https://www.wsj.com/articles/SB124562668777335653.
[37] Véase la opinión de la CNIL (autoridad francesa de protección de datos) sobre el uso del "video inteligente" para monitorear el uso de tapabocas en el transporte público: CNIL, La CNIL publie son avis sur le décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports, publicado el 12 de marzo de 2021, disponible en https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque.
[38] Lo anterior sería fundamental, por ejemplo, para cumplir con el principio de "limitación de la finalidad" del Reglamento General de Protección de Datos de la UE, que exige que los datos personales serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines" (Artículo 5(1)(b)). El principio de limitación de la finalidad debería aplicarse con mayor amplitud a todos los usos de una tecnología que afecte el goce de los derechos humanos de las personas.

	Problema	Ejemplo(s)	Salvaguardia(s)
	internos para demostrar el cumplimiento de los regímenes de derechos humanos, pero estos consejos no son transparentes y operan a puerta cerrada por causa de las obligaciones de confidencialidad	(PCAP, por sus siglas en inglés) para que le ayudara a "navegar el panorama europeo e internacional de la privacidad de datos".[39] El PCAP es solo una instancia consultiva, sus miembros son remunerados por su tiempo y sus discusiones son confidenciales.[40] NSO se comprometió a consultar sus prácticas con expertos en derechos humanos, pero nunca reveló la identidad de los expertos ni el contenido del asesoramiento recibido.[41]	derechos humanos y cumplen la legislación, **las deliberaciones, conclusiones y decisiones de estos consejos o auditorías deben ser públicas.** Estos consejos deberían seleccionar los marcos nacionales, regionales o internacionales de derechos humanos que deben cumplirse y revelar qué marcos fueron seleccionados para cada tecnología o despliegue. Se deben realizar auditorías periódicas que evalúen si los productos y servicios de la empresa se ajustan a estos marcos y los resultados deben publicarse.
15	Está demostrado que depender de tecnologías basadas en datos	Palantir y la distribución de vacunas: un algoritmo privado desarrollado por Palantir ha sido	Los algoritmos y otros procesos de toma de decisiones desplegados como parte de una APP deben estar **sujetos a control e impugnación** por medio de auditorías (como se exige en la salvaguardia 21 más

[39] Palantir, Privacy & Civil Liberties Engineering, disponible en https://www.palantir.com/pcl/.
[40] *Ibíd.*
[41] Véase Letter from Rights Groups to NSO Group, NSO Group continues to fail in human rights compliance, 27 de abril de 2021, disponible en https://www.accessnow.org/cms/assets/uploads/2021/04/Rights-groups_NSO-Group-continues-to-fail-in-human-rights-compliance_27-April-2021.pdf.

	Problema	Ejemplo(s)	Salvaguardia(s)
	perpetúan las desigualdades, las imprecisiones y la injusticia, sin ofrecer la posibilidad de cuestionar las decisiones de las mismas o las decisiones que inducen en sus usuarios	utilizado para distribuir vacunas para la Covid-19 en Estados Unidos, creando disparidades y desigualdades inexplicables en la asignación de dosis entre estados.[42]	adelante). La posibilidad de auditar las tecnologías es especialmente crucial para la adecuada supervisión y reparación de daños (por ejemplo, si una tecnología produce resultados que luego son impugnados ante los tribunales, la correcta administración de justicia requiere que la totalidad de la tecnología sea auditable). En el marco del proceso de contratación, se deben **comparar el grado de sesgo discriminatorio** de los diferentes sistemas. Si se detecta un sesgo discriminatorio, debe ser corregido y cuando no sea posible su corrección, no debe desplegarse la tecnología.

[42] The New York Times, Where Do Vaccine Doses Go, and Who Gets Them? The Algorithms Decide, 7 de febrero de 2021, disponible en https://www.nytimes.com/2021/02/07/technology/vaccine-algorithms.html?referringSource=articleShare.

IV. LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD

El uso de una tecnología o un sistema para ejercer funciones públicas sólo puede ser legítimo si es "legal", es decir, si se enmarca en una normativa adecuada que autoriza el uso de la tecnología para esos fines. Este es el principio de legalidad, un principio fundamental del derecho internacional de los derechos humanos que exige que cualquier injerencia en los derechos humanos haya sido "prescrita por la ley".[43] Además, el derecho internacional de los derechos humanos exige que toda injerencia en el derecho a la privacidad sea necesaria y proporcional.[44] Por lo tanto, cualquier tecnología implementada por un Estado que afecte la privacidad de sus ciudadanos debe demostrar "de forma concreta e individualizada la naturaleza precisa de la amenaza" que pretende abordar.[45] Además, el principio de proporcionalidad exige que la injerencia en la privacidad sea a la vez "proporcional al objetivo y la opción menos perturbadora de las disponibles".[46]

En el contexto de las APP, las evaluaciones de legalidad, necesidad y proporcionalidad deben realizarse *antes* de cualquier contratación con empresas privadas y también *durante* la relación contractual, con anterioridad a cada despliegue específico de la tecnología.

[43] Véanse los artículos 8-11 del Convenio Europeo de Derechos Humanos, los artículos 12 y 17-22 del Pacto Internacional de Derechos Civiles y Políticos y los artículos 11-13, 15 y 16 de la Convención Interamericana de Derechos Humanos.
[44] Ver Comité de Derechos Humanos de la ONU, *Toonen v Australia*, Comm. No. No. 488/1992, UN Doc CCPR/C/50/D/488/1992, 31 de marzo de 1994, párrafo 8.3 ("Cualquier injerencia en la vida privada debe ser proporcional al propósito perseguido y necesaria en las circunstancias particulares del caso."); Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, U.N. Doc. A/HRC/27/37, 30 June 2014) ("Informe del ACNUDH sobre la privacidad en la era digital"), párrafo 23 ("Estas fuentes autorizadas [las Observaciones Generales 16, 27, 29, 31 y 34 del Comité de Derechos Humanos de la ONU y los Principios de Siracusa] apuntan a los principios generales de legalidad, necesidad y proporcionalidad …").
[45] Comité de Derechos Humanos de la ONU, Observación General nº 34 (artículo 19 del PIDCP), 12 de septiembre de 2011, párrafo 35.
[46] Informe del ACNUDH sobre el derecho a la intimidad en la era digital (nota 44), párrafo 23.

	Problema	Ejemplo(s)	Salvaguardia(s)
16	Tecnologías invasoras de la privacidad son desplegadas sin un marco legal adecuado que autorice y regule su uso	Durante años, la tecnología para extraer datos de teléfonos celulares (Mobile Phone Extraction o MPE, en inglés) ha sido utilizada por las fuerzas policiales en el Reino Unido sin un marco legal adecuado.[47] Huawei en Valenciennes, Francia: Huawei instaló cámaras de vigilancia equipadas con tecnología de reconocimiento facial en la ciudad de Valenciennes, a pesar de que la TRF no está legalmente permitida en Francia.[48]	Al considerar la necesidad de una tecnología y su despliegue para satisfacer necesidades públicas o desarrollar funciones públicas, el Estado debe considerar si **un marco jurídico adecuado autoriza el uso de esa tecnología para el fin previsto**. No debe experimentar con la tecnología ni tampoco desplegarla sin la promulgación de leyes (no simples reglamentaciones) adecuadas. La legislación es adecuada si autoriza el uso de la tecnología específica, por parte de autoridades específicas, para el propósito específico; no basta con una legislación general (por ejemplo, que otorgue poderes generales o discrecionalidad absoluta a las autoridades policiales). Un marco jurídico adecuado también debe contemplar políticas y directrices concretas que regulen el uso de la tecnología (como la política para el uso de tecnología planteada en la salvaguardia 13).
17	Las tecnologías desplegadas mediante las APP no siempre son necesarias para	Huawei en Belgrado, Serbia: la EIPD no demostró que el uso de videovigilancia	Una EIDP y/o EIDH adecuadas deben incluir un **análisis de necesidad** que demuestre claramente que recurrir a una tecnología o un sistema de análisis de datos específicos es necesario y

[47] Privacy International, Digital Stop and Search: how the UK police can secretly download everything from your mobile phone, marzo de 2018, disponible en https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.
[48] Privacy International, Huawei in Valenciennes: a bad romance (18 de noviembre de 2021), disponible en https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.

	Problema	Ejemplo(s)	Salvaguardia(s)
	alcanzar los objetivos previstos	inteligente fuera necesario para la seguridad pública, porque sobrevaloró su efecto positivo sobre la reducción de la delincuencia.[49]	no simplemente ventajoso para lograr los objetivos propuestos. La evaluación de los posibles efectos positivos de la tecnología debe hacerse a partir de la recopilación de fuentes probatorias independientes y prácticas comparativas.
18	A menudo, los efectos sobre los derechos humanos de las tecnologías desplegadas mediante APP son desproporcionados en relación con su finalidad	Huawei en Como, Italia: la documentación oficial justificó la necesidad de un sistema de reconocimiento facial mediante un incidente aislado ocurrido años atrás.[50]	Una EIPD y/o EIDH adecuada debe incluir una **evaluación de proporcionalidad** que mida el efecto adverso sobre los derechos y libertades de los ciudadanos y muestre que se justifica por el correspondiente efecto positivo sobre el bienestar de los ciudadanos. Dichas evaluaciones deben considerar los posibles efectos disuasivos o intimidatorios sobre otros derechos, como el derecho a la libertad de expresión y a la libertad de reunión, que pueden ser afectados por los sistemas de vigilancia y procesamiento de datos de maneras poco previsibles y difíciles de medir.

[49] SHARE, "Thousands of Cameras" - a citizen response to mass biometric surveillance, 25 de junio de 2020, disponible en https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-biometric-surveillance.
[50] Véase Wired y Privacy International (nota 17).

V. SUPERVISIÓN

Los Principios Rectores de la ONU sobre las empresas y los derechos humanos exigen que los Estados ejerzan "una supervisión adecuada con vistas a cumplir sus obligaciones internacionales de derechos humanos cuando contratan los servicios de empresas, o promulgan leyes a tal fin, que puedan tener un impacto sobre el disfrute de los derechos humanos".[51]

La supervisión continua del despliegue y los resultados de una tecnología es esencial para garantizar que los mecanismos de rendición de cuentas sean empleados adecuadamente y sirvan para que el uso de la tecnología se ciña a la finalidad expresada, se detecten los abusos o los daños resultantes y se exija la reparación. El Relator Especial de la ONU sobre la lucha contra el terrorismo y los derechos humanos explicó que "los sistemas de vigilancia requieren una supervisión efectiva que minimice los daños y los abusos". El Relator Especial recomendó que "se deben establecer mandatos de supervisión estrictos e independientes para examinar las políticas y prácticas a fin de garantizar la existencia de una rigurosa supervisión del uso de técnicas intrusivas de vigilancia y del procesamiento de la información personal".[52] Por lo tanto, las salvaguardias de esta sección recomiendan maneras concretas de establecer mecanismos de supervisión pertinentes que aborden los daños potenciales a las personas y comunidades afectadas con el despliegue de tecnologías privadas.

	Problema	Ejemplo(s)	Salvaguardia(s)
19	No hay una entidad independiente encargada de supervisar la APP	MPE en el Reino Unido: durante años, las fuerzas policiales del RU utilizaron	Cuando se despliegue una nueva APP, **establecer o designar un organismo de supervisión independiente** (dependiendo de la tecnología y la autoridad de que se

[51] Principio Rector 5 de la ONU
[52] Informe de 2009 del Relator Especial de la ONU sobre la lucha contra el terrorismo (nota 4), párrafo 62.

	Problema	Ejemplo(s)	Salvaguardia(s)
	y el cumplimiento de sus obligaciones con el público	tecnología de extracción de teléfonos móviles (**MPE**, en inglés) de maneras que posteriormente fueron consideradas inapropiadas e ilícitas por la Oficina del Comisario de Información (ICO, por sus siglas en inglés).[53]	trate, podría ser la autoridad de protección de datos del país, si existe, o una autoridad responsable de supervisar los poderes de investigación) que sea responsable de: (1) Revisar, aprobar o rechazar nuevas propuestas para el uso de la tecnología o el sistema desplegado como parte de la APP, (2) auditar periódicamente el despliegue de la tecnología, lo que incluye consultas públicas sobre el impacto de la misma sobre los derechos de los civiles y el cumplimiento de los objetivos propuestos, y (3) recibir quejas y servir de mediador entre el público y las entidades que utilizan la tecnología.[54] Esta instancia de supervisión independiente debe contar con los recursos adecuados (humanos y financieros) para poder desempeñar sus funciones.
20	Falta de consulta con las comunidades y civiles afectados por el despliegue de tecnologías	Amazon Ring y las fuerzas policiales: no se consultó a las comunidades antes de que las fuerzas policiales empezaran a utilizar cámaras	Cuando es probable que una tecnología afecte a algunas comunidades de forma desproporcionada, **establezca una "junta de control civil"** integrada por personas afectadas directamente por la tecnología, en especial, las personas que están en riego de ser discriminadas. La junta de control civil debe consultarse antes de la

[53] Véanse las recomendaciones sobre supervisión en Information Commissioner's Office (ICO), Mobile phone data extraction by police forces in England and Wales – Investigative Report, junio de 2020, disponible en https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf.

[54] En el Reino Unido, por ejemplo, el Comisario de Cámaras de Vigilancia recomienda que "cuando las fuerzas policiales consideren la posibilidad de utilizar el reconocimiento facial instantáneo (LFR, por sus siglas en inglés), deben desarrollar mecanismos que permitan una 'supervisión ética' significativa e independiente de sus decisiones y de su conducta operativa. Tales consideraciones deberían aplicarse como parte de los procesos iniciales de planificación policial y establecerse antes de que se inicie cualquier actividad operativa". (Facing the Camera, nota 32, párrafo 2.26).

	Problema	Ejemplo(s)	Salvaguardia(s)
		de vigilancia privadas.[55]	implementación de la tecnología, solicitar el consentimiento de la población afectada y encargarse de recibir y expresar las quejas sobre el impacto de la tecnología en los derechos de las personas durante todo el ciclo de vida del despliegue de la tecnología.
21	Inexistencia de evaluaciones de impacto continuas	Las fuerzas policiales en los Estados Unidos no llevan registros de los resultados cuestionables o negativos del uso de tecnología de reconocimiento facial (**TRF**), lo que genera una visión unilateral y totalmente positiva de la TRF.[56]	A lo largo del ciclo de vida del despliegue de una tecnología, las autoridades públicas deberían llevar registros de los indicadores de desempeño de la tecnología, incluidos, por ejemplo, éxitos, fracasos, grado de precisión, propósito y resultado.[57] A través de un organismo de supervisión independiente, y en colaboración con una junta de control civil, deberían llevar a cabo **auditorías** periódicas de la tecnología y la **actualización de las EIDH pertinentes**. Las auditorías deberían incluir **consultas periódicas** con los grupos y las personas afectadas por la tecnología (especialmente los que están en riesgo de sufrir discriminación) y con las organizaciones de la sociedad civil, para evaluar en su conjunto los efectos reales o potenciales de la tecnología.

[55] Véase Wired y Privacy International (nota 26).
[56] Jennifer Valentino-DeVries, How the Police Use Facial Recognition, and Where It Falls Short, 12 de enero de 2020, The New York Times, disponible en https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[57] El Comisario de Cámaras de Vigilancia recomendó que el Consejo Nacional de Jefes de Policía del Reino Unido desarrollara indicadores de desempeño similares para evaluar el impacto de las operaciones de la LFR (Facing the Camera, nota 32, párrafo 6.10).

	Problema	Ejemplo(s)	Salvaguardia(s)
			También debería realizarse una **"auditoría retrospectiva"** después de que finalice la relación contractual, ya que a veces los efectos de una tecnología sobre los derechos humanos se producen de manera diferida. Las conclusiones de la auditoría deben ser publicadas y deben ser tenidas en cuenta para las evaluaciones de todas la APP futuras.

VI. REPARACIÓN

Muchas cosas pueden fallar durante el despliegue de una tecnología privada para el ejercicio de funciones públicas estatales, lo que puede afectar gravemente los derechos humanos de las personas. Frente a estas fallas, el derecho internacional de los derechos humanos dispone que los Estados tienen la obligación de garantizar un "recurso efectivo" para las personas cuyos derechos fueron vulnerados.[58] Los Estados tienen la obligación legal de ofrecer recursos efectivos de reparación de "los daños a los derechos humanos relacionados con las empresas, incluidos los daños a los derechos humanos asociados con el desarrollo y el uso de tecnologías digitales por parte de las empresas".[59]

En el contexto de la vigilancia o el tratamiento de datos personales, el secretismo en torno a las tecnologías utilizadas hace que sea especialmente difícil lograr la reparación. Si bien reconoce que "la notificación por adelantado o simultánea podría atentar contra la eficacia de la vigilancia", el Relator Especial de las Naciones Unidas para la Libertad de Expresión ha resaltado que "debe notificarse a las personas una vez que la vigilancia haya finalizado, y

[58] Véase la Declaración Universal de los Derechos Humanos, Resolución 217 (III) A de la Asamblea General de la ONU, 10 de diciembre de 1948, Art. 8 ("Toda persona tiene derecho a un recurso efectivo ante los tribunales nacionales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley"); Art. 2(3), Pacto Internacional de Derechos Civiles y Políticos ("Cada uno de los Estados Partes en el presente Pacto se compromete a garantizar que: (a) Toda persona cuyos derechos o libertades reconocidos en el presente Pacto hayan sido violados podrá interponer un recurso efectivo, aun cuando tal violación hubiera sido cometida por personas que actuaban en ejercicio de sus funciones oficiales"); Art. 25, CADH ("1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales"); Artículo 13, CEDH ("Toda persona cuyos derechos y libertades reconocidos en el presente Convenio hayan sido violados tiene derecho a la concesión de un recurso efectivo ante una instancia nacional, incluso cuando la violación haya sido cometida por personas que actúen en el ejercicio de sus funciones oficiales"). Véanse, además, los Principios y directrices básicas de la Asamblea General de las Naciones Unidas sobre el derecho de las víctimas de violaciones manifiestas de las normas internacionales de derechos humanos y de violaciones graves del derecho internacional humanitario a interponer recursos y obtener reparaciones, Resolución 60/147 de la AGNU, 16 de diciembre de 2005.

[59] Alto Comisionado de las Naciones Unidas para los Derechos Humanos, B-Tech Foundational Paper, Access to remedy and the technology sector: basic concepts and principles. Citando el Principio Rector 25 de la ONU, disponible en https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf.

darles la posibilidad de obtener reparación por el uso de medidas de vigilancia, con posteridad a ella".[60]

En el contexto de las APP, la reparación puede verse afectada por la falta habitual de información derivada de las restricciones de confidencialidad. La reparación debe ser justificada, concebida y asignada de una forma que corresponda a la forma en que funciona y se utiliza una tecnología, lo que exige que se hayan respetado adecuadamente otros principios, en particular la transparencia, la responsabilidad y la supervisión.

Del mismo modo, los Estados deben tener recursos contra las empresas que violen cualquier condición de su contrato con el Estado o que son responsables de facilitar el abuso de los derechos humanos. Lo anterior es crucial para que los Estados puedan cumplir sus obligaciones frente a los ciudadanos cuando la culpa es imputable en todo o en parte a la empresa con la que celebró un contrato.

	Problema	Ejemplo(s)	Salvaguardia(s)
22	Falta de avenidas de reparación cuando se abusa de una tecnología	El malware de NSO fue utilizado para atacar a los abogados de las víctimas en México; cuando esto fue descubierto, NSO no cooperó con las iniciativas para exigir la rendición de cuentas y la reparación del daño.[61]	Recurrir a los tribunales u otros sistemas judiciales de alto rango no suele ser una opción viable para las personas afectadas por los usos aislados de una tecnología, especialmente si se tiene en cuenta que el abuso puede ser difícil de establecer a través de mecanismos de justicia tradicionales. La política de uso de la tecnología recomendada en la salvaguardia 13 debe incluir **disposiciones de reparación**, señalando los mecanismos y las entidades ya existentes o estableciendo otros

[60] Informe del Relator Especial de la ONU sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, UN Doc. A/HRC/23/40, 17 de abril de 2013, párrafo 82, disponible en https://undocs.org/A/HRC/23/40.
[61] Citizen Lab, Reckless IV – Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware, 2 de agosto de 2017, disponible en https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

	Problema	Ejemplo(s)	Salvaguardia(s)
			nuevos para la gestión de las reclamaciones y la aplicación de sanciones por la violación de la política (incluso señalando el organismo de supervisión independiente adecuado que tenga la capacidad de investigar y brindar reparación). Dichos mecanismos de reparación y las entidades responsables deben ser aptos para la naturaleza de la tecnología, el propósito que se pretende y los impactos identificados. Deben atribuir responsabilidades y obligaciones de reparar tanto al Estado como a la empresa involucrada, y deben adherirse a los ocho "criterios de eficacia" establecidos en el Principio Rector 31 de la ONU. No obstante, las disposiciones de reparación no deben impedir el acceso a los tribunales u otros mecanismos judiciales existentes. Deben lograr el equilibrio correcto entre el acceso a la reparación y el cumplimiento del Estado de derecho. El Estado debe asegurar, además, que la empresa contratada dispone de un mecanismo de reclamación[62] mediante el cual puedan señalarse y remediarse tempranamente los posibles daños a los derechos humanos.

[62] Esto es exigido por el Principio Rector 29 de la ONU.

	Problema	Ejemplo(s)	Salvaguardia(s)
23	Los contratos de APP tienden a "atar" a las autoridades públicas y a las empresas a la asociación mediante onerosas cláusulas de cambio o de terminación	La Agencia de Fronteras del Reino Unido es demandada por Raytheon Systems Limited por la rescisión indebida de un contrato para el suministro de un sistema informático de inmigración.[63] Palantir y el Departamento de Policía de Nueva York: al finalizar el contrato, Palantir se negó a presentar los análisis generados por su software para ser transferidos a un nuevo sistema distinto al de Palantir.[64]	Los contratos de APP deben incluir **cláusulas de rescisión** que permitan (1) que la empresa rescinda el contrato si descubre que su tecnología ha sido utilizada o se pretende utilizar para actividades que no cumplen con el marco de derechos humanos vigente y (2) que el Estado rescinda el contrato si descubre que cualquier producto de la empresa ha sido utilizado por otros Estados para cometer abusos contra los derechos humanos (independientemente de si se trata del producto contratado u otro producto) o si se pone de manifiesto que las estipulaciones del contrato impiden que el Estado actúe de acuerdo con el interés público. Los contratos de APP también deben incluir cláusulas rigurosas sobre **interoperabilidad y transferibilidad**. La interoperabilidad y la transferibilidad son esenciales en el ámbito de la contratación pública, ya que los Estados están obligados a contratar servicios que cumplan ciertos requisitos y a hacerlo de una cierta manera. Si la empresa con la que se contrató cambia el funcionamiento de sus servicios o sus políticas, volviéndolos incompatibles con las obligaciones del Estado, este debe tener total libertad para

[63] Véase Computer Weekly, UK government pays £150m to Raytheon to settle e-Borders dispute, 27 de marzo de 2015, disponible en https://www.computerweekly.com/news/4500243244/UK-government-pays-150m-to-Raytheon-to-settle-e-Borders-dispute.
[64] Véase Buzzfeed News, There's A Fight Brewing Between The NYPD And Silicon Valley's Palantir, 28 de junio de 2018, disponible en https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley.

	Problema	Ejemplo(s)	Salvaguardia(s)
			retirarse de la APP y contratar otra, sin que la empresa retenga los datos o la información, ni que el cambio suponga costos “punitivos” o indebidos que ejerzan presión sobre los fondos públicos.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org