CUESTIONANDO LAS ASOCIACIONES PUBLICO-PRIVADAS DE VIGILANCIA: Manual para la sociedad civil

Junio de 2022

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.

Privacy International
62 Britton Street, Londres EC1M 5UY, Reino Unido
Teléfono +44 (0)20 3422 4321
privacyinternational.org

Privacy International es una organización benéfica registrada (1147471) y una asociación de responsabilidad limitada registrada en Inglaterra y Gales (04354366).

CONTENIDO

AGRADECIMIENTOS

Agradecemos la colaboración de nuestros aliados: ADC, TEDIC y otra organización que desea permanecer en el anonimato y que ha contribuido a este manual.

- La Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación (TEDIC) es una ONG paraguaya fundada en 2012 que desarrolla tecnología cívica abierta y defiende los derechos digitales para una cultura libre en internet.
- La Asociación por los Derechos Civiles (ADC) es una organización de la sociedad civil con sede en Argentina que, desde su fundación en 1995, trabaja para defender y promover los derechos civiles y humanos en Argentina y América Latina.

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 la misma genera, 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.

La sociedad civil tiene el poder de denunciar los riesgos y los problemas que se derivan de estas asociaciones mediante la investigación y la información pública.

Pero identificar riesgos concretos y posibles abusos de los derechos humanos no es una tarea fácil para nadie, porque requiere comprender los varios niveles de la tecnología, la legislación y la gobernanza implicados. Con base en nuestro propio trabajo de investigación y en la experiencia de nuestros socios, Privacy International ha diseñado un manual para que las organizaciones de la sociedad civil, las organizaciones no gubernamentales, los académicos y las personas naveguen estas asociaciones, aportando claves para obtener información crucial, comprender la tecnología en juego e identificar las preocupaciones relacionadas con la privacidad y la gobernanza.

Con el propósito de apoyar a cualquier persona que pretenda obtener más información sobre una asociación de vigilancia público-privada e identificar los principales riesgos y preocupaciones, este manual se divide en cuatro secciones principales: la **primera sección** se centra en cómo recolectar información clave sobre la asociación a través de diferentes vías; la **segunda sección** trata sobre la tecnología que utiliza la asociación, adoptando un enfoque integral que comprende desde maneras de definir en términos generales qué es la tecnología hasta métodos para comprender cómo funciona realmente; la **tercera sección** trata sobre las preocupaciones de gobernanza y las salvaguardias, incluidas las mejores prácticas internacionales, las preocupaciones de protección de datos y las salvaguardias correspondientes.

Las listas de chequeo incluidas en la última parte del manual pueden ser usadas como un resumen de los aspectos clave por investigar y como una ayuda para hacerle seguimiento a su trabajo.

El manual está pensado para ayudar a:

- Investigar una asociación público-privada, recoger información relevante
- Plantear las preguntas adecuadas a los socios pertinentes (públicos y privados)
- Identificar las preocupaciones en relación con la tecnología en juego y la gobernanza de la asociación

También hemos desarrollado por separado una serie de salvaguardias para las asociaciones de vigilancia público-privadas que pueden servirle como ideas para su

labor de incidencia después de haber identificado las preocupaciones usando el manual.

1. EVALUANDO LOS RIESGOS

Investigar una asociación público-privada acarrea una serie de riesgos jurídicos, técnicos y humanos que deben ser evaluados antes de emprender cualquier actividad. Estos riesgos varían de acuerdo con el marco de la investigación y el contexto general en el que opera la asociación. Sugerimos que identifique y evalúe los riesgos relacionados con su proyecto de investigación antes de desarrollar cualquier actividad. Para facilitar esta tarea, puede consultar las listas no exhaustivas que figuran a continuación.

A. RIESGOS A TENER EN CUENTA

- **Difamación**: las normas sobre difamación protegen la reputación de una persona frente a interferencias injustificadas. Es posible que lo demanden por difamación los actores particulares contra los cuales haga sus denuncias. Las normas sobre difamación varían de una jurisdicción a otra y puede que usted tenga que asumir toda la carga de la prueba.
- **Recolección ilegal de la información**: según su jurisdicción, algunas investigaciones podrían ser contrarias a la ley (como la publicación de información filtrada o el hackeo).
- **Propiedad intelectual (PI)**: el secreto comercial y los derechos de autor son dos ejemplos de las normas de propiedad intelectual que podría infringir al llevar a cabo su investigación.
- **Riesgos para las personas (personal, fuentes, aliados...)**: no se debe realizar ninguna actividad que ponga en riesgo la vida de las personas implicadas, salvo que se adopten medidas concretas para mitigar los riesgos. Los riesgos podrían incluir, entre otros: lesiones físicas, lesiones psicológicas, daños sociales, daños económicos y daños jurídicos.
- **Deterioro de la reputación**: riesgos para la objetividad, imparcialidad o credibilidad de su organización. Algunos de los posibles riesgos son: hechos

inexactos, afirmaciones sin sustento suficiente y la explotación del monitoreo en redes sociales (SOCMINT – inteligencia obtenida en redes sociales) y de otras fuentes abiertas (OSINT – inteligencia obtenida de fuentes abiertas) sin respeto de la privacidad, etc.

B. MEDIDAS DE MITIGACIÓN SUGERIDAS

A continuación, se sugieren algunas medidas para mitigar estos riesgos. No se trata de una lista exhaustiva, y puede que, por sí solas, estas medidas no alcancen a mitigar todos los riesgos.

- **Solidez de la metodología de investigación**: citar las fuentes, evaluar la calidad de las mismas, tomar fotos y videos, utilizar un lenguaje adecuado.
- **Corroboración de la información**: corroborar múltiples fuentes y testimonios para garantizar la validez de la información.
- **Edición y limpieza de los documentos**: eliminar los datos personales y limpiar los metadatos.
- **Prepararse** antes de hablar en público o conceder entrevistas a los medios a fin de adoptar un lenguaje adecuado.
- **Conservar las fuentes originales** y almacenarlas de forma segura.
- **Considerar la seguridad de las personas** (consentimiento, anonimato, etc.) antes de emprender cualquier acción.

2. DESCUBRIENDO LA INFORMACIÓN

Obtener información adecuada sobre una asociación público-privada suele ser difícil, especialmente cuando se trata de áreas delicadas del gobierno, como la inteligencia y la fuerza pública. A menudo, la información sobre estas actividades se mantiene al margen del público a propósito y se protege con normas y castigos excesivos.

Pero, si se puede acceder a acceder de manera segura, existen muchos métodos y recursos que pueden ayudar. Muchas de estas fuentes ya están disponibles en internet, mientras que otras requieren trabajar con documentación y recurrir a personas que puedan ayudar.

No siempre ni en todas partes se puede acceder a estos recursos de manera fácil o segura: se sabe que gobiernos de todo el mundo castigan a activistas, periodistas y otras personas por sacar a la luz o tan solo buscar información sobre este tipo de contratos, por lo cual es necesario evaluar y mitigar los riesgos.

A. USO DE LAS NORMAS DE ACCESO A LA INFORMACIÓN

Una solicitud conforme a normas sobre libertad de información (FOI por sus siglas en inglés) u otras normas sobre acceso a la información (como las leyes sobre el derecho a la información –RTI por sus siglas en inglés–) es una petición formal que se hace a un organismo público (las autoridades locales, regionales o municipales, la policía, un ministerio, etc.) para acceder a información que el público tiene derecho a conocer. Quizás esté intentando obtener un contrato suscrito por los socios, correspondencia (correos electrónicos o cartas) entre los socios, estadísticas oficiales, o simplemente una respuesta a una pregunta, o incluso otros documentos, como una presentación realizada por una empresa ante la autoridad

pública. Algunas leyes especifican lo que puede y no puede solicitar: Uganda, por ejemplo, exige que solicite documentos específicos, es decir, no puede hacer preguntas.

La información obtenida mediante estas solicitudes es una herramienta valiosísima para periodistas, activistas y el público: cuanta más información esté a disposición del público, mejor informados estaremos como sociedad y más será fácil exigir cambios.

Sin embargo, aunque este tipo de normas suelen prometer mucho, y aunque más de noventa países tienen normas que obligan a los funcionarios a entregar documentos públicos, en la práctica no es tan sencillo lograr que lo hagan.

Al presentar estas solicitudes, es importante tener en cuenta algunas recomendaciones clave:

- Compruebe que lo que busca no esté ya disponible
- Sepa a quién enviar la solicitud
- ¡Mantenga su enfoque!
- Hable su idioma
- ¡Esté dispuesto a tener paciencia!

Privacy International tiene una guía que describe algunas de las lecciones que hemos aprendido al presentar este tipo de solicitudes en todo el mundo.

La Red Global de Periodismo de Investigación tiene una excelente lista de los recursos de libertad de información (FOI) disponibles en muchos países de todos los continentes. Realmente recomendamos que le eche un vistazo: muchas de las guías sobre libertad de información que más nos gustan están en ese repositorio.

Es importante recordar que tal vez existan archivos públicos valiosos en otras jurisdicciones. En los casos en que una empresa tiene su sede en un país, pero opera en otro, podría ser útil presentar solicitudes en cualquiera de las jurisdicciones. Por ejemplo, los periodistas han podido obtener más información sobre tecnología de vigilancia suministrada a Macedonia del Norte presentando solicitudes ante las autoridades del Reino Unido que supervisaron la autorización de

la exportación. Sin embargo, algunos países (por ejemplo, India) solo permiten solicitudes de ciudadanos.

Lo que dicen nuestros aliados:

Las normas de acceso a la información pueden ser herramientas útiles, pero también pueden ser decepcionantes. Debe tener en cuenta que es posible que su solicitud no reciba respuesta y, por tanto, prever otras maneras de obtener información.

Algunos de nuestros socios nos dijeron que las solicitudes de información eran muy útiles para confirmar información que ya habían averiguado de otras fuentes, y a otros les resultaban más útiles desde la perspectiva de las comunicaciones públicas o para obtener más información sobre la razón por la fue rechazada la solicitud.

B. OTRAS FUENTES

i. Inteligencia de fuentes abiertas

Al tratar de obtener más información sobre las asociaciones público-privadas, hay muchas fuentes de acceso público que pueden proporcionar información adicional: la recolección y el uso de esta información a veces se conoce como inteligencia de fuente abierta (OSINT por sus siglas en inglés).

Organizaciones como Bellingcat han utilizado extensamente la OSINT para descubrir las prácticas ilegales y los abusos de los derechos humanos de los gobiernos, incluso respecto a algunas de las agencias gubernamentales mejor protegidas y sigilosas del mundo.

Sin embargo, poder acceder a información útil depende de una serie de factores, incluido el país en el que tiene su sede la asociación, el tipo de empresa involucrada y el tipo de tecnología o servicio que suministra.

Existen numerosos recursos en línea y en publicaciones que proporcionan información sobre la recolección de la OSINT, entre ellos:

- Bellingcat
- i-intelligence
- El Centro Tow de Periodismo Digital
- El OSINT Framework

Sin embargo, muchas técnicas plantean importantes preguntas de seguridad, éticas y legales que deben ser consideradas. El Centro de Derechos Humanos de la Facultad de Derecho de Berkeley y la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos han elaborado una guía sobre el uso de la OSINT en la investigación de violaciones al derecho penal internacional, los derechos humanos y el derecho humanitario, que proporciona algunas pautas sobre estas consideraciones.

Por ejemplo, como señala la guía, en algunas jurisdicciones tergiversar o falsear su identidad en las redes sociales es ilegal. Y, aun cuando no sea ilegal, podría ser una violación de los términos de servicio de la empresa de redes sociales, y utilizar una identidad falsa para acceder a información sobre un individuo o grupo que, de otro modo, sería inaccesible, podría ser contrario a los principios éticos o la ley.

Las fuentes abiertas de datos para acceder a información sobre asociaciones público-privadas incluyen:

- Los sitios web de la empresa, que suelen describir sus productos y, a veces, incluso publicar listas de clientes.
- Los documentos presentados por las empresas a los organismos reguladores, que suelen contener información importante como sus actividades comerciales, estructura e ingresos. Los investigadores han podido realizar análisis detallados de las estructuras corporativas de las empresas utilizando dicha información. Esta información está disponible en plataformas como OpenCorporates.

- Anuncios de empleo publicados en sitios de empleo y redes sociales de fácil acceso, como LinkedIn. Con frecuencia estas fuentes proporcionan pistas o detalles sobre cuáles son las actividades comerciales de una empresa y en dónde las realiza, así como sobre las innovaciones en fase de desarrollo: por ejemplo, un periodista británico pudo acceder a información sobre una misteriosa “super base de datos” del gobierno utilizando información sobre ofertas de empleo.
- Datos sobre embarques y comercio, que algunos gobiernos y empresas publican habitualmente. Por ejemplo, las autoridades indias publican datos sobre embarques de importaciones y exportaciones, algunos de los cuales se pueden consultar en sitios web comerciales. Esta información puede servir para identificar algunas exportaciones: por ejemplo, Forensic News descubrió que una empresa israelí de spyware había enviado equipos a la policía secreta de Uzbekistán gracias a la información de embarques.
- Datos sobre la transparencia de la cooperación gubernamental. A menudo, estos datos muestran los casos en los que las autoridades gubernamentales han proporcionado equipos, financiación o formación a sus homólogos de todo el mundo y, por consiguiente, revelan información sobre el software o los equipos a los que tienen acceso. Por ejemplo, utilizando los datos de la asistencia estadounidense, es posible identificar las empresas de vigilancia cuyos productos han sido suministrados a los gobiernos de Centroamérica.
- Redes sociales, incluidas, por ejemplo, redes sociales profesionales como LinkedIn. Esta es una fuente usada frecuentemente por los periodistas y puede utilizarse para identificar cierta información relativa a personas y empresas, pero debe utilizarse de forma ética y legal (véase más arriba).

ii. Información de la contratación pública

Los datos de la contratación pública son una de las mejores fuentes abiertas para encontrar información sobre asociaciones público-privadas. Se pueden consultar los sitios web centralizados de contratación pública del gobierno, así como también la documentación de las licitaciones en los sitios web específicos de cada organismo, aunque a menudo la información detallada está restringida.

La información de acceso público sobre licitaciones –anuncios informando que una autoridad gubernamental está tratando de adquirir un servicio o producto del sector privado– puede proporcionar información valiosa. A menudo, la licitación solo ofrece información general, pero puede servir de base para futuras investigaciones, por ejemplo, a través de la presentación de solicitudes basadas en la libertad información (FOIA por sus siglas en inglés).

Por ejemplo, en el Reino Unido, existe una plataforma centralizada, pública y con función de búsqueda que permite que cualquiera consulte las licitaciones de los organismos gubernamentales (aunque en la práctica muchos detalles se ocultan por motivos de seguridad nacional).

Del mismo modo, los EE.UU., la UE, Rusia y otros países del mundo publican licitaciones en sitios web gubernamentales.

Por ejemplo, gracias a estos documentos de contratación pública en el periodo previo a los Juegos Olímpicos de Invierno de Sochi en 2014, los periodistas pudieron determinar y mapear la manera en que los servicios de seguridad rusos planeaban vigilar las comunicaciones telefónicas y por internet durante los juegos.

Tras detectar una licitación de Frontex (la agencia de fronteras de la UE) en la que se buscaba una empresa de vigilancia para rastrear a personas en las redes sociales, Privacy International respondió con preguntas detalladas sobre la licitud del plan. Dos días después Frontex canceló la licitación.

A veces, estos mismos sitios u otros sitios similares también brindan información sobre qué contratos se han adjudicado a qué empresas. Por ejemplo, en los Estados Unidos, el sitio web de contratación federal proporciona datos sobre las empresas a las que se han adjudicado contratos. Los periodistas con frecuencia utilizan estas páginas para acceder a la información y hacer reportajes sobre la misma, aunque los detalles suelen ser mínimos. Tech Inquiry ofrece una plataforma de búsqueda a través de la cual se pueden buscar los contratos reportados por las autoridades australianas, canadienses, estadounidenses y británicas.

Privacy International también tiene una guía dirigida a investigadores y periodistas sobre algunas de las fuentes abiertas disponibles que pueden ser usadas para identificar las exportaciones de vigilancia.

Privacy International desarrolló un curso en línea gratuito para aprender más sobre la privacidad y la investigación de la tecnología de vigilancia que está disponible en Advocacy Assembly.

iii. Los interesados como fuentes de información

Además de la investigación documental y las solicitudes formales, entablar contacto con personas que participan o conocen una asociación público-privada puede darle acceso a información o perspectivas fundamentales para su trabajo.

Los académicos, los funcionarios públicos y las personas que trabajan en empresas privadas similares pueden ser buenas fuentes de información para su trabajo si se les aborda adecuadamente y con las prácticas de investigación adecuadas (como la anonimización).

Es posible que los periodistas que han cubierto la asociación sobre la cual está haciendo la investigación también hayan tenido acceso a fuentes importantes y estén dispuestos a compartir información adicional con usted si los contacta directamente.

Del mismo modo, puede haber otras organizaciones o grupos que están investigando la misma asociación. Trate de coordinar con estos grupos para compartir información y, potencialmente, reforzar su labor de incidencia más adelante.

Cuando se acerque a las personas involucradas directamente con la asociación en cuestión, debe asegurarse de que se sientan seguras y de que comprende su postura. Ser flexible y evitar acusaciones es clave para obtener información importante. Siempre hay que tener consideración con las preocupaciones que esas personas puedan tener. En todos los casos, es fundamental discutir y acordar de antemano las condiciones de este intercambio de información. Siempre busque ayuda y consejo si no está seguro de cómo manejar una fuente.

Aclaración: antes de realizar una entrevista, asegúrese de hacer una valoración del riesgo adecuada y considerar seriamente los riesgos para su organización y para las personas con las que está hablando. Asegúrese de que puede ofrecer un nivel

adecuado de privacidad y seguridad, y de que comprende las implicaciones legales, antes de hablar con personas que se exponen a riesgos al compartir información.

Lo que dicen nuestros aliados:

Si la APP que está investigando se enfoca en una región o área específica, buscar en periódicos locales, grupos de Facebook y organizaciones locales puede revelar información importante. Puede que estos grupos tengan acceso a información de poca divulgación o que estén en contacto con personas clave de la asociación.

En Argentina, en una ocasión, la ADC obtuvo información clave al mirar en un grupo de Facebook de lugareños que intentaban movilizarse contra un proyecto que se estaba desarrollando en su zona.

Nuestro aliado anónimo descubrió que entrevistar a interesados que hayan salido recientemente de una organización puede ayudar a entender, por ejemplo, en qué casos las políticas no son un reflejo fiel de la realidad.

C. LISTA DE CONTROL – DESCUBRIENDO LA INFORMACIÓN

Para facilitar su investigación, quizás desee utilizar esta lista de control:

- □ ¿Ha considerado las implicaciones éticas, legales y de seguridad de acceder y/o compartir la información que está buscando?
- □ ¿Ha considerado posibles riesgos y mitigaciones propias de su contexto y circunstancias?
- □ ¿La información que busca puede consultarse fácilmente en el dominio público?
- □ En la jurisdicción que le interesa, ¿existe legislación sobre libertad de información o acceso a documentos a las que pueda recurrir?
- □ ¿Existen guías o cursos relevantes sobre cómo aplicar ciertas técnicas de investigación de fuentes abiertas que puedan ayudarle a encontrar lo que busca?
- □ ¿Existen fuentes abiertas a la que pueda acceder en su país para encontrar la información?
- □ ¿Existen fuentes abiertas en el extranjero a las que pueda acceder para encontrar la información?
- □ ¿Hay alguna persona u organización que pueda ayudarle a encontrar la información y con la que pueda ponerse en contacto de forma segura?
- □ ¿Sus fuentes le han dado su consentimiento adecuado y debidamente informado?
- □ ¿Ha considerado cómo manejar la información que recibe de sus fuentes?
    - □ ¿Dónde guardará la información?
    - □ ¿Necesita volverla anónima? ¿Usar un seudónimo?
    - □ ¿Es necesario redactar información? ¿Cómo lo hará minuciosamente?
    - □ ¿Hay algún detalle contextual en la información que apunte hacia su fuente o hacia cualquier otra persona?

3. DESVELANDO Y ENTENDIENDO LA TECNOLOGÍA SUBYACENTE

Las tecnologías en el corazón una asociación público-privada pueden estar rodeadas de secretismo y opacidad, lo que dificulta que actores externos evalúen los riesgos. Desde palabras de moda hasta terminología técnica confusa, no es fácil tener una idea precisa de qué es la tecnología en cuestión y de lo que hace en realidad. Esta sección está diseñada para guiarlo en la búsqueda de más información sobre la tecnología, su comprensión y la identificación de posibles fallas.

A. IDENTIFICACIÓN DE LOS BLOQUES DE LA TECNOLOGÍA EN CUESTIÓN

El primer paso a la hora de analizar una tecnología es encontrar información básica sobre ella, para definirla y clasificarla. Consultar la página de Wikipedia de una tecnología concreta suele ser un buen punto de partida y le ayudará a aclarar lo que implica la tecnología (por ejemplo, en el caso del reconocimiento facial). Esto es especialmente útil cuando la asociación no menciona ninguna tecnología específica o al examinar una licitación. También puede consultar el material de marketing de la empresa para tener una idea de su especialidad y del tipo de producto que ofrece.

A veces, una asociación involucra más de una tecnología, a veces a través de más contratos y/o múltiples asociaciones - como un sistema de identificación que requiera un escáner de huellas dactilares y una base de datos, que podrían ser suministrados por diferentes empresas.

Hacerse una idea general de lo que se está analizando es un paso sencillo pero muy importante para poder avanzar e identificar los riesgos. **El objetivo es poder dar una definición de alto nivel, amplia pero precisa, de cuál es la tecnología de la asociación.**

Ejemplos de descripciones de alto nivel de una tecnología:

- Sistema de reconocimiento facial: un sistema capaz de cotejar rostros identificados en una imagen o video específico con un conjunto de datos de rostros humanos previamente identificados.
- Brazalete o tobillera de rastreo: brazalete físico que se sujeta a la extremidad de una persona y es capaz de registrar y transmitir la geolocalización o la proximidad con un marcador de base.
- Vehículo aéreo no tripulado: vehículo aéreo autónomo o controlado a distancia capaz de realizar acciones predeterminadas y de recoger, tratar y transmitir datos medioambientales como imágenes, temperaturas y sonidos.

Después de este primer paso, pronto notará que las tecnologías suelen depender de múltiples elementos físicos y lógicos para funcionar. Descomponerla e identificar cada capa es, por consiguiente, el siguiente lógico paso para comprender cómo funciona la tecnología y cuáles son los posibles puntos débiles. Por ejemplo, un sistema de reconocimiento facial captura, transmite, almacena y trata datos. Diferentes elementos desempeñan un papel clave en cada uno de estos pasos.

Las capas pueden ser hardware, software o una combinación de ambos. El conjunto de tecnologías que hay detrás de un término tan simple como “una base de datos” puede ser complejo. Cuanto más minucioso sea al dividirla en bloques, comprenderá mejor lo que está en juego y los posibles riesgos.

Utilizando un enfoque centrado en los datos, los distintos elementos que componen la tecnología suelen encajar en una de las **cuatro** categorías a continuación:

i. Sistema de recolección/captura de datos (hardware/software)

La recolección de datos consiste en capturar información. Podría ser una cámara que toma fotos, un sensor que capta información como la temperatura, un software que registra acciones como pulsar un botón o un dispositivo que extrae de datos de teléfonos móviles. Los sistemas de recolección de datos pueden ser dispositivos

físicos, como un satélite equipado con sensores, o virtuales, como una aplicación o un raspador web (un fragmento de código que rastrea el internet para recolectar datos).

¿Por qué es importante?

Entender qué parte de la tecnología se encarga de recolectar los datos le permite comprender qué datos se recolectan (imágenes, sonido, datos introducidos por el usuario), de dónde proceden (sensores, interacciones con el usuario) y en qué circunstancias se recolectan (con o sin el conocimiento de la persona, con qué frecuencia, etc.). Esto le permite identificar posibles problemas relacionados con la licitud de la recolección o la exactitud de los datos recolectados.

Ejemplos de un sistema de recolección de datos:

- Una red de cámaras en una ciudad
- Un sitio web para inscribirse en un evento público
- Un satélite con una variedad de sensores que toman fotos de una zona determinada
- Una máquina lectora de huellas dactilares en el aeropuerto

Posibles riesgos en la recolección de datos

Los datos recolectados podrían ser incorrectos, los sensores podrían ser manipulados, los datos podrían recogerse sin consentimiento o fundamento jurídico, los sensores físicos podrían degradarse con el tiempo, la lógica o el conjunto de instrucciones (para un programa informático) podría tener sesgos o errores, el dispositivo podría ser vulnerable a ataques (sobrecarga, datos incorrectos, etc.).

ii. Sistema de transmisión de datos (hardware/software)

Después de recoger los datos, éstos pueden ser transmitidos a otro sistema para su almacenamiento o tratamiento, por ejemplo, a un servidor. Usualmente, las transmisiones se hacen a través de soluciones existentes con protocolos

claramente definidos, como el conjunto de protocolos (TCP/IP) para la comunicación entre dispositivos en la misma red (como dos servidores conectados a internet o una cámara inteligente y una computadora conectados a una red privada), pero en ocasiones podría tratarse de la innovación en cuestión (por ejemplo, la propuesta New IP presentada por China en la Unión Internacional de Telecomunicaciones (UIT) o 5G New Radio, el estándar mundial para la interfaz aérea de las redes 5G).

¿Por qué es importante?

Entender si los datos son transmitidos y la manera en que se transmiten permite identificar riesgos potenciales para la seguridad (por ejemplo, si la transmisión no está protegida porque se utiliza una red Wi-Fi no segura), problemas existentes (si un protocolo/red está desactualizado y presenta vulnerabilidades ya identificadas, como la 2G) o requisitos técnicos (por ejemplo, la distancia a la que Bluetooth puede funcionar para transmitir datos con fiabilidad) para evaluar mejor la idoneidad en un contexto concreto.

Ejemplos de sistemas de transmisión de datos:

- El conjunto de protocolos (TCP/IP, el protocolo sobre el que se basan la mayoría de las tecnologías de internet)
- El Sistema Global para Comunicaciones Móviles (GSM por sus siglas en inglés)
- Bluetooth
- Comunicaciones por satélite a través de ondas de radio de alta frecuencia

Posibles riesgos de la transmisión de datos

La tecnología puede ser poco segura (nivel de encriptación bajo o deficiente, vulnerabilidades conocidas, etc.), los datos pueden degradarse/perderse en tránsito, los datos pueden ser interceptados/manipulados, el sistema puede plantear amenazas para la salud, el sistema puede verse interrumpido por factores externos (ataque de denegación de servicio a una red, destrucción del emisor/receptor, etc.).

Nota: para información adicional sobre protocolos, normas y organismos de normalización, consulte “Nota sobre protocolos y normas técnicas” al final de este capítulo.

iii. Sistema de almacenamiento de datos (hardware/software)

Después de capturar y trasmitir los datos, es posible que sean almacenados en algún lugar para ser tratados o archivados. Por lo general, los sistemas de almacenamiento dependen de algún tipo de dispositivo de almacenamiento, como un disco duro, una tarjeta SD, una memoria USB, muchas veces como parte de un sistema más amplio si es necesario accederlo con regularidad (portátil, servidor...). Existe una amplísima variedad de software para almacenar y acceder a estos datos, desde programas de bases de datos como MySQL hasta sistemas basados en una *blockchain* o cadena de bloques que ofrece inmutabilidad.

¿Por qué es importante?

Identificar dónde y cómo se almacenan los datos permite comprender mejor las implicaciones (el software o el método usado podría ser susceptible a vulnerabilidades de seguridad o ser blanco frecuente de ataques, como una base de datos ElasticSearch o algún producto bucket similar), la **retención** (el sistema podría limitar el almacenamiento de datos solo a ciertos periodos de tiempo o podría, por el contrario, almacenarlos indefinidamente, como un sistema blockchain, el **control de acceso** (un sistema con permisos demasiado laxos puede permitir accesos no autorizados) y la **durabilidad** (la vida útil previsible de una tarjeta SD es menor que la de una SSD, por ejemplo). ¿El sistema de almacenamiento de datos elegido es adecuado para el propósito que se pretende lograr? Saber dónde está un sistema de almacenamiento, a qué está conectado y quién tiene acceso al mismo también ofrece claves para evaluar mejor el riesgo.

Ejemplos de sistemas de transmisión de datos:

- Un disco duro/llave USB con algún sistema de archivos (NTFS, exfat, ext4...)

- Una base de datos SQL (una base de datos de software diseñada para usar SQL como lenguaje de acceso)
- Una blockchain duplicada en varios clientes
- Un CD no regrabable (CDR-R)
- Un programa de hoja de cálculo como Microsoft Excel

Posibles riesgos en el almacenamiento de datos

La mala gestión de permisos que posibilita accesos no autorizados a los datos, fallas de los equipos físicos de almacenamiento (por ejemplo, un disco puede fallar y perder los datos que almacenaba), capacidad de retención de datos inadecuada (por ejemplo, una blockchain que almacena datos que deberían borrarse), capacidad de almacenamiento inadecuada (por ejemplo, no puede almacenar nuevos datos porque está llena), poca vida útil (por ejemplo, elegir un software de gestión de bases de datos que no recibe soporte de su fabricante y que no recibe o pronto dejará de recibir actualizaciones de seguridad), etc.

iv. Sistema de tratamiento de datos (software)

Tras su captura o almacenamiento, los datos pueden ser tratados para producir nueva información. Podría ser un software de análisis de imágenes que define cuáles son los objetos visibles en una imagen capturada, un algoritmo que resuelve un problema matemático o un programa que predice temperaturas basándose en datos recolectados previamente. Los sistemas de tratamiento de datos pueden tratar datos sobre la marcha (sin almacenar datos en pasos intermedios) o usar datos almacenados. Estos sistemas suelen ser software desarrollado utilizando un conjunto de lenguajes de programación (Java, Python, Go…) y pueden funcionar conectados con el sistema de almacenamiento de datos. Pueden ejecutarse en una gran variedad de dispositivos que abarcan desde un servidor hasta un teléfono inteligente o un microcontrolador de placa única. Algunos sistemas como la inteligencia artificial (IA) basada en redes neuronales funcionarán de forma diferente dependiendo de los datos que estén tratando, pero también los datos con los que fueron entrenados. En este caso, puede que valga la pena considerar el conjunto de

datos de entrenamiento para el sistema de IA como un bloque independiente dentro de la categoría de recolección/captura de datos. Cuanto mejor separe los diferentes componentes, mejor comprenderá lo que está en juego.

¿Por qué es importante?

Los sistemas de tratamiento de datos pueden producir información sesgada e inexacta, ya sea por los datos introducidos en el sistema (incompletos, inexactos, no representativos...) como por defectos de lógica (algo que no tiene en cuenta la lógica del algoritmo). Entender para qué fue diseñado el tratamiento de datos, qué datos trata y qué tipo de información genera puede servir para detectar posibles errores en la lógica del código, variables omitidas o evaluar si un sistema tiene la capacidad de tomar decisiones adecuadas.

Ejemplos de sistemas de tratamiento de datos:

- Un software de reconocimiento facial que trata fotos tomadas por cámaras públicas
- Un software para detectar el movimiento de embarcaciones que utiliza IA e imágenes satelitales
- Un sistema publicitario que deduce los rasgos de su personalidad a partir de datos recogidos en línea
- Un asistente virtual como Siri/Google/Alexa

Posibles riesgos del tratamiento de datos

Fallas en la lógica del algoritmo (ignora algo o errores humanos que hacen que los resultados sean falsos), falta de soporte del fabricante (el software/programa no recibe soporte después de cierto tiempo, lo que complica o imposibilita que el comprador lo desarrolle y corrija en el futuro), poca transparencia/rendición de cuentas debido a las licencias (software propietario que complica o imposibilita el proceso de auditoría), sesgos derivados del conjunto de datos sobre el que se ha entrenado o de los datos que se han incluido, vulnerabilidad de seguridad (acceso no autorizado, pirateo...), etc.

v. Nota sobre la prioridad de los bloques tecnológicos

Si está examinando una empresa o un contrato específicos, puede utilizar esta información y análisis para enfocarse en las capas donde la empresa está más presente. Si está mirando una empresa especializada en software y tratamiento de datos (como Palantir), sabrá que es probable que esta sea la capa clave.

Eso no significa que deba descuidar las otras capas de la tecnología desplegada, por el contrario, es posible que estos elementos, puesto que no necesariamente forman parte de la experiencia de la empresa o el organismo público, terminen siendo descuidados y gestionados mal. Por ejemplo, el Reino Unido almacenó y finalmente extravió datos relacionados con la covid en un archivo de Excel, lo que dejó al descubierto la poca atención prestada al sistema de almacenamiento de datos, especialmente en comparación con el esfuerzo dedicado a recolectarlos.

B. EVALUANDO LA NOVEDAD/INNOVACIÓN

Es muy posible que la asociación público-privada implique una tecnología muy conocida y ampliamente desplegada en otros contextos, pero también puede que sea un terreno fértil para la innovación y la novedad.

Podemos identificar dos tipos principales de innovación:

1. Una nueva tecnología poco usada o que aún no ha sido desplegada en el mundo real (fuera del laboratorio o un trabajo de investigación);
2. Un nuevo paquete de funcionalidades añadidas a una tecnología existente que amplían enormemente su rendimiento y capacidad.

Otro tipo de “innovación” puede implicar el despliegue de tecnologías existentes en nuevos contextos. Evaluar estos despliegues exige principalmente la identificación de los problemas de gobernanza (Sección 4, a continuación).

i. Tecnología completamente nueva

En el caso de tecnologías totalmente nuevas, el factor de novedad suele ser obvio porque es probable que la tecnología en cuestión sea poco conocida. Las tecnologías revolucionarias novedosas son escasas y plantean varios riesgos, puesto que no siempre han sido probadas adecuadamente o puede que tengan efectos secundarios inesperados. Acercarse a una tecnología completamente nueva es difícil para los actores externos y puede ser difícil recolectar información relevante. No obstante, la innovación conlleva una serie de riesgos comunes que vale la pena explorar:

- Disparidades entre el entorno de prueba y el mundo real que afectan la eficacia de la tecnología
- Pruebas insuficientes, lo que significa que la población contra quien se despliega la está probando en fase beta
- Sobreestimación de la capacidad y exactitud de la tecnología: la tecnología no funciona o produce demasiados errores
- Se pasa por alto la creación de nuevos problemas, como el coste de mantenimiento, la sostenibilidad del proyecto en el futuro, los problemas derivados de los casos extremos o el hecho de que el organismo público queda atrapado en un contrato que no puede ejecutar nadie más
- Desviación progresiva del uso: a tecnología puede ser utilizada para más fines de los inicialmente previstos
- Falta de transparencia/rendición de cuentas si la tecnología es protegida por el secreto comercial y/o por licencias de propiedad intelectual

ii. Nuevas funcionalidades/capacidades

En el caso de una tecnología existente con nuevas funcionalidades o capacidades, la innovación puede ser más difícil de detectar, pero puede tener un impacto importante sobre la forma en que se utiliza la tecnología. Las nuevas funcionalidades y capacidades podrían ser el resultado de un salto tecnológico en el hardware o el software. Puede tratarse, por ejemplo, de nuevas unidades de procesamiento informático (CPU por sus siglas en inglés) mucho más potentes que la generación anterior, o de avances técnicos novedosos como la computación cuántica. En cuanto al software, puede ser el desarrollo de nuevas técnicas de

procesamiento, como el auge del aprendizaje profundo y soluciones de IA equivalentes.

Estas innovaciones también podrían ser simplemente la adición de una tecnología existente a una solución, por ejemplo, el montaje de sensores de Frecuencia Radion en multitud de pequeños satélites (como CubeSat), una innovación que es posible gracias al bajo precio de estos satélites. Los riesgos que surgen con la adición de nuevas funcionalidades o capacidades son más específicos y deberían ser más fáciles de identificar. Estos son algunos de los riesgos que surgen con estas innovaciones:

- Las nuevas capacidades no son necesarias para que la tecnología cumpla su función inicial (por ejemplo, equipar cámaras corporales con sensores de temperatura)
- La nueva capacidad no se ha probado adecuadamente para el entorno en el que se está desplegando y podría generar resultados inadecuados (por ejemplo, desplegar un algoritmo de red neuronal para el sistema judicial)
- La nueva funcionalidad o capacidad permite que la tecnología tenga un alcance mucho más intrusivo (por ejemplo, mejorar la calidad de imagen de las cámaras de videovigilancia)
- La nueva funcionalidad/capacidad hace que la tecnología sea mucho más eficiente y permite su aplicación en masa (por ejemplo, interceptación y tratamiento en masa de datos de internet)

iii. Nota sobre protocolos y normas técnicas

Como ya se ha mencionado en la sección dedicada a los *sistemas de transmisión de datos*, puede resultar interesante examinar y comprender los protocolos y las normas a la hora de analizar una tecnología. Pueden aportar información sobre si la tecnología se está implantando en un entorno ya desarrollado y normalizado o si se está intentando definir nuevas normas. A continuación, se indican algunas definiciones útiles y organismos de normalización que podrían ser relevantes:

Definiciones:

- **Protocolo**: un protocolo es un lenguaje concertado que permite que diferentes elementos se comuniquen. Uno de los protocolos más conocidos es el conjunto de protocolos conocido como TCP/IP. Los protocolos suelen estar normalizados y responden a un conjunto específico de normas. Permiten que cualquier nuevo participante en un mercado desarrolle fácilmente un producto que puede utilizar la infraestructura existente y comunicarse con otros productos. Por ejemplo, con TCP/IP, cualquiera puede crear un dispositivo conectado a internet que pueda comunicarse con un servidor o dispositivos similares en todo el mundo.
- **Norma técnica**: norma o requisito para realizar una tarea técnica. Las normas técnicas son más abstractas que los protocolos en la medida en que no plantean reglas definidas de forma precisa y estricta para tecnologías o lenguajes de programación concretos. Establecen principios, métodos y procesos uniformes que deben ser seguidos al desarrollar una tecnología. El objetivo es garantizar la interoperabilidad entre dispositivos y sistemas (por ejemplo, para garantizar que discos duros externos fabricados por una empresa distinta a la empresa fabricó su computadora funcionen en cualquier computadora). Las normas pueden ser desarrolladas en privado o unilateralmente por organizaciones de normalización. Ejemplo: Bus Serie Universal (USB por sus siglas en inglés).

Organismos de normalización

- **Unión Internacional de Telecomunicaciones (UIT):** la UIT es una organización de las Naciones Unidas que se ocupa de las radiocomunicaciones y la normalización. Trabaja para que los países y los actores particulares se pongan de acuerdo sobre las normas y los protocolos para evitar choques y fomentar el desarrollo. Las normas desarrolladas por la UIT se denominan Recomendaciones. Algunos ejemplos de sus actividades:
    - Gestionar el espectro de radiofrecuencias (define el uso de cada parte del espectro y a quién le corresponde; por ejemplo, Wifi y Bluetooth operan entre 2400 y 2500 MHz);
    - Desarrollar y hacer mantenimiento de la Arquitectura de Documento Abierta, un ejemplo de formato de archivo de documentos normalizado

gratuito y de código abierto que cualquier desarrollador de software puede utilizar para procesar textos;
    - Publicar recomendaciones sobre el blindaje de cables para limitar las interferencias;
    - Los grupos de trabajo elaboran recomendaciones sobre temas como las tecnologías de información cuántica para redes y la inteligencia artificial para la conducción asistida y autónoma.
- **Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés)**: una organización de normas abiertas, que desarrolla y promueve normas voluntarias de internet, en particular los estándares que componen el conjunto de protocolos de internet (TCP/IP).
- **Organización Internacional de Normalización (ISO por su sigla en inglés):** organismo de normalización compuesto por representantes de diversas organizaciones nacionales de normalización que publica normas técnicas, industriales y comerciales de alcance mundial. Ejemplo de normas: ISO 80601, que garantiza que los termómetros se calibren de la misma manera en distintos hospitales.
- **W3C** : organización de normalización para la World Wide Web.

Los organismos de normalización que tienen discusiones abiertas sobre normas son lugares interesantes (aunque a menudo difíciles de penetrar) para identificar grupos de presión e influencias. A veces, las empresas privadas o los países los utilizan como puerta de entrada para impulsar una solución técnica que puede tener consecuencias políticas. Por ejemplo, en 2021, el W3C creó un grupo de trabajo sobre “mejora de la publicidad web” en el que Google propuso sustituir las cookies de terceros que continúan permitiendo el rastreo y la segmentación.

C. ENTENDIENDO CÓMO FUNCIONA LA TECNOLOGÍA EN CUESTIÓN

Aquí identificamos tres formas principales de entender mejor cómo funciona una tecnología:

i. Revisión de bibliografía adicional
ii. Uso y prueba de las alternativas existentes
iii. Consulta de expertos

i. Revisión de bibliografía adicional

Existen varios recursos que simplifican y popularizan tecnologías complejas, comenzando por Wikipedia. Otros recursos pueden ser tremendamente útiles incluso cuando se posee poco o ningún conocimiento técnico, como la prensa semiespecializada. Por ejemplo:

- MIT Technology Review (por ejemplo, sobre computación cuántica)
- ArsTechnica, (por ejemplo, sobre NFTS)
- PC Mag (por ejemplo, sobre 5G Mag)

Los artículos académicos son otra vía para encontrar información, aunque el lenguaje puede ser menos accesible si no se tienen conocimientos técnicos previos. Aun así, vale la pena buscar en Google Scholar y otros recursos para encontrar artículos sobre la tecnología que está estudiando, idealmente en un contexto similar al suyo o que se enfoquen en preocupaciones parecidas.

Algunas ONG con recursos técnicos también publican materiales que pueden servir de guía para entender cómo funciona una tecnología específica y cómo puede utilizarse en contextos concretos, por ejemplo:

- Privacy International (manuales técnicos básicos sobre Bluetooth y GPS)
- EFF (guías sobre Amazon Sidewalk e IMSI catchers)
- Citizen Lab (análisis del software de filtración de contenido en la popular aplicación china YY)

Hasta cierto punto, los sitios web de los fabricantes pueden ofrecer información útil sobre la tecnología que está examinando y la manera en que funciona. La documentación técnica o promocional de los productos que fabrican estas empresas

puede ser una gran herramienta para comprender las especificaciones de una tecnología determinada y entender cómo funciona. Tal vez quiera usar métodos como Google Dorking para encontrar folletos oficiales de las empresas y otros documentos que le ayuden en su búsqueda.

Como en cualquier investigación, ¡es crucial contrastar los resultados y verificarlos con más de una fuente para evitar la desinformación!

ii. Uso y prueba de las alternativas

Buscar sistemas equivalentes a precios asequibles y estudiar su funcionamiento puede ayudarle a comprender mejor en qué consiste el sistema que está estudiando. Si está estudiando sistemas de reconocimiento facial, por ejemplo, puede ser útil buscar proyectos de código abierto que pueda analizar y desglosar libremente, como este.

Es posible que el uso de estas alternativas precise ciertos conocimientos técnicos y no sea fácilmente accesible para todo el mundo. Los tutoriales y las guías para principiantes pueden ayudarle a configurar y probar estos sistemas y deben considerarse como una forma más fácil de abordar esta estrategia. Del mismo modo, un curso en línea sobre “cómo empezar con X” puede ayudarle a comprender mejor cómo funciona una tecnología. Los capítulos introductorios del libro de D2L sobre aprendizaje profundo, por ejemplo, le ayudarán a comprender los distintos elementos en juego en la tecnología de IA.

Las organizaciones con conocimientos técnicos también pueden compartir guías, documentación y metodologías para utilizar los sistemas que emplean en su trabajo. Por ejemplo, PI tiene un Entorno de Interceptación de Datos (*Data Interception Environment*) para analizar el tráfico de aplicaciones Android y lo ha puesto a disposición de todo el mundo.

Podría valer la pena buscar a otras personas que hayan hecho antes este tipo de pruebas, como expertos que intenten encontrar fallos o demostrar el sesgo de una determinada tecnología. El trabajo de Joy Buolamwini sobre sistemas racistas de

reconocimiento facial es un buen ejemplo de cómo expertos ponen a prueba una tecnología para descubrir sus puntos débiles.

iii. Consulta de expertos

Después de hacer la investigación, puede que aún haya preguntas sin resolver, puntos que no sabe cómo conectar o, simplemente, cosas que no tiene el conocimiento técnico para comprender. Recurrir a expertos del mundo académico, la prensa especializada o las organizaciones de la sociedad civil puede ser útil en estos casos.

Al hacerlo, le sugerimos que explique lo más claramente posible qué intenta hacer, con qué fin, qué ha entendido hasta ahora y formule preguntas lo más precisas posible. Los expertos en la materia suelen tener menos interés en dictar una clase sobre una tecnología determinada que en ayudarle a entender su aplicación en un contexto específico. Hacer una lista de preguntas precisas con información detallada del contexto maximizará sus posibilidades de recibir una respuesta o una llamada de un experto.

Para saber a quién dirigirse, puede empezar por los académicos que hayan escrito artículos sobre la tecnología que está estudiando, sobre todo si su investigación se centra en uno de los riesgos clave que ha identificado. También puede escribirle a profesionales que trabajen con la tecnología en cuestión, ya que suelen tener mucha experiencia práctica sobre su uso. Buscar personas en grupos de trabajo, grupos de intercambio y grupos para compartir conocimientos es un buen primer paso, ya que indica el deseo de compartir y aprender, lo que aumenta las posibilidades de encontrar a alguien dispuesto a ayudarle. Preguntar en comunidades online especializadas como StackOverflow o Reddit también puede conseguir información muy relevante.

Algunas organizaciones, como PI, también cuentan con tecnólogos a los que puede dirigirse. Puede que no sean expertos en la tecnología que le interesa, pero podrían indicarle recursos u otras personas con quienes hablar.

Lo que dicen nuestros aliados:

Es difícil entender completamente la tecnología que se analiza. La ADC sugiere aceptar que no siempre se puede saber cómo funcionan todos los bloques implicados e intentar que el trabajo sea revisado por expertos para asegurarse de que no se está diciendo algo totalmente equivocado. Es más importante asegurarse de que entiende bien los conceptos básicos y de que el análisis se basa en información corroborada

D. LISTA DE CONTROL - ENTENDIENDO LA TECNOLOGÍA

Esta lista de control le ayudará a asegurarse de que ha identificado correctamente los problemas relacionados con la tecnología que está investigando:

- ¿Puede definir a grandes rasgos la tecnología en cuestión y qué es lo que hace?
- ¿Qué papel desempeñan los datos en la tecnología en cuestión? (sistema de recolección de datos, sistema de transmisión de datos, sistema de almacenamiento de datos, sistema de tratamiento de datos)
- ¿Cuáles son los riesgos asociados con esta tecnología para cada sistema específico?
- ¿Qué tan innovadora y revolucionaria es la tecnología?
    - ¿Cuáles son los riesgos asociados con el factor de innovación?
- ¿Puede explicar cómo funciona la tecnología en la práctica?
    - [Opcional] ¿Cuáles son los riesgos asociados con la manera específica en que funciona la tecnología?

4. PREOCUPACIONES SOBRE LA GOBERNANZA

Gracias a nuestra labor de investigación y a la de nuestros aliados en todo el mundo, hemos detectado una serie de preocupaciones persistentes de gobernanza que son habituales en las asociaciones público-privadas. Detallamos cada uno de ellas y las correspondientes salvaguardias, aquí. En esta sección ofrecemos una orientación a nivel general sobre cómo identificar este tipo de preocupaciones.

A. PRINCIPIOS RECTORES DE LAS NACIONES UNIDAS SOBRE LAS EMPRESAS Y LOS DERECHOS HUMANOS

Según los Principios Rectores de la ONU sobre las empresas y los derechos Humanos ("Principios Rectores de la ONU"), las empresas deben respetar los derechos humanos, lo que significa que 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 (Principio Rector 11).

Los Principios Rectores de la ONU son un conjunto de directrices para que los Estados y las empresas prevengan, hagan frente y reparen los abusos contra los derechos humanos cometidos en las actividades empresariales. El Consejo de Derechos Humanos de la ONU aprobó por unanimidad los Principios Rectores de la ONU en su resolución 17/4 del 16 de junio de 2011.

Los Principios Rectores de la ONU constituyen el estándar mundial para la protección de los derechos humanos en el contexto empresarial. Por ello, en el curso de una investigación, pueden utilizarse para evaluar el cumplimiento de las normas de derechos humanos por parte de una asociación público-privada. Además, son un recurso para hacer incidencia por las medidas específicas que deben adoptar las

empresas y los gobiernos. En esta sección, destacamos las principales responsabilidades de las empresas derivadas de los Principios Rectores de la ONU y explicamos cómo, a pesar de su carácter no vinculante, se han convertido en la norma a la hora de evaluar las responsabilidades en materia de derechos humanos de las actividades empresariales.

i. Los Principios Rectores de la ONU como estándar de conducta para las empresas

Los Principios Rectores contienen tres capítulos o pilares: proteger, respetar y remediar. Cada uno define medidas concretas y prácticas para que los gobiernos y las empresas cumplan sus respectivas obligaciones y responsabilidades de prevenir los abusos contra los derechos humanos durante las actividades de la empresa y de remediar en caso de que se produzcan.

Las empresas deben, entre otras cosas:

- adoptar un compromiso explícito y de política pública de cumplir su responsabilidad de respetar los derechos humanos (compromisos de políticas de derechos humanos);
- llevar a cabo evaluaciones de riesgos que examinen las repercusiones reales y potenciales sobre los derechos humanos de las herramientas y los servicios propuestos (debida diligencia y evaluación de impacto en materia de derechos humanos - debida diligencia de derechos humanos); y
- establecer mecanismos internos de rendición de cuentas en relación con la aplicación de las políticas de derechos humanos y disponer de procesos que garanticen la reparación (mecanismos de reclamación).

El proceso de debida diligencia de derechos humanos incluye cuatro componentes básicos: identificar y evaluar los efectos adversos reales o potenciales sobre los derechos humanos que la empresa pueda causar, a los que pueda contribuir o con los que esté directamente relacionada; tomar las medidas adecuadas e integrar las conclusiones de las evaluaciones de impacto en todos los procesos pertinentes de la

empresa; hacer un seguimiento de la eficacia de las medidas para evaluar si están funcionando; y comunicar a los interesados cómo se está haciendo frente a los efectos y mostrarles que existen políticas y procesos adecuados.

ii. Las empresas de tecnología y los Principios Rectores de la ONU

Los Principios Rectores de la ONU se aplican a todas las empresas y, por tanto, también al sector de la tecnología. Sin embargo, las empresas tecnológicas no han recibido el mismo nivel de escrutinio que otras industrias, principalmente por la complejidad inherente a los productos y servicios, y por el carácter novedoso de los efectos sociales que suscitan. El Proyecto B-Tech de la ONU proporciona sólidas pautas y recursos para implementar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos (PRNU) en el espacio tecnológico. Este proyecto se inició en 2019 y está dirigido por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Por ejemplo, "Introducción a los Principios Rectores de las Naciones Unidas en la era de la tecnología".

Además, los procedimientos especiales de la ONU y otros órganos de derechos humanos ofrecen cada vez más orientación sobre la aplicación de los Principios Rectores de la ONU en el sector de la tecnología. Por ejemplo, el informe elaborado bajo los auspicios del mandato del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, por la Dra. Krisztina Huszti-Orbán y la Profesora Fionnuala Ní Aoláin, sobre el "Uso de datos biométricos para identificar terroristas: ¿Buena práctica o negocio arriesgado?" Así mismo, el Informe de 2019 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre "Vigilancia y derechos humanos" utiliza el Principio Rector de la ONU como punto de partida al examinar la responsabilidad de las empresas (A/HRC/41/35).

iii. Los Principios Rectores de la ONU como estándar mundial

Se considera hoy día que los Principios Rectores de las Naciones Unidas son el estándar mundial por excelencia sobre la responsabilidad de las empresas de respetar los derechos humanos, y el Consejo de Derechos Humanos de las Naciones Unidas los acogió unánimemente en 2011 (Resolución 17/4). Aunque los Principios Rectores de la ONU no son jurídicamente vinculantes, se están convirtiendo en la norma que regula las operaciones de las empresas a través de nueva legislación nacional y su incorporación en las iniciativas de los inversores.

1) Base para la legislación nacional: en varios países, los Principios Rectores de la ONU han servido como base para el desarrollo de legislación nacional sobre responsabilidad empresarial. En 2017, por ejemplo, el Parlamento francés aprobó una nueva ley que impone a las multinacionales la obligación de prevenir las violaciones graves de los derechos humanos en todas sus filiales y cadenas de suministro (*loi de vigilance*). Otros países están preparando iniciativas legislativas similares. El 11 de junio de 2021, el Parlamento alemán aprobó la "Ley de Debida Diligencia Corporativa en las Cadenas de Suministro" (Ley de Debida Diligencia en las Cadenas de Suministro - "Ley" o "LkSG"). El 23 de febrero de 2022, la Comisión Europea adoptó una propuesta de directiva sobre la debida diligencia de las empresas en materia de sostenibilidad, que se basa en parte en los Principios Rectores de las Naciones Unidas.

Otros países y Estados han implementado legislación de debida diligencia para derechos humanos específicos: por ejemplo, Australia, California y el Reino Unido sobre la esclavitud moderna y los Países Bajos sobre el trabajo infantil. Puede consultar un resumen de la evolución reciente en Centro de Información sobre Empresas y Derechos Humanos.

Además, varios países, entre ellos Chile, Colombia, Dinamarca, Finlandia, Alemania, Países Bajos, Noruega, Italia, España, Suiza, Tanzania, Tailandia, Kenia, Uganda, el Reino Unido y los Estados Unidos, han incorporado los Principios Rectores de la ONU en sus planes de acción nacionales. Un plan de acción nacional sobre empresas y derechos humanos es una estrategia política para garantizar que los Estados protejan adecuadamente a las personas de las consecuencias negativas de las actividades de las empresas sobre los derechos humanos.

Con bastante frecuencia, la aplicación de la legislación nacional se extiende a las operaciones empresariales fuera del territorio de los Estados legisladores. Por ejemplo, la directiva de la UE pretende garantizar el respeto de los derechos humanos y el medio ambiente a lo largo de toda la cadena de suministro.

2) Inversión responsable: se ha entendido que los Principios Rectores de la ONU también sirven de guía para la inversión responsable. En 2018, un informe del Grupo de Trabajo de las Naciones Unidas sobre empresas y derechos humanos hizo un llamado específico a los inversionistas para que aplicaran la debida diligencia en materia de derechos humanos como parte de su propia responsabilidad bajo los Principios Rectores, exigieran de manera más sistemática a las empresas en las que invierten una debida diligencia efectiva en materia de derechos humanos y coordinaran con otras organizaciones y plataformas para garantizar una alineación e interacción significativa con las empresas. Cada día son más los inversionistas que asumen esta responsabilidad, respaldados por iniciativas como la Alianza de Inversionistas por los Derechos Humanos y los Principios para la Inversión Responsable.

B. PREOCUPACIONES DE PROTECCIÓN DE DATOS/PRIVACIDAD

Una vez tenga una buena comprensión de cómo funciona una tecnología, puede que tenga que evaluar las distintas implicaciones que tiene para la privacidad y la protección de datos. Con este fin, hemos esbozado algunos aspectos generales del tratamiento de datos que puede servirle para identificar cualquier preocupación.

No existen normas de protección de datos reconocidas universalmente, pero los organismos regionales e internacionales han creado códigos, prácticas, decisiones, recomendaciones e instrumentos políticos concertados a nivel internacional. Los instrumentos más importantes son:

- El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (No. 108), 1981, modificado en 2018;
- Directrices de la Organización para la Cooperación y el Desarrollo Económicos sobre la protección de la privacidad y flujos transfronterizos de datos personales (1980), modificadas en 2013.
- Directrices para la regulación de los ficheros computarizados de datos personales (resolución 45/95 y E/CN.4/1990/72 de la Asamblea General).

También existen otros marcos regionales, como el Marco de Privacidad de la APEC - Cooperación Económica Asia-Pacífico. Y algunas leyes de protección de datos tienen alcance extraterritorial, por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea aplica a los responsables y encargados del tratamiento que no tienen su sede en la UE, siempre y cuando estén tratando los datos de personas que se encuentran en la UE, y ese tratamiento esté relacionado con la oferta de bienes o servicios en la UE, o equivalga a monitorear su comportamiento.

Cuando existe una ley de protección de datos de carácter integral, las organizaciones (públicas o privadas) que recogen y utilizan datos personales tienen la obligación de tratar estos datos de acuerdo con dicha ley. Por consiguiente, es preciso consultar las normas de su propia jurisdicción, pero esta sección le ofrece una visión general de los distintos aspectos a los que debe prestar atención. Sin embargo, esta no es una lista exhaustiva de todas las posibles preocupaciones de protección de datos. Para una orientación más completa sobre la protección de datos, puede consultar nuestra guía.

i. Fuentes de los datos

El primer paso para evaluar el tratamiento de datos que hace una tecnología es entender dónde se recogen los datos, es decir, de dónde provienen. Es posible que ya

haya identificado esto en la etapa de evaluación del sistema de recolección/captura de datos de la tecnología (véase la investigación tecnológica anterior), pero puede complementar este análisis con cualquier documentación sobre la tecnología o la asociación (por ejemplo, contratos, memorandos de entendimiento, evaluaciones de impacto sobre la protección de datos, acuerdos de tratamiento de datos...), y tener en cuenta cualquier:

- Conjuntos de datos/bases de datos que alimentarán la tecnología
- Listas o categorías de titulares de datos cuyos datos serán tratados (por ejemplo, miembros generales del público, sospechosos, víctimas o testigos de delitos, personas que viven en el área X…)
- Fuentes de datos (por ejemplo, ¿los datos provendrán de bases de datos existentes o de organismos gubernamentales o autoridades particulares?)

Una vez que comprenda de dónde provienen los datos, debe evaluar si la recolección o el intercambio de datos es lícito (es decir, si lo autoriza algún fundamento legal, como el consentimiento del interesado, o una obligación legal de compartir estos datos), y si este fundamento legal se establece explícitamente en la documentación. La licitud de la recolección de datos dependerá de la jurisdicción a la que esté sujeta la asociación o la tecnología.

ii. Licitud y lealtad

El tratamiento de los datos personales debe ser lícito, leal y transparente. Este principio es clave para abordar prácticas como la venta y/o transferencia de datos personales que fueron obtenidos de forma negligente o fraudulenta.

Licitud significa que los datos deben tratarse de una manera que satisfaga un fundamento legal para el tratamiento. Debe evaluar la licitud del tratamiento para cada tipo o categoría de datos que vaya a tratar la tecnología, y para cada finalidad del tratamiento. Por ejemplo, si se van a tratar datos de una base de datos de rostros de la ciudadanía en general para cotejarlos con una base de datos de fotografías policiales, se debe evaluar (1) si cada base de datos fue compilada con base en un fundamento

legal para el tratamiento de datos (tenga en cuenta que esto requiere no solo corroborar que la autoridad pública tiene fundamentos legales para recolectar los rostros en primer lugar (como se abordó en la sección anterior) y construir la base de datos, sino también corroborar que si las bases de datos fueron compiladas por una empresa privada, la misma también tiene fundamentos legales para recolectar los datos en primer lugar), y (2) si el proceso de cotejar se basa en un fundamento legal para el tratamiento.

Los fundamentos para el tratamiento más comunes en la legislación sobre protección de datos son:

- **Consentimiento** del interesado
- Necesidad de tratar los datos para ejecutar un **contrato** con el interesado o para realizar gestiones para celebrar un contrato
- Necesidad de tratar los datos para cumplir una **obligación legal**
- Necesidad de tratar los datos para proteger los **intereses vitales** de un interesado u otra persona
- Necesidad de tratar los datos para desempeñar una **función** de interés público o en el **ejercicio de la autoridad pública** conferida al responsable del tratamiento
- Necesidad de tratar los datos por causa de **intereses legítimos** del responsable del tratamiento o de un tercero, salvo que prevalezcan sobre dichos intereses los intereses, derechos o libertades del interesado

Encontrará más información sobre los fundamentos que justifican el tratamiento de datos en esta sección de nuestra Guía sobre la protección de datos sobre los Fundamentos para el tratamiento de datos personales.

La **lealtad** exige que los datos no se utilicen de maneras que los interesados no esperarían razonablemente, ni de maneras que tuvieran "efectos adversos injustificados sobre ellos".

Se trata de un principio amplio que debe regir todos los aspectos del tratamiento: la recolección de los datos, la finalidad del tratamiento y las consecuencias del mismo. Para evaluar la lealtad, debe valorar si la autoridad responsable del tratamiento ha tenido en cuenta las expectativas razonables de los interesados a la luz del contexto y la finalidad del tratamiento, los riesgos para sus derechos y libertades fundamentales y la relación general entre el responsable del tratamiento y los interesados (por ejemplo, si existe algún vínculo o relación entre ambos que haga que los interesados esperen que se lleve a cabo dicho tratamiento).

iii. Transparencia y derecho a ser informado

Que el tratamiento sea leal dependerá también en gran medida de si se ofrece a los interesados suficiente **transparencia** sobre el tratamiento. Debe informarse a las personas cuando se recogen sus datos personales y deben poder obtener información sobre su tratamiento. Al evaluar el despliegue de una tecnología, es preciso que usted determine si los interesados son informados del tratamiento de sus datos y a través de qué mecanismos.

En el momento en que se recogen los datos, y cada vez que vayan a ser tratados con un fin no previsto en el momento de su recolección, los interesados deben recibir como mínimo la siguiente **información** (tanto cuando proporcionaron los datos directamente al responsable del tratamiento, como cuando este los obtuvo de otra fuente):

- Información sobre la identidad del responsable del tratamiento (e información de contacto)
- Los fines del tratamiento
- Lo(s) fundamento(s) legal(es) del tratamiento
- Las categorías de datos personales que se tratarán
- Los receptores de los datos personales
- Si el responsable del tratamiento tiene intención de transferir datos personales a un tercer país y qué garantías se ofrecen para la transferencia
- El periodo durante el cual se almacenarán los datos personales

- Los derechos del interesado (como el derecho de acceso, el derecho de objetar, los derechos de rectificación, bloqueo y eliminación, los derechos relacionados con la elaboración de perfiles y la toma de decisiones automatizadas, el derecho a la portabilidad de los datos)
- El derecho a presentar una reclamación ante la autoridad de control
- La existencia de elaboración de perfiles, incluido el fundamento legal, la importancia y las consecuencias que se prevé tendrá dicho tratamiento para el interesado
- La existencia de la toma de decisiones automatizada y, como mínimo, información significativa sobre la lógica implicada, la importancia y las consecuencias que se prevé tendrá dicho tratamiento para el interesado
- La fuente de los datos personales (si no se obtuvieron del interesado)
- Si suministrar los datos es obligatorio o voluntario
- Las consecuencias de no suministrar los datos
- Si no se ha informado a las personas, debe evaluar si aplica una exención al derecho a ser informado. Por ejemplo, si negar el derecho a ser informado es necesario y proporcional para prevenir o detectar delitos, para salvaguardar la seguridad nacional o con fines sanitarios, sociales o educativos. No obstante, cualquier exención a este derecho debe estar prevista en la ley, y debe estar justificada y sustentada por una evaluación de necesidad y proporcionalidad. Para mayor información sobre exenciones, consulte esta sección de nuestra Guía sobre la protección de datos sobre Disposiciones generales, definiciones y alcance

iv. Almacenamiento de datos y control de acceso

Una vez que esté convencido (¡o quizás no!) de que los datos se tratarán de forma lícita, justa y transparente, debe plantearse dónde y durante cuánto tiempo permanecerán **almacenados**. La primera pregunta que debe plantearse es si los datos se almacenarán en servidores de la autoridad pública, de la empresa o de algún otro tercero (por ejemplo, un encargado del tratamiento de datos). Es posible que ya lo haya identificado en la fase de evaluación del sistema de almacenamiento de datos de la tecnología (véase la sección de investigación tecnológica antes mencionada). Esto

afectará la distribución de responsabilidades para garantizar la seguridad de los datos y gestionar los controles de acceso.

Los datos personales, en reposo y en tránsito, así como la infraestructura empleada para su tratamiento, deben estar protegidos por salvaguardias de seguridad contra riesgos como el acceso, el uso y la divulgación ilícitos o no autorizados, así como la pérdida, la destrucción o los daños. Consulte la sección de tecnología de este manual para más información sobre lo que debe tener en cuenta. Las salvaguardias de seguridad deben ser detalladas en la documentación relacionada con la asociación, con la clara asignación de responsabilidades a la autoridad pública, la empresa y cualquier tercero.

Para evaluar la idoneidad del **control de acceso**, debe considerar qué tipo de acceso tendrá la empresa a los datos. En especial, cuando los datos se almacenan en los servidores de la empresa, debe verificar si la empresa tendrá pleno acceso a los datos o si este se restringirá para que solo la autoridad pública tenga acceso a los datos. Aun así, incluso si los datos se almacenan en los servidores del gobierno o de la autoridad, la empresa puede tener acceso, así que revise la letra menuda. La documentación de la asociación debe prever reglas sobre control de acceso, con excepciones claras y estrictas para, por ejemplo, el acceso de emergencia, el acceso de mantenimiento y otros.

A veces, los contratos permiten que las empresas accedan a los datos para cosas como “mejorar sus servicios”, “realizar análisis sobre el rendimiento de sus productos”, etc. Desconfíe de este tipo de contratos y pregúntese exactamente qué forma tomará el acceso de la empresa y si, de hecho, se estaría beneficiando del acceso a la base de datos de una autoridad pública para desarrollar sus propios servicios y, por consiguiente, sacar provecho de la asociación más allá del valor monetario del contrato.

Para mayor información sobre exenciones, consulte esta sección de nuestra Guía sobre la protección de datos sobre Principios de protección de datos.

v. Transferencias internacionales de datos

Debe evaluar si el almacenamiento de datos, el acceso a los mismos o cualquier otro acuerdo de transferencia implicará que los datos se transfieran a otro país (por ejemplo, si la empresa contratante está ubicada en EE.UU.). El principio básico es que cualquier transferencia de datos personales a un tercer país no debe reducir el nivel de protección de los derechos de privacidad de las personas. Las distintas jurisdicciones tienen diferentes normas que regulan cómo se puede garantizar que una transferencia a un tercer país sea “adecuada” en términos de protección de derechos, pero generalmente debe verificar:

- ¿Su país/jurisdicción ha determinado que el territorio donde se transferirán los datos ofrece una protección “adecuada” a los derechos de las personas (es decir, existe lo que a menudo se denomina una “decisión de sobre el carácter adecuado”)?
- ¿La transferencia en cuestión ha sido revisada y autorizada por una autoridad de control?
- ¿Existe un acuerdo con cláusulas estándar de protección de datos aprobado por una autoridad de control?

Es posible que apliquen excepciones a las restricciones a las transferencias internacionales de datos. Si se supone que procede una excepción, debe estar prevista en la ley y se debe revisar cuidadosamente para que no se interprete de una forma demasiado amplia o susceptible de abuso, y para que la transferencia se ajuste las normas de derechos humanos.

Puede que quiera considerar otras cuestiones en relación con las transferencias internacionales de datos. Por ejemplo, si los datos que se transferirán son muy sensibles o están relacionados con poblaciones altamente vulnerables, incluso si existe una decisión sobre el carácter adecuado u otras salvaguardas, es posible que desee considerar si el país receptor tiene leyes o prácticas que le permitan solicitar los datos y, por consiguiente, si existe el riesgo de que las personas sufran daños si los datos terminan en manos del gobierno del país receptor.

Para más detalles sobre las exenciones, consulte esta sección de nuestra Guía sobre la protección de datos sobre Las obligaciones de los responsables y encargados del tratamiento de datos.

C. RENDICIÓN DE CUENTAS Y CONTROL

Otro aspecto importante al valorar la gobernanza de una asociación público-privada es el análisis de los mecanismos de rendición de cuentas y control existentes, incluidos los mecanismos a través de los cuales se estableció la asociación (por ejemplo, los procesos de contratación pública).

Es preciso verificar que existan ciertos documentos y procesos para que el Estado contratante y la empresa rindan cuentas, que exista un control adecuado y mecanismos de reparación apropiados. Tenga en cuenta que debe considerar todo el ciclo de vida de la asociación. En primer lugar, durante el **proceso de contratación**, ¿se siguieron las normas de contratación locales o internacionales? ¿Son adecuadas estas normas de contratación? ¿Ha existido una transparencia adecuada a lo largo del proceso de contratación?

Las **evaluaciones de riesgo e impacto** sobre los derechos humanos y/o las evaluaciones de impacto sobre la protección de datos/privacidad usualmente se realizan antes de la adjudicación de cualquier contrato. Se deben llevar a cabo con diligencia, siguiendo las plantillas adecuadas que hayan sido aprobadas en su jurisdicción o que, en su defecto, sean reconocidas por la sociedad civil mundial. Un ejemplo sería la guía y caja de herramientas de evaluación de impacto sobre los derechos humanos del Instituto Danés de Derechos Humanos. Una evaluación de impacto apropiada debe (en particular, pero entre otros aspectos) hacer una valoración de la necesidad y la proporcionalidad que considere adecuadamente los riesgos para los derechos de las personas.

Luego debe considerar si existe algún tipo de control independiente, que garantice que la asociación se limite a su propósito declarado, a fin de detectar abusos o daños resultantes y exigir reparación. ¿Dónde y cómo se define y establece?

Cuando se establezca una asociación público-privada, debería designarse un **organismo de control independiente** (por ejemplo, una autoridad de control de la protección de datos, un organismo de supervisión de 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 asociación, (2) auditar periódicamente el despliegue de la tecnología, lo que incluye consultas públicas sobre el impacto de la tecnología 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. Esta instancia de control independiente debe contar con los recursos adecuados (humanos y financieros) para poder desempeñar sus funciones.

Si existen estos documentos y procesos, le ayudarán a determinar si la implantación de la tecnología es legal, necesaria y proporcional al problema que pretende resolver. Si no existen, es importante que intente determinar si la solución es adecuada o si va demasiado lejos o se extralimita: puede, entre otras cosas, escribir a la autoridad pública competente para solicitar que implante estos documentos o procesos.

A continuación, es preciso considerar si la asociación se rige por determinadas normas de **transparencia** o requisitos legales. En caso afirmativo, ¿son adecuados?

A continuación, puede analizar cómo se responsabilizará a los socios participantes de las consecuencias de desplegar la tecnología. La **rendición de cuentas** requiere que las obligaciones, responsabilidades y normas estén definidas, sean adecuadas y se asignen a las partes implicadas. ¿Existen mecanismos adecuados que permitan a terceros examinar e impugnar las consecuencias?

Toda asociación público-privada debe regirse por **políticas** adecuadas que regulen y documenten los diferentes requisitos antes mencionados, como cuáles datos se tratarán, quién tendrá acceso a los datos y en qué condiciones, qué salvaguardias deben existir para mitigar el riesgo que corren las personas, qué organismo independiente se encargará de supervisar el despliegue de la tecnología, etc. Estas

políticas también deben regular el uso de la tecnología por parte de la autoridad pública y definir claramente los límites de su finalidad y su uso, e incluir una lista taxativa de usos autorizados y una lista no taxativa de usos prohibidos. También deben prever **mecanismos de reparación**, definiendo procesos para tramitar las quejas y aplicar las sanciones derivadas de infracciones a las políticas, y asignando responsabilidades y obligaciones de reparación tanto al Estado como a la empresa.

Creemos que las salvaguardias que hemos descrito anteriormente constituyen un marco razonable de protección para hacer cumplir las responsabilidades descritas en los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos, y garantizar que las asociaciones público-privadas de vigilancia no se traduzcan en abusos de los derechos humanos.

Para mayor información sobre las diversas salvaguardias que deben regir las asociaciones público-privadas de vigilancia, consulte las salvaguardias para las APP de Privacy International.

D. LISTA DE CONTROL – GOBERNANZA

Protección de datos y privacidad

- ☐ Una vez que haya evaluado de dónde provienen los datos, ¿ha evaluado si la recolección o el intercambio de datos es lícito?
    - ☐ ¿El fundamento legal figura explícitamente en la documentación de la asociación?
- ☐ ¿Los datos son recolectados de maneras las personas podrían esperar razonablemente?
- ☐ ¿Los responsables del tratamiento han considerado los riesgos para los derechos y libertades fundamentales de las personas cuyos datos se recogerán?
- ☐ ¿Cuáles serán las consecuencias de que los datos de las personas se traten de esta manera?
- ☐ ¿Se informará a las personas cuando sus datos personales estén siendo recolectados?
    - ☐ ¿Mediante qué mecanismos?
    - ☐ ¿Aplica alguna exención en este caso? ¿Está justificada? ¿Se fundamenta en una evaluación de necesidad y proporcionalidad?
- ☐ ¿Las personas pueden obtener información sobre el tratamiento de datos?
    - ☐ ¿A través de qué mecanismos?
- ☐ ¿Durante cuánto tiempo se almacenarán los datos?
- ☐ ¿Quién alojará los datos?
- ☐ ¿Existen salvaguardias adecuadas para proteger los datos en reposo y en tránsito?
    - ☐ ¿Están especificadas en la documentación de la asociación?
    - ☐ ¿Existe una asignación clara de responsabilidades a las partes contratantes?
- ☐ ¿Qué tipo de acceso a los datos tendrán las empresas implicadas?
- ☐ ¿Los datos serán transferidos a otros países?
    - ☐ En caso afirmativo, ¿el nivel de protección de los derechos de las personas en el país al que se transfieren es inferior, superior o igual?

- ¿Su país/jurisdicción ha determinado que el territorio donde se transferirán los datos ofrece una protección “adecuada” a los derechos de las personas (es decir, existe lo que a menudo se denomina una “decisión de sobre el carácter adecuado”)?
- ¿La transferencia en cuestión ha sido revisada y autorizada por una autoridad de control?
- ¿Existe un acuerdo con cláusulas estándar de protección de datos aprobado por una autoridad de control?
- En caso negativo, ¿el contrato invoca una exención? ¿La exención está prevista en la ley? ¿La transferencia cumple las normas de derechos humanos?

Rendición de cuentas y control

- ¿El proceso de adjudicación del contrato se ajusta a un marco de contratación adecuado?
- ¿El contrato con la empresa se ajusta a las normas nacionales e internacionales?
- ¿La solución tecnológica es necesaria y una respuesta proporcional al problema que busca resolver?
- ¿Las empresas que participan en el contrato han adoptado un compromiso político explícito y público de cumplir su obligación de respetar los derechos humanos?
- ¿Las partes han realizado evaluaciones de riesgos en las que examinan las repercusiones reales y potenciales sobre los derechos humanos de las herramientas y servicios propuestos (diligencia debida en materia de derechos humanos y evaluaciones de impacto) antes de la adjudicación del contrato, y las mantienen actualizadas durante el despliegue?
- ¿La documentación de la asociación contempla algún tipo de control independiente?
    - ¿Dónde y cómo se define esto?
    - ¿El órgano de control dispone de recursos adecuados para desempeñar su función?

- ¿Existen normas o requisitos legales en materia de transparencia?
    - ¿Estas normas/requisitos son adecuados?
    - ¿Se cumplen estas normas/requisitos?
- ¿Existen mecanismos de rendición de cuentas para la entidad pública involucrado en el contrato?
- ¿Existen mecanismos de rendición de cuentas para el ente privado involucrado en el contrato?
    - ¿El ente privado ha establecido mecanismos internos de rendición de cuentas para la implementación de las políticas de derechos humanos?
    - ¿Existen procedimientos para la reparación?
- ¿Los terceros pueden examinar y objetar a estos mecanismos de rendición de cuentas o a sus consecuencias?
- ¿Cuáles son, si las hay, las políticas que rigen y documentan cualquiera de estos requisitos?
- ¿Incluyen reglas sobre el uso de la tecnología por parte de la autoridad pública, con límites claros para el propósito y el uso de la tecnología?
- ¿Existen mecanismos de reparación en caso de incumplimiento de estas políticas? ¿Incluyen sanciones adecuadas y la aplicación de las mismas?

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org