

Marco de políticas para los intermediarios de Internet y el contenido

Enero de 2025

Resumen ejecutivo

Internet no existiría sin funciones de intermediarios para dirigir el tráfico de Internet a los puntos de conexión y desde los puntos de conexión (incluidos individuos, servidores, proveedores de servicio, entre otros) y sin las demás diversas funciones de los intermediarios que facilitan el tráfico.

Las funciones de los intermediarios son cruciales para la existencia de Internet. Este documento proporciona un marco para comprender las funciones intermediarias de Internet y desarrollar políticas relativas a la responsabilidad por el contenido en línea sin perjudicar la capacidad de las personas de utilizar Internet para crear contenido y comunicarse entre sí.

Nos enfocamos en las funciones que llevan a cabo los intermediarios de Internet para facilitar la comunicación en línea, tal como transmitir, enrutar, almacenar, guardar en caché, alojar, proteger, seleccionar y moderar contenido. Este enfoque reconoce que muchos intermediarios desempeñan funciones múltiples que plantean diferentes asuntos de políticas y que muchos tipos de intermediarios ofrecen funciones fundamentalmente equivalentes, aunque sus servicios puedan parecer bastante diferentes.

Nuestro objetivo con este documento es ayudar a los formuladores de políticas a comprender dichas funciones y a desarrollar políticas relativas a ellas. Las políticas bien diseñadas pueden mejorar la disponibilidad, la diversidad, la seguridad y la privacidad de la participación individual en línea. No obstante, las políticas que no están bien elaboradas pueden debilitar la seguridad de Internet, perjudicar la competencia, restringir la comunicación en línea, ampliar la brecha digital y fragmentar Internet.

El objetivo no es eximir de responsabilidad a los intermediarios sino recalcar el rol fundamental de las protecciones de responsabilidad para habilitar la participación individual en Internet. Las políticas mal diseñadas y centradas en los intermediarios pueden tener efectos perjudiciales en Internet y en la comunicación. A menudo, suele haber mejores alternativas disponibles, tales como legislación existente en materia de privacidad, protección del consumidor y discriminación.

En este documento, analizamos el **desarrollo de las protecciones de responsabilidad de los intermediarios** y la motivación detrás de ellas, a partir de la Sección 230 de EE. UU, el Marco Civil de Internet de Brasil y

la Directiva sobre el Comercio Electrónico y la Ley de Servicios Digitales de la UE. Explicamos por qué estas y otras leyes semejantes han sido cruciales para el crecimiento de Internet y la capacidad de los individuos de participar en línea.

Asimismo, destacamos **algunas tendencias en la formulación de políticas orientadas a los intermediarios**, por ejemplo, los regímenes de notificación y eliminación, moderación del contenido subido y requisitos específicos por edad. Observamos que estos enfoques corren el riesgo de dañar Internet al socavar su funcionamiento técnico y su fiabilidad, debilitar la seguridad y la privacidad, reducir la competencia, bloquear excesivamente contenidos legales y excluir a los usuarios de participar en Internet.

Ofrecemos varios principios importantes para la formulación de políticas:

1. **Realizar una evaluación del impacto de Internet** para comprender si una política propuesta, relacionada con las funciones de los intermediarios o con una concepción más amplia, puede tener un efecto adverso en Internet y sus operaciones.
2. **Determinar cuidadosamente el alcance de cualquier política propuesta** según la función intermediaria específica que le está causando el daño. Prestar atención a los daños secundarios potenciales. Evitar afectar un conjunto de funciones y entidades excesivamente amplia.
3. **Proteger las funciones intermediarias de la responsabilidad por el contenido creado por otros**, incluido el “contenido generado por el usuario”. Las entidades que proporcionan funciones intermediarias deben estar protegidas de la responsabilidad por el contenido creado por otros que lo transmiten, reciben, alojan, muestran, filtran o manejan de otra manera. Esto garantiza que los usuarios puedan seguir hablando y compartiendo contenido en línea.
4. **Proteger las funciones intermediarias de selección y moderación del contenido generado por el usuario**. Las entidades que alojan contenido generado por el usuario tienen el derecho legítimo de definir las reglas de sus servicios y deben tener protecciones contra la responsabilidad al imponer sus propias normas y eliminar contenido objetable.
5. **Para abordar las preocupaciones sobre el contenido en línea, los formuladores de políticas pueden utilizar leyes existentes o nuevas** centradas en la privacidad y la seguridad, la no discriminación, la accesibilidad, los derechos humanos, la competencia, la elección y el control del usuario, la transparencia y la apertura, entre otros.

Incluimos varios **“Aspectos destacados”** sobre consideraciones de políticas para sectores en línea específicos, incluidos los medios sociales, las redes federadas, los juegos en línea, la realidad aumentada/realidad virtual, la publicidad, así como los modelos comerciales de pago por contenido, la gestión de la libertad de expresión, los derechos de autor y la inteligencia artificial (IA).

El **Anexo** al final de este documento analiza la amplia gama de **funciones de los intermediarios** que permiten o facilitan las comunicaciones por Internet. Proporciona una amplia **lista** y descripción de las funciones intermediarias e incluye consideraciones técnicas y prácticas para la formulación de políticas, así como recomendaciones de políticas para cada función.

Índice

Marco de políticas para los intermediarios de Internet y el contenido	1
Resumen ejecutivo	1
1 Introducción	8
1.1 Desafíos de las políticas en materia de intermediarios	9
1.2 Internet ha transformado las comunicaciones con impactos socioeconómicos positivos contundentes	10
1.3 Internet empodera las comunicaciones individuales activas	11
1.4 El rol de las funciones de los intermediarios en la habilitación de la comunicación en Internet	13
1.5 Comparación entre la responsabilidad del contenido generado por el sitio y el contenido generado por el usuario	15
2 Internet y la responsabilidad de los intermediarios	17
2.1 Los defectos críticos del modelo de comunicaciones de “conmutación de circuitos” del siglo XIX que precedió a Internet	17
2.2 Explicación del Modo Internet de Interconectarse	18
2.3 El rol de las funciones de los intermediarios	20
3 Protecciones de responsabilidad para las funciones de los intermediarios	23
3.1 El desarrollo inicial de las leyes de protección de intermediarios: definición del contexto	23
3.2 Primera legislación en materia de responsabilidad de intermediarios de Internet: Sección 230 de Estados Unidos	25
3.3 Protecciones iniciales de intermediarios de Europa	29
3.4 El Marco Civil de Internet de Brasil	30
3.5 Actualizaciones de protecciones de intermediarios de Europa	32
3.6 Protecciones de intermediarios en otros contextos nacionales e internacionales	33

3.7 Últimas tendencias en responsabilidad de los intermediarios y riesgos para Internet	37
3.8 Diversidad global de los países.....	41
4 Principios para la formulación de políticas para las funciones de los intermediarios de Internet	43
4.1 Principios generales para la formulación de políticas prudentes en materia de Internet	44
4.2 Principios específicos respecto de la protección de la responsabilidad de los intermediarios.....	46
4.3 Principios legales y de políticas específicos que se pueden aplicar a las funciones de los intermediarios sin perjudicar las comunicaciones de Internet.....	48
5 Puntos destacados: consideraciones de políticas para funciones de intermediarios específicas	52
5.1 Punto destacado: consideraciones de políticas para las plataformas de “medios sociales” que alojan, seleccionan y moderan contenido generado por el usuario	52
5.2 Punto destacado: consideraciones de políticas para redes federadas que habilitan nuevos enfoques para facilitar la participación del usuario.....	55
5.3 Punto destacado: consideraciones de políticas para el ecosistema de juegos interactivos en línea.....	57
5.4 Punto destacado: consideraciones de políticas para los sistemas de realidad virtual y realidad aumentada conectados a Internet	58
5.5 Punto destacado: consideraciones de políticas para las funciones de intermediarios que habilitan la publicidad en Internet	59
5.6 Punto destacado: consideraciones de políticas para pagos y otras retribuciones económicas para el contenido generado por el usuario contemplado en los principios de intermediarios de Internet.....	61
5.7 Punto destacado: el impacto de los diversos niveles de protección del derecho de libertad de expresión a escala nacional.....	62
5.8 Punto destacado: diferenciación de la protección de la responsabilidad de intermediarios y la legislación, y políticas de derecho de autor	64

5.9 Punto destacado: inteligencia artificial.....	65
---	----

6 Conclusión	67
---------------------------	-----------

Anexo – Funciones de los intermediarios 69

1 Transmisión de paquetes de datos70

1.1 Medios de comunicación (por cable e inalámbrico)	70
--	----

1.2 Ruta de comunicación del Protocolo de Internet	71
--	----

1.3 Redes troncales y de tránsito	73
---	----

1.4 Intercambio de tráfico	74
----------------------------------	----

1.5 Acceso a Internet de último tramo	76
---	----

2 Enrutamiento y funciones auxiliares que facilitan las comunicaciones a través de Internet.78

2.1 Asignación de direcciones IP.....	79
---------------------------------------	----

2.2 Asignación de números de sistema autónomo	80
---	----

2.3 Registro y administración de DNSt.....	82
--	----

2.4 Publicación de DNS.....	83
-----------------------------	----

2.5 Búsqueda de DNS.....	85
--------------------------	----

2.6 Servicios de DNSSEC	87
-------------------------------	----

2.7 Servicios de certificados TLS.....	88
--	----

3 Servicios de alojamiento y almacenamiento en caché90

3.1 Alojamiento en la red	90
---------------------------------	----

3.2 Alojamiento de correo electrónico.....	91
--	----

3.3 Otros servicios de alojamiento	93
--	----

3.4 Servicios de distribución de contenido y almacenamiento en caché.....	94
---	----

3.5 Distribución de contenido de Interfaz de programación de aplicaciones (API).....	96
--	----

3.6 Selección, moderación y visualización de contenido.....	97
---	----

4 Comunicaciones entre personas.	99
4.1 Comunicaciones de uno a uno.	99
4.2 Comunicaciones de uno a muchos.	101
4.3 Comunicaciones de muchos a muchos.	102
5 Búsqueda	104
5.1 Búsqueda en la web.	104
5.2 Búsqueda integrada	105
5.3 Búsqueda específica	106
5.4 Búsqueda proporcionada por el sitio	107
6 Protección de la ciberseguridad, protección de la privacidad y control del contenido de los usuarios.	109
6.1 Protección del tráfico a escala de red	109
6.2 Herramientas y filtros de contenido controlados por el usuario.	111
6.3 Protección del tráfico centrada en el usuario.	113
7 Aplicaciones, software y su desarrollo y distribución.	115
7.1 Software de sistema operativo	115
7.2 Software de navegación y servicios web	117
7.3 Software de correo electrónico	119
7.4 Software de mensajería	121
7.5 Otros software usados en el envío, la recepción y la visualización de comunicaciones por Internet	122
7.6 Desarrollo y distribución de software/aplicaciones	123
8 Entornos complejos.	126
8.1 Medios sociales	126
8.2 Redes federadas	128
8.3 Entornos de juego	129
8.4 Entornos de realidad virtual y aumentada	131

1 Introducción

Este documento proporciona un marco para comprender las funciones de los intermediarios de Internet y desarrollar políticas relativas a la responsabilidad por el contenido en línea. Las funciones de los intermediarios de Internet facilitan la distribución y la visualización del contenido o las comunicaciones en Internet. Los proveedores de servicios de Internet (ISP), los sitios de medios sociales, los alojamientos web, los servicios de streaming y los servicios de correo electrónico son ejemplos de entidades que prestan funciones de intermediarios. Nuestro objetivo es motivar a los formuladores de políticas a la creación de políticas que preserven lo que consideramos son las características más importantes de Internet: la transparencia, la conexión global, la seguridad y la confianza.

Ofrecemos una descripción general de Internet y de algunas funciones de intermediarios significativas para ayudar a los formuladores de políticas a trabajar en el área de contenido en línea. Analizamos de qué manera las políticas enfocadas en Internet pueden afectar las funciones de los intermediarios y las interacciones de los usuarios, así como también, en algunos casos, perjudicar la seguridad, la confiabilidad y otras características clave deseables de Internet. Por último, ofrecemos recomendaciones específicas para los responsables de políticas que buscan abordar objetivos sociales y políticos a través de políticas que afectan las funciones de intermediación de Internet y las entidades que las proporcionan.¹

¿Qué son las políticas y cómo se implementan?

Las políticas que afectan Internet pueden tener varias formas e incluir obligaciones legales, protecciones legales, regulaciones administrativas, acuerdos internacionales, incentivos impositivos, devoluciones, sistemas de certificaciones, requisitos para adquisiciones e, incluso, decisiones que **impidan** la legislación o regulación.

¹ En los regímenes de protección de responsabilidad de los intermediarios correspondientes a Internet, la atención se centra en las funciones de los intermediarios que respaldan la creación, el descubrimiento, la búsqueda, la selección, la entrega o la visualización de contenido. Esto puede comprender correos electrónicos, tuits y otras publicaciones de individuos, así como texto, audio o videos alojados y mostrados en sitios web y en las principales plataformas en línea. Estos regímenes de responsabilidad generalmente no contemplan otros tipos de entidades que brindan un servicio de “intermediación”, como la transferencia de dinero de una persona a otra. Este documento no aborda este tipo de servicios que no se centran en el contenido

1.1 Desafíos de las políticas en materia de intermediarios

Como se explica a continuación en la Sección 2, es necesaria una amplia gama de funciones de intermediarios para el funcionamiento de Internet. En consecuencia, las políticas que se aplican a las entidades intermediarias de Internet o las funciones que desempeñan también podrían afectar significativamente la capacidad de las personas para crear contenido y comunicarse entre sí.

La influencia de las políticas puede ser positiva y constructiva. Creemos que la mayoría de los formuladores de políticas reconocen el valor de Internet en su trabajo. Las políticas pueden mejorar la manera en que los individuos y las comunidades experimentan Internet, por ejemplo, al fomentar servicios que aseguren los datos y protejan la privacidad de sus usuarios, y pueden aprovechar el poder de Internet para impulsar algo positivo.

No obstante, también es posible que la formulación de políticas tenga consecuencias significativamente negativas: el debilitamiento de la seguridad y la privacidad de Internet, la expulsión de competidores pequeños y el desaliento a nuevos participantes, el impedimento de que los usuarios se comuniquen en línea, la ampliación de la brecha digital y la fragmentación de Internet. Creemos que los formuladores de políticas quieren evitar estas consecuencias negativas y este es el motivo por el cual Internet Society publica este documento.

Para los formuladores de políticas que consideran políticas aplicables a Internet, es esencial considerar los muchos y diversos tipos de funciones intermediarias fundamentales para la comunicación en Internet. Además, es importante recordar que las mismas entidades que ofrecen funciones de intermediarios son extremadamente diversas: desde ISP rurales a pequeñas y grandes empresas de alojamiento web hasta servicios troncales de Internet y sitios enormes de uso compartido de videos y medios sociales. Esta diversidad significa que es crucial que las obligaciones propuestas apunten lo más precisamente posible a la función de intermediario exacta.

Reconocemos que no todo el contenido de Internet es legal y beneficioso para la sociedad y que los países buscan maneras eficaces de limitar la divulgación de información falsa, contenido perjudicial y actividades delictivas en línea. En este sentido, los intermediarios pueden presentar un objetivo político atractivo debido a su amplia interacción con el

contenido generado por los usuarios. No estamos argumentando que las entidades que realizan funciones intermediarias “no puedan” o “no deban” estar sujetas a políticas de alguna manera. Nuestro objetivo es demostrar que las políticas que afectan las funciones intermediarias podrían tener importantes consecuencias no deseadas y ser perjudiciales para Internet o la capacidad de las personas de comunicarse a través de Internet y, por lo tanto, deberían evitarse. También destacamos una gama de herramientas de políticas, tales como leyes de privacidad categóricas, que los gobiernos tienen a disposición para el abordaje de asuntos sociales en línea.

1.2 Internet ha transformado las comunicaciones con impactos socioeconómicos positivos contundentes

Internet ha transformado drásticamente la manera en la que se comunican las personas. Antes de la era de Internet, el teléfono y el correo postal eran las principales herramientas disponibles para la comunicación entre las personas. La comunicación masiva, tal como los diarios, la radio y la televisión, ofrecía a los individuos pocas posibilidades de hablar y participar.

Internet, en marcado contraste con los periódicos, la radio y la televisión, permite a las personas participar en la conversación, en tiempo real y en todo el mundo. En el abanico de opciones habilitadas para Internet, se incluyen comunicaciones de uno a uno (p. ej.,

The Internet Empowers Participation

Al redactar este documento, el objetivo de Internet Society es explicar el motivo por el cual se debe proteger de responsabilidad a las funciones de los intermediarios respecto de la habilitación y facilitación de la comunicación de contenido que genera el usuario. Asimismo, queremos destacar que hay otras herramientas de políticas disponibles para abordar de manera constructiva los asuntos en torno a los servicios en línea y el contenido de sus usuarios. No es nuestra intención aconsejar a los formuladores de políticas sobre cómo se debe regular Internet, pero sí sobre cómo crear políticas que permitan que el resultado más importante de Internet, las comunicaciones individuales, siga prosperando.

“Una característica clave de Internet, la que lo distingue de todos los demás tipos de medios de comunicación, es que su concepción inicial fue que sea abierta para todos. Los individuos pueden hablar, debatir, crear, inventar y participar con otros, ya sea que se encuentren cruzando la ciudad o en cualquier lugar del mundo”. (Testimonio ante el Congreso de Andrew Sullivan, director ejecutivo de Internet Society, 8 de marzo de 2023)

aplicaciones de mensajería cifrada), comunicaciones de uno a muchos (p. ej., publicación de un sitio web) y comunicación de muchos a muchos (p. ej., plataformas de medios sociales). Durante los primeros años, Internet admitía comunicaciones a través de tableros de anuncios, listas de correo, grupos de discusión, blogs y un sinnúmero de otras formas de participación de usuarios.

La capacidad de los individuos de utilizar Internet para comunicarse, enviar y recibir información de otras personas al otro lado de la ciudad o de todo el mundo, también trae consigo beneficios directos, beneficios que recaen sobre esos individuos, sus comunidades y sus países. Las personas usan Internet para generar oportunidades socioeconómicas nuevas para sí mismos y para los demás. Los emprendedores pueden desarrollar productos y servicios que atiendan las necesidades de sus comunidades. Los gobiernos pueden interactuar con sus ciudadanos de manera mucho más categórica, rápida y económica. Las comunicaciones facilitadas por Internet mejoran el conocimiento global y las oportunidades económicas. Más allá de estos beneficios, Internet ha generado de manera evidente oportunidades económicas para las naciones, las empresas, las organizaciones y las personas de todo el mundo.²

1.3 Internet empodera las comunicaciones individuales activas

Con Internet, los individuos ya no son receptores pasivos del contenido en gran medida generado de forma corporativa o autorizado por los gobiernos. Las personas participan de manera activa en la creación de contenido y en la determinación de cómo ese contenido puede ponerse a disposición de personas de todo el mundo. En este documento, usamos el término **“contenido generado por el usuario”** para referirnos a todo lo que un usuario publica o comparte en línea a diferencia del propietario de un sitio.

El concepto de **contenido generado por el usuario**, a menudo, surge en casos jurídicos y debates de políticas por sobre quién debe ser legalmente responsable de dicho contenido. El **contenido generado por el usuario** puede ser un trabajo original creado por el usuario que lo publica en Internet, o puede haber sido creado por otra persona y publicado, con o sin el permiso del creador original.

2 Como se señala en el informe de la OCDE de 2010 sobre El papel económico y social de los intermediarios de Internet, el crecimiento de las entidades que brindan funciones de intermediarios de Internet contribuyó al crecimiento económico y la productividad, la inversión en infraestructura, el aumento del empleo y de emprendedores, la innovación, el empoderamiento, la confianza y la privacidad de los usuarios. Consulte <https://doi.org/10.1787/5kmh79zsz8vb-en>.

La característica definitoria clave del **contenido generado por el usuario** es que fue creado o publicado en un sitio o compartido en línea por alguien que no es el propietario de un sitio o servicio. Se distingue del **“contenido original del sitio”**, es decir, el contenido creado por los empleados, los contratistas y los servicios de desarrollo de contenido del propietario del sitio, sobre el cual el propietario tiene la responsabilidad legal evidente.

El espectro que contempla el contenido generado por el usuario es amplio. Podría ser contenido publicado por individuos, pero también podría ser publicado por una organización o corporación. Existe una variedad ilimitada de tipos de **contenido generado por el usuario**: publicaciones en medios sociales, correos electrónicos, mensajes, videos cortos o largos, revisiones de productos, poesía, música o datos de observación por científicos ciudadanos. **El contenido generado por el usuario** puede ser serio, tonto, artístico, objetivamente correcto, objetivamente incorrecto, inteligente, ofensivo, acosador, profundo, útil, inútil, todo lo que rodea el vasto abanico de ideas y expresiones humanas. No obstante, por supuesto que algunos contenidos pueden ser dañinos, difamatorios, engañosos, amenazantes o, incluso, ilegales.

El contenido original del sitio en comparación con el contenido generado por el usuario

Si un fabricante de automóviles decide crear un sitio web básico para mostrar modelos de automóviles nuevos que están disponibles para la compra, el contenido de ese sitio sería creado por el fabricante y sus empleados y contratistas. Tal como el fabricante de automóviles es responsable del contenido de un folleto o de otro documento impreso, también es responsable del contenido que publica en línea. A este contenido lo llamamos **contenido original del sitio**. En general, el fabricante debería tener responsabilidad evidente y potencial responsabilidad legal por el contenido que creó y puso a disposición en línea.

Si el fabricante de automóviles elige agregar funciones interactivas al sitio web y permite que los visitantes particulares publiquen comentarios acerca de los modelos de automóviles, dichos comentarios deberían considerarse contenido generado por el usuario. El sitio web tendría una combinación de contenido original del sitio, en su mayoría, y **contenido generado por el usuario**, en menor medida.

Por el contrario, un sitio web de medios sociales típicos para los entusiastas de los automóviles, quizá, incluiría principalmente **contenido generado por el usuario**: los visitantes particulares del sitio publican contenido corto y largo, y tienen discusiones con otros visitantes. Es posible que haya algo de **contenido original del sitio** creado por los propietarios del sitio web, por ejemplo, información de asistencia y los términos de uso.

La cuestión de la responsabilidad y la obligación de las entidades que proporcionan funciones intermediarias que ayudan a facilitar la comunicación de **contenido generado por el usuario** es un tema central que se analiza en este documento.

1.4 El rol de las funciones de los intermediarios en la habilitación de la comunicación en Internet

Internet no existiría sin las entidades que prestan funciones de intermediarios. Su arquitectura fundamental descentralizada y distribuida, la cual es esencial para posibilitar los beneficios socioeconómicos de Internet, depende de cientos de miles de entidades que ofrecen funciones de intermediarios.

Las funciones de los intermediarios de Internet incluyen distribuir, proteger, alojar y facilitar las comunicaciones de Internet. Para comprender mejor las funciones de los intermediarios en Internet, puede ser útil una comparación con los servicios postales: los servicios postales usan distintos intermediarios para entregar el correo: transportistas que recogen y entregan el correo, camiones y aviones para transportarlo, guardias de seguridad para protegerlo, buzones para almacenarlo, oficinas postales para administrar todo, entre otros. Todas estas entidades son agentes del servicio postal.

Internet tiene entidades intermediarias que llevan a cabo servicios y funciones análogos, pero con una diferencia clave: las funciones de los intermediarios de Internet son realizadas por entidades independientes y no existe una oficina central coordinadora que controle la entrega de las comunicaciones. Los servicios postales controlan cómo se entregan los correos desde el punto en que se reciben; en Internet, no hay una sola entidad que controle la forma en que se entrega el contenido o quién es responsable de cada etapa del proceso. Además, a diferencia del servicio

postal, el contenido de Internet casi siempre se divide en partes que se transmiten por separado y pueden viajar a través de redes independientes distintas. Por otro lado, a diferencia del servicio postal, muchas páginas o sitios web están conformados por componentes dinámicos creados y alojados por diferentes entidades. Los protocolos técnicos de Internet abiertos e interoperables son los que permiten que una inmensa diversidad de comunicaciones, incluidas las páginas web compuestas dinámicamente, fluyan sin un controlador central.

Pero, en ambos casos, el servicio postal y sus agentes, así como los diversos intermediarios involucrados en las comunicaciones de Internet, están comunicando contenido generado por el usuario. Sin embargo, las funciones de los intermediarios son diferentes.

En este documento, hemos elegido centrarnos en las “funciones” de los intermediarios (tales como “ofrecer acceso a Internet”) en lugar de enfocarnos en los tipos de entidades (tales como “Proveedor de servicios de Internet” o sitio de “medios sociales”). Creemos que este enfoque ofrece más rigor y precisión cuando definimos la política porque muchas entidades desempeñan diferentes funciones de intermediarios y esas funciones diferentes plantean diferentes asuntos de políticas.

Por ejemplo, un proveedor de servicio de Internet (ISP), además de proporcionar acceso a Internet a los hogares, puede prestar funciones de intermediarios adicionales, tales como telefonía de voz sobre IP, búsqueda de DNS, alojamiento de correo electrónico y filtrado de contenido o malware. Una plataforma de medios sociales, además de dar a sus miembros la posibilidad de publicar contenido y reaccionar a este, puede realizar otras funciones de intermediarios, por ejemplo, mensajería de uno a uno, alojamiento de sitios web y conferencias de audio y video en vivo. Asimismo, algunos servicios en línea pueden incorporar las mismas funciones de intermediarios o funciones equivalentes. La introducción de políticas o reglas, por ejemplo, respecto del uso de contenido incrustado en sitios de medios sociales puede afectar inadvertidamente el uso que todos hacen del contenido incrustado en Internet.

Nuestro enfoque es en las funciones de los intermediarios de Internet que, de alguna manera, participan en la muestra, la selección o la distribución del *contenido creado por otros*, es decir, contenido generado por el usuario.

1.5 Comparación entre la responsabilidad del contenido generado por el sitio y el contenido generado por el usuario

Un punto de partida de comparación es que alguien que crea contenido en línea es responsable de tal contenido, y no es un intermediario de ese contenido. No obstante, si transmite, muestra, aloja o, de algún modo, facilita contenido creado *por otros*, sería considerado un intermediario y, en general, no sería responsable legal de ese contenido.

Para algunas entidades, *todo* contenido que se encuentre en sus sitios web o en sus servicios es contenido creado “por otros”. Los sitios web de otras entidades pueden contener una combinación de contenido creado “por otros” (que, como tal, merece las protecciones de responsabilidad de los intermediarios) y contenido creado por las propias entidades (que, por ende, no tiene protección de responsabilidad). Tres ejemplos pueden ayudar a ilustrar la distinción:

- Para un proveedor de servicio de Internet residencial, *todo* contenido transmitido a esa casa o desde esa vivienda es creado por una entidad que no es el ISP. El ISP no crea contenido; solo es responsable de su tráfico. El ISP típicamente solo ofrece funciones de intermediario para el contenido que maneja entre el usuario final y el resto de Internet. Desde el punto de vista de la responsabilidad, el ISP no es responsable del contenido que transporta.
- En el caso de un fabricante de automóviles con un sitio web que describe sus productos, pero que *también* permite a los usuarios publicar reseñas o comentarios sobre el contenido, la empresa es responsable de la mayor parte del contenido del sitio web y no se la considera como una función intermediaria para ese contenido en particular. No obstante, la compañía **proporciona una función de intermediario** respecto de los comentarios de los clientes publicados en su sitio web. Esto se debe a que dichos comentarios fueron creados por alguien que no es de la compañía. El fabricante de automóviles es responsable legal del contenido que crea y publica, pero el contenido publicado por otras personas exige un enfoque diferente en cuanto a la responsabilidad.
- Para la compañía de alojamiento web independiente que administra los servidores y la infraestructura usada por el fabricante de automóviles, la función que cumple es meramente de intermediario: *todo* el contenido del sitio web (el de la compañía

automotriz junto con los comentarios de los clientes) representa contenido generado por el usuario. Tal como sucede con el ISP, la compañía de alojamiento web no debe ser responsable del contenido publicado por otros en los sitios web que esta aloja.

Importancia de las funciones intermediarias para la capacidad de los individuos de utilizar Internet y compartir contenidos

A nivel de vecindario, las personas dependen de intermediarios (es decir, proveedores de servicios de Internet y redes comunitarias) para conectarse a Internet. Cuando ya hay conexión, *toda* comunicación por Internet requiere de la participación de numerosas entidades independientes que brinden las funciones de intermediarios: transportar, alojar, proteger y entregar miles de millones de comunicaciones diarias.

Todos usan Internet por diferentes motivos, pero todo uso exige que las personas, a menudo sin saberlo, accedan y dependan de decenas, cientos o más entidades que proporcionen funciones de intermediarios en cada momento en que se encuentran en línea. Esta dependencia en las funciones de intermediarios es fundamental para el funcionamiento diario de Internet. Por esto, la política que afecta las funciones de los intermediarios debe elaborarse muy minuciosamente de modo de no tener un impacto negativo en el funcionamiento de Internet.

2 Internet y la responsabilidad de los intermediarios

Esta sección revisa brevemente algunos aspectos técnicos de Internet y menciona algunas de sus características importantes, parte de lo cual denominamos “El Modo Internet de Interconectarse”. Además, describimos el rol fundamental que tienen las funciones y de las entidades de intermediarios en todas las comunicaciones de Internet.

2.1 Los defectos críticos del modelo de comunicaciones de “conmutación de circuitos” del siglo XIX que precedió a Internet

Antes de Internet, el sistema de comunicación de persona a persona principal era el sistema telefónico por “conmutación de circuitos”, en el que se usaban conmutadores para crear un circuito eléctrico dedicado entre el originador de una llamada telefónica y el receptor de esta. Hace sesenta años, para realizar una llamada desde la ciudad de Nueva York hasta Johannesburgo, la operadora telefónica estadounidense unía un cable local para formar un circuito que se conectara a un cable submarino hasta la operadora telefónica sudafricana. A su vez, en el otro extremo, la compañía sudafricana construía un circuito para transportar las voces a través del océano. Después de la llamada, el circuito se desarmaba y los recursos usados para la llamada quedaban disponibles para transportar otra llamada. Durante casi todo el siglo XX, la mayoría de las llamadas telefónicas dentro de un país se realizaban mediante una única compañía telefónica monopólica que controlaba la red, cobraba las llamadas y era la responsable de llevar a cabo el mantenimiento y la ampliación de la red. En algunos países, las compañías eran propiedad del gobierno o administradas de forma estatal.

El enfoque de conmutación de circuitos de la telefonía tradicional es extremadamente ineficaz. La reserva de recursos necesaria para realizar

una llamada telefónica significaba que un hogar o una comunidad con una sola línea telefónica podía tener una única conversación en algún momento y, quizá, debía esperar hasta que las líneas de los destinatarios estuvieran disponibles. La red tenía que ser sobredimensionada para manejar las cargas pico y los costos eran muy elevados. A menudo, la capacidad en las horas pico era insuficiente, por ejemplo, durante las vísperas de Navidad y de Año Nuevo. El uso de un circuito dedicado para una sola llamada telefónica no era eficaz en sí, porque los cables podían transportar más contenido que una única llamada. La ineficacia técnica y económica de la telefonía tradicional fue un impulso esencial en el desarrollo de redes de “conmutación de paquetes”, la base de lo que es Internet en la actualidad.

La telefonía por conmutación de circuitos presentaba otros riesgos y costos. Una red vertical con control centralizado es vulnerable a interrupciones originadas por fallas de centros de comando claves o partes de la red.³ La compañía telefónica nacional monopólica, sin incentivo para incorporar productos y servicios nuevos en el mercado, solía omitir la innovación de los servicios al consumidor con regulaciones onerosas y costos inalcanzables. Es posible que, si hubiera existido más competencia en la telefonía por conmutación de circuito, hubiera habido más innovación. Sin embargo, la centralización intrínseca de la conmutación por circuito significó que, en algún punto, cada red estuviera controlada exclusivamente por una entidad, la cual tenía poco incentivo para invertir en servicios nuevos.

Estos y otros inconvenientes llevaron a los investigadores de las décadas de 1960 y 1970 a desarrollar y perfeccionar la “conmutación de paquetes” y, en última instancia, a desarrollar lo que se convirtió en Internet.

2.2 Explicación del Modo Internet de Interconectarse

Internet, a menudo llamada “red de redes”, es una red conectada conformada por redes que han elegido conectarse entre sí. Los primeros diseñadores de Internet reconocieron los beneficios de un diseño flexible para permitir el surgimiento de las nuevas tecnologías y la conexión de nuevas redes. Además, reconocieron que la mejor manera de implementar una red muy grande y distribuida era aprovechar las redes existentes mediante la conexión de estas con tecnología simple, de bajo costo y comúnmente disponible.

3 Internet, en comparación, está extremadamente distribuida, lo que mejora su confiabilidad, robustez y capacidad para esquivar los problemas de la red.

A diferencia de la telefonía por conmutación de circuitos, las comunicaciones de Internet fluyen por esta red de redes mediante el uso de la conmutación de paquetes:⁴ cada comunicación se divide en “paquetes” pequeños y cada paquete viaja de forma independiente. Por ejemplo, cada correo electrónico se divide en varios paquetes más pequeños, que pueden tomar, y a menudo lo hacen, diferentes rutas a través de Internet para llegar al destinatario previsto. A medida que llegan, al destino, se vuelven a unir sin inconvenientes antes de entregar el correo electrónico al usuario final. Esto significó una innovación importante en la manera en que se comunicaba el contenido a través de las redes.

A Internet la conforman casi 76.000 redes independientes que utilizan los mismos protocolos técnicos y eligen funcionar entre sí. Si bien muchas de estas redes son de propiedad privada, algunas son de propiedad y control gubernamental. Cada red toma decisiones independientes sobre cómo dirigir el tráfico hacia sus vecinos en función de sus propias necesidades, el modelo de negocio y los requisitos locales. Además, existen cientos de miles de otras entidades, tales como proveedores de alojamiento web, servicios de correo electrónico, servicios de dominio, servicios de identidad y proveedores de seguridad, que prestan servicios fundamentales para sostener y facilitar las comunicaciones a través de Internet. No hay un control o una coordinación centralizada de las redes o de las entidades de apoyo.⁵

Este diseño distribuido y descentralizado es fundamental para el éxito de Internet. Internet se ha extendido en todo el mundo y se ha desarrollado de tal manera gracias a este principio de diseño esencial. A medida que surjan nuevas necesidades, áreas de funcionamiento o invenciones, se pueden sumar nuevas redes a Internet de forma simple y económica. En particular, este diseño permitió que hasta redes pequeñas o remotas se conecten a Internet a un costo relativamente modesto, en general, sin negociaciones o acuerdos mediante, aparte de los proveedores de servicios locales.

Internet es totalmente diferente de las redes de comunicaciones por conmutación de circuito usadas en el pasado; estas diferencias en el funcionamiento distribuido y el diseño descentralizado son fundamentales para el buen estado y el crecimiento continuos de Internet.

4 Si desea obtener una descripción de conmutación de paquetes, consulte <https://www.internetsociety.org/blog/2022/04/common-internet-network-interconnection-and-charging-practices/>; además, vea https://en.wikipedia.org/wiki/Packet_switching.

5 En un documento de Internet Society, “El Modo Internet de Interconectarse: definición de las propiedades esenciales de Internet”, Internet Society, 9 de septiembre de 2020, <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>, se identifican las propiedades fundamentales que hacen de Internet “La Internet” y se sustentan el crecimiento y la adaptabilidad de Internet. Este documento forma parte de un esfuerzo más grande denominado El Modo Internet de Interconectarse; hay recursos adicionales en <https://www.internetsociety.org/action-plan/internet-way-of-networking/>.

2.3 El rol de las funciones de los intermediarios

Las entidades que brindan funciones de intermediarios tienen un papel fundamental no solo en dar conectividad global y uso compartido de contenido, sino en proveer seguridad, protección, privacidad y accesibilidad. Internet depende de diversas funciones de intermediarios para funcionar.

Lo que sostiene a la Internet moderna es una amplia diversidad de funciones de intermediarios. Algunas pueden sonar conocidas para los usuarios y los formuladores de políticas, como las funciones que prestan los ISP, los “proveedores de tráfico” que conectan a otras redes entre sí, los servicios de alojamiento que apoyan el servicio de contenido web y de correo electrónico, de motores de búsqueda y de medios sociales. Otros tipos de funciones de intermediarios pueden ser menos conocidas. Estas incluyen: almacenamiento de contenido en caché, red y ciberdefensa, resolución de “sistema de nombre de dominio” (DNS) y registro de dominio.⁶ Incluso, algunos tipos de software, tales como los navegadores web, ofrecen funciones de intermediarios, ya que reciben contenido de Internet y lo muestran a un usuario final (a menudo, con bloqueo de seguridad de sitios web maliciosos).

Internet no existiría sin las funciones de intermediarios para dirigir el tráfico de Internet a los puntos de conexión y desde los puntos de conexión (incluidos individuos, servidores, proveedores de servicio, entre otros) y sin las demás diversas funciones de intermediarios que facilitan el tráfico.

Los usuarios pueden optar por interactuar directamente con algunos proveedores de funciones de intermediarios, como su proveedor de servicio de Internet para acceder a Internet, su herramienta de búsqueda preferida y su navegador para mostrar y, a veces, filtrar contenido. El tener una variedad de opciones a disposición permite que el usuario tenga más posibilidades de elegir y controlar. Por ejemplo, los usuarios pueden elegir usar funciones de intermediarios que se centren en la protección de privacidad o que ofrezcan experiencias en línea para la familia.

Sin embargo, la mayoría de los usuarios no conocen o incluso no comprenden la enorme gama de funciones de intermediarios que facilitan

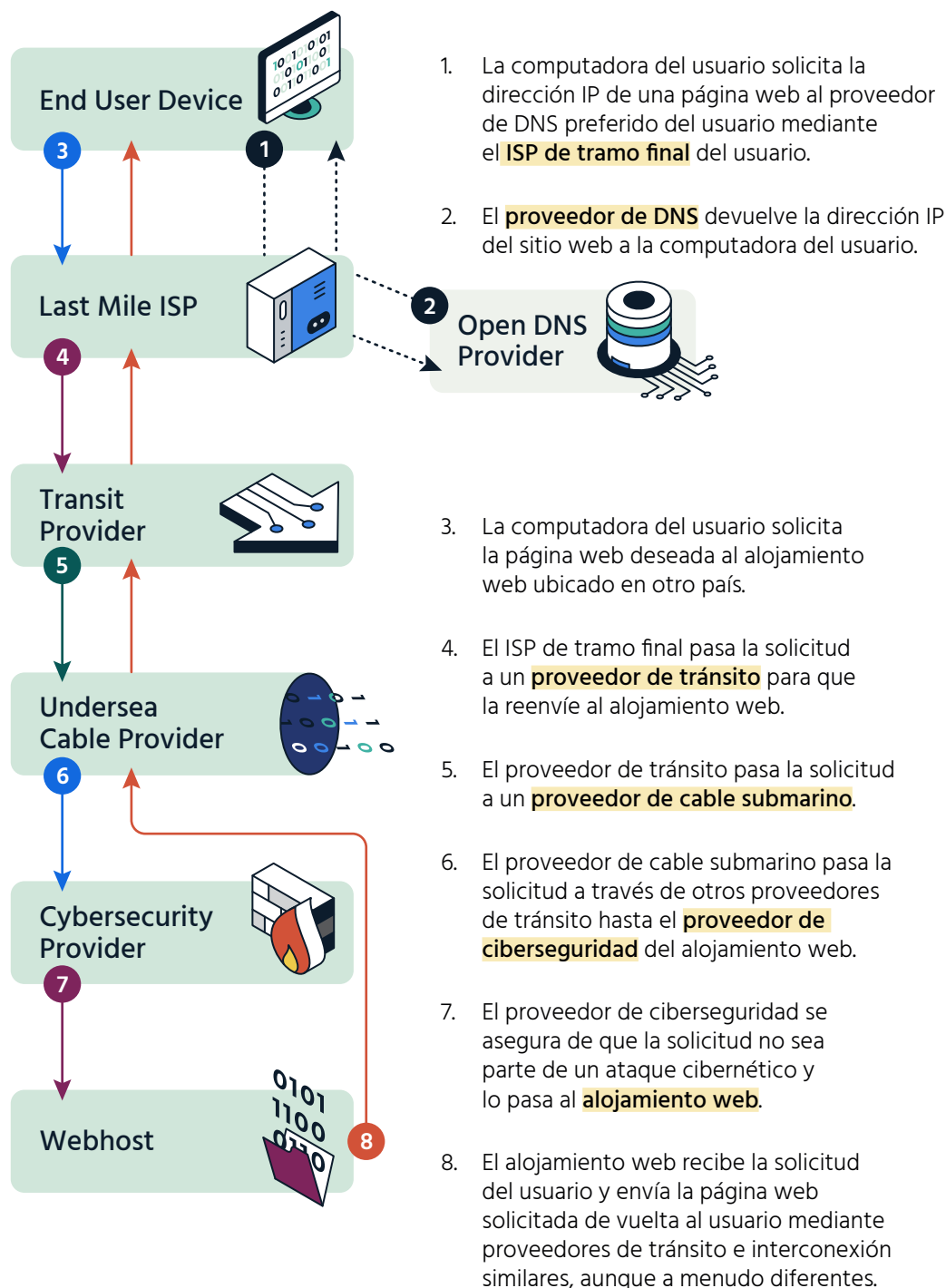
⁶ En el Anexo de este documento, se ofrece una lista más larga de intermediarios, que abarca docenas de tipos, junto con recomendaciones específicas para los formuladores de políticas y consejos sobre los peligros que se deben tener en cuenta para cada tipo de intermediario.

su comunicación. Por ejemplo, los usuarios posiblemente no sepan acerca de la búsqueda de DNS o quién provee esta función para sus búsquedas web, o quién y qué facilita el tráfico de sus paquetes cuando dejan el ISP local. Además, es posible que muchas de las entidades que ofrecen funciones de intermediarios no tengan relación (ni legal ni de ningún otro tipo) con el usuario que inicia la comunicación, el destinatario, ni entre ellos. Si bien muchas entidades son comerciales, algunas funciones de intermediarios de Internet son proporcionadas por comunidades sin fines de lucro o voluntarias. Las entidades pueden tener distintas jurisdicciones de remitente y destinatario. Este enfoque descentralizado y distribuido es “una característica y no un error”. Sería imposible tener relaciones directas de uno a uno para todas las funciones de intermediarios a escala de Internet. El enfoque distribuido de Internet ofrece flexibilidad, resiliencia y la posibilidad de ampliarse y reducirse según sea necesario.

Por lo general, las entidades que permiten el funcionamiento de Internet y ayudan a los usuarios a acceder a la red (a veces, se denominan de forma imprecisa “intermediarios de infraestructura”) no conocen el contenido específico que se comunica. Por el contrario, las entidades que ayudan a los usuarios a interactuar con contenido en Internet (p. ej., una plataforma de uso compartido de videos o de medios sociales) suelen estar implicadas en la manera en la que el contenido se muestra, se selecciona, se comparte, etc. Sin embargo, no siempre hay una línea clara entre estas entidades y no todas las “plataformas” conocen el contenido que se distribuye a los usuarios

Proveedores de funciones intermediarias

Vista muy simplificada de algunos de los **proveedores de funciones intermediarias** involucradas cuando un usuario solicita una página web.



3 Protecciones de responsabilidad para las funciones de los intermediarios

Esta sección analiza las protecciones de responsabilidad, comenzando con una breve historia de los orígenes y los elementos clave de la Sección 230 de los Estados Unidos. También describimos el Marco Civil da Internet de Brasil de 2014 y Directiva de Comercio Electrónico de 2000 y la Ley de Servicios Digitales de 2022 de Europa; luego, analizamos otros enfoques nacionales o regionales relacionados.

Concluimos con un análisis de las tendencias recientes en torno a las políticas asociadas a las funciones de intermediarios e identificamos algunos riesgos específicos que pueden traer aparejados estos enfoques tanto para Internet como para sus usuarios.

3.1 El desarrollo inicial de las leyes de protección de intermediarios: definición del contexto

El Internet inicial se desarrolló en la década de 1970 con financiación proporcionada por el gobierno de los Estados Unidos (EE.UU.). Utilizada inicialmente para colaboración e investigación por un pequeño grupo de investigadores académicos, gubernamentales y comerciales, comenzó como una red exclusiva de EE. UU., pero rápidamente creció para incluir conexiones con Europa, Asia y Oceanía. Las prohibiciones de tráfico personal y comercial se eliminaron de manera gradual en la década de 1990. En 1995, el gobierno de Estados Unidos transfirió formalmente la red al sector privado, lo que comenzó a atraer a la gente común a Internet.

Mientras más y más individuos tenían la posibilidad de hablar públicamente en Internet, comenzaron a surgir cuestiones rápidamente

de cómo se asignaría la responsabilidad del contenido dañino o ilegal en el contexto de Internet. En Estados Unidos se presentaron demandas argumentando que las empresas que permitían a las personas publicar en línea deberían ser legalmente responsables de las palabras que esas personas habían publicado. En la década de 1990, dos decisiones judiciales fundamentales de Estados Unidos decidieron que los servidores de contenido en línea, los intermediarios, **serían** responsables de las palabras publicadas por sus usuarios *si dichos host habían tomado medidas para moderar el discurso en línea y eliminar contenido sexual, ofensivo o de otro tipo*.⁷

Esas sentencias judiciales establecieron dos escenarios inviables y poco atractivos para el surgimiento de Internet.

Por un lado, si las compañías tomaban medidas para “moderar” el discurso en línea de los usuarios, hubieran sido responsables del contenido, pero esas entidades⁸ no contaban con el personal o los recursos para revisar, bloquear o eliminar contenido que pudiera ser motivo de responsabilidad legal.⁹

Por otro lado, las compañías podrían haber evitado la responsabilidad legal si no tomaban medidas para eliminar contenido sexual, ofensivo o, de algún modo, objetable de lo que publicaban los usuarios. Pero, ese entorno hubiera provocado la existencia de conversaciones y publicaciones en línea llenas de contenido objetable. En lugar de convertirse en una plataforma útil para la interacción social y cívica y el crecimiento económico, Internet habría perdido su utilidad como herramienta de comunicación, expresión y comercio individual.

Estas sentencias judiciales generaban gran incertidumbre y responsabilidad potencialmente perjudicial del contenido generado por el usuario para el desarrollo de Internet.

7 *Cubby, Inc. c. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), en el cual se sostuvo que un proveedor de servicios en línea no debía considerarse responsable por la opinión expresada por un participante en un foro en línea, solamente por el hecho de que el proveedor no había moderado ningún contenido. Luego, en *Stratton Oakmont, Inc. c. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 24 de mayo de 1995), se concluyó que el proveedor de servicios en línea sería responsable de la opinión de los participantes debido a que el proveedor participó en el monitoreo y la regulación de parte del contenido.

8 Si bien los grandes sitios de redes sociales de la actualidad son un ejemplo evidente, Internet de la década de 1990 tenía menos “megasitios” y, a menudo, no había un intermediario manifiesto que tuviera el derecho o la responsabilidad de moderar el contenido. Cuando se identificaba un moderador, con frecuencia se trataba de un individuo privado que se dedicaba a eso como voluntario, en lugar de ser una compañía privada.

9 Incluso en un entorno de abundantes recursos, algunos tipos de moderación, como la de contenido difamatorio, son en sí mismos problemáticos, ya que suele ser imposible para un moderador individual determinar si el contenido es difamatorio o no.

3.2 Primera legislación en materia de responsabilidad de intermediarios de Internet: Sección 230 de Estados Unidos

Frente a este desafío del potencial de Internet y la posibilidad de que los individuos participen en línea, desde 1995 hasta 1996, el Congreso de los Estados Unidos decidió enfrentar la realidad acerca del hecho de que los regímenes de responsabilidad no funcionaban para Internet:

- La responsabilidad basada en el editor que se aplicaba a los periódicos de papel llevaría a una potencial responsabilidad masiva que perjudicaría el discurso individual en Internet o una Internet en la cual los sitios no aplicarían reglas de comportamiento o cortesía.
- El régimen de transporte común aplicable al servicio telefónico básico no podía aplicarse ni a las redes de acceso a Internet, que tenían algunos aspectos de los operadores de comunicaciones, pero no los suficientes para ajustarse a ese modelo, ni a los hosts de contenido, que operan de manera completamente diferente a los operadores comunes.
- El régimen de responsabilidad que se aplicaba a la radio, la televisión y al cable (que se basa en acuerdos contractuales negociados individualmente entre redes y corporaciones proveedoras de contenido) no se podía usar para un universo de millones y, finalmente, miles de millones de usuarios en línea.

Era necesario tener un enfoque nuevo en lo que respecta a la responsabilidad.

Fue en este contexto que el Congreso de los Estados Unidos consideró y promulgó la “Ley de Libertad en Internet y Empoderamiento de la Familia”, que se convirtió en la Sección 230 del Título 47 del Código de los Estados Unidos (USC) (a menudo llamada simplemente “Sección 230”).¹⁰ Uno de los objetivos explícitos del Congreso para la Sección 230 era “promover el desarrollo continuo de Internet y otros servicios informáticos interactivos,

¹⁰ El texto que, finalmente, se convirtió en la Sección 230 provino en sus inicios de una propuesta legislativa de la Cámara de Representantes, la Ley de Libertad en Internet y Empoderamiento Familiar. Durante la conferencia de la Cámara de Representantes y el Senado para conciliar la legislación de la Ley de Telecomunicaciones, el texto de la Sección 230 se colocó inmediatamente después del anteproyecto y en la misma sección estatutaria que el proyecto de ley del Senado, el cual se conoce como Ley de Decencia en las Comunicaciones. Se puede encontrar contexto más amplio sobre la Ley de Telecomunicaciones en “What’s in a Name” (Qué esconde este nombre) (<https://www.lawfaremedia.org/article/whats-name-quiet-bit-if-youre-talking-about-section-230>), “Section 230: An Overview” ([Descripción general de la Sección 230] del Servicio de Investigaciones del Congreso <https://crsreports.congress.gov/product/pdf/R/R46751>), entre otros. El texto definitivo se puede encontrar en <https://www.congress.gov/bills/104/congress/senate-bill/652>.

y otros medios interactivos”¹¹. El Congreso reconoció que los servicios informáticos interactivos en general y que Internet en particular, incluso en su etapa inicial cuando se sancionó la Sección 230, ofrecían una plataforma absolutamente diferente para la comunicación interactiva por parte de los individuos.

El Congreso de los Estados Unidos observó en la legislación que “Internet y otros servicios informáticos interactivos ofrecían un foro para una diversidad real del discurso político, oportunidades únicas para el desarrollo cultural y un sinnúmero de vías para la actividad intelectual”.¹²

El Congreso resolvió que se debían fomentar estas comunicaciones interactivas que fomentaban el discurso público. A diferencia de las formas “de publicación” anteriores de comunicación masiva, Internet transforma al individuo de un destinatario pasivo de productos creado mayormente por corporaciones a un participante activo en la conformación de la comunicación y del contenido. El Congreso reconoció que esta “interactividad” impulsada por el individuo era un atributo esencial de la Internet emergente que justificaba protección.

11 47 USC § 230(b)(1), disponible en <https://www.congress.gov/104/statute/STATUTE-110/STATUTE-110-Pg56.pdf>

12 47 USC § 230(a)(3).

Texto clave de la Sección 230:

§ 230(c)(1): **Tratamiento del editor o vocero.** Ningún proveedor o usuario de un servicio informático interactivo será tratado como editor o vocero de ningún tipo de información proporcionada por otro proveedor de contenido informativo.

§ 230(c)(2): **Responsabilidad civil.** Ningún proveedor o usuario de un servicio informático interactivo se considerará responsable de:

(A) las medidas tomadas voluntariamente y de buena fe para restringir el acceso o la disponibilidad de materiales que el proveedor o el usuario consideren obscenos, indecentes, lascivos, procaces, excesivamente violentos, intimidantes o, de algún modo, objetables, ya sea que los materiales estén amparados por la Constitución o no; ni

(B) las medidas tomadas que permitan o pongan a disposición de proveedores de contenido de información u otros actores los medios técnicos para restringir el acceso a los materiales descritos en el párrafo ([A]).

§ 230(f): **Definiciones.**

(2) Servicio informático interactivo

El término “servicio informático interactivo” hace referencia a cualquier servicio, sistema o proveedor de software de acceso de información que ofrezca o habilite el acceso informático por parte de múltiples usuarios a un servidor informático, entre los que se incluyen específicamente un servicio o un sistema que proporcione acceso a Internet y esos sistemas administrados o servicios ofrecidos por bibliotecas o instituciones educativas.

(3) Proveedor de contenido de información

El término “proveedor de contenido de información” significa toda persona o entidad que es responsable, total o parcialmente, de la creación o el desarrollo de información brindada a través de Internet o cualquier otro servicio informático interactivo.

(4) Proveedor de software de acceso

El término “proveedor de software de acceso” se refiere a un proveedor de software (incluido un software de cliente o de servidor) o herramientas habilitantes que hacen una o más de las siguientes acciones:

- (A) filtrar, seleccionar, permitir o prohibir contenido;
- (B) escoger, elegir, analizar o asimilar contenido; o
- (C) transmitir, recibir, mostrar, enviar, almacenar en caché, buscar, subagrupar, organizar, reorganizar o traducir contenido.

La Sección 230 de los **Estados Unidos** contiene tres elementos fundamentales:

1. Los servicios informáticos interactivos (un término legal usado en la Sección 230 que, esencialmente, se refiere a las entidades que brindan funciones de intermediarios) en Internet no son legalmente responsables del contenido que otras entidades, ya sea individuos, corporaciones y otros proveedores de contenido, publiquen en Internet. En cambio, la responsabilidad legal del contenido sigue recayendo en la persona o la entidad que creó o publicó el contenido. Este elemento es lo que permite a los proveedores de servicio de Internet, a los servicios de alojamiento web y a muchos otros a transportar y alojar contenido sin perjuicio de ser potenciales responsables masivos.
2. Los servicios informáticos interactivos no son responsables si deciden bloquear o eliminar contenido no deseado de sus plataformas. Este elemento garantiza que los host o las plataformas en línea queden protegidos si eliminan contenido de odio, ofensivo o, de algún modo, objetable de sus sitios. Por ejemplo, si un individuo publica contenido sexual explícito en una plataforma en línea, dicho individuo no podría demandar a la plataforma si se elimina o bloquea ese contenido. Por ende, los intermediarios quedan protegidos de sus decisiones en cuanto a la moderación de contenido.
3. Las compañías que desarrollan herramientas tecnológicas para permitir a los usuarios filtrar y bloquear contenido no deseado en Internet no pueden ser consideradas responsables de la creación de esa capacidad de bloqueo. Si, por ejemplo, un sitio web que incluye contenido de odio o malicioso es bloqueado con un software instalado por un padre en una computadora doméstica, el sitio no puede demandar al fabricante del software por bloquear su contenido. Este elemento fomenta el desarrollo de herramientas que permitan a los *usuarios* elegir limitar los tipos de contenido legítimo a los que ellos (y sus familias) pueden acceder.

Todas las protecciones anteriores se extienden ampliamente a cualquier servicio informático interactivo que participe en la transmisión, transporte, alojamiento, conservación, visualización o, de otro modo, facilite la transmisión o visualización de contenido que otros hayan creado, no solo el servicio en el que se publicó o compartió el contenido.

En la Sección 230 no se usan los términos “intermediario” ni “función de intermediario”; en cambio, la ley define de manera amplia el término “servicios informáticos interactivos” para referirse a las funciones básicas de acceso, tráfico, alojamiento, búsqueda de Internet y los servicios relacionados. Por lo tanto, la Sección 230 aplica las anteriores protecciones de responsabilidad a todo “proveedor o usuario de un servicio informático interactivo”.

Observe que hasta los usuarios particulares quedan amparados con la Sección 230 en casos en los que, por ejemplo, reenvíen una publicación en línea a otro destinatario.

La Sección 230 se ve como un motivo fundamental por el cual el discurso a nivel individual ha prosperado en Internet dentro de los Estados Unidos.¹³ Al mismo tiempo, el Congreso de los EE. UU. buscaba proteger y fomentar el potencial económico de Internet. Y los beneficios económicos y sociales combinados que Estados Unidos obtuvo de Internet llevaron a otros gobiernos importantes a adoptar reglas similares.

Estados Unidos fue la primera nación en adoptar protecciones de responsabilidad legal para los intermediarios de Internet. Otras naciones y regiones han adoptado protecciones similares aunque presentan algunas diferencias considerables.

3.3 Protecciones iniciales de intermediarios de Europa

En el año 2000, la **Unión Europea** (UE) adoptó la Directiva sobre el Comercio Electrónico (2000/31/EC),¹⁴ para abordar las protecciones de los intermediarios. Por temas prácticos, la Directiva sobre el Comercio Electrónico adoptaba un enfoque muy parecido al de la Sección 230, pero tenía tres diferencias significativas:

¹³ Jeff Kosseff, un intelectual jurídico estadounidense, fue más allá y escribió un libro completo, titulado “The Twenty-Six Words that Created the Internet” (Las veintiséis palabras que crearon Internet), en el que se hace referencia a la Sección 230 y se le responsabiliza de gran parte de lo sucedido en la industria de Internet de los Estados Unidos. Si desea obtener contexto adicional, consulte también <https://www.propublica.org/article/nsu-section-230>.

¹⁴ Consulte <https://eur-lex.europa.eu/eli/dir/2000/31/oj>; https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000.

- La directiva de la UE separaba a los intermediarios en categorías básicas de (a) mero transporte, (b) proveedores de almacenamiento en caché; y (c) proveedores de alojamiento.
- Si bien la directiva no definía los tipos de entidades que estaban cubiertas, trataba los tipos de “actividades” específicos que recibirían protección de responsabilidad (igual que, en este documento, se centra en las “funciones” de los intermediarios en lugar de las categorías de intermediarios).
- Lo más importante es que, en la Directiva de la UE, se exige que los intermediarios con conocimiento de contenido presuntamente ilegal tomen medidas para eliminarlo con rapidez razonable.¹⁵

Con la Directiva sobre el Comercio Electrónico, se regularon los asuntos de protección de los intermediarios en la Unión Europea durante más de 20 años, hasta que fue modificada y complementada por la Ley de Servicios Digitales y otras medidas que se analizan más adelante.

3.4 El Marco Civil de Internet de Brasil

A partir de 2009, un amplio grupo de partes interesadas de **Brasil** (entre ellos, el gobierno, la comunidad académica, la sociedad civil y el sector industrial) emprendieron un esfuerzo colaborativo para elaborar un conjunto de leyes que trataran el tema de Internet. Gracias a la participación de múltiples actores, este intento recibió numerosos comentarios y aportes, y se redactaron y perfeccionaron anteproyectos. La legislación resultante se sancionó en 2014, la ley federal brasileña número 12965/2014, conocida como el Marco Civil de Internet.¹⁶ El estado brasileño especifica que el Marco Civil “establece los principios, las garantías, los derechos y los deberes para el uso de Internet en Brasil”.¹⁷

La Sección III del Marco Civil presenta un enunciado muy directo acerca de la protección de la responsabilidad de los intermediarios, con disposiciones adicionales para permitir la eliminación de contenido por

¹⁵ El régimen de “notificación y eliminación de contenido” que se creó con la Directiva sobre el Comercio Electrónico se contraponen al abordaje empleado en los Estados Unidos, donde la Primera Enmienda de la Constitución de EE. UU. (fuera del contexto de copyright) en general prohíbe los mandatos jurídicos para eliminar contenido sin una resolución judicial específica en la cual se establezca que el contenido es ilegal.

¹⁶ Consulte <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6> o la versión oficial en inglés de la ley en <https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180> y <https://www.daniel-ip.com/en/articles/the-brazilian-internet-bill-of-rights-and-online-infringement-of-ip-rights/>.

¹⁷ La versión en inglés del Marco Civil está disponible en http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/brazilian_framework_%20internet.pdf.

orden judicial y la protección de la privacidad con aviso. Los preceptos clave de las disposiciones en materia de intermediarios incluyen:

Artículo 18. El proveedor de conexión a Internet no tendrá responsabilidad civil respecto de los daños y perjuicios derivados del contenido generado por terceros.

Artículo 19. Con el fin de garantizar la libertad de expresión y evitar la censura, los proveedores de aplicaciones de Internet solo tendrán responsabilidad civil por los daños y perjuicios derivados del contenido generado por terceros si, ante una orden judicial específica, no toman medidas para eliminar la disponibilidad del contenido identificado como infractor, con sujeción en las disposiciones legales vigentes, y dentro del alcance y los límites técnicos de su servicio, en el tiempo indicado.

...

Artículo 20. Si el proveedor de la aplicación de Internet dispone de los datos de contacto del usuario que es directamente responsable del contenido mencionado en el Artículo 19, será responsabilidad del proveedor comunicar al usuario los motivos y la información relativa a la no disponibilidad del contenido, con información que permita la defensa contradictoria y plena en juicio, salvo previsión legal expresa o determinación judicial expresa en contrario.

...

Artículo 21. Los proveedores de aplicaciones de Internet que pongan a disposición contenido generado por terceros serán responsables subsidiarios de la vulneración de la privacidad derivada de la divulgación, sin autorización de los participantes, de imágenes, videos u otros materiales que contengan desnudez o actos sexuales de carácter privado cuando, recibida la notificación del participante o de su representante legal, no promuevan con diligencia la eliminación de la disponibilidad de dicho contenido dentro de los límites técnicos de su servicio.

El enfoque de Brasil ha sido considerado en la región como una vía para la protección de las funciones de los intermediarios y, al mismo tiempo, para normalizar una ruta judicial que permita tratar las inquietudes de los gobiernos y de los ciudadanos en materia de contenido ilegal o dañino.

3.5 Actualizaciones de protecciones de intermediarios de Europa

En 2022, la **Unión Europea**, motivada por las inquietudes sobre la seguridad en línea, la difusión de desinformación y los discursos de odio, además de otras conductas ilegales o dañinas observadas en las grandes plataformas y servicios ampliamente utilizados, adoptó una importante actualización y ampliación de la Directiva sobre el Comercio Electrónico de 2000 para continuar su enfoque general en el cual se tratan los servicios (muchos de los cuales abarcan las “funciones de los intermediarios” analizadas aquí) en lugar de las compañías. Esto reconoce que algunas entidades pueden proporcionar diferentes funciones de intermediarios y, por lo tanto, tener derecho a diferentes tipos de protecciones o tener otras obligaciones según la función específica que se preste.

El objetivo general del *Reglamento 2022/2065 de la UE establecido por el Parlamento y el Consejo Europeo del 19 de octubre de 2022, en materia de un Mercado Único de Servicios Digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales)*¹⁸, es proporcionar un mercado único de servicios en línea en la UE. La Ley de Servicios Digitales incluye protecciones de responsabilidad por el contenido generado por el usuario (a excepción de cuando el proveedor de servicios tiene conocimiento de la ilegalidad), pero las combina con requisitos de “diligencia debida”. Estas obligaciones hacen que los proveedores tengan más responsabilidad de lo que sucede en sus servicios. En vez de imponer responsabilidad, la Ley de Servicios Digitales utiliza multas para disuadir y castigar el incumplimiento de dichas obligaciones.

A partir de la Directiva sobre el Comercio Electrónico, la Ley de Servicios Digitales se aplica a un subconjunto de “servicios de la sociedad de la información” definidos como tres categorías de “servicio de intermediarios”.¹⁹

1. Un servicio de “mero transporte”, que consiste en la transmisión en una red de comunicación de información llevada a cabo por un destinatario del servicio o la provisión de acceso a una red de comunicación.

¹⁸ Consulte <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>, además de las Preguntas frecuentes presentadas por la Comisión Europea en https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 y un resumen de la información en https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

¹⁹ Ibid., Artículo 3, “Definiciones” de la Ley de Servicios Digitales.

2. Un servicio de “almacenamiento en caché” compuesto de la transmisión en una red de comunicación de información proporcionada por un destinatario del servicio, lo que implica el almacenamiento automático, intermedio y temporal de dicha información, realizado con el único propósito de hacer más eficiente la subsiguiente transmisión de la información a otros destinatarios a solicitud de estos.
3. Un servicio de “alojamiento” que consiste en el almacenamiento de información proporcionada por, y a solicitud de, un destinatario del servicio.

Además, la Ley implementa obligaciones particulares a dos categorías de servicios: proveedores designados de motores de búsqueda de muy gran tamaño (VLOSES) y plataformas en línea de muy gran tamaño (VLOPS) (que se definen como los que tienen más de 45 millones de usuarios de la UE/mes). Incluyen

- Un punto de contacto para las autoridades y los usuarios de la UE.
- Términos y condiciones simples para los usuarios.
- Transparencia en cuanto a publicidad, sistemas de recomendación y decisiones de moderación de contenido.
- Una evaluación basada en riesgos de su servicio y medidas de mitigación correspondientes.
- Auditoría independiente.
- Intercambio de datos con autoridades a efectos de cumplimiento y con investigadores examinados para comprender los riesgos sistémicos.
- Obligación de proporcionar una opción de sistema de recomendación que no se base en la elaboración de perfiles de usuario.²⁰

3.6 Protecciones de intermediarios en otros contextos nacionales e internacionales

A principios de la década de 2000, varios países también adoptaron leyes nacionales centradas en Internet y promulgaron distintos niveles de protección para las funciones de intermediarios.

²⁰ Consulte la orientación de la Comisión Europea en <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.

Por ejemplo, en 2000, **India** aprobó la Ley de Tecnología de la Información de 2000, que establecía que los intermediarios no serían responsables del contenido de terceros disponible si podían probar que la ofensa o contravención había sido cometida sin su conocimiento o que habían hecho la debida diligencia para impedir que se cometa tal ofensa o contravención.²¹ La ley también concede directivas gubernamentales para eliminar cierto contenido en línea.

En **Nigeria**, en 2003, en las Directrices para la Prestación del Servicio de Internet publicadas por la Comisión de Comunicaciones de Nigeria, se estipulaba que los proveedores de servicio de Internet que actuaran como simple transporte (es decir, alojamiento o almacenamiento en caché) no tendrían responsabilidad alguna por el contenido y las comunicaciones generados por usuarios con algunas salvedades: no debían demorarse al tener que eliminar o deshabilitar el acceso a la información al recibir una notificación para la eliminación de contenidos o cuando tuvieran conocimiento de que la información había sido eliminada o deshabilitada en la fuente inicial de transmisión.²²

En **Sudáfrica**, con la Ley de Comunicaciones y Transacciones Electrónicas de 2002, se adoptó un enfoque similar, pero condicionó las limitaciones de responsabilidad a que el proveedor de servicios fuera miembro de un ente representativo y estuviera sujeto al código de conducta de dicho ente reconocido por el Ministro, así como a un proceso de notificación y eliminación de contenido.²³

La Ley de Comunicaciones Digitales Dañinas de Nueva Zelanda de 2015 protege a los “host de contenido en línea” de toda responsabilidad, siempre que cumplan con el proceso de quejas legal. La ley incluye un requisito para que el host de contenido en línea notifique a la persona que presenta la queja y puede contemplar un requisito para eliminar y deshabilitar contenido.²⁴

21 Consulte el Artículo 79 de la Ley de Tecnología de la Información del 2000 (India), que está disponible en <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf>.

22 Directrices para la Prestación del Servicio de Internet publicadas por la Comisión de Comunicaciones De Nigeria en el año 2003 conforme a la Sección 70(2) de la Ley de Comunicaciones de Nigeria de 2003, disponible en <https://ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file>.

23 Ley de Comunicaciones y Transacciones Electrónicas de 2002 (Sudáfrica) disponible en https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

24 Ley de Comunicaciones Digitales Dañinas de 2015 (Nueva Zelanda) disponible en <https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM6512504>.

Por su parte, en **Australia** existe un avance activo en 2024 para adoptar un régimen de protección de responsabilidad de intermediarios enfocado en denuncias legales por difamación.²⁵ Las Disposiciones de la Enmienda Modelo sobre Difamación (Intermediarios Digitales) propuestas para 2023 modificarían las leyes de difamación “uniformes” de Australia, que entraron en vigor en 2006, para armonizar las leyes de difamación en todo el país. Las nuevas disposiciones pretenden aclarar la posición jurídica de los intermediarios respecto del contenido difamatorio digital. Proporcionan exenciones de responsabilidad por difamación para los intermediarios digitales que ofrecen servicios de almacenamiento en caché, transporte, almacenamiento y búsqueda.²⁶ Sin embargo, esas exenciones no estarán disponibles si el intermediario digital, entre otras cosas, seleccionó alguno de los destinatarios o promovió el contenido difamatorio. No está claro si eso incluiría la promoción de contenido a los usuarios a través de algoritmos de recomendación. La exención para los motores de búsqueda no tendría validez para los “resultados de búsqueda patrocinados”, es decir, “los resultados [que] son promocionados o priorizados por el proveedor del motor de búsqueda debido a un pago u otro beneficio otorgado al proveedor por un tercero o en nombre de este”.

Además de la legislación vinculante adoptada por los gobiernos, varias organizaciones multilaterales o de múltiples partes interesadas han emitido declaraciones de apoyo a las protecciones de la responsabilidad de los intermediarios. Estos acuerdos y declaraciones internacionales reflejan un consenso creciente sobre el valor de tales protecciones. Brindamos un resumen de algunas de estas declaraciones en la tabla a continuación.

25 Consulte <https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf> o <https://www.parliament.nsw.gov.au/bill/files/18503/Passed%20by%20both%20Houses.pdf> (versión de Nueva Gales del Sur).

26 Apéndice 1, Secciones 10C y 10D de la Modificatoria Modelo de las Disposiciones sobre Difamación (Intermediarios Digitales) de 2023 disponible en <https://pcc.gov.au/uniform/2023/pcc-584-d40.pdf>.

Declaraciones multilaterales y de múltiples partes interesadas sobre las protecciones de la responsabilidad de los intermediarios

2011

El Relator Especial de las Naciones Unidas (ONU) sobre la Libertad de Opinión y de Expresión, el Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre la Libertad de los Medios de Comunicación, el Relator Especial de la Organización de los Estados Americanos (OEA) sobre la Libertad de Expresión y el Relator Especial de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) sobre la Libertad de Expresión y el Acceso a la Información²⁷ emitieron una declaración conjunta en la que se solicita la protección de los intermediarios de “simple transporte” y de otras funciones de intermediarios, se expresa la opinión de que no se les debe exigir que monitoreen el contenido generado por los usuarios ni deben quedar sujetos a normas extrajudiciales de eliminación de contenido que no otorgan suficiente protección a la libertad de expresión

2013

En el Foro Africano de Gobernanza de Internet, una iniciativa panafricana para promover las normas de los derechos humanos y los principios de apertura en la formulación e implementación de políticas de Internet en África, se publicó la Declaración Africana sobre Derechos y Libertades en Internet,²⁸ que contenía un principio muy simple de protección de los intermediarios: “Nadie debe ser considerado responsable del contenido de Internet del que no es autor”.²⁹

2014

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) publicó una extensa guía sobre la limitación de la responsabilidad de los intermediarios.³⁰

27 <https://www.osce.org/representative-on-freedom-of-media/78309>.

28 <https://africaninternetrights.org/en>.

29 <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>.

30 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387>.

Limitación de la responsabilidad de los intermediarios de Internet.

Las limitaciones adecuadas de la responsabilidad de los intermediarios de Internet desempeñan un papel fundamental en la promoción de la innovación y la creatividad, el libre flujo de la información, los incentivos para la cooperación entre las partes interesadas y el crecimiento económico. Los intermediarios de Internet, al igual que otros actores, también desempeñan un papel importante en lo que respecta al tratamiento y la disuasión de las actividades ilegales, el fraude y las prácticas engañosas y desleales que se llevan a cabo a través de sus redes y servicios. La proporcionalidad y el cumplimiento de las protecciones de todos los derechos fundamentales pertinentes son importantes a este respecto.

Aunque los principios no son vinculantes, esta orientación de la OCDE reflejó un amplio reconocimiento por parte de muchos gobiernos de que las protecciones de responsabilidad de los intermediarios desempeñan un rol significativo para facilitar la expresión en línea y la participación creativa.

2018

En 2018, el Consejo de Europa adoptó la Recomendación del Comité de Ministros a los estados miembros sobre las funciones y las responsabilidades de los intermediarios de Internet (CM/Rec(2018)2)³¹, la cual le da a las responsabilidades de los estados y los intermediarios de Internet un enfoque basado en los derechos humanos y deja de lado las cuestiones de responsabilidad.

3.7 Últimas tendencias en responsabilidad de los intermediarios y riesgos para Internet

Las protecciones para los intermediarios se consideran decisivas en el crecimiento de Internet y para la prosperidad del discurso individual en Internet. Algunos países, mediante el reconocimiento de los beneficios ganados con los amparos a los intermediarios, han redactado leyes sobre protección de responsabilidad. En otros países, la ausencia de

³¹ <https://rm.coe.int/1680790e14>.

legislación en materia de protección de intermediarios puede derivar en protecciones judiciales o un tratamiento más problemático de las funciones de los intermediarios.

En esta sección, identificamos algunos enfoques propuestos recientemente para la formulación de políticas sobre las funciones de los intermediarios de Internet. Según la implementación precisa, estos enfoques pueden presentar riesgos significativos para Internet y los usuarios de Internet, incluidos:

- Deterioro de las operaciones técnicas y la confiabilidad de Internet.
- Debilitamiento de la seguridad y la privacidad de Internet.
- Reducción de la competencia en Internet en un país debido a las cargas o responsabilidades impuestas al ISP.
- Limitación de la capacidad de los individuos para compartir opiniones y otros discursos en Internet.
- Bloqueo excesivo de contenido legítimo.
- Exclusión inadecuada de segmentos de población en la participación en Internet.

Recomendamos sopesar detenidamente los riesgos enumerados anteriormente y otros posibles impactos en Internet al considerar estos enfoques de formulación de políticas para funciones intermediarias. En secciones posteriores de este documento, ofrecemos asesoramiento general y específico a los responsables de las políticas sobre cómo evitar estos y otros riesgos.

Notificación y eliminación de contenido: no todos los regímenes regulatorios han adoptado el mismo enfoque en torno a la responsabilidad de los intermediarios. En una variante común, los intermediarios pueden ser considerados responsables e incluso obligados a responder por el contenido de sus usuarios si no toman determinadas medidas. Por ejemplo, algunos fueros judiciales tienen un enfoque de “notificación y eliminación de contenido”, que exige que un intermediario elimine el contenido al recibir una notificación autorizada judicialmente emitida por un tribunal o una agencia gubernamental autorizada. Es importante destacar que no suele existir una obligación general para que los intermediarios monitoreen el contenido.³²

32 Sin embargo, las modificaciones de la Ley de Protección de Datos y Cibernética de Zimbabue de 2021 a la Ley de Evidencia y Procedimiento Penal establecen que un proveedor de alojamiento, si “entra en conocimiento o se da cuenta de que hay información ilegal almacenada, debe informar de inmediato a la autoridad competente para permitirle evaluar la naturaleza de la información y, si es necesario, emitir una orden para la eliminación”. Texto disponible en <https://www.law.co.zw/download/cyber-and-data-protection-act-chapter-1207/>.

Conocimiento: otros han exigido que los intermediarios eliminen contenidos ilegales o dañinos cuando tienen conocimiento de ellos, con distintos niveles de “conocimiento” requeridos, siendo el más estricto el “conocimiento real”.³³

Estas modificaciones (notificación, eliminación de contenido y conocimiento) al enfoque general entran en juego después de que un usuario haya cargado o compartido el contenido.

Moderación del contenido subido: cada vez hay más interés en hacer responsables a los intermediarios, especialmente a los que alojan contenidos, de la filtración de ciertos tipos de contenidos antes de que se compartan, como el material de abuso sexual infantil (CSAM). A esto, a veces se le denomina “Moderación del contenido subido” y, en algunas propuestas, existe la intención de imponer esta obligación incluso a las aplicaciones de mensajería cifradas de extremo a extremo.³⁴

Este tipo de responsabilidades en materia de contenido previas a la publicación están empezando a denominarse responsabilidades de “diligencia debida” o “deber de cuidado”. A veces, también existen enfoques de “responsabilidad condicional”, en los que un intermediario no será responsable **siempre que** haga algo o impida algo.

Requisitos específicos según la edad: algunos países han presionado para imponer más responsabilidad a las entidades de intermediarios a fin de excluir a ciertos grupos etarios de sus servicios o de modificar los servicios o el contenido que muestran a esos usuarios. El incumplimiento de estos requisitos puede provocar la prohibición, el bloqueo del servicio de intermediario o puede causar que la entidad del intermediario sea responsable conforme a cómo se implemente la política.

Por ejemplo, en Indonesia, los intermediarios pueden estar protegidos de la responsabilidad en cuanto al contenido generado por los usuarios si garantizan que sus sistemas no contienen ni facilitan la difusión de contenido prohibido. También deben tener un marco de gobernanza para el contenido generado por el usuario que incluya derechos, obligaciones, informes, quejas, responsabilidad, y deben brindar información sobre los usuarios que realizan cargas con contenido prohibido y responder a “notificaciones de eliminación de contenido”.³⁵

33 Consulte, por ejemplo, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE) (España), disponible en <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758>.

34 Obviamente, si se requiere que un intermediario que ofrece mensajería cifrada de extremo a extremo modere el contenido que envían los usuarios, entonces los mensajes ya no pueden considerarse cifrados de extremo a extremo.

35 Regulación del Ministro de Comunicaciones e Información, República de Indonesia, Número 5 de 2020 en materia de Operadores de Sistemas Electrónicos Privados, consulte el Artículo 11, disponible en https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

Con este enfoque de las políticas, se está impulsando el interés en mecanismos técnicos para verificar la edad y la identidad del usuario antes de que pueda utilizar servicios o acceder al contenido. No obstante, los mecanismos actualmente disponibles plantean serias cuestiones sobre su eficacia, privacidad, seguridad y prevención del acceso a contenido legal en línea.³⁶

Requisitos de trazabilidad: otro enfoque que ha surgido es la exigencia de que los intermediarios puedan identificar quién publicó el contenido, incluso cuando una comunicación está cifrada de extremo a extremo. Por ejemplo, en la India, los grandes intermediarios de mensajería de medios sociales deben poder identificar al primer originador de un mensaje cuando así lo exige una orden judicial.³⁷

Eliminación de las protecciones de responsabilidad de los

intermediarios: las reacciones a las primeras experiencias sobre las políticas específicas de Internet han servido de inspiración de algunas propuestas radicales. Por ejemplo, en Estados Unidos, algunas inquietudes sobre las plataformas más grandes han dado lugar a propuestas demasiado amplias para eliminar *todas* las protecciones de los intermediarios de *todas* las entidades que están protegidas por la ley pertinente, la Sección 230. De manera similar, en Brasil, se han planteado cuestiones sobre la validez actual del enfoque adoptado en el Marco Civil da Internet respecto de la responsabilidad de los intermediarios. Estas propuestas de modificar o derogar las protecciones de los intermediarios, aunque estén en la etapa de propuesta, tienen el impacto directo de amenazar la existencia de las operaciones de Internet al generar incertidumbre y presentar la amenaza de una responsabilidad sin restricciones por el contenido producido por otros.

Códigos obligatorios para la industria: algunas jurisdicciones están imponiendo códigos o normas obligatorios para la industria³⁸ para implementar nuevas obligaciones legales (como seguridad por diseño, evaluaciones de riesgos y cumplimiento de los términos de servicios) para

36 Consulte Internet Society, “La Ley de Verificación Obligatoria de la Edad de Texas debilitará la privacidad y la seguridad en Internet,” 23 de septiembre de 2024, disponible en <https://www.internetsociety.org/blog/2024/09/texas-mandatory-age-verification-law-will-weaken-privacy-and-security-on-the-internet/>.

37 Disponible en el sitio web de MeitY <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf>. Al momento de la redacción de este documento, la constitucionalidad de estas normas está sujeta a diversas acciones legales.

38 Consulte, por ejemplo, el registro de los códigos y las normas industriales en materia de seguridad en línea de Australia, disponible en <https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards>.

categorías de intermediarios, por ejemplo, medios sociales y motores de búsqueda, especialmente en el contexto de la seguridad en línea.

Observamos que, con frecuencia, las políticas de cada jurisdicción se elaboran de manera muy amplia. A veces esto es intencional, una forma de poder mantenerse al día con la evolución de la tecnología y los usos de Internet. No obstante, a menudo, estas políticas generales tienen un profundo efecto adverso en Internet y en la posibilidad de que las personas se expresen en línea.

3.8 Diversidad global de los países

Con este documento, se busca brindar orientación útil sobre políticas a países de todo el mundo, desde aquellos con altos niveles de penetración de Internet e industrias de Internet bien desarrolladas hasta aquellos países que todavía están en proceso de ampliación del acceso y de sus economías digitales.

Reconocemos que existen enormes diferencias en la legislación, la cultura, la economía, la política, los valores y hasta en los objetivos de las políticas en lo concerniente al contenido de Internet. Creemos que nuestras recomendaciones sobre políticas servirán a todos los formuladores de políticas que consideren las regulaciones que deberán aplicar a los intermediarios. El documento comienza centrándose en el enfoque político de proteger a los intermediarios de la responsabilidad y por qué ese enfoque ha sido importante para permitir que las personas participen en línea. Además, damos recomendaciones de políticas constructivas para abordar una amplia variedad de asuntos en torno a las políticas.

Observamos que los sistemas jurídicos difieren en cómo abordan el contenido problemático en línea: algunos se centran principalmente en la persona que publica el contenido, mientras que otros se enfocan en los intermediarios que alojan o transmiten ese contenido. Además, si bien la mayoría de los países tienen litigios públicos y privados para abordar el contenido problemático en línea, algunos tienen más litigios privados que otros. Estas diferencias pueden haber llevado a los países a centrarse en distintos grados en la cuestión de la protección de los intermediarios frente a la responsabilidad. Sin embargo, en todas las situaciones, una recomendación clave es evitar responsabilizar, ya sea civil o penalmente, a las funciones de los intermediarios debido al contenido que un usuario o un tercero hayan publicado. Si se impusiera tal responsabilidad, la posibilidad de los usuarios de Internet de expresarse y publicar contenidos en línea se vería perjudicada. No obstante, tal como se señala en la

Sección 4, existen muchas maneras en que los gobiernos pueden abordar de manera constructiva los asuntos de las políticas relacionadas con los proveedores de servicios en línea.

También es importante, al formular políticas, tener en cuenta que las entidades que prestan funciones de intermediarios varían en tamaño, ingresos, márgenes de ganancia y modelo de negocio. Algunas son entidades sin fines de lucro y otras, según el país y el entorno empresarial, también pueden ser administradas por los gobiernos. Algunas entidades ofrecen solo una función específica, mientras que otras están sólidamente integradas en una variedad de negocios relacionados. Esto genera intereses muy diversos y a veces contrapuestos incluso dentro de la misma industria, y diferencias significativas en su capacidad de contribuir eficazmente a la formulación de políticas en esta área.

Asimismo, la jurisdicción sobre los proveedores de servicios en línea puede variar de un país a otro. De acuerdo con dónde esté ubicada la entidad que ofrece funciones de intermediarios, los asuntos jurisdiccionales pueden ser complejos. Quizá, sea más fácil para los países ejercer la función jurisdiccional cuando una entidad que presta funciones de intermediario tiene oficinas comerciales o infraestructura en ese país. Cuando el contenido está alojado fuera del país, la jurisdicción puede ser más complicada, en particular cuando los países llegan a conclusiones diferentes sobre la naturaleza jurídica del mismo contenido.

Los asuntos jurisdiccionales son importantes porque las leyes incompatibles y los reclamos jurisdiccionales extraterritoriales hacen que sea costoso y hasta imposible para las entidades prestar funciones de intermediarios de Internet a nivel global. Instamos a los formuladores de políticas a evitar la creación de leyes con efectos extraterritoriales y a considerar los riesgos que esto plantea para Internet a escala global.

4 Principios para la formulación de políticas para las funciones de los intermediarios de Internet

Esta sección establece tres conjuntos de principios que Internet Society considera de utilidad para los formuladores de políticas que estén pensando en políticas que afecten los servicios de Internet:

1. Principios generales que se aplican a cualquier formulación de políticas relativa a Internet o a su uso.
2. Principios centrados específicamente en proteger a los intermediarios de la responsabilidad.
3. Ejemplos más amplios de principios jurídicos y de políticas que pueden aplicarse a las funciones de intermediarios sin perjudicar las protecciones de los intermediarios frente a la responsabilidad.

El Anexo de este documento profundiza sobre estos principios y se brindan recomendaciones sobre políticas detalladas acerca de una amplia gama de **funciones de intermediarios de Internet**. En el Anexo, también discutimos consideraciones técnicas y prácticas para cada una de las funciones de los intermediarios. La información del Anexo está agrupada por tipo de función de intermediarios, que abarca desde funciones de intermediarios de contenido comúnmente reconocidas, como alojamiento y distribución de contenido, hasta funciones cruciales que permiten comunicar datos, localizar contenido y proteger las comunicaciones a través de Internet..

4.1 Principios generales para la formulación de políticas prudentes en materia de Internet

Los siguientes principios deben servir como una orientación amplia para toda acción de formulación de políticas respecto de Internet en general y de las funciones de los intermediarios en particular:

- A. **Incluir a las partes interesadas en la elaboración de políticas:** si los formuladores de políticas incluyen a otros actores durante todo el proceso de elaboración de políticas, estas serán más eficaces y se implementarán más rápidamente. La participación estrecha de las partes interesadas garantizará que se incluyan los conocimientos y las perspectivas pertinentes. Recomendamos encarecidamente que los gobiernos garanticen la más amplia participación de todos los actores relevantes en la elaboración de políticas que afecten Internet.
- B. **Realizar una evaluación de impacto en Internet:** la arquitectura técnica y las operaciones de Internet pueden verse afectadas directamente, y a menudo de manera involuntaria, por políticas, regulaciones o leyes aplicadas al contenido de Internet o a las funciones de los intermediarios que posibilitan la comunicación a través de Internet. Recomendamos encarecidamente que los formuladores de políticas lleven adelante una evaluación de impacto en Internet de todas las propuestas de políticas nuevas, incluso aquellas que parezcan muy limitadas, para comprender si pueden tener algún efecto adverso en Internet y sus operaciones. Internet Society ha analizado las propiedades y los facilitadores fundamentales que son esenciales para que Internet exista y prospere, y ha desarrollado un kit de herramientas para la evaluación de Impacto en Internet para ayudar a los responsables de las políticas en este proceso.³⁹
- C. **Es importante limitar cuidadosamente cualquier proyecto de ley o regulación** a las funciones intermediarias específicas que están causando el daño a la política: existe el riesgo de abarcar un conjunto demasiado amplio de funciones intermediarias, especialmente cuando la preocupación en materia de política social la plantea un conjunto muy reducido de empresas o funciones

³⁹ Consulte Internet Society, El Modo Internet de Interconectarse: definición de las propiedades esenciales de Internet, 9 de septiembre de 2020, que se encuentra en <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>; Internet Society, Kit de herramientas para la evaluación del impacto en Internet, 8 de noviembre de 2021, disponible en <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/introduction/>.

intermediarias. Por ejemplo, si existe preocupación acerca de determinados tipos de contenido alojado por un grupo de sitios web, una propuesta de formulación de políticas debería estar orientada específicamente a ese tipo de contenido y a ese grupo específico de sitios web. Dado que las funciones de los intermediarios son tan fundamentales para las operaciones básicas de Internet y la capacidad de los individuos de participar en conversaciones en línea, toda formulación de políticas debe orientarse cuidadosamente a impedir que haya un impacto en un conjunto demasiado amplio de funciones y entidades de intermediarios.

- D. **No se deben usar las protecciones de los intermediarios como amenaza ni para negociación:** las protecciones de las funciones de los intermediarios son tan fundamentales para las operaciones de Internet que no deben emplearse como forma para presionar en un debate de políticas públicas ni como sanción en una regulación o una ley. Por ejemplo, una legislatura no debería tratar un proyecto de ley en el que se declare que, si un grupo de compañías no cumple con un requisito particular, perderían sus protecciones como intermediarias. La capacidad de los individuos de expresarse en línea no debe depender de otros objetivos de formulación de políticas. Los formuladores de políticas deben regular o legislar directamente para lograr sus objetivos sin amenazar las protecciones de las funciones de los intermediarios ni perjudicar las operaciones de Internet.
- E. **La política debe promover la apertura:** el acceso a Internet, los servicios, las aplicaciones, los sitios y el contenido facilitan la participación de los individuos. El acceso abierto mejora la experiencia del usuario y el potencial de Internet de propiciar la innovación, la creatividad y el desarrollo económico. Los formuladores de políticas deben evitar limitar o bloquear la disponibilidad de las funciones de intermediarios que proporcionan acceso a Internet, sus aplicaciones y servicios.
- F. **Las intervenciones de las políticas deben estar lo más cerca posible del daño:** es menos probable que se produzcan daños colaterales a otros usuarios de Internet y a Internet si las intervenciones de las políticas se centran en el contenido problemático y su origen. Por ejemplo, en lugar de intentar bloquear el acceso al contenido a través de la dirección IP o el bloqueo de DNS, lo que también podría impedir el acceso a contenido legítimo e interrumpir el tráfico de Internet, se podría exigir a la persona que publica el contenido que lo elimine.

4.2 Principios específicos respecto de la protección de la responsabilidad de los intermediarios

Los cuatro principios siguientes se concentran en diferentes aspectos de las operaciones y el trabajo de las entidades que prestan funciones de intermediarios, y en la necesidad de brindar protección para ese trabajo:

- G. **Proteger las funciones de los intermediarios que habilitan las comunicaciones en Internet de la responsabilidad por el “contenido generado por el usuario”, es decir, el contenido creado por otros:** sin protecciones de responsabilidad, la infraestructura de Internet, así como las herramientas básicas que las personas usan para acceder e interactuar con el contenido, se verían paralizadas con un potencial ilimitado de acciones legales. Sin protección para estas funciones de los intermediarios, Internet básicamente no podría funcionar. Recomendamos encarecidamente que las entidades que brindan estas funciones de intermediarios de Internet estén protegidas de toda responsabilidad por el contenido que transmiten, reciben, almacenan en caché, filtran o, de algún modo, manejan y es creado por terceros.
- H. **Proteger las funciones de los intermediarios que alojan, facilitan y optimizan la distribución de “contenido original del sitio” (es decir, contenido creado por el propietario del sitio):** las entidades que alojan más de mil millones de sitios web de Internet deben estar protegidas para que en ellas no recaiga la responsabilidad del contenido que sus clientes publican en línea. Si se responsabilizara a las compañías de alojamiento del contenido publicado en línea por sus clientes, la mayoría no podría continuar con la prestación de este servicio. Esto afectaría especialmente a los proveedores de alojamiento web pequeños y medianos, ya que aumentaría los costos, eliminaría la competencia y reduciría la disponibilidad y la diversidad de contenido en línea. Los propietarios de sitios deben seguir siendo obligados y potencialmente responsables legales del contenido de sus sitios web, pero las entidades que brindan funciones de intermediarios, como alojamiento web, motores de búsqueda y almacenamiento en caché, no deben considerarse responsables.
- I. **Proteger las funciones de los intermediarios que alojan y muestran contenido generado por el usuario:** las entidades que proporcionan funciones de intermediarios para alojar contenido generado por el usuario deben estar protegidas de la responsabilidad frente

a ese contenido. Sin esta protección, dichos intermediarios no podrían seguir transmitiendo el contenido. Esto afectaría drásticamente y negativamente la posibilidad de los individuos de publicar contenido y de participar en conversaciones y debates con otros usuarios de Internet. Las funciones de los intermediarios son un requisito fundamental para que los individuos comuniquen sus ideas, opiniones, creaciones artísticas y conversaciones con otros. Las entidades que alojan contenido generado por los usuarios deben disponer de protecciones de intermediarios para garantizar que los usuarios puedan seguir comunicándose y compartiendo contenido en línea.

- J. **Proteger las funciones de los intermediarios de selección y moderación de contenido generado por el usuario:** una entidad que aloja contenido generado por el usuario *debe* poder establecer las reglas de juego para los tipos de debates, las obras creativas u otro contenido que desee alojar. Por ejemplo, si una entidad que aloja contenido generado por el usuario decide no alojar contenido “para adultos” o decide establecer reglas con respecto al comportamiento de los usuarios, la entidad debe tener la libertad de hacerlo. Estas entidades, que realizan funciones de intermediarios de alojamiento de contenido de usuarios, también deben tener protección de la responsabilidad por eliminar contenido irrelevante u objetable. Dada la enorme cantidad de contenido generado por los usuarios que se carga y comparte por minuto, la selección suele ser de vital importancia para ayudar a los usuarios a encontrar una pieza o un tipo de contenido en particular. Por lo general, la selección implica el uso de uno o más algoritmos, desde un algoritmo simple que presenta el contenido en el orden en que se recibe hasta algoritmos más sofisticados que presentan contenido en función del perfil del usuario y sus interacciones con el servicio. El filtrado y las “reglas de juego” permiten que los servicios de contenido alojado y sus usuarios eviten verse abrumados por material irrelevante, molesto y malicioso que oculta el contenido legítimo y aleja la participación individual en Internet. Los regímenes de protección de intermediarios deben proteger a las entidades de la responsabilidad legal por hacer cumplir sus propias reglas o eliminar contenido objetable.

4.3 Principios legales y de políticas específicos que se pueden aplicar a las funciones de los intermediarios sin perjudicar las comunicaciones de Internet

Las funciones de los intermediarios son esenciales para cualquier contenido transmitido, alojado o, de algún modo, manejado y dichas funciones exigen protección de la responsabilidad frente al manejo de ese contenido. Pero, esto no significa que las entidades que prestan estas funciones no se puedan regular. Existe una amplia gama de políticas, regulaciones y leyes que ya se aplican o pueden aplicarse a las entidades que prestan funciones de intermediarios, incluidas, por ejemplo, las leyes de competencia y de protección del consumidor. A continuación, se presentan algunos principios de políticas que pueden ayudar a abordar algunas de las cuestiones en materia de políticas que han surgido sobre las funciones de los intermediarios en Internet:

Privacidad y seguridad del usuario

- La privacidad y la seguridad son fundamentales para proteger la confidencialidad, la integridad y la privacidad de las comunicaciones de los individuos.
- Las políticas deben implementar reglas estrictas para proteger la privacidad y mejorar la seguridad de las comunicaciones en Internet.
- Las entidades que prestan funciones de intermediarios en Internet también deben esforzarse por incorporar “seguridad por diseño” y “privacidad por diseño”, al adoptar las prácticas recomendadas de la industria e innovar para mejorar las características de privacidad y seguridad de sus funciones.

Control y elección del usuario

- El brindar a los usuarios la capacidad de elegir y controlar el contenido que consumen les permite protegerse mediante el filtrado de contenido y fuentes irrelevantes y no deseadas.
- Las políticas deben intentar mejorar la elección y el control de los usuarios sobre qué servicios en línea utilizan y qué contenido eligen ver.

Accesibilidad del usuario

- Internet debe estar disponible para todos.
- Las políticas que promueven una accesibilidad sólida pueden orientar de manera útil el diseño y la implementación de funciones de intermediarios para permitir que los individuos con diferentes necesidades de accesibilidad participen en la comunicación en línea.⁴⁰
- Las entidades que proporcionan funciones de intermediarios de Internet también deben esforzarse por ofrecer contenido y controles en línea que interactúen de forma predecible y exitosa con la tecnología de asistencia.

Derechos del usuario

- Internet permite que los usuarios ejerzan sus derechos humanos en línea. Las funciones de los intermediarios de Internet desempeñan un papel vital a la hora de facilitar derechos, incluida la libertad de expresión, la libertad de asociación y la libertad de acceder a la información en línea. La interferencia gubernamental en la operación de las funciones de los intermediarios corre riesgo de impedir o dificultar el ejercicio de los derechos de los individuos.
- Los formuladores de políticas deben evaluar y evitar o minimizar el impacto potencial que las políticas propuestas relativas a las funciones de los intermediarios tienen en el ejercicio de los derechos humanos por parte de las personas.

Competencias digitales del usuario

- Las competencias digitales (también conocidas como alfabetización digital) permiten a los usuarios ser más selectivos en cuanto al contenido que consumen, reconocer contenido que puede ser desinformación, administrar configuraciones de privacidad y seguridad para proteger sus datos personales y denunciar contenido no deseado.
- Las políticas deben promover las competencias digitales para todos los usuarios de todas las edades y necesidades, por ejemplo, al brindar apoyo a la educación digital a través de escuelas, bibliotecas públicas, programas financiados por el gobierno e iniciativas lideradas por la comunidad.

40 Consulte las Pautas de accesibilidad al contenido web 2.2 de W3C, Comprensión de los Documentos en <https://www.w3.org/WAI/WCAG22/Understanding/intro>.

No discriminación del usuario

- Los individuos tienen derecho a ser tratados con igualdad, independientemente de categorías como raza, color, sexo, nacionalidad, idioma, religión o etnia, origen nacional o social.⁴¹
- Las políticas deben prevenir la discriminación contra usuarios individuales o grupos de usuarios en función de las clases y características protegidas por ley en la prestación de servicios de Internet.

Conocimiento del usuario

- El acceso a la información acerca de términos de servicio asociados con el alojamiento, la selección y la moderación del contenido generado por el usuario empodera a los usuarios para que tomen decisiones informadas acerca de los servicios que usan.
- Las políticas deben fomentar la transparencia significativa sobre cómo se alojará, seleccionará y moderará el contenido.

Acceso del usuario a servicios competitivos

- Históricamente, Internet ha sido un lugar estupendo para que pequeños innovadores y emprendedores inicien y desarrollen negocios.
- Los formuladores de políticas que aplican políticas en materia de competencia deben ser cuidadosos de no disminuir las protecciones de los intermediarios.

Riesgos del usuario

- Las nuevas funciones de los intermediarios o la aplicación de funciones conocidas a situaciones nuevas pueden tener consecuencias no deseadas para los usuarios. Esto puede plantear riesgos para la seguridad, la protección y la privacidad de los usuarios, así como para la propia Internet.
- Las políticas deben fomentar un enfoque basado en el riesgo para el ejercicio de las funciones de intermediarios, mediante una recompensa por la mitigación de los efectos adversos y el reconocimiento al mismo tiempo de que no existe el riesgo cero.

⁴¹ La lista de clases y características protegidas puede variar según el país o la jurisdicción legal. Esta lista se extrae del Artículo 1 de la Convención de las Naciones Unidas sobre la Eliminación de todas las Formas de Discriminación Racial, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>.

Denuncias por parte del usuario

- Con la enorme cantidad de contenido que se carga y se comparte por segundo, los usuarios pueden ser los primeros en detectar contenido problemático.
- Las políticas deben motivar a las entidades con funciones de intermediarios que muestran contenido generado por el usuario a ofrecer un medio sencillo para que los usuarios denuncien contenido problemático.

5 Puntos destacados: consideraciones de políticas para funciones de intermediarios específicas

En esta sección, nos basamos en las consideraciones de políticas mencionadas anteriormente. Los “Puntos destacados” identifican casos específicos que ameritan un análisis más profundo. En el Anexo de este documento se describe información más detallada sobre la gama completa de las funciones de intermediarios.

5.1 Punto destacado: consideraciones de políticas para las plataformas de “medios sociales” que alojan, seleccionan y moderan contenido generado por el usuario

Gran parte de la atención de las políticas públicas globales puesta en las entidades que alojan contenido generado por los usuarios se ha centrado en una pequeña cantidad de “plataformas” muy grandes, en particular sitios de medios sociales utilizados por muchos usuarios en todo el mundo. Muchas de estas inquietudes *no* están relacionadas directamente con las protecciones de los intermediarios que cubren contenido generado por el usuario. En cambio, los formuladores de políticas están preocupados por asuntos, tales como la recopilación y el uso de datos personales de los usuarios por parte de una entidad, las prácticas publicitarias, la discriminación, la falta de transparencia y control del usuario, y las técnicas para retener la participación continua de los usuarios en la plataforma, por mencionar algunos temas polémicos de la actualidad. Ninguna de estas cuestiones tiene nada que ver con

el objetivo general de las protecciones de los intermediarios: proteger y fomentar la participación individual en Internet. No es correcto abordar estas cuestiones eliminando o imponiendo condiciones a las protecciones intermedias.

Desde la perspectiva de las protecciones de los intermediarios, una plataforma de medios sociales grande que aloja contenido generado por el usuario, en esencia, no difiere de un sitio web pequeño que aloja contenido generado por el usuario. Ninguno de ellos podría operar si fuera responsable de contenido difamatorio, acosador o ilegal publicado por sus usuarios. Existen formas más efectivas de abordar el contenido problemático que evitan exponer a los intermediarios a la responsabilidad por el contenido generado por el usuario (descritas en la sección 4.3 anterior). Ambos tipos de intermediarios necesitan protecciones sólidas para desempeñar las funciones de intermediarios que conlleva el alojamiento de contenido generado por el usuario. Un sitio web pequeño no tiene los recursos para revisar previamente todo el contenido generado por el usuario y no puede operar si se arriesga a enormes amenazas de responsabilidad. Una plataforma muy grande tiene limitaciones similares aunque tenga más recursos debido a la enorme cantidad de contenido generado por el usuario (en múltiples idiomas) que millones de usuarios suben cada minuto.

Sin embargo, las protecciones de los intermediarios frente a la responsabilidad por el contenido generado por los usuarios no significan que los formuladores de políticas carezcan de poder para tratar inquietudes importantes en materia de política pública. Por ejemplo, si la preocupación es que una plataforma selecciona contenido de manera sistemática y discriminatoria para los usuarios, entonces se podrían aplicar a la plataforma leyes de no discriminación existentes o nuevas. Si la cuestión es porque una plataforma está diseñando su interfaz de usuario para intentar que los usuarios se vuelvan “adictos” a la plataforma, entonces se podrían emplear leyes de salud o de protección al consumidor para proteger a los usuarios de ser expuestos a una interfaz que sea perjudicial para su salud o que los someta a manipulación. Si la preocupación es que una plataforma hace mal uso de los datos personales de sus usuarios, entonces se podrían aplicar leyes de privacidad y protección de datos para sancionar y disuadir esas prácticas. Si es que una plataforma está haciendo un mal uso de los datos personales de sus usuarios, entonces se podrían aplicar leyes de privacidad y protección de datos para castigar y disuadir esas prácticas. Si se trata de que una plataforma está engañando a sus usuarios acerca de su servicio, se pueden aplicar leyes antifraude.

Existen riesgos en *todos* los lugares de reunión para la interacción social, ya sea en línea o fuera de línea. A pesar de las mejores intenciones, la interacción social de los niños en un patio de juegos a veces puede implicar acoso y otros comportamientos no deseados. Las interacciones sociales en persona entre compañeros de trabajo a veces pueden implicar acoso. El ecosistema en línea puede exacerbar y mitigar simultáneamente algunos de los problemas: la falta de interacción física directa puede aumentar la cantidad de acoso o intimidación, pero puede presentar oportunidades de apoyo entre pares. Además, el espacio en línea contiene una gran cantidad de lugares para la interacción social, por lo que las personas pueden abandonar un espacio en línea excesivamente tóxico y unirse a uno en el que haya más compañerismo.

Un área importante de preocupación es el uso de algoritmos por parte de las plataformas para elegir y mostrar contenido a los usuarios. Los formuladores de políticas han identificado el riesgo de que los algoritmos puedan utilizarse para manipular el comportamiento de los usuarios con efectos adversos, discriminarlos o difundir contenidos ilegales o dañinos. Sin embargo, siempre se han utilizado algoritmos en las plataformas de medios sociales y se están empleando en un número cada vez mayor de otros sitios web, y son esenciales para su funcionamiento. El gran volumen de contenido compartido en Internet ha causado que se produzca una dependencia cada vez mayor en algoritmos que clasifican y muestran contenido de manera automática. Los algoritmos buscan contenido erróneo o malicioso. Los algoritmos mejoran los sitios web de comercio electrónico y administran el contenido que se muestra en las plataformas de medios sociales. Asimismo, los algoritmos son vitales para aumentar la accesibilidad y convertir la voz en subtítulos de texto para individuos sordos y con dificultades auditivas.⁴²

Nuestro aviso a los formuladores de políticas es que recuerden que, si bien los algoritmos no son problemáticos *per se*, sí puede ser problemática la forma en que se utilizan. Por ejemplo, un algoritmo que produce sistemáticamente resultados discriminatorios contra miembros de clases protegidas, como la raza o la religión, es un objetivo legítimo para la formulación de políticas. El objetivo debe ser diseñar políticas que aborden el problema directamente y, al mismo tiempo, permitan el uso apropiado de la moderación y selección algorítmica.

42 Para tener un debate más detallado de estos asuntos, consulte el escrito Amicus Curiae de Internet Society (ISOC) en *Gonzalez v. Google LLC*, 598 US 617 (2023), disponible en <https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf>.

5.2 Punto destacado: consideraciones de políticas para redes federadas que habilitan nuevos enfoques para facilitar la participación del usuario.

Las “redes federadas” han ganado cada vez más atención en los últimos años. Las destacamos porque tienen un enfoque más descentralizado respecto del alojamiento, el intercambio, la selección y la moderación de contenido generado por el usuario que las plataformas de medios sociales más tradicionales. En lugar de que una sola entidad controle una comunidad de medios sociales, por ejemplo, las tecnologías federadas pueden permitir que muchas comunidades más pequeñas se conecten y compartan contenido en todo el ecosistema federado. Esto crea una experiencia social similar, pero con un enfoque más local hacia la moderación.

Los servicios “federados” han estado en las noticias recientemente porque algunos ahora compiten más directamente con algunas de las empresas y plataformas de redes sociales más grandes. Un ejemplo es Mastodon, basado en el protocolo ActivityPub del World Wide Web Consortium.⁴³ Las funciones de Mastodon son directamente análogas al potencial de discusión global de tipo Twitter/X. Sin embargo, una diferencia importante es que Mastodon es una colección de servidores operados por diferentes entidades que han elegido participar en la red federada, en lugar de ser un conjunto de servidores controlados por una compañía. Es importante destacar que cada servidor individual que participa en la red federada Mastodon puede establecer y controlar sus propias reglas de moderación de contenido.⁴⁴

Si bien los medios sociales federados han sido un tema importante hace poco, los servicios federados no son un fenómeno nuevo en Internet. Por ejemplo, el correo electrónico de Internet utiliza un modelo federado: millones de entidades operan sus propios servidores de correo separados para su compañía, organización, universidad o incluso hogares. Detrás de escena, estos servidores federados emplean protocolos de correo electrónico para enviar y recibir correos electrónicos entre sí sin problemas, sin ningún acuerdo previo.

43 <https://www.w3.org/TR/activitypub/>.

44 Mastodon ganó popularidad rápidamente después de que X cambiara de manera drástica sus políticas de moderación de contenido. Mastodon permite a los usuarios tener más control sobre el contenido que ven y los otros usuarios con los que interactúan. Se trata de un enfoque distribuido de los medios sociales que permite a entidades más pequeñas e incluso a individuos alojar medios sociales generados por los usuarios, tomar decisiones sobre qué contenido permitir o no en su propio servidor y con qué otros servidores de Mastodon conectarse.

En el área de los medios sociales, estas redes federadas emergentes tienen el potencial de democratizar el alojamiento de los medios sociales. Ofrecen la posibilidad de seleccionar y moderar el contenido de manera mucho más detallada y más cercana al usuario final participante. El modelo distribuido requiere muchos servidores de Mastodon y ha dado lugar a una nueva función de intermediarios: alojar un servidor de Mastodon, el equivalente de Mastodon de un proveedor de servicios de correo electrónico o de alojamiento web.⁴⁵ Significativamente, el éxito actual de las redes federadas de medios sociales impulsó a Meta a explorar la posibilidad de permitir que sus usuarios de Threads compartan sus publicaciones con otros servidores compatibles con ActivityPub, que llegaba así a los usuarios de Mastodon.⁴⁶

Nos preocupa que las redes federadas puedan verse perjudicadas involuntariamente por regulaciones o leyes que no estén diseñadas teniendo en cuenta la forma en que las redes federadas modernas encajan en el panorama de los “medios sociales”. Nos preocupa que las redes federadas puedan verse perjudicadas involuntariamente por regulaciones o leyes que no estén diseñadas teniendo en cuenta cómo las redes federadas modernas encajan en el panorama de las “medios sociales”. Como ejemplo posible, si un país promulgara legislación en materia de “servicios de medios sociales” con la intención de llegar a las plataformas más grandes, esa terminología bien podría aplicarse a toda la red federada del sistema Mastodon y sus miles de servidores cooperadores. Una ley dirigida a las compañías tecnológicas más grandes podría terminar afectando, y perjudicando, a un conjunto totalmente diferente de entidades.

Nuestra recomendación para los formuladores de políticas que buscan regular las plataformas de medios sociales es que sean cuidadosos y conscientes del posible impacto que una norma o regulación propuesta tendría en las redes federadas. Sin esa precaución, puede dañarse involuntariamente a las redes federadas que ofrecen una alternativa a las plataformas de medios sociales más grandes.

45 Por ejemplo, el proveedor de SaaS Cloudflare ofrece un producto: “Welcome to Wildebeest: The Fediverse on Cloudflare” (Bienvenido a Wildebeest: el fediverso de Cloudflare), The Cloudflare Blog, 2 de agosto de 2023, <https://blog.cloudflare.com/welcome-to-wildebeest-the-fediverse-on-cloudflare>.

46 Threads ha entrado en el fediverso, Engineering at Meta Blog, 21 de marzo de 2024, <https://engineering.fb.com/2024/03/21/networking-traffic/threads-has-entered-the-fediverse/>.

5.3 Punto destacado: consideraciones de políticas para el ecosistema de juegos interactivos en línea

Los juegos en línea han recibido especial atención por parte de las políticas públicas porque muchos de sus usuarios son niños y adolescentes. Por ejemplo, en 2011, en Corea del Sur, se aprobó (pero posteriormente se derogó) la Ley de Revisión de Protección Juvenil, que restringía las horas en que los niños menores de 16 años podían jugar videojuegos en línea y bloqueaba el acceso entre la medianoche y las 6 a.m.⁴⁷ En 2019, en China, se restringió el tiempo de juego de los menores a 90 minutos por día y se les prohibió jugar juegos en línea entre las 10 p.m. y las 8 a.m.. En 2021, se impusieron más restricciones.⁴⁸ Las preocupaciones van desde la adicción hasta el comportamiento similar al juego, la exposición a contenido inapropiado, el contacto con extraños y las violaciones de la privacidad.

Los juegos en línea suelen ser interactivos con otros usuarios y, con frecuencia, tienen características que permiten a los usuarios comunicarse entre sí en tiempo real. Las herramientas de comunicación de juegos más comunes son las funciones de audio y mensajería, pero existen muchos más métodos sutiles de comunicación: elegir y modificar avatares, comportamientos particulares durante el juego e intercambio de puntos, calificaciones y otros logros. Algunos juegos en línea también permiten a los usuarios cargar y compartir modificaciones al juego. Los juegos en línea también han inspirado nuevos géneros de participación en otras plataformas, como YouTube y Twitch, y el campo de los deportes electrónicos.⁴⁹

Nuestro consejo a los formuladores de políticas es que tengan en cuenta las funciones de intermediarios desempeñadas por las plataformas de juegos interactivos en línea. En la actualidad, la mayoría de los sistemas de juegos interactivos conectados a Internet, ya sea con o sin consola de hardware, permiten un amplio abanico de “contenido generado por el usuario”: este va desde simples conversaciones entre jugadores hasta módulos complementarios desarrollados por jugadores que completan

47 Posteriormente, en 2021, la ley se derogó. Consulte https://en.wikipedia.org/wiki/Shutdown_law.

48 China mantiene un límite diario de una hora para que los niños jueguen en línea, Associated Press, Zen Soo, 19 de enero de 2023 <https://apnews.com/article/gaming-business-children-00db669defcc8e0ca1fc2dc54120a0b8>.

49 Para obtener más información sobre los deportes electrónicos, consulte Wikipedia en <https://en.wikipedia.org/wiki/Esports>.

y amplían el entorno de juego. Las plataformas de juegos interactivos cumplen funciones de intermediarios y los principales regímenes de protección de los intermediarios se aplican de igual modo al ecosistema de juegos.

Sin embargo, como se señala en nuestro punto destacado anterior sobre las plataformas de medios sociales, los formuladores de políticas tienen la autoridad para abordar las prácticas dañinas. Por ejemplo, si la inquietud es que algunas de las llamadas “cajas de recompensas” en un juego constituyen prácticas engañosas o juegos de azar ilegales, las leyes de protección al consumidor o de juegos de azar ilegales deben aplicarse directamente a tales conductas.

5.4 Punto destacado: consideraciones de políticas para los sistemas de realidad virtual y realidad aumentada conectados a Internet

Los productos de realidad virtual (RV) y realidad aumentada (RA) se están integrando rápidamente al ecosistema de Internet. Si bien los propósitos de la RV y la RA son diversos, a menudo, se utilizan como parte de un sistema de comunicaciones interactivo.⁵⁰ Algunos de estos sistemas requieren un dispositivo especializado, como gafas, guantes o auriculares, pero a otros se puede acceder con un teléfono inteligente.

Al igual que ocurre con el ecosistema de juegos, los sistemas de RV y RA conectados a Internet suelen admitir “contenido generado por el usuario”, incluida una amplia gama de comunicaciones de usuario a usuario.⁵¹ Por ende, al igual que en el caso de los juegos, la mayoría de los principales regímenes de protección de intermediarios podrían aplicarse a los sistemas de RV y RA.

Desde una perspectiva de las políticas, los sistemas de RV y RA se superponen considerablemente con los medios sociales y otros servicios de comunicación de uno a uno o de uno a muchos. Sin embargo, la RV y la RA plantean desafíos adicionales en materia de políticas, como los siguientes:

50 Una visión de cómo se puede usar la realidad virtual es el “metaverso”, descrito por primera vez en la novela de ciencia ficción “Snow crash” de 1992 escrita por Neal Stephenson. En su visión, el metaverso es un espacio de realidad virtual en el que los usuarios pueden interactuar entre ellos con el uso de un avatar en un entorno tridimensional gestionado por computadora.

51 Por su naturaleza, los sistemas de RV y RA pueden admitir un gran conjunto de herramientas de comunicación: escritas, habladas y no verbales, como movimientos de cabeza y manos, expresiones faciales, orientación corporal, proximidad y postura.

- La configuración y el uso de avatares representativos pueden generar, al menos, en la percepción, una conexión más estrecha entre la identidad real del individuo y su identidad en la realidad virtual.
- Algunos sistemas de RA se pueden usar en cualquier lugar del espacio físico, superponiendo elementos virtuales en el entorno físico. En teoría, estos sistemas pueden provocar daños directos en el mundo físico, como accidentes de tráfico o lesiones personales.⁵²
- Los sistemas de RA pueden atraer al entorno aumentado a personas que no están en línea y que no han dado su consentimiento.

Al igual que con los medios sociales y los juegos en línea, nuestro consejo a los formuladores de políticas es que los asuntos sobre cuestiones como la privacidad, la adicción del usuario y la seguridad personal se resuelven mejor mediante la implementación de leyes existente en esas áreas en lugar de modificar las protecciones de los intermediarios o de tratar de elaborar un nuevo conjunto de políticas específicas para la RV y la RA.

5.5 Punto destacado: consideraciones de políticas para las funciones de intermediarios que habilitan la publicidad en Internet

El contenido publicitario es un tipo especial de contenido en línea. Si bien suele aparecer junto con contenido generado por el usuario, en general, no es una contribución de los individuos. Algunos anuncios pueden considerarse contenido original del sitio, por ejemplo, un anuncio de una cena especial de Año Nuevo en el sitio web de un restaurante. Sin embargo, la gran mayoría del contenido publicitario que se muestra en Internet es contenido creado por entidades que no son los propietarios del sitio web con el objetivo publicitario específico y se ubica para obtener ingresos por publicidad. Este tipo de contenido suele estar integrado y ser dinámico.

La posibilidad de mostrar contenido publicitario en Internet ha permitido a las compañías ofrecer sus servicios por poco o ningún costo monetario y a los individuos a ganar dinero a través de sitios donde los usuarios generan contenido y lo comparten. Algunos sostienen que el sistema de anuncios publicitarios debe protegerse de toda responsabilidad porque sin la publicidad “que paga las cuentas”, Internet tendría muchos menos

52 Consulte, por ejemplo, el Pokémon Go Death Tracker en <https://pokemongodeathtracker.com/>.

servicios y funciones, y menos participación individual. Sin ingresos por publicidad, más servicios impondrían una tarifa por su uso, lo que, por ende, aumentaría la brecha digital.

Otros consideran que el sistema publicitario, en particular, el sistema de publicidad conductual, es muy problemático y debería restringirse significativamente. Creen que la publicidad dirigida explota las protecciones de privacidad que son insuficientes, porque permite que los servicios en línea y la industria se beneficien económicamente del contenido generado por los usuarios y de las interacciones en línea.

A raíz de la naturaleza global de Internet, el alcance y el impacto de la publicidad en línea pueden ser mucho mayores que los de la publicidad en periódicos, radio y televisión. Los anuncios en línea pueden adaptarse y dirigirse a un usuario particular o a grupos muy pequeños de personas en función del tiempo, la ubicación física y el contexto. Los anunciantes y el ecosistema de compañías que sostienen los anuncios publicitarios en línea rastrean a los usuarios en todos los dispositivos e incluso en el mundo real.

Más allá de los debates sobre el sistema publicitario actual, el sistema publicitario depende sin duda alguna de las protecciones de responsabilidad de los intermediarios en algunos contextos.⁵³ En el extremo visible de los sistemas publicitarios (los sitios web y los servicios donde se muestran los anuncios) es muy posible que haya protecciones de intermediarios. En la mayoría de los servicios, la esencia de los anuncios que se muestran junto al contenido generado por el usuario está fuera del control del usuario y, por lo general, ni siquiera lo controla el propietario del sitio web. Técnicamente, el contenido publicitario que se muestra en un sitio web *no* suele estar alojado en la infraestructura del servicio, sino en un servidor administrado por la red publicitaria.

Nuestro consejo a los formuladores de políticas es que procedan con cuidado en la elaboración de regulaciones para el ecosistema publicitario debido al difícil equilibrio entre los beneficios esperados y los daños potenciales. El ecosistema publicitario en línea desempeña un papel importante, ya que permite un acceso extendido a la posibilidad de expresión, pero al mismo tiempo plantea cuestiones de políticas sobre la privacidad, la segmentación inapropiada y la desinformación. Pero, como ocurre con cualquier otra función de intermediarios, eso no

53 El funcionamiento interno de los sistemas de publicidad en línea es poco transparente, con múltiples entidades interconectadas e independientes que trabajan en conjunto, tanto de forma explícita como implícita. Desentrañar estos sistemas para comprender cómo pueden aplicarse las protecciones de responsabilidad de los intermediarios está mucho más allá del alcance de este documento.

significa que un gobierno no pueda regular los sistemas publicitarios de manera directa. Por ejemplo, en la Unión Europea, la primera Directiva sobre el Comercio Electrónico impuso directamente algunos requisitos específicos de transparencia sobre los anuncios en línea y la más reciente Ley de Servicios Digitales amplió significativamente esas exigencias de transparencia y prohibió determinadas técnicas de diseño que buscaban manipular o engañar a los usuarios.

5.6 Punto destacado: consideraciones de políticas para pagos y otras retribuciones económicas para el contenido generado por el usuario contemplado en los principios de intermediarios de Internet

El sistema de publicidad en Internet apunta a una cuestión mucho más amplia: si las protecciones de los intermediarios son apropiadas para contemplar el contenido por el cual se transfirió dinero u otra forma de valor económico como parte de la colocación de contenido en un sitio web. El tema puede plantearse en distintos escenarios:

- Si un sitio web contiene artículos escritos por usuarios, pero solo lo hace si un usuario paga al sitio web para que incluya el artículo, ¿el sitio web debiera tener protección de la responsabilidad por el contenido por el cual recibió el pago? ¿Qué pasa si el pago es ínfimo? ¿Qué sucede si el monto es elevado?
- Si un sitio web paga a un proveedor de contenido (como a un “influencer” conocido u otra figura) para publicar contenido en el sitio web, ¿el sitio web debiera tener alguna responsabilidad legal por el contenido por el cual pagó y, luego, alojó? ¿El monto de los pagos marcaría alguna diferencia en el análisis?
- Si un sitio web comparte los ingresos publicitarios con el proveedor de contenido, ¿esto cambia la relación y la responsabilidad del sitio web?⁵⁴

54 Por ejemplo, YouTube tiene un sistema ampliamente abierto para todos sus usuarios que publican videos en el sitio. A cambio del permiso para publicar anuncios junto a los videos de un usuario, YouTube obtendrá una parte de los ingresos publicitarios que deriven de los anuncios colocados. Si los videos de los usuarios son muy populares, recibirán ingresos por los anuncios, a veces, esto representa un monto sustancial. En la actualidad, algunos creadores de contenido obtienen sus ingresos o los complementan significativamente gracias a los pagos de YouTube. Si YouTube fuera responsable de los videos por los que se paga a los usuarios, ¿podría seguir ofreciendo los pagos?

- Si la relación comercial entre anunciantes y sitios web elimina protecciones y hace al operador del sitio web responsable del contenido de los anuncios, ¿cómo afectaría esto al sistema publicitario? ¿Podría perjudicar a los sitios web que reciben una cantidad modesta de ingresos proveniente de un nivel de publicidad bajo?
- Si se eliminaran las protecciones de responsabilidad de las funciones de los intermediarios por el alojamiento de contenido generado por el usuario que se creó a cambio de una compensación económica, ¿eso causaría impactos económicos, sociales o técnicos en el mercado del contenido? ¿Las compañías producirían alternativas artificiales o con menos obligaciones para evitar la responsabilidad?⁵⁵
- Si el mercado de contenido pago está dominado por unas pocas entidades que están plenamente integradas horizontal y verticalmente en todos los servicios en línea, ¿de qué manera esto perjudica el panorama competitivo del contenido?

En el contexto de los Estados Unidos, los pagos por contenido en cualquier dirección generalmente no tienen ningún impacto en las protecciones de los intermediarios.⁵⁶ Las preguntas que planteamos anteriormente ayudan a mostrar las complejidades, las ventajas y las desventajas que surgen si nos centramos en la compensación económica.

5.7 Punto destacado: el impacto de los diversos niveles de protección del derecho de libertad de expresión a escala nacional

Para comprender y elaborar políticas relacionadas con las protecciones frente a la responsabilidad de las funciones de los intermediarios, es importante reconocer la influencia que las protecciones jurídicas nacionales para la libertad de expresión y el discurso tendrán sobre las políticas que pueden afectar la capacidad de los individuos de comunicarse en línea, ya sea al compartir su propio contenido o el de otros.

⁵⁵ Por ejemplo, ¿buscarían evitar la responsabilidad mediante la compensación a determinados creadores de contenido por “tener una cuenta” en lugar del contenido que producen? u ¿ofrecerían otros servicios y suscripciones de forma gratuita?

⁵⁶ Las propuestas para eliminar las protecciones contempladas en la ley estadounidense para ciertos tipos de publicidad pagada no han tenido éxito.

Existen protecciones significativamente diferentes en cuanto a la libertad de expresión y de opinión en distintos países del mundo, y esas diferencias afectan las opciones de políticas disponibles dentro de un país. Algunos países establecen el derecho a la libertad de expresión en sus constituciones, entre ellos, Brasil,⁵⁷ Ecuador,⁵⁸ Japón,⁵⁹ Perú⁶⁰ y Estados Unidos.⁶¹ Otros países y jurisdicciones tienen menos restricciones respecto de la capacidad del gobierno para, por ejemplo, exigir que las compañías privadas tomen medidas que restrinjan o prevengan ciertos tipos de discurso. Otros, pueden priorizar distintos objetivos de políticas, como la privacidad por encima de la libertad de expresión o la cohesión social por encima de los derechos individuales. La existencia de diferentes regímenes nacionales puede explicar, en cierta medida, los distintos enfoques nacionales respecto de la protección frente a la responsabilidad de los intermediarios. Un ejemplo de diferentes enfoques impulsados por leyes constitucionales o nacionales son los regímenes de “notificación y eliminación de contenido”, que se utilizan en la Unión Europea y en algunos otros países para exigir que se borre contenido en línea. Este tipo de obligación enfrentaría serios desafíos constitucionales si se implementara en países con derechos a la libertad de expresión o de opinión consolidados, como Estados Unidos.⁶²

Nuestro consejo a los formuladores de políticas es que comprendan cuidadosamente las restricciones a las regulaciones de la libertad de expresión impuestas por las leyes constitucionales y jurídicas nacionales, así como por las convenciones y los acuerdos internacionales vigentes en materia de libertad de expresión.

57 Consulte el Artículo 5 de la Constitución de la República Federativa de Brasil, disponible en https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

58 Consulte el Artículo 66, inciso 6 de la Constitución del Ecuador, disponible en https://www.gob.ec/sites/default/files/regulations/2018-11/constitucion_de_bolsillo.pdf.

59 Consulte el Artículo 21 de la Constitución de Japón, disponible en https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

60 Consulte el Artículo 2, inciso 4 de la Constitución Política del Perú, disponible en <https://www.congreso.gob.pe/constitucionyreglamento/>.

61 Consulte la Primera Enmienda de la Constitución de los Estados Unidos, disponible en <https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say>.

62 Los regímenes de “Notificación y eliminación de contenido” han quedado considerablemente sujetos a abuso y uso indebido. Consulte, p. ej., “Warning: repressive regimes are using DMCA takedown demands to censor activists” (Advertencia: los regímenes represivos usan demandas de eliminación de contenido de DMCA para censurar activistas), 13 de enero de 2023, disponible en <https://www.accessnow.org/dmca-takedown-demands-censor-activists/>; “Notice and Takedown Mechanisms: Risks for Freedom of Expression Online” (Mecanismos de notificación y eliminación de contenido: riesgos para la libertad de expresión en línea) 7 de septiembre de 2020, disponible en https://www.eff.org/files/2020/09/04/mcsherry_statement_re_copyright_9.7.2020-final.pdf; “Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech” (Problemas de eliminación de contenido de campañas: cómo los reclamos por copyright con falta de mérito amenazan el discurso político en línea), septiembre de 2010, disponible en https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf.

Más allá de estas cuestiones, si un país quiere respaldar la participación de sus ciudadanos en conversaciones en línea e iniciar esfuerzos empresariales para crear nuevos servicios en línea, debe adoptar medidas de protección para las funciones de los intermediarios a fin de garantizar que los servicios de Internet puedan incluir la opinión de los usuarios sin riesgos de responsabilidad significativos.

5.8 Punto destacado: diferenciación de la protección de la responsabilidad de intermediarios y la legislación, y políticas de derecho de autor

En muchos países y regiones, incluidos Estados Unidos⁶³ y la Unión Europea⁶⁴, existen enfoques jurídicos distintos que cubren las protecciones de los intermediarios frente a la responsabilidad por el “contenido generado por el usuario”, de manera diferente a la del “uso por parte de terceros de contenido protegido por derechos de autor”. En el caso del contenido generado por el usuario, el cuestionamiento jurídico es si el contenido en sí es ilegal o causa perjuicio. En el caso de los derechos de copyright, las cuestiones legales pertinentes son si quien publica el contenido (a) es el propietario del copyright, (b) tiene una licencia para publicar el contenido o (c) está protegido, de alguna manera, por el “uso justo” u otras restricciones que impone la ley de copyright. Este documento se centra en el primer panorama y no en el contenido que infringe el copyright.

Muchas leyes específicas sobre copyright contienen requisitos de notificación y eliminación según los cuales el propietario del copyright puede notificar a una compañía de alojamiento sobre contenido cubierto por copyright. Tras el aviso, el host tiene un tiempo determinado para eliminar el contenido especificado. El abordaje centrado en el copyright, que generalmente no requiere una orden judicial, a veces ha dado lugar a abusos, ya que las personas utilizan notificaciones de eliminación de contenido por copyright para impedir la expresión legítima. Por el contrario, como se señala en la Sección 3.5, típicamente, los pocos países que han adoptado un enfoque de notificación y eliminación de contenido problemático generado por el usuario han exigido una orden judicial.

63 Consulte la Ley de Derechos de Autor del Milenio Digital, Código de EE. UU. 17 § 512, disponible en <https://www.law.cornell.edu/uscode/text/17/512>.

64 Consulte el Artículo 17 de la Directiva de la UE sobre Derechos de Autor (Directiva sobre Derechos de Autor en el Mercado Único Digital), disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ.L:2019:130:TOC.

5.9 Punto destacado: inteligencia artificial

Tras el lanzamiento de servicios de IA generativa centrados en el consumidor⁶⁵, una pregunta común que ha surgido entre los formuladores de políticas es si las protecciones de los intermediarios se aplican a los servicios que utilizan inteligencia artificial (IA) y en qué medida. La IA es un término muy amplio que abarca todo, desde algoritmos bastante simples hasta redes neuronales artificiales. Las herramientas de IA pueden realizar tareas específicas (p. ej., reconocer imágenes), reaccionar a situaciones específicas (p. ej., filtrar elementos no deseados, aumentar la eficiencia del enrutamiento) y aprender y adaptar respuestas (p. ej., interactuar con usuarios como chatbots). La IA ya está presente en todo el ecosistema de Internet, desde el enrutamiento del tráfico de Internet hasta la búsqueda y localización de páginas web y la gestión de miles de millones de elementos de contenido.

En el marco del contenido en línea, existen al menos tres aspectos de la IA que valen la pena destacar. El primero se refiere al uso de la IA en la prestación de servicios en línea. Durante muchos años, se han empleado diversos tipos de IA para brindar servicios en línea. Por ejemplo, la tecnología utilizada para seleccionar y compilar el contenido que se mostrará a los usuarios incluye aspectos de IA desde, al menos, 2006.⁶⁶ El uso de la IA en la búsqueda en línea se remonta aún más atrás.⁶⁷ Como se analiza más arriba en este documento y en el Anexo, por lo general, las leyes de protección de intermediarios protegen actividades que incluyen la selección, el filtrado, la evaluación, la elección y la búsqueda de contenido. Es probable que estas protecciones tengan efecto independientemente de si la tecnología incluye un componente de IA.

Un segundo aspecto, más nuevo, se relaciona con las respuestas generadas por IA a las búsquedas de información de los usuarios: si el resultado de la IA entrenada con grandes cantidades de contenido generado por el usuario debe considerarse en sí mismo “contenido generado por el usuario”. Las opiniones difieren en cuanto a cuándo el contenido generado por IA debe caracterizarse como “contenido creado por otros” y, por lo tanto, estar amparado en virtud de las

65 Para obtener una explicación de la IA generativa, consulte Wikipedia en https://en.wikipedia.org/wiki/Generative_artificial_intelligence.

66 Consulte Cait McNamara, “The Evolution of AI on Social Media” (La evolución de la IA en los medios sociales), mayo de 2024, disponible <https://favola.co.uk/the-evolution-of-ai-on-social-media/>.

67 Consulte Dan Katcher, “The Evolution of AI Search: Past, Present, Future” (La evolución de la búsqueda con IA: pasado, presente y futuro), 12 de febrero de 2024, disponible en <https://www.rocketfarmstudios.com/blog/the-evolution-of-ai-search-past-present-future/>.

protecciones de los intermediarios frente a la responsabilidad. Pese a que algunos resultados de dichos servicios de IA pueden incluir contenido específico generado por el usuario, la totalidad de esos resultados puede considerarse contenido nuevo creado por el servicio.

Un tercer aspecto de la IA que se está analizando activamente es si la responsabilidad de producir contenido ilegal o ilícito debe recaer en los servicios de IA que producen texto, imágenes, sonido o videos en respuesta a solicitudes de los usuarios. Estos tipos de servicios de IA evidentemente pueden posibilitar la creatividad del usuario individual, pero también se puede argumentar que el servicio de IA es un cocreador del contenido resultante.

Con este documento, no se pretende resolver estas preguntas ni ofrecer recomendaciones de políticas detalladas sobre el tratamiento de los servicios basados en IA. Estas no son preguntas fáciles de responder y, probablemente, sea necesario dedicarles algún tiempo y un análisis minucioso para desarrollar enfoques apropiados para las políticas. La IA ofrece un enorme potencial para avances en el campo de la medicina, las ciencias e incluso la creatividad, y las protecciones para los servicios basados en IA pueden ser apropiadas. Sin embargo, algunos servicios de IA pueden crear riesgos importantes para la sociedad y pueden justificar regulaciones.

Al igual que con todos los demás tipos de formulación de políticas analizados en este documento, Internet Society recomienda que las intervenciones a las políticas para el abordaje de la IA tengan un alcance y una dirección cuidadosamente definidos. Sin esa precaución, las regulaciones o las restricciones demasiado amplias en materia de IA podrían tener un impacto negativo en otros usos contemplados de las funciones de los intermediarios que facilitan la comunicación de las personas en Internet.

6 Conclusión

Este documento proporciona un marco para comprender las funciones de los intermediarios de Internet y desarrollar políticas relativas a la responsabilidad por el contenido en línea. Nuestro objetivo es proporcionar información a los formuladores de políticas a fin de que puedan elaborar políticas para preservar lo que, según Internet Society, son las características más importantes de Internet: la apertura, la conexión global, la seguridad y la confiabilidad. Internet es cada vez más importante para la vida de las personas y la prosperidad socioeconómica. Mientras los responsables de las políticas abordan preocupaciones sociales legítimas sobre el contenido en línea, es fundamental que las políticas garanticen que Internet pueda seguir siendo un recurso positivo para la comunicación, la educación y el discurso globales.

La responsabilidad por el contenido generado por los usuarios es un tema que ha crecido a la par del crecimiento de Internet, que se convirtió en un medio de comunicación esencial para las sociedades modernas. Para la existencia de una Internet saludable, sigue siendo necesario aproximarse a las políticas que brindan protección de responsabilidad para los diferentes tipos de funciones de intermediarios que posibilitan la comunicación a través de Internet. Al mismo tiempo, existe una variedad de herramientas políticas para abordar las preocupaciones en línea sin perjudicar la participación individual en Internet.

Observamos cinco estrategias clave que los formuladores de políticas deben seguir al momento de diseñar políticas centradas en Internet:

1. Definir cuidadosamente el alcance de la formulación de políticas para lograr los objetivos. Utilizar el conjunto más limitado de políticas posible para controlar y mitigar directamente el problema.
2. Siempre que sea posible, utilizar las herramientas políticas existentes para abordar preocupaciones específicas. Las leyes en materia de privacidad, antidiscriminación, protección del consumidor y otras ya ofrecen formas de proteger a los usuarios y mejorar la responsabilidad en línea.
3. Mantener o, cuando aún no existan, crear protecciones de responsabilidad para las funciones que posibilitan las comunicaciones en Internet. Esto es de especial importancia para aquellas funciones que permiten el funcionamiento de Internet, pero también para aquellas que interactúan más directamente con

las comunicaciones de los usuarios, tales como el alojamiento y la visualización de contenido. Sin estas protecciones, Internet no puede seguir siendo un medio para comunicarse.

4. Proteger de toda responsabilidad a las entidades que prestan funciones de selección y moderación de contenido generado por el usuario. La escala de Internet exige selección y moderación. Con la transparencia adecuada, una entidad que aloja contenido generado por el usuario debe poder seleccionar y moderar tanto de forma automática como manual sin temor a incurrir en cargos por responsabilidad.
5. Trabajar con las partes interesadas de Internet (incluida la sociedad civil, las comunidades académicas y técnicas, las compañías y los ciudadanos) para realizar una “Evaluación de impacto en Internet” de las políticas propuestas con el fin de ayudar a comprender las posibles consecuencias o efectos no deseados en Internet o en sus usuarios.

Internet Society se esfuerza por colaborar y trabajar con los gobiernos de todo el mundo para asistir en la elaboración de políticas que aborden las preocupaciones sociales y, al mismo tiempo, sostengan Internet. Trabajamos para respaldar el desarrollo de Internet como una infraestructura técnica global, un recurso para enriquecer la vida de las personas y una fuerza para impulsar algo positivo en la sociedad. Agradecemos los debates sobre las oportunidades, los desafíos y las preocupaciones que enfrentan los formuladores de políticas en el ecosistema de Internet y las formas de abordarlos.

Anexo – Funciones de los intermediarios

Este anexo a “Un marco de políticas para los intermediarios de Internet” (“Marco de políticas”) describe, en detalle, la gama de funciones de los intermediarios necesarias para que las comunicaciones fluyan a través de Internet. Para cada una de estas funciones, ofrecemos enfoques de políticas recomendadas.

Nos centramos principalmente en la protección de la responsabilidad de los intermediarios. Sin embargo, como se indica en la sección 4.3 del Marco de políticas,¹ también existen otros enfoques de políticas que pueden aplicarse para abordar las inquietudes sobre políticas relativas a las funciones de los intermediarios, como las leyes de protección de la privacidad y del consumidor.

Para ayudar a organizar estos enfoques de políticas recomendados, hemos agrupado las funciones de los intermediarios en ocho secciones diferentes (tal como se indica en el índice).

¹ Marco de políticas Sección 4.3, Principios legales y de políticas específicos que se pueden aplicar a las funciones de los intermediarios sin perjudicar las comunicaciones de Internet.

1 Transmisión de paquetes de datos

Esta sección describe las funciones de los intermediarios más básicas y fundamentales que intervienen en la transmisión de las comunicaciones a través de Internet: la transmisión de datos por cable o de manera inalámbrica.

- **La sección 1.1** describe la función de proporcionar un medio de comunicación para las comunicaciones a través de Internet.
- **La sección 1.2** describe la función de proporcionar una ruta de comunicación a través de un medio de comunicación.
- **La sección 1.3** describe la función de proporcionar servicios troncales o de tránsito que permiten a los proveedores de acceso a Internet (también conocidos como proveedores de servicios de Internet) la capacidad de enviar y recibir tráfico a través de Internet.
- **La sección 1.4** describe la función de proporcionar a los proveedores de acceso a Internet la posibilidad de intercambiar su tráfico de manera local en lugar de utilizar proveedores de red troncal o de tránsito.
- **La sección 1.5** describe la función de proporcionar acceso a Internet a un punto de conexión (el dispositivo de un usuario).

1.1 Medio de comunicación (por cable e inalámbrico)

Descripción de la función: proporcionar los medios de comunicación para soportar la transmisión de paquetes de red del Protocolo de Internet (IP). Los medios de comunicación se utilizan en todos los rincones de Internet, desde la conexión a un dispositivo doméstico o móvil, hasta los proveedores de redes “troncales” e incluso bajo los océanos. Esta función de los intermediarios es esencial incluso para las comunicaciones más básicas de Internet.

Consideraciones técnicas y prácticas: los paquetes IP pueden transmitirse por un cable, por el aire e incluso a través del espacio mediante el uso de diversos protocolos de red específicos del medio. Los medios de comunicación pueden ser propiedad de un proveedor o estar

alquilados a un proveedor de una ruta de comunicación de Protocolo de Internet (consulte la sección 1.2 a continuación) y pueden transportar otro tipo de tráfico, además de paquetes IP. Por ejemplo, la capacidad de un cable submarino de fibra óptica puede usarse, en parte, para el tráfico IP y, en parte, para otros protocolos de transmisión de datos patentados. Algunos ejemplos de medios de comunicación son: cables submarinos; de cobre, coaxial, de fibra hasta el hogar; inalámbricos a través del espectro radioeléctrico con o sin licencia.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de medios de comunicación no deben ser responsables del contenido que circula por sus medios.	Sin protecciones contra la responsabilidad, los proveedores de medios de comunicación se preocuparían por la posibilidad de ser responsables del contenido que circula por sus medios de comunicación. Podrían limitar el acceso a sus medios únicamente al contenido procedente de un pequeño número de fuentes previamente verificadas. Esto reduciría en gran medida las fuentes y el tipo de contenido transmitido a través de los medios de comunicación y obstaculizaría la capacidad de las personas para participar en línea. También fragmentaría Internet en diferentes redes de contenido.

1.2 Ruta de comunicación del Protocolo de Internet

Descripción de la función: enviar y recibir paquetes de red del Protocolo de Internet (IP) mediante un sistema de conmutación de paquetes de red a través de uno o varios medios de comunicación. Esta función incluye el acceso de último tramo (tratada más adelante en la sección 1.5). En Internet, las comunicaciones de extremo a extremo se consiguen atravesando rutas de comunicación interconectadas (moviéndose de

una red a otra). Al igual que los medios de comunicación (descritos anteriormente), las rutas de comunicación IP se utilizan en cada rincón de Internet. Una red IP entrega tráfico IP sin que su cliente sepa necesariamente qué rutas de comunicación se utilizarán o se utilizan. Esta función de los intermediarios de proporcionar la ruta de comunicación IP es esencial incluso para la comunicación más básica de Internet.

Consideraciones técnicas y prácticas: las principales rutas de comunicación IP entre grandes redes informáticas estratégicamente interconectadas y los enrutadores centrales de Internet se conocen colectivamente como la red troncal de Internet (descrita más adelante en la sección 1.3). En su mayoría, estas rutas (también conocidas como rutas IP) utilizan cables de fibra óptica por su gran ancho de banda, velocidad y atenuación limitada de la señal. Las redes que participan en la red troncal de Internet suelen tener peering sin acuerdos con redes vecinas para interconectarse y transportar tráfico. Algunas redes, sobre todo las que están más cerca del usuario final, pueden tener que pagar por el tránsito para que su tráfico llegue a Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de rutas de comunicación IP (servicios de red IP) no deben ser responsables del contenido que circula por sus redes.	Sin protecciones contra la responsabilidad, los proveedores de servicios de redes IP se preocuparían por la posibilidad de ser responsables del contenido que circula por sus redes. En consecuencia, podrían limitar el acceso a sus rutas de comunicación únicamente al contenido procedente de una cantidad reducida de fuentes previamente verificadas. En su extremo, la falta de protección de la responsabilidad podría restringir el uso de Internet al contenido difundido por una pequeña cantidad de compañías e impedir que los individuos puedan compartir su propio contenido. Esto socavaría en gran medida a la naturaleza abierta y globalmente conectada de Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
No se debe exigir a los proveedores de rutas de comunicación IP que monitoreen e intercepten el contenido del tráfico de los usuarios.	Es probable que el monitoreo o interceptación del contenido del tráfico a través de las rutas de comunicación IP (redes IP) degrade gravemente la velocidad y la confiabilidad de las comunicaciones a través de dichas rutas. También incumplirá las expectativas de confidencialidad, seguridad y privacidad de los usuarios. La Internet Engineering Task Force (IETF) considera que el monitoreo generalizado ² de las redes IP es un ataque, independientemente de la motivación.

1.3 Redes troncales y de tránsito

Descripción de la función: proporcionar un tipo específico de rutas de comunicación IP conocidas como redes troncales o de tránsito. Estas redes interconectan y agregan el tráfico de otras redes IP, como los proveedores de acceso de último tramo. Al hacerlo, permiten que el flujo de tráfico IP se conecte con todas las demás partes de Internet. Esta función de los intermediarios es esencial incluso para facilitar las comunicaciones más básicas de Internet.

Consideraciones técnicas y prácticas: los proveedores de servicios de redes troncales o de tránsito suelen estar ubicados en zonas geográficas donde la demanda es mayor y resulta más eficiente agregar tráfico. Estas redes son esenciales para transportar el tráfico de Internet desde y hacia los ISP de origen y otros puntos de conexión, hasta los ISP y puntos de conexión de destino.

² Marco de políticas Sección 4.3, Principios legales y de políticas específicos que se pueden aplicar a las funciones de los intermediarios sin perjudicar las comunicaciones de Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de redes troncales o de tránsito no deben ser responsables del contenido que circula por sus redes	Sin protecciones contra la responsabilidad, estos proveedores se preocuparían por la posibilidad de ser responsables del contenido que circula por sus redes. En consecuencia, podrían limitar el acceso solo a una pequeña cantidad de redes. Esto dificultaría la accesibilidad global y reduciría la capacidad de las personas para comunicarse en línea.
No se debe exigir a los proveedores troncales y de tránsito que monitoreen o intercepten el contenido del tráfico de los usuarios.	La función de proporcionar servicios de red troncal o de tránsito mueve grandes volúmenes de tráfico de Internet a través de la red de la manera más eficiente posible. Internet no sería confiable ni segura si los proveedores de estos servicios monitorearan o interceptaran el contenido del tráfico que transportan.

1.4 Intercambio de tráfico

Descripción de la función: proporcionar una ubicación física donde varias redes IP y redes de distribución de contenido puedan intercambiar paquetes. Esta función de los intermediarios es fundamental para una Internet eficaz, robusta, confiable y segura. Con un punto de intercambio de Internet, los ISP pueden intercambiar tráfico de manera local en lugar de enviarse tráfico entre sí a través de un proveedor de red troncal o de tránsito.

Consideraciones técnicas y prácticas: los IXP son las ubicaciones físicas y, por lo general, neutrales donde las diferentes redes locales se conectan para intercambiar tráfico entre sí, así como con los proveedores de red troncal o de tránsito que participan en el IXP, según sea necesario. Los IXP crean rutas más cortas, rápidas y directas para el tráfico de Internet. Ofrecen una alternativa más asequible y de menor latencia que tener que

enrutar el tráfico local a través de redes internacionales. El intercambio de tráfico en los IXP acorta y optimiza la ruta de tránsito, lo que reduce la latencia y el costo.

Enfoques de políticas recomendados	Motivos para este enfoque
Los IXP no deben ser responsables del contenido que se intercambia.	Sin protecciones contra la responsabilidad, probablemente nadie estaría dispuesto a operar o participar en un punto de intercambio de tráfico de Internet. El tráfico tomaría rutas ineficientes y más lentas, los costos aumentarían e Internet sería menos asequible, resistente y sostenible.
Salvo con fines de gestión eficaz del tráfico, se debería disuadir a los puntos de intercambio de Internet de monitorear el contenido del tráfico o interceptar el tráfico que pasa por ellos.	A menudo, la función de proporcionar un punto de intercambio de Internet es compartida por varios proveedores de rutas de comunicación IP o proveedores de servicios de red IP. Es esencial que las redes que utilizan un IXP puedan estar seguras de que no se está monitoreando ni interceptando el contenido de su tráfico. De lo contrario, podrían mostrarse reacias a usar el punto de intercambio porque sus clientes no quieren que se vigilen sus comunicaciones.
No se debe exigir a los puntos de intercambio de Internet que intercepten, filtren o monitoreen el tráfico que pasa por ellos.	Exigir a los IXP que inspeccionen o escaneen contenido específico disuadiría a los ISP de participar y perjudicaría la seguridad de las comunicaciones y la privacidad de los usuarios. Un enfoque de este tipo socavaría la confianza en Internet y dificultaría el intercambio eficaz de tráfico de Internet.

1.5 Acceso a Internet de último tramo

Descripción de la función: proporcionar a los usuarios finales (y a sus dispositivos) acceso a Internet, a menudo denominado “acceso de último tramo”. Se trata de un tipo específico de ruta de comunicación IP (descrito en la sección 1.2 anterior). Esta función, que incluye el transporte de tráfico IP hacia y desde el usuario final, es esencial incluso para las comunicaciones más básicas de Internet.

Consideraciones técnicas y prácticas: se puede proporcionar acceso a Internet a los usuarios finales a través de uno o varios medios, entre ellos, DSL, cable, inalámbrico, móvil, conexiones de fibra óptica y satélite. El acceso a Internet suele ser suministrado por un proveedor de servicio de Internet (ISP) comercial, pero algunos usuarios finales acceden a Internet a través de una red comunitaria. Desde un punto de vista técnico, el acceso de último tramo no difiere de otras rutas de comunicación IP, pero a menudo recibe un trato diferente en algunas jurisdicciones debido a la regulación histórica de los proveedores de servicios de comunicaciones a los usuarios finales.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de acceso a Internet para usuarios finales no deben ser responsables del contenido que circula por sus redes.	Sin protecciones contra la responsabilidad, estos proveedores se preocuparían por ser responsables del contenido que sus clientes envían y reciben. Como resultado, podrían limitar el contenido al que los usuarios finales pueden acceder o transmitir a través de Internet. Podrían intentar imponer filtros de descarga y carga que atenten contra la seguridad y privacidad del uso que sus clientes hacen de Internet. Además, para reducir el riesgo de responsabilidad, los proveedores probablemente bloquearían excesivamente el contenido, evitando así que los usuarios finales compartan contenido legal en línea. Sin estas protecciones, la Internet abierta, conectada a nivel mundial, segura y confiable se vería socavada.

Enfoques de políticas recomendados	Motivos para este enfoque
No se recomienda que los proveedores de acceso a Internet para usuarios finales monitoreen o intercepten el contenido del tráfico de los usuarios, excepto con fines de seguridad y de administración eficaz del tráfico.	Un principio fundamental del acceso a Internet (a menudo descrito como “neutralidad de la red”) es que los proveedores de acceso a Internet deben proporcionar acceso a Internet sin tener en cuenta el contenido que se transporta por sus redes. Si los proveedores de acceso a Internet para usuarios finales no siguen este principio y aplican un acceso diferente en función del contenido, se incumpliría con una propiedad esencial de Internet, que es la de ser una red de uso general (consulte Modo Internet de Interconectarse: definición de las propiedades fundamentales de Internet ³). Los usuarios finales también pueden restringir la forma en que se comunican en línea, por temor a que sus comunicaciones estén siendo monitoreadas.

3 Internet Society, “Modo Internet de Interconectarse: definición de las propiedades fundamentales de Internet”, septiembre de 2020, disponible en <https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf>.

2 Enrutamiento y funciones auxiliares que facilitan las comunicaciones a través de Internet

Esta sección describe las diversas funciones de los intermediarios involucradas en el direccionamiento y enrutamiento, que son esenciales para una Internet eficiente, robusta, confiable y segura.

2.1 Asignación de direcciones IP

Descripción de la función: asignar direcciones IP únicas a redes y usuarios. Esta función de los intermediarios es esencial incluso para las comunicaciones de Internet más básicas, ya que cada ruta de comunicación de Internet necesita un punto de partida y un destino, así como “saltos” intermedios, los cuales están identificados por una dirección IP única.

Consideraciones técnicas y prácticas: las direcciones IPv4 e IPv6 (también conocidas como recursos numéricos de Internet) son delegadas por la Autoridad de Asignación de Números de Internet (IANA) a los registros regionales de Internet [RIR⁴](#) para su asignación justa en las respectivas regiones. Dentro de una región, los RIR asignan direcciones IP a los proveedores de redes IP y a organizaciones de usuarios finales. En algunos países, los RIR también asignan direcciones IP a los registros nacionales de Internet. La IANA y los RIR son organizaciones sin fines de lucro que se rigen por procesos de múltiples partes interesadas para redes y usuarios de todo el mundo. Los cinco RIR incluyen [AfriNIC⁵](#) en

4 <https://www.nro.net/about/rirs/>.

5 <https://www.afrinic.net/>.

África, el Centro de Información de Redes de Asia-Pacífico ([AP-NIC⁶](https://www.apnic.net/)), el Registro Estadounidense de Números de Internet ([ARIN⁷](https://www.arin.net/)), el Registro de Direcciones de Internet para América Latina y el Caribe ([LACNIC⁸](https://www.lacnic.net/)) y el Centro de Coordinación de Redes RIPE ([RIPE NCC⁹](https://www.ripe.net/)).

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de asignación de direcciones IP no deben ser responsables del contenido que se comunica mediante el uso de las direcciones IP que asignaron.	Sin protecciones contra la responsabilidad, los proveedores de servicios de asignación de direcciones IP, preocupados por la posibilidad de ser responsables del contenido transmitido mediante el uso de las direcciones IP que asignaron, podrían restringir fuertemente a quién asignan direcciones IP y en qué condiciones. Esto reduciría Internet e impediría que muchos usuarios pudieran comunicarse en línea.
No se debe exigir que los servicios de asignación de direcciones IP controlen el contenido ilegal o no deseado en Internet.	A menudo, las direcciones IP son compartidas por más de un usuario final y pueden reasignarse a otros usuarios en el mismo país o en otro. Asimismo, las direcciones IP a menudo son compartidas por más de un host de contenido. La interferencia con la asignación de direcciones IP o el uso de direcciones IP para controlar contenido corre el riesgo de impedir directamente que los usuarios compartan contenido legal, así como de impedir que los hosts de contenido pongan contenido legal a disposición en Internet.

6 <https://www.apnic.net/>.

7 <https://www.arin.net/>.

8 <https://www.lacnic.net/>.

9 <https://www.ripe.net/>.

2.2 Asignación de números de sistema autónomo

Descripción de la función: asignar números únicos a un grupo de redes IP operadas por uno o más operadores de redes (proveedores de rutas de comunicación IP, descritos en la sección 1.2 anterior) que tiene una política de enrutamiento externa única y claramente definida. A este grupo de redes se le denomina Sistema Autónomo (AS) y el número único que lo identifica es su Número de Sistema Autónomo (ASN). Esta función es similar a la función de asignación de direcciones IP (descrita anteriormente). Es una pieza fundamental del sistema de enrutamiento del tráfico de Internet que se utiliza para identificar qué vías de comunicación se utilizan para enrutar el tráfico de Internet.

Consideraciones técnicas y prácticas: los ASN son delegados por la Autoridad de Asignación de Números de Internet (IANA) para los registros regionales de Internet (RIR) a fin de que los asignen en sus respectivas regiones. Los RIR asignan ASN tanto a los proveedores de redes IP como a organizaciones de usuarios finales. Consulte la sección 2.1 anterior “Consideraciones técnicas y prácticas”, para obtener más información sobre la IANA y los RIR. Existe una gran diversidad en los ASN. Mientras que algunos son muy complejos y están compuestos por diferentes redes y usuarios independientes, otros son más sencillos.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de asignación de ASN no deben ser responsables del contenido que se comunica mediante el uso de los ASN que asignaron.	Sin protecciones contra la responsabilidad, los proveedores de servicios de asignación de ASN podrían estar dispuestos a asignar ASN solo a un número muy pequeño de grandes proveedores establecidos de servicios de red, lo que limitaría el crecimiento y la diversidad de las redes en Internet. Esto probablemente tendría efectos graves, negativos e impredecibles en Internet y el acceso a Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
No se debería exigir que los servicios de asignación de ASN controlen el contenido ilegal o no deseado en Internet.	Interferir en la asignación de un ASN probablemente impediría el enrutamiento confiable y eficiente del tráfico de Internet, podría impedir que las redes participen en Internet y se correría el riesgo de impedir que una amplia gama de usuarios comparta y acceda a contenido legal.

2.3 Registro y administración de DNS

Descripción de la función: facilitar el registro, la renovación y la administración de nombres de dominio para su publicación en el Sistema de Nombres de Dominio (DNS). Esta función de los intermediarios es esencial para las comunicaciones por Internet que implican el uso de nombres de dominio. Los nombres de dominio son las direcciones “legibles por el ser humano” de las redes, los servidores, los sitios web y otros puntos de conexión de Internet.

Consideraciones técnicas y prácticas: los nombres de dominio son importantes porque permiten que las personas naveguen por Internet, en lugar de que recuerden direcciones IP como “192.0.2.1”. El registro y la administración de DNS incluyen el registro de nombres de dominio a través de registradores acreditados, lo que garantiza la integridad de la zona DNS y mantiene la información del Servicio de Directorio de Datos de Registro (RDDS, históricamente llamado WHOIS). Una administración eficaz incluye garantizar el cumplimiento de las políticas, incluidas las políticas de consenso establecidas por la comunidad que trabaja a través de la Corporación de Internet para la Asignación de Nombres y Números (ICANN) para los “gTLD” (dominios de nivel superior genéricos), y las políticas establecidas por los organismos nacionales para los “ccTLD” (dominios de nivel superior de código de país¹⁰) que controla cada país. Esta función la realizan varias organizaciones que trabajan en colaboración. Esto incluye los registros DNS (que gestionan los dominios de primer nivel gTLD y ccTLD) y los registradores (que gestionan el registro de nombres de dominio a particulares o entidades para que estos

10 Los países pueden establecer sus propias políticas para los ccTLD. El país delegó la operación de algunos ccTLD a una entidad externa que asigna dominios con fines comerciales.

puedan utilizarlos en Internet).

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de registro y administración de DNS no deben ser responsables del contenido que se comunica mediante el uso de nombres de dominio que ellos registran o gestionan.	Si los proveedores de servicios de registro y administración de DNS no cuentan con protecciones contra la responsabilidad por el contenido alojado bajo determinados nombres de dominio, es probable que se produzca un efecto intimidatorio sobre la capacidad de las personas para expresarse en línea. Sin protecciones contra la responsabilidad, es probable que los proveedores restrinjan significativamente quién puede registrar nombres de dominio y cómo pueden utilizarse. Incluso podría expulsar a los competidores más pequeños del mercado de DNS, disminuyendo la competencia y aumentando el costo del registro de nombres de dominio.
No se debería exigir que los servicios de registro y gestión de DNS controlen el contenido ilegal o no deseado en Internet.	Los nombres de dominio son una parte fundamental del modo en que las personas interactúan con Internet. Sobrecargar el sistema de registro de DNS exigiéndole que sea parte de los controles de contenido generaría límites sobre quién puede registrar nombres de dominio y con qué propósito, lo que reduciría en gran medida la capacidad de las personas para usar Internet.

2.4 Publicación de DNS

Descripción de la función: poner a disposición la información de DNS registrada en servidores DNS autoritativos de manera que la información esté disponible para que cualquier persona en Internet pueda consultar el DNS (discutido en la sección 2.5 más adelante). Esta función de los intermediarios es esencial para las comunicaciones por Internet que implican el uso de nombres de dominio. Esta función también incluye (a) operar los “servidores raíz” que proporcionan información sobre cómo llegar al servidor DNS autoritativo para cada dominio ccTLD o gTLD de primer nivel y (b) proporcionar copias de la información del servidor DNS autoritativo para lograr resistencia, confiabilidad y respuestas más eficientes en las consultas al DNS.

Consideraciones técnicas y prácticas: el DNS es un sistema jerárquico. Para cada dominio de nivel superior (como .com), existe un intermediario que publica la información autoritativa sobre ese dominio en un servidor DNS conocido como un [servidor raíz](#).¹¹ Estos intermediarios suelen denominarse “operadores de servidores raíz”. En general, son el registro DNS en el que ICANN ha delegado la función de gestión de ese dominio de primer nivel. Prácticamente todas las comunicaciones a través de Internet dependen del correcto funcionamiento de la función de publicación del DNS para garantizar que el tráfico se enrute a la ubicación correcta en Internet. La integridad y confiabilidad del sistema de servidores DNS es esencial para el funcionamiento de Internet. Para mejorar la eficiencia y velocidad del sistema DNS, pueden usarse copias de la información DNS autoritativa

¹¹ <https://root-servers.org/>.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de publicación de DNS no deben ser responsables del contenido que se comunica mediante el uso de los nombres de dominio que publican.	La interrupción de los servicios de registro y gestión de DNS perjudicaría directamente el funcionamiento de Internet al perturbar la capacidad de los usuarios para localizar los servidores donde se aloja el contenido y otros recursos. Si los proveedores de servicios de publicación de DNS pudieran ser considerados responsables del contenido alojado en los nombres de dominio que publican, podrían dejar de prestar la función de publicación de DNS o prestarla únicamente a dominios previamente verificados. Esto tendría efectos graves, negativos e imprevisibles en las comunicaciones a través de Internet.
No se debería exigir que los servicios de publicación de DNS controlen el contenido ilegal o no deseado en Internet.	El acceso confiable y rápido a datos DNS publicados que sean fidedignos y de confianza es fundamental para un funcionamiento eficiente de Internet. Impedir la publicación de DNS o especificar qué dominios y en qué circunstancias pueden publicarse fragmentaría Internet y la haría poco confiable.

2.5 Búsqueda de DNS

Descripción de la función: traducir nombres de dominio a sus direcciones IPv4 o IPv6 numéricas correctas (así como alguna otra información). Normalmente, los usuarios utilizan los nombres de dominio para localizar los sitios web y otros recursos de Internet a los que desean acceder. Los nombres de dominio deben convertirse en la dirección IP correcta para que las redes, los servidores y los usuarios finales (dispositivos) puedan conectarse entre sí. Esta función la proporcionan servidores

especializados llamados servidores de nombres de dominio recursivos (servidores DNS recursivos) que obtienen su información DNS de servidores DNS autoritativos (consulte la sección 2.4 anterior). Almacenan la correspondencia entre los nombres de dominio y las direcciones IP y responden a las solicitudes de búsqueda de nombres de dominio y de devolución de direcciones IP (u otra información solicitada).

Consideraciones técnicas y prácticas: los servidores DNS recursivos están ubicados en muchas partes diferentes de Internet. Para agilizar el sistema de nombres de dominio, la mayoría de las computadoras de los usuarios finales no se comunican con los servidores DNS autoritativos. Solicitan información DNS a servidores DNS recursivos. Algunos servidores recursivos se ofrecen a todo el mundo (a menudo denominados “servidores DNS abiertos”). Otros son operados por proveedores de servicios de Internet (ISP), otros operadores de redes y empresas privadas, principalmente para uso de sus usuarios. Ocasionalmente, algunas personas operan sus propios servidores recursivos en sus propias computadoras, por lo general, para su uso personal. Aunque la función principal, la búsqueda de DNS, puede ser la misma, muchos usuarios eligen un proveedor de DNS concreto por motivos de seguridad y privacidad.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de búsqueda de DNS no deben ser responsables del contenido que se comunica mediante el uso de las respuestas que proporcionan a las consultas de búsqueda de DNS.	Sin protecciones contra la responsabilidad, los proveedores de servicios de búsqueda de DNS probablemente limitarían la capacidad de los usuarios de utilizar el sistema DNS para acceder a contenido de Internet. El contenido sería inaccesible sin conocer la dirección IP específica del sitio web u otro recurso en Internet. Esto tendría un impacto grave y negativo en las comunicaciones a través de Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
No se debe exigir que los servicios de búsqueda de DNS controlen el contenido ilegal o no deseado en Internet.	Bloquear el acceso a los nombres de dominio a través de servicios de búsqueda de DNS (servidores DNS recursivos) crea riesgos significativos de bloqueo excesivo de contenido, lo que impediría el acceso y fragmentaría la Internet. Los intentos de exigir el filtrado de contenido a través de servidores DNS recursivos rompen la integridad del DNS y lo vuelven poco confiable.

2.6 Servicios de DNSSEC

Descripción de la función: proporcionar autenticación para los registros de nombres de dominio almacenados en servidores DNS autoritativos. Esta función se cumple al proporcionar firmas criptográficas de clave pública para esos registros. El objetivo de esta función es proteger la integridad de los registros de nombres de dominio y proporcionar un mecanismo para validar que la dirección IP (u otra información) devuelta por una consulta DNS es la que el operador del dominio pretendía proporcionar. DNSSEC es una función de intermediarios esencial para garantizar que no se haya manipulado el registro del nombre de dominio.

Consideraciones técnicas y prácticas: DNSSEC, un protocolo de seguridad desarrollado por la Internet Engineering Task Force (IETF), ayuda a prevenir una serie de ataques de ciberseguridad en las comunicaciones a través de Internet. Sin DNSSEC, un atacante podría, por ejemplo, corromper los datos DNS en tránsito al cambiar la dirección IP que corresponde al sitio web al que un usuario quiere acceder y dirigirlo así al sitio web del atacante. Cuando se implementa correctamente, DNSSEC protege todos los registros DNS relacionados con un nombre de dominio. Estos registros pueden utilizarse para localizar servicios como la mensajería instantánea y el correo electrónico, así como para respaldar medidas contra los correos electrónicos o mensajes no deseados que dependen del DNS.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de DNSSEC no deben ser responsables del contenido que se comunica mediante el uso de dominios protegidos por DNSSEC.	DNSSEC protege la integridad de los resultados del DNS independientemente del contenido subyacente. Sin protecciones contra la responsabilidad, los proveedores de servicios de DNSSEC reducirían directamente el uso de DNSSEC. Esto reduciría en gran medida la seguridad de las comunicaciones a través de Internet.

2.7 Servicios de certificados TLS

Descripción de la función: crear, almacenar y emitir certificados de seguridad de la capa de transporte (certificados TLS) firmados criptográficamente para crear conexiones seguras con un servidor en Internet. Por lo general, los certificados TLS son emitidos por una Autoridad de certificación (“CA”). Un uso común de los certificados TLS es proteger el tráfico web para evitar escuchas y manipulaciones. La emisión de certificados TLS es una función esencial de los intermediarios necesaria para una Internet confiable y segura.

Consideraciones técnicas y prácticas: un certificado TLS está firmado digitalmente, es emitido por una CA y contiene información como el nombre de dominio, la entidad (persona, organización o dispositivo) para la que se emitió, el nombre de la CA emisora y su periodo de validez. Los certificados TLS protegen la integridad y autenticidad de las claves públicas criptográficas que se utilizan para establecer sesiones HTTP cifradas (HTTPS) con el fin de proteger el tráfico web contra escuchas y manipulaciones. TLS es una herramienta vital para mantener seguras las comunicaciones a través de la web.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan certificados TLS no deben ser responsables del contenido protegido mediante dichos certificados TLS.	El objetivo de TLS es proteger el tráfico en Internet, independientemente de su contenido. Imponer la responsabilidad del contenido a los proveedores de certificados TLS socavaría la seguridad de las comunicaciones en Internet. Si las entidades que proporcionan certificados TLS pudieran ser responsables del contenido que se transmite mediante el uso de sus certificados, se mostrarían reacias a emitir estos certificados, especialmente a individuos y entidades más pequeñas, lo que haría que Internet fuera menos segura para todos los usuarios de Internet.

3 Servicios de alojamiento y almacenamiento en caché

Los dos primeros grupos de funciones (descritos en las secciones anteriores) permiten las comunicaciones a través de Internet. Esta tercera sección describe las funciones que permiten que el contenido esté disponible en Internet, incluido el contenido generado por los usuarios y creado por individuos y entidades más pequeñas.

3.1 Alojamiento en la red

Descripción de la función: proporcionar y operar servidores y otros recursos necesarios para alojar sitios, aplicaciones u otros recursos web y hacerlos accesibles a través de Internet. Esta función de los intermediarios permite a los individuos y a otros usuarios compartir contenido a través de la World Wide Web.

Consideraciones técnicas y prácticas: alojar un sitio web implica operar servidores que (a) almacenan los archivos, bases de datos, software y código de un sitio o una aplicación web y (b) reciben y responden a las solicitudes de los usuarios para acceder al contenido del sitio. Las entidades que proporcionan alojamiento también pueden prestar otros servicios relacionados, incluido soporte técnico, soluciones de respaldo y seguridad. Muchas personas, empresas, organizaciones sin fines de lucro y gobiernos confían en los servicios de alojamiento web de terceros en lugar de actuar como sus propios servidores web. Estos servicios de alojamiento web suelen ofrecer un alojamiento más seguro, menos costoso y más fiable.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de alojamiento web no deben ser responsables del contenido de sus clientes directos ni del contenido facilitado por los usuarios de los sitios web de sus clientes.	Si las entidades que prestan servicios de alojamiento web pudieran ser responsables del contenido de los sitios web de sus clientes, los proveedores de servicios se mostrarían reacios o incapaces de prestar servicios de alojamiento web, especialmente a los individuos y las organizaciones más pequeñas. Sin protecciones contra la responsabilidad, los proveedores de servicios de alojamiento podrían restringir de manera importante quién puede publicar contenido en línea y qué contenido pueden publicar, lo que limitaría significativamente la capacidad de las personas para comunicarse en Internet.
No debe exigirse a los proveedores de servicios de alojamiento web que inspeccionen o retiren el contenido publicado por sus clientes.	Obligar a los proveedores a inspeccionar y retirar contenido socavaría su capacidad para operar como hosts de sitios web, especialmente para proveedores más pequeños. Podrían restringir sus servicios a contenido previamente aprobado de una pequeña cantidad de sitios web y los usuarios tendrían opciones limitadas para poner su contenido a disposición en Internet.
No se debe exigir a los proveedores de servicios de alojamiento web que controlen el contenido ilegal o no deseado.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo ha publicado, no en el proveedor de servicios que lo aloja.

3.2 Alojamiento de correo electrónico

Descripción de la función: proporcionar y operar servidores de correo electrónico para enviar, recibir, almacenar, reenviar y gestionar servicios de correo electrónico en Internet. Esta función de los intermediarios es esencial para el correo electrónico, una herramienta fundamental para las comunicaciones a través de Internet

Consideraciones técnicas y prácticas: el alojamiento de correo electrónico implica operar servidores que envían, reciben, almacenan, reenvían y administran de otro modo el correo electrónico. Los proveedores de alojamiento de correo electrónico también pueden prestar otros servicios relacionados, como soporte técnico, archivo, filtrado de correo no deseado y soporte de cumplimiento. La mayoría de los usuarios de Internet, ya sean individuos u organizaciones, ahora dependen del alojamiento de correo electrónico de terceros. Por lo general, los proveedores externos pueden ofrecer servicios de correo electrónico más seguros, menos costosos y más fiables que los que muchos individuos y empresas podrían proporcionar por sí mismos.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de correo electrónico no deben ser responsables del contenido del correo electrónico enviado o recibido por sus usuarios.	Si las entidades que prestan servicios de correo electrónico pudieran ser responsables del contenido de los correos electrónicos enviados o recibidos por sus clientes, se mostrarían reacios o incapaces de prestar servicios de correo electrónico, en especial a los individuos y las organizaciones más pequeñas. Sin protecciones contra la responsabilidad, los proveedores de servicios de correo electrónico podrían verse obligados a vigilar y censurar los mensajes de correo electrónico. En consecuencia, el correo electrónico dejaría de ser una herramienta útil para las comunicaciones de persona a persona.

Enfoques de políticas recomendados	Motivos para este enfoque
No se debe exigir a los proveedores que retiren contenido o bloqueen la capacidad de los usuarios para utilizar sus servicios.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo haya transmitido, no en el proveedor de alojamiento de correo electrónico ni en otros proveedores que faciliten su transmisión. Imponer una carga al proveedor de alojamiento socavaría la capacidad de los pequeños proveedores para operar en el mercado y podría perjudicar la confianza, integridad y fiabilidad del correo electrónico.

3.3 Otros servicios de alojamiento

Descripción de la función: proporcionar y operar servidores que alojan contenido, archivos, bases de datos, software y código, y otros recursos que permiten a otros operar una amplia gama de aplicaciones, sitios y servicios para enviar y recibir comunicaciones a través de Internet. Dado que la gran mayoría de las aplicaciones y ofertas en Internet, en especial las que ofrecen las empresas nuevas y las empresas pequeñas o medianas, utilizan servicios de alojamiento, esta función de los intermediarios es esencial para la disponibilidad de un conjunto diverso de servicios y aplicaciones en Internet.

Consideraciones técnicas y prácticas: el alojamiento implica el funcionamiento de servidores que (a) almacenan contenido, archivos, bases de datos, software y código que conforman un servicio o una aplicación en línea y (b) permiten a los usuarios interactuar con el servicio o la aplicación. Los proveedores de la función de alojamiento también pueden prestar otros servicios relacionados, incluido soporte técnico, soluciones de respaldo, seguridad y acceso a Internet. Muchos usuarios confían en los servicios de alojamiento de terceros porque estos proveedores pueden ofrecer un alojamiento más seguro, menos costoso y más fiable que el que muchos individuos y empresas podrían proporcionarse a sí mismos.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de alojamiento no deben ser responsables del contenido de sus clientes ni de los usuarios de los clientes.	Si las entidades que prestan servicios de alojamiento pudieran ser responsables del contenido enviado o recibido por los clientes o los usuarios de los clientes, los proveedores de servicios se mostrarían reacios o incapaces de prestar esa función, en especial a los individuos y las entidades más pequeñas. Sin protecciones contra la responsabilidad, la innovación en Internet disminuiría y el alojamiento de contenido se limitaría a una pequeña cantidad de grandes proveedores.
Los proveedores de servicios de alojamiento no deben utilizarse para controlar contenido ilegal o no deseado en Internet.	La responsabilidad del contenido problemático debe recaer en el individuo o entidad que transmitió el contenido y no en el proveedor de servicios que los aloja. Imponer una carga al proveedor de alojamiento socavaría la capacidad de los pequeños proveedores para operar en el mercado y los usuarios tendrían opciones más limitadas para poner su contenido a disposición en línea.

3.4 Servicios de distribución de contenido y almacenamiento en caché

Descripción de la función: almacenar temporalmente copias de contenido más cerca del usuario final para reducir la latencia y los costos del contenido a los que se accede con frecuencia. Los servicios de almacenamiento en caché son un tipo especial de servicio de alojamiento que generalmente implica el almacenamiento temporal de copias de otro contenido en un lugar más cercano al usuario final. Las redes de distribución de contenido (CDN) utilizan centros de datos y

redes geográficamente dispersos para hacer llegar más rápidamente el contenido de sus clientes a los usuarios finales. Normalmente, sus clientes son grandes distribuidores de contenido, como los servicios de streaming. Estos servicios de almacenamiento en caché y distribución de contenido son esenciales para el funcionamiento eficaz de Internet.

Consideraciones técnicas y prácticas: los navegadores ofrecen algunas funciones de almacenamiento en caché (que se comentan más adelante). Sin embargo, en Internet, la principal función de almacenamiento en caché suele ofrecerla una CDN, que opera una red de servidores distribuidos. Los proveedores de servicios de Internet también pueden ofrecer la función de almacenamiento en caché para acelerar el acceso al contenido por parte de los clientes del ISP. En ambos casos, los servidores de almacenamiento en caché almacenan copias temporales de contenido populares, como páginas web, videos o imágenes. Como estos servidores están distribuidos en distintas redes de Internet, las copias del contenido deseado pueden estar más cerca de los usuarios y se puede acceder a ellas más rápidamente. Esto reduce la distancia que debe recorrer el contenido, lo que reduce el tiempo de carga y la latencia, y mejora la experiencia del usuario. El almacenamiento en caché también reduce el costo de distribución de contenido al evitar que el mismo contenido se retransmita una y otra vez. Las decisiones sobre qué contenido almacenar en caché, y durante cuánto tiempo, suelen estar automatizadas en función de algoritmos específicos de almacenamiento en caché.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de almacenamiento en caché y distribución de contenido no deben ser responsables del contenido almacenados en caché.	Si las entidades que prestan servicios de almacenamiento en caché o de distribución de contenido pudieran ser responsables del contenido almacenado temporalmente en sus servidores, los proveedores de servicios se mostrarían reacios o incapaces de prestar los servicios, lo que aumentaría los costos, reduciría directamente la eficiencia y afectaría de forma negativa a la experiencia del usuario.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de almacenamiento en caché no deben utilizarse como puntos de control del contenido ilegal o no deseado en Internet.	Si se exigiera a los proveedores de servicios de almacenamiento en caché que controlaran el contenido, solo almacenarían en caché el contenido conocido e investigado. Esto aumentaría efectivamente los costos para los proveedores de contenido más pequeños y los haría menos atractivos para los usuarios de Internet debido a la menor calidad de la experiencia del usuario. Los usuarios perderían el acceso a una rica diversidad de contenido y, es probable que el contenido local sería el más perjudicado.

3.5 Distribución de contenido de Interfaz de programación de aplicaciones (API)

Descripción de la función: alojar y entregar contenido a través de una API, o interfaz de programación de aplicaciones, que es un conjunto de reglas o protocolos que permite a los servidores informáticos comunicar información de una máquina a otra. Las API son herramientas muy comunes utilizadas en una amplia gama de contextos para enviar y recibir información a través de Internet y, en algunos de esos contextos, se utilizan para transmitir contenido generado por los usuarios. Por ejemplo, un caso de uso común es que las API pueden permitir la visualización de publicaciones de blogs o medios sociales integradas dentro de otras páginas web.

Consideraciones técnicas y prácticas: esta función es muy similar al alojamiento general de contenido basado en la web, sobre el que se discutió anteriormente, pero, en ocasiones, usando protocolos o capacidades técnicas diferentes para solicitar y enviar el contenido.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de API no deben ser responsables del contenido de los usuarios distribuidos a través de sus servicios.	Si las entidades que prestan servicios API pudieran ser responsables del contenido de los usuarios distribuidos a través de sus servicios, se mostrarían reacias o incapaces de prestar tales servicios, lo que reduciría la capacidad de los individuos para publicar y recibir contenido legal a través de Internet.
No se debe usar a los proveedores de servicios API para controlar contenido ilegal o no deseado en Internet.	Las API son herramientas fundamentales en todo el ecosistema de Internet, y cualquier intento de utilizarlas como medio para controlar el contenido en línea corre el riesgo de amurallar el contenido dentro de los servicios, lo que reduciría enormemente la interoperabilidad y la innovación.

3.6 Selección, moderación y visualización de contenido

Descripción de la función: organizar y, en algunos casos, seleccionar el contenido que se mostrará a los usuarios. Lo distinguimos del alojamiento web, descrito anteriormente en la sección 3.1, por las funciones adicionales que ofrece, como la selección o moderación. Esta función es muy común en los sitios web de contenido generado por los usuarios. Se puede proporcionar tanto de forma automatizada mediante algoritmos y automatización como, en ocasiones, de forma manual por parte de individuos.

Consideraciones técnicas y prácticas: la función de selección suele estar a cargo de hosts de contenido generado por los usuarios, que necesitan gestionar y organizar un enorme volumen de presentaciones. Existen muchas razones para ofrecer esta función. Por ejemplo, los hosts pueden filtrar contenido que infrinjan sus condiciones de servicio. También

es probable que presenten el contenido a los usuarios en función de sus intereses y preferencias, historial de visualización y otros criterios. Estas funciones permiten la gestión práctica del contenido en sitios de contenido generado por el usuario. Es probable que las decisiones de selección y moderación sean más pertinentes y comprensibles para los usuarios si se tienen en cuenta factores culturales, lingüísticos y contextuales.

Enfoques de políticas recomendados	Motivos para este enfoque
Las organizaciones que ofrecen funciones de selección, moderación y visualización de contenido a los usuarios deben poder hacerlo sin riesgo de responsabilidad por ese contenido.	Si las entidades que brindan funciones de selección y moderación pudieran ser responsables del contenido o de dichas funciones, se mostrarían reacias o incapaces de brindarlas. Sin ningún tipo de selección o moderación, el contenido que generan los usuarios estaría sin clasificar y desorganizado. Sería un desafío para los usuarios compartir contenido con sus audiencias y localizar el contenido que desean.
No debe restringirse la capacidad de selección y moderación.	Sin selección y moderación, que son esenciales para bloquear el contenido no deseado e irrelevante y ofrecer contenido de interés para los usuarios, los sitios de alojamiento de contenido se volverían probablemente inmanejables para los operadores e indeseables para los visitantes.

4 Comunicaciones entre personas

Esta sección incluye un cuarto grupo de funciones que se centran en diferentes modos de comunicación que permiten a las personas entablar comunicaciones de persona a persona a través de Internet. Estas funciones son esenciales para que las personas, y las pequeñas organizaciones y empresas, interactúen a través de Internet.

Algunos aspectos de estas funciones se superponen con otras funciones de los intermediarios incluidas en este Anexo. Sin embargo, es importante describirlas de forma independiente porque se trata de funciones fundamentales que se repiten una y otra vez en los nuevos servicios prestados a través de Internet. Por ejemplo, las aplicaciones de mensajería son una innovación relativamente reciente que combina las funciones de comunicación de uno a uno y de uno a muchos.

4.1 Comunicaciones de uno a uno

Descripción de la función: proporcionar un medio confiable de envío, recepción, visualización, enrutamiento y otro tipo de soporte para las comunicaciones discretas, en tiempo real (sincrónicamente) o para su entrega posterior (asincrónicamente) entre un emisor y un receptor. En algunos casos, esta función puede ir acompañada de una función de “descubrimiento” para buscar a otros usuarios de un servicio concreto (por ejemplo, por nombre o número de teléfono) de modo que los usuarios puedan conectarse unos con otros

Consideraciones técnicas y prácticas: esta función define una amplia capacidad para que las personas (y las organizaciones) se comuniquen entre sí. La función es parte de una amplia gama de servicios que incluyen lo que a menudo se denomina correo electrónico, mensajería de texto, chat, mensajería directa y otras herramientas. Puede incluir comunicaciones de persona a persona en una amplia gama de entornos, como sitios web, videoconferencias, juegos, medios sociales y otros contextos. Algunos entornos también pueden incluir la capacidad de un

hablante individual de dirigir el mismo contenido a más de un destinatario a la vez (lo que se superpone con la función de uno a muchos analizada en la sección 4.2). Algunos de estos servicios ofrecen seguridad y privacidad mejoradas como una característica distintiva, usando cifrado de extremo a extremo (E2EE), descentralización u otras tecnologías.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de comunicaciones de uno a uno no deben ser responsables del contenido enviado o recibido por sus usuarios.	Si las entidades que prestan servicios de comunicaciones de uno a uno pudieran ser responsables del contenido de las comunicaciones de sus usuarios, se mostrarían reacias o incapaces de prestar los servicios, en especial a individuos y entidades más pequeñas. Sin protección de la responsabilidad, los proveedores podrían verse obligados a dejar de ofrecer el servicio o a censurar en exceso los mensajes, incluido el discurso legal, para evitar responsabilidades. El resultado sería una reducción de la capacidad de las personas para comunicarse en línea.
Los proveedores de servicios de comunicación de uno a uno no deben ser responsables del contenido problemático enviado o recibido por los clientes	La responsabilidad del contenido problemático debe recaer en la persona o entidad que los ha transmitido, no en el proveedor de servicios que los aloja o distribuye. Imponer cargas proactivas de revisión de contenido a los proveedores de comunicaciones de uno a uno bien podría expulsar del negocio a los proveedores (especialmente a los más pequeños) y reducir así la capacidad de los usuarios para comunicarse uno a uno. También podría llevarlos a eliminar protecciones fundamentales de privacidad y seguridad, como el cifrado de extremo a extremo.

4.2 Comunicaciones de uno a muchos

Descripción de la función: proporcionar un medio confiable de envío, recepción, visualización, enrutamiento y otro tipo de soporte para las comunicaciones discretas, en tiempo real (sincrónicamente) o para su distribución posterior (asincrónicamente) de un remitente a un grupo definido de destinatarios (que *pueden o no* estar definidos o controlados por el remitente). Los destinatarios pueden o no tener la capacidad de responder y entablar una conversación dentro del grupo más amplio

Consideraciones técnicas y prácticas: esta función define una amplia capacidad para que las personas (y las organizaciones) se comuniquen con grupos de destinatarios. La función es parte de una amplia gama de servicios, que van desde servicios de listas de correo electrónico con décadas de antigüedad hasta los servicios de seminarios web en video más modernos. Algunos de estos servicios pueden ofrecer como característica distintiva una mayor seguridad y privacidad, como el cifrado de extremo a extremo (E2EE) o la descentralización. Por lo general, los participantes en comunicaciones de uno a muchos tienen opciones para abandonar o “darse de baja” del grupo o para bloquear las comunicaciones de determinados remitentes.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de comunicaciones de uno a muchos no deben ser responsables del contenido enviado o recibido por sus usuarios.	Si las entidades que prestan servicios de comunicaciones de uno a muchos pudieran ser responsables del contenido de las comunicaciones de sus usuarios, se mostrarían reacias o incapaces de prestar los servicios. Sin protección de la responsabilidad, los proveedores podrían verse obligados a dejar de ofrecer el servicio o a censurar en exceso los mensajes, incluido el discurso legal, para evitar responsabilidades. El resultado sería una reducción de la capacidad de las personas para comunicarse en línea.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de comunicaciones de uno a muchos no deben ser responsables de abordar el contenido problemático enviado o recibido por los clientes a través de la revisión y el filtrado de contenido.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo ha transmitido, no en el proveedor de servicios que lo aloja o distribuye. Si se exige a los proveedores que monitoreen de forma proactiva el foro para detectar contenido no deseado, esa carga probablemente reduciría la capacidad de los proveedores (especialmente los más pequeños) de alojar dicho foro. Los proveedores deben estar protegidos si deciden eliminar o bloquear a un usuario que infringe las condiciones del servicio o las normas del grupo.

4.3 Comunicaciones de muchos a muchos

Descripción de la función: proporcionar un medio confiable de envío, recepción, visualización, enrutamiento y otro tipo de soporte a las comunicaciones, en tiempo real (sincrónicamente) o para su distribución posterior (asincrónicamente), de los remitentes o creadores de contenido a todos los usuarios de un servicio o a otro amplio grupo indefinido de destinatarios no controlados por el remitente. Los destinatarios o espectadores pueden tener o no la capacidad de responder y entablar una conversación dentro del grupo más amplio.

Consideraciones técnicas y prácticas: esta función define una amplia capacidad para que las personas (y organizaciones) se comuniquen con el público u otros grupos grandes de personas (como todos los usuarios de un servicio concreto). Esta función forma parte de una amplia gama de servicios, entre los que se incluyen los sitios colaborativos tipo “wiki”, los sitios colaborativos de desarrollo de contenido/software, los sitios de intercambio de imágenes/videos pregrabados, los servicios de *streaming* de video y las redes sociales. Algunos de estos servicios pueden ofrecer a los usuarios la posibilidad de limitar la distribución de sus publicaciones o contenido a un grupo definido de personas (lo que puede superponerse

con la función de uno a muchos descrita anteriormente en la sección 4.2). Algunos proveedores de comunicaciones de muchos a muchos ofrecen a los usuarios la posibilidad de bloquear las comunicaciones de determinados remitentes o de darse de baja del grupo.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de comunicaciones de muchos a muchos no deben ser responsables del contenido enviado o recibido por sus usuarios.	Si las entidades que prestan servicios de comunicaciones de muchos a muchos pudieran ser responsables del contenido de las comunicaciones de sus usuarios, se mostrarían reacias o incapaces de prestar los servicios. Sin protecciones contra la responsabilidad, los proveedores podrían verse obligados a dejar de ofrecer el servicio o a censurar en exceso los mensajes, incluido el discurso legal, para evitar responsabilidades. El resultado sería una reducción de la capacidad de las personas para comunicarse en línea.
Los proveedores de servicios de comunicaciones de muchos a muchos no deben ser responsables de abordar el contenido problemático enviado o recibido por los clientes a través del monitoreo y filtrado de contenido.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo ha transmitido, no en el proveedor de servicios que lo aloja o distribuye. Si se exige a los proveedores que monitoreen de forma proactiva el foro para detectar contenido no deseado, esa carga probablemente reduciría la capacidad de los proveedores (especialmente de los más pequeños) de alojar comunicaciones de muchos a muchos. Los proveedores deben estar protegidos si deciden eliminar o bloquear a un usuario que infrinja las condiciones del servicio o las normas del grupo.

5 Búsqueda

Esta sección se ocupa de un quinto grupo de funciones que incluyen los principales métodos utilizados por las personas para localizar contenido en Internet. Las funciones de búsqueda se utilizan tanto porque las personas desean acceder a información o contenido nuevo como porque desean volver a visitar contenido que ya vieron anteriormente.

Muchas herramientas y técnicas de búsqueda muestran una parte del contenido del recurso que se sugiere en respuesta a una consulta de búsqueda.¹² Por lo tanto, la función de búsqueda no sólo incluye localizar contenido, sino también mostrar contenido generado por el usuario. Las funciones de búsqueda son esenciales para que los usuarios descubran y accedan al contenido en Internet.

5.1 Búsqueda en la web

Descripción de la función: responder a las solicitudes de búsqueda con los medios para conectar al buscador con el contenido y, a menudo, mostrar una parte del contenido. La búsqueda se suele realizar a través de “motores de búsqueda”, que son servicios de terceros que permiten a los usuarios buscar recursos relevantes en la World Wide Web al proporcionar palabras clave, una pregunta o cargar o vincular una imagen.

Consideraciones técnicas y prácticas: proporcionar esta función de búsqueda normalmente implica (a) indexar contenido en Internet mediante algoritmos que evalúan y registran información como la relevancia de las palabras clave, el tipo de contenido, la vigencia del contenido, la participación del usuario y la calidad de la página y (b) identificar, proporcionar un enlace de acceso y mostrar resultados sugeridos (a menudo con “fragmentos” del contenido) en respuesta a una consulta de búsqueda del usuario, usando algoritmos que evalúan factores como la ubicación y el idioma del usuario, el historial de búsqueda y el tipo de dispositivo.

¹² Sin embargo, algunas herramientas de búsqueda ofrecen ahora resúmenes de contenido generados por IA en respuesta a las consultas de búsqueda. Para un análisis de estas cuestiones, consulte la Sección 5.9 del Marco de políticas, Punto destacado: inteligencia artificial.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de búsqueda no deben ser responsables del contenido de Internet creado por terceros que se muestran a los usuarios en respuesta a consultas de búsqueda.	Si los motores de búsqueda fueran responsables del contenido que generan los usuarios, probablemente dejarían de indexar la mayor parte del contenido de la web. Esto tendría como resultado práctico dejar grandes franjas de Internet prácticamente inaccesibles para los usuarios de todo el mundo.
Los proveedores de servicios de búsqueda no deben ser responsables de abordar el contenido problemático que aparezca en los resultados de búsqueda.	La búsqueda es una función de los intermediarios vital que permite la comunicación en Internet ya que facilita el acceso de los usuarios a <i>contenido creado por otros</i> y los ayuda a encontrar y localizar contenido “relevante” en Internet. Sin búsqueda, los usuarios tendrían que conocer de antemano la URL o dirección IP de cada sitio web u otro recurso en línea al que quieran acceder, lo cual es imposible a escala de Internet.

5.2 Búsqueda integrada

Descripción de la función: ofrecer resultados de búsqueda integrada específicos como un servicio para sitios web y otras entidades que no dispongan de los recursos técnicos o medios financieros para desarrollar sus propias herramientas de búsqueda específicas.

Consideraciones técnicas y prácticas: al subcontratar una función de búsqueda a un motor de búsqueda de terceros, un sitio web puede ofrecer búsquedas directamente en su sitio a los usuarios. Esta función la ofrecen a menudo, aunque no exclusivamente, los motores de búsqueda que, a su vez, ofrecen búsquedas en la web (tal como se discutió anteriormente). Los resultados de la búsqueda pueden adaptarse a las necesidades del sitio web específico que utiliza la búsqueda integrada.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de búsqueda integrada no deben ser responsables del contenido de Internet administrado por el sitio web subyacente que utiliza el servicio para una función de búsqueda integrada.	Si los proveedores de servicios de búsqueda integrada fueran responsables del contenido mostrado en los resultados de búsqueda, probablemente dejarían de ofrecer ese servicio, especialmente a los sitios web más pequeños y a las empresas u organizaciones menos establecidas, lo que repercutiría directamente en la experiencia del usuario de Internet ya que los sitios carecerían de buenas funciones de búsqueda.
Los proveedores de servicios de búsqueda integrada no deben ser responsables de abordar el contenido problemático mostrado en los resultados de las búsquedas integradas.	Si se exigiera a los proveedores de motores de búsqueda integrados que monitorearan el contenido del sitio, el servicio resultaría probablemente demasiado costoso para los sitios web más pequeños y las empresas u organizaciones menos establecidas. Esto obstaculizaría directamente la capacidad de los sitios web pequeños para competir con los más grandes.

5.3 Búsqueda específica

Descripción de la función: proporcionar resultados de búsqueda centrados en medios o temas específicos (como, por ejemplo, servicios de audio inverso o herramientas de búsqueda de podcasts o imágenes) de sitios operados por alguien distinto del proveedor de búsquedas. Esta función aumenta la capacidad de los usuarios para localizar contenido de interés en Internet, especialmente aquel que no es fácil de buscar mediante un motor de búsqueda general.

Consideraciones técnicas y prácticas: las herramientas de búsqueda general suelen ser demasiado amplias, por lo que han surgido una serie de herramientas de búsqueda más específicas que permiten a los usuarios de

Internet buscar determinados tipos de contenido de forma más eficaz y eficiente. Los resultados de las búsquedas pueden adaptarse a los tipos de medios o contenido.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de búsqueda específica no deben ser responsables del contenido de Internet creado por otros que se muestra a los usuarios en respuesta a consultas de búsqueda.	Si las empresas de búsqueda específica fueran responsables del contenido que se muestra en los resultados de sus búsquedas, probablemente no podrían seguir operando y, por lo tanto, los usuarios de Internet perderían herramientas vitales que ayudan a descubrir contenido valioso en línea.
Los proveedores de servicios de búsqueda específica no deben ser responsables de abordar el contenido problemático que aparezca en los resultados de búsqueda.	Así como la búsqueda web es una herramienta fundamental que ha permitido a Internet convertirse en un enorme recurso de información, las herramientas de búsqueda específica han aportado el mismo valor para los tipos de contenido menos cubiertos por las herramientas de búsqueda general. Generar una carga para los proveedores de estos servicios probablemente llevaría a algunos a eliminar o reducir este tipo valioso de herramienta de búsqueda.

5.4 Búsqueda proporcionada por el sitio

Descripción de la función: proporcionar búsqueda de contenido dentro del sitio. Algunos de los principales servicios en línea (especialmente los que alojan gran cantidad de contenido generado por los usuarios, como los servicios de medios sociales) ofrecen sus propias herramientas de búsqueda interna, adaptadas a su servicio, para permitir a los usuarios descubrir contenido en sus sitios.

Consideraciones técnicas y prácticas: proporcionar herramientas para que los usuarios localicen contenido es una función básica de los sitios

que admiten contenido generado por los usuarios. Los resultados de la búsqueda pueden adaptarse a los tipos concretos de contenido que admite el sitio o el usuario individual.

Enfoques de políticas recomendados	Motivos para este enfoque
Los operadores de sitios web que ofrecen sus propias herramientas de búsqueda para localizar contenido en el sitio no deben asumir la responsabilidad del contenido creado por terceros por ofrecer una herramienta de búsqueda dentro del sitio para permitir que se descubra ese contenido.	Si no se permitiera a estos sitios ofrecer herramientas de búsqueda en sus páginas, los usuarios se verían privados de herramientas locales eficaces para localizar contenido.

6 Protección de la ciberseguridad, protección de la privacidad y control del contenido de los usuarios

Esta sección cubre un sexto grupo de funciones que:

- (a) pretenden combatir los ciberataques en Internet, funciones que son esenciales para una Internet segura, robusta, confiable y eficiente,
- (b) permiten que los usuarios individuales tomen medidas para proteger la seguridad y privacidad de sus propias comunicaciones por Internet y
- (c) permiten a los usuarios ejercer control sobre las categorías de contenido que pueden recibir.

Nota: algunas leyes de protección de la responsabilidad de los intermediarios amplían explícitamente su protección al software y a los servicios que permiten a los usuarios controlar el contenido que reciben a través de Internet. Por ejemplo, los proveedores de software de filtrado controlado por el usuario y orientado a la familia pueden estar protegidos de demandas interpuestas por sitios que son bloqueados por dicho software. *Consulte, por ejemplo, Código estatutario de los Estados Unidos, 47 U.S.C. §§ 230(f)(2) & (4).*

6.1 Protección del tráfico a escala de red

Descripción de la función: proteger redes, servicios en línea, sitios web y otros recursos de Internet frente a una amplia gama de tráfico malicioso, incluidos los ataques de denegación de servicio distribuidos (DDoS) y otras amenazas a la ciberseguridad. Esta función es parte de

un [esfuerzo colaborativo general de ciberseguridad](#)¹³ para proteger las comunicaciones a través de Internet.

Consideraciones técnicas y prácticas: las protecciones a escala de red implican el uso de técnicas diferentes y en constante evolución (como bases de datos de firmas, detección de anomalías e inteligencia artificial) e infraestructuras dedicadas para defenderse de los ciberataques y mitigar el impacto del tráfico malicioso en la disponibilidad, accesibilidad o confiabilidad de las redes, los servicios en línea, los sitios web y otros recursos de Internet. Algunas de estas técnicas requieren que las comunicaciones pasen por una red operada por un proveedor de ciberseguridad antes de llegar a la red prevista. Así, en ocasiones, las redes de los proveedores de servicios de ciberseguridad transportan “contenido generado por los usuarios” y otros tipos de contenido “creado por terceros” en Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de protección del tráfico a escala de red no deben ser responsables del contenido que circula por sus redes.	Sin protección de la responsabilidad, los proveedores estarían preocupados por la posible responsabilidad por el contenido que circula por sus redes o que examinan por motivos de seguridad. Podrían retirar o restringir la protección de las redes u otros recursos en Internet, lo que aumentaría drásticamente el riesgo de ciberataques dañinos en Internet.

13 Internet Society, “Collaborative Security: An approach to tackling Internet Security issues”, abril de 2015, disponible en <https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf>.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de protección del tráfico a escala de red no deben ser responsables de abordar el contenido problemático enviado o recibido por las redes, los servicios en línea, los sitios web y otros recursos de Internet protegidos.	La protección del tráfico a escala de red es un proceso altamente dinámico e iterativo para responder a ciberataques en constante evolución. Imponer cargas adicionales y no relacionadas para tratar de bloquear determinados tipos de contenido socavaría la eficacia del esfuerzo más amplio de ciberprotección. También podría incentivar a los proveedores a exigir a sus clientes que permitan el descifrado cuando el tráfico circule por sus sistemas. Esto socavaría la confidencialidad, integridad y seguridad de las comunicaciones de los usuarios de Internet. Cualquier esfuerzo por escanear en busca de contenido específico requeriría intentar reunir en medio de la red todos los paquetes de datos separados que componen el elemento de contenido (para poder determinar qué contenido se está transmitiendo), lo cual sería muy difícil para un proveedor de servicios hacer de forma coherente.

6.2 Herramientas y filtros de contenido controlados por el usuario

Descripción de la función: proporcionar al usuario herramientas para bloquear o limitar la entrega de ciertos tipos de contenido a sus dispositivos. Existen diferentes tipos de herramientas. Por ejemplo, hay herramientas de filtrado de contenido controladas por el usuario que pueden utilizarse para reducir la entrega de correo electrónico no deseado, bloquear la entrega de código malicioso a través de un sitio web o evitar que un dispositivo hogareño o de usuario pueda ver contenido web no deseado, como pornografía.

Consideraciones técnicas y prácticas: los filtros y las herramientas controlados por el usuario ofrecen importantes protecciones (como contra spam y malware en páginas web) y opciones de protección familiar (como contra pornografía u otro contenido). Estas herramientas utilizan diversos métodos técnicos y no siempre son totalmente eficaces (aunque pueden ser muy útiles). A veces se ofrecen como un servicio adicional de un proveedor de servicios de Internet, pero también suelen instalarse como software en las computadoras y los dispositivos de los usuarios. Reconociendo el valor de dichas herramientas para permitir a los usuarios decidir qué contenido bloquear, la *Ley de Protección de Responsabilidad de los Intermediarios* de EE. UU., en su Sección 230, incluye específicamente protecciones para las entidades que proporcionan estas herramientas. Consulte, por ejemplo, Código estatutario de los Estados Unidos, 47 U.S.C. §§ 230(f)(2) & (4).

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de filtros y herramientas controlados por el usuario no deben ser responsables del contenido que circula a través de sus herramientas, y no deben ser responsables de bloquear determinado contenido.	Sin protecciones contra la responsabilidad, los proveedores probablemente no podrían operar, lo que privaría a los usuarios de Internet de importantes protecciones de ciberseguridad, protecciones contra el correo no deseado y herramientas de filtrado de contenido.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de filtros y herramientas controlados por el usuario no deben ser responsables de abordar el contenido problemático enviado o recibido por sus usuarios.	El objetivo de estos filtros y herramientas es que los usuarios puedan decidir a qué contenido quieren acceder y cuál prefieren bloquear. Obligar a los proveedores a bloquear también el contenido problemático antes de que llegue a los usuarios complicaría la herramienta (y podría incluso no ser posible). Un mandato de este tipo socavaría la autonomía de los usuarios para controlar el contenido que reciben y les haría temer que sus comunicaciones por Internet estén siendo monitoreadas. Como consecuencia, probablemente evitarían utilizar estas herramientas para proteger sus interacciones en línea, lo que conduciría a una menor ciberseguridad general en Internet.

6.3 Protección del tráfico centrada en el usuario

Descripción de la función: permitir a los usuarios individuales proteger su tráfico de Internet contra los ciberataques, la vigilancia (por parte de entidades privadas y gobiernos) y la censura.

Consideraciones técnicas y prácticas: las protecciones del tráfico centradas en el usuario son aquellas que pueden aplicarse a discreción del usuario para dirigir el tráfico de Internet por rutas y protocolos de red de confianza. Estas protecciones también pueden ayudar a los usuarios a ocultar su identidad o ubicación y, de este modo, mejorar su privacidad y seguridad. Estos servicios de protección del tráfico utilizan diversos métodos técnicos, como redes privadas virtuales (VPN), servicios de enrutamiento de cebolla (el más común es la red Tor) y otros enfoques. En la mayoría de los casos, los proveedores de estos servicios no determinan y, a menudo, no pueden determinar, qué contenido circula por sus redes.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de protección del tráfico centrados en el usuario no deben ser responsables del contenido que pasa a través de sus redes.	Sin protecciones contra la responsabilidad, los proveedores probablemente no podrían operar, lo que privaría a los usuarios de Internet de una importante herramienta de ciberseguridad que los protege de ciberataques, robos de identidad, vigilancia y censura.
Los proveedores de protección del tráfico centrados en el usuario no deben ser responsables de abordar el contenido problemático enviado o recibido por sus usuarios.	Inspeccionar y potencialmente bloquear tráfico específico sería directamente contrario a la intención de los proveedores de servicios de protección del tráfico centrados en el usuario. Esto socavaría la eficacia de estos servicios, lo que reduciría la privacidad y aumentaría los riesgos de seguridad para los usuarios.

7 Aplicaciones, software y su desarrollo y distribución

El séptimo grupo de funciones de los intermediarios incluye las aplicaciones, los programas y las bibliotecas de software más comunes que se utilizan para enviar, recibir y mostrar comunicaciones a través de Internet. En esta sección, también se analizan las funciones de distribución de aplicaciones y software. Las aplicaciones y el software mencionados en esta sección también pueden incluir capacidades no relacionadas con las comunicaciones por Internet.

Debido al papel primordial que desempeña el software a la hora de facilitar, mostrar, proteger y filtrar contenido en Internet, algunas leyes de protección de la responsabilidad de los intermediarios incluyen específicamente dentro de su protección a los creadores y distribuidores del software que se utiliza en las comunicaciones por Internet. *Consulte, por ejemplo, Código estatutario de los Estados Unidos, 47 U.S.C. §§ 230(f) (2) & (4).*

Las funciones de esta sección (como el desarrollo de software web y de correo electrónico) están estrechamente relacionadas con las funciones tratadas en las secciones 3 y 4 anteriores (incluidos, por ejemplo, el alojamiento web y las comunicaciones de uno a uno). Esta sección, sin embargo, se centra en el desarrollo y la distribución del software subyacente utilizado para ofrecer los servicios abordados anteriormente, que podrían ameritar protecciones de los intermediarios independientes de la prestación de servicios.

7.1 Software de sistema operativo

Descripción de la función: proporcionar software para dispositivos que permita (1) que el dispositivo se conecte a Internet y envíe o reciba comunicaciones a través de Internet, (2) que los usuarios del dispositivo

introduzcan contenido para su transmisión a Internet y (3) que los usuarios del dispositivo reciban y visualicen contenido transmitido a través de Internet. Estas funciones se encuentran entre las muchas otras actividades y funciones que un sistema operativo lleva a cabo en un dispositivo.

Consideraciones técnicas y prácticas: el sistema operativo de un dispositivo lleva a cabo funciones esenciales que permiten la transmisión, recepción y visualización de comunicaciones hacia y desde Internet. Esencialmente, todos los dispositivos informáticos tienen un sistema operativo subyacente, desde los dispositivos de consumo como computadoras, teléfonos móviles y televisores hasta enrutadores, conmutadores, servidores y otros dispositivos esenciales para el funcionamiento de Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan sistemas operativos no deben ser responsables del contenido de Internet que se transmite, recibe o muestra a través del sistema operativo.	Los sistemas operativos son esenciales para las comunicaciones en Internet y para la propia Internet. Imponer a los proveedores de sistemas operativos la responsabilidad por el contenido de Internet creado o transmitido por usuarios o terceros limitaría enormemente, o eliminaría, la capacidad de los usuarios para comunicarse a través de Internet.
Los sistemas operativos no deben tener la obligación de bloquear ni interferir de otro modo con el contenido problemático de Internet.	La seguridad, estabilidad, confiabilidad e integridad de los sistemas operativos son fundamentales para el acceso a Internet y para toda la informática en general. Exigir que los sistemas operativos controlen o bloqueen el acceso a contenido socavaría la velocidad, seguridad y fiabilidad de las funciones de los sistemas operativos.

7.2 Software de navegación y servicios web

Descripción de la función: proporcionar software para solicitar, enviar, recibir y mostrar contenido mediante protocolos de la World Wide Web. Estas acciones las llevan a cabo dos grandes tipos de software: el software de “servidor” web (que recibe y responde a las solicitudes de contenido en línea de los clientes web) y el software de “cliente”, normalmente los navegadores web, que permite a los usuarios solicitar, recibir y visualizar una amplia gama de contenido web. Esta función de los intermediarios también incluye las “aplicaciones” (software que se ejecuta en teléfonos inteligentes, computadoras y otros dispositivos) que recuperan contenido mediante el uso de protocolos de la World Wide Web. Una gran cantidad de contenido de Internet llega a los usuarios a través de las funciones del software de servidor web y cliente web, que es un método fundamental para que los usuarios accedan al contenido en línea.

Consideraciones técnicas y prácticas: la web se basa en la interoperabilidad que ofrecen los protocolos de la World Wide Web, sobre todo el lenguaje de marcado de hipertexto, o HTML, para dar formato al contenido, y el protocolo seguro de transferencia de hipertexto, o HTTPS, para solicitar y entregar contenido de forma segura. Esta interoperabilidad proporciona uno de los beneficios fundamentales de Internet: la posibilidad de que cualquiera pueda crear, formatear y vincular contenido al que puedan acceder personas de cualquier parte del mundo. Muchos sitios web integran contenido de varias fuentes (por ejemplo, un video integrado de un servicio de streaming o una foto de un servicio para compartir fotos que aparece en medio de la página web). Los navegadores web son una herramienta habitual para acceder al contenido de Internet y ofrecen al usuario un rico conjunto de opciones para controlar el contenido que se le presenta y, en cierta medida, para proteger su propia privacidad y seguridad.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan software de cliente y servidor web no deben ser responsables del contenido que se transmite, recibe o muestra a través del software.	Los programas de software de navegación y servicios web son fundamentales para que las personas puedan acceder al contenido de Internet. Sin protecciones contra la responsabilidad, las entidades que proporcionan estas funciones de intermediarios vitales estarían preocupadas por la posibilidad de ser responsables del contenido manejado por su software. Podrían restringir el uso de sus herramientas para limitar la responsabilidad, por ejemplo al limitar el uso a los recursos web que hayan inspeccionado o que hayan aceptado indemnizarlos en caso de alguna acción legal. Los sitios y recursos web modernos suelen incluir contenido dinámico que puede cambiar con frecuencia y sin previo aviso. Esto hace prácticamente imposible que alguien evalúe si el contenido que los usuarios desean enviar o recibir podría generar responsabilidad. El riesgo de responsabilidad probablemente restringiría en gran medida el contenido disponible en la web y obstaculizaría la capacidad de los individuos para comunicarse en línea.

Enfoques de políticas recomendados	Motivos para este enfoque
El software de navegación web no debe tener la obligación de bloquear ni interferir de otro modo con el contenido problemático de Internet.	Obligar a un servidor web o a un software cliente a supervisar o bloquear el acceso al contenido probablemente socavaría la velocidad, la seguridad, la confianza y la confiabilidad de Internet. Por ejemplo, si los navegadores filtran o bloquean contenido de formas que el usuario no puede controlar y manejar, el usuario utilizará herramientas alternativas para modificar o sustituir su navegador (lo que podría exponer a los usuarios a programas maliciosos y robo de identidad).
No se debe obligar a los programas de navegación web a reducir la seguridad para permitir a terceros examinar y bloquear contenido problemático en Internet.	Se han propuesto políticas que obligan a los navegadores a reducir la seguridad general para permitir a terceros examinar y bloquear el tráfico que, de otro modo, estaría cifrado entre el navegador y el servidor web. Por ejemplo, el requisito de instalar certificados raíz controlados por el gobierno ¹⁴ permitiría este tipo de bloqueo, pero también socavaría la seguridad, confianza y fiabilidad de Internet.

7.3 Software de correo electrónico

Descripción de la función: proporcionar software para enviar, recibir, almacenar y visualizar mensajes de correo electrónico. Estas acciones son realizadas por dos grandes tipos de software: software de servidor de correo electrónico y software de cliente de correo electrónico. El software del servidor realiza las funciones de “back-end” de transmitir, recibir y

14 Internet Society, “Mauritius Must Not Fall into the ‘Mass Surveillance’ Trap”, 28 de mayo de 2021, disponible en <https://www.internetsociety.org/blog/2021/05/mauritius-must-not-fall-into-the-mass-surveillance-trap/>.

almacenar correos electrónicos, mientras que el software del cliente permite a los usuarios enviar, recibir, reenviar y ver correos electrónicos. El correo electrónico es un mecanismo de comunicación ampliamente utilizado, basado generalmente en un modelo asíncrono, federado, de almacenamiento y reenvío, con servidores o sistemas de correo independientes que transmiten y reciben correo electrónico en nombre de remitentes y destinatarios.

Consideraciones técnicas y prácticas: la interoperabilidad de los servidores y clientes de correo que utilizan protocolos de correo electrónico mundialmente aceptados significa que remitentes y destinatarios pueden intercambiar correos electrónicos independientemente del software de correo electrónico o de los proveedores de servicios que utilicen. Existen tecnologías de cifrado como S/MIME y PGP para proteger el correo electrónico de extremo a extremo de los usuarios que decidan cifrarlo.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan software de cliente y servidor de correo electrónico no deben ser responsables del contenido que se transmite, recibe o muestra a través del software.	El software de cliente y servidor de correo electrónico es una herramienta fundamental para la comunicación en Internet. Sin protecciones contra la responsabilidad, es probable que los desarrolladores de software dejen de proporcionar correo electrónico a grandes clases de usuarios, lo que limitaría la capacidad de los usuarios para comunicarse por correo electrónico a través de Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
El software de correo electrónico no debe tener la obligación de bloquear ni interferir de otro modo con el contenido problemático de Internet.	Exigir que el software de correo electrónico controle o bloquee el acceso al contenido socavaría la seguridad, privacidad y confiabilidad del correo electrónico. También disuadiría a los proveedores de correo electrónico de ofrecer a sus clientes la posibilidad de proteger sus comunicaciones por correo electrónico con cifrado de extremo a extremo.

7.4 Software de mensajería

Descripción de la función: proporcionar software para una amplia gama de herramientas a fin de enviar, recibir, almacenar y visualizar mensajes. Estas funciones son realizadas por dos tipos de software: el software del “servidor” de mensajería (que realiza funciones de “back-end” de enrutamiento de mensajes y también puede recibir, transmitir y almacenar mensajes) y el software del “cliente” (que permite a los usuarios enviar, recibir y ver mensajes, y también almacenarlos). Al igual que el correo electrónico, la mensajería es un mecanismo de comunicación muy utilizado.

Consideraciones técnicas y prácticas: existe una amplia gama de sistemas de mensajería, muchos de los cuales no son interoperables entre sí (y su arquitectura interna de los distintos sistemas puede ser muy diferente). Algunos sistemas de mensajería se basan en estándares de Internet ampliamente desarrollados, mientras que otros han desarrollado tanto el software del cliente como el del servidor para admitir la mensajería. Algunos sistemas de mensajería admiten la mensajería cifrada de extremo a extremo, que puede proporcionar protecciones críticas para mantener los mensajes privados y seguros.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan el software del cliente y el servidor no deben ser responsables del contenido que se transmite, recibe o muestra a través del software.	El software de mensajería es una herramienta de comunicación fundamental en Internet, especialmente para la comunicación segura y privada de extremo a extremo. Sin estas protecciones, los proveedores de software temerían ser responsables del contenido que comparten sus usuarios. Como resultado, podrían dejar de proporcionar la función o sentirse obligados a debilitar la seguridad y privacidad de las comunicaciones de sus usuarios al desactivar el cifrado de extremo a extremo o examinar las comunicaciones de sus usuarios.
El software de mensajería no debe tener la obligación de bloquear ni interferir de otro modo con el contenido problemático de Internet.	Exigir que el software de mensajería controle o bloquee el acceso al contenido socavaría la seguridad, privacidad y confiabilidad de la mensajería.

7.5 Otros software usados en el envío, la recepción y la visualización de comunicaciones por Internet

Descripción de la función: proporcionar una aplicación o programa con una función secundaria que ofrece la capacidad de enviar, recibir y mostrar contenido y comunicaciones. Por ejemplo, una aplicación que proporciona información sobre rutas de senderismo en una zona geográfica también puede permitir que los usuarios publiquen comentarios sobre las rutas que se entregan a otros usuarios.

Consideraciones técnicas y prácticas: existe una gran variedad de programas y aplicaciones que permiten a los usuarios publicar o enviar

contenido y recibir contenido de otros.

Enfoques de políticas recomendados	Motivos para este enfoque
Las entidades que proporcionan aplicaciones que permiten a los usuarios publicar, transmitir o recibir contenido o comunicaciones no deben ser responsables del contenido generado por los usuarios que se transmite, recibe o muestra a través de la aplicación.	Dado que un gran número de aplicaciones permiten a los usuarios transmitir contenido y comunicaciones, una normativa formulada de manera amplia podría fácilmente abarcar cientos o incluso miles de aplicaciones, muchas de ellas de empresas nuevas y pequeños proveedores. Sin protecciones contra la responsabilidad por el contenido generado por los usuarios, los desarrolladores y proveedores de tales aplicaciones probablemente no ofrecerían la funcionalidad de comunicación añadida como parte de su servicio, lo que socavaría la capacidad de las personas para comunicarse a través de esas aplicaciones y limitaría la innovación y los nuevos productos en Internet. También podría expulsar del mercado a algunos proveedores, especialmente a los más pequeños.
No se debe obligar a las aplicaciones a bloquear o interferir de otro modo con el contenido problemático generado por los usuarios en Internet.	Obligar a las entidades que ofrecen funciones de comunicación como parte de su software de programas y aplicaciones a monitorear o bloquear el acceso al contenido generado por los usuarios probablemente limitaría las comunicaciones legítimas y socavaría la seguridad, la privacidad, la confianza y la confiabilidad de Internet.

7.6 Desarrollo y distribución de software/aplicaciones

Descripción de la función: desarrollar y facilitar la distribución de software y aplicaciones que respalden la comunicación de contenido a través de Internet. Esta función incluye, por ejemplo, aplicaciones, software, bibliotecas de software y complementos de software que transmiten, reciben, muestran, reenvían, almacenan en caché, buscan, crean subconjuntos, organizan, reorganizan, traducen, filtran, seleccionan, permiten, no permiten, eligen, analizan, digieren contenido o facilitan de algún otro modo la comunicación de contenido a través de Internet. Esta categoría de software y aplicaciones, y su distribución, puede estar destinada a usuarios finales, proveedores de infraestructuras de Internet u otros participantes en el ecosistema de Internet. Dado que en la actualidad pocas personas tienen los conocimientos técnicos necesarios para crear sus propias aplicaciones de cliente y servidor de Internet, la capacidad de localizar y recuperar software escrito por terceros es una función esencial para el funcionamiento de Internet.

Consideraciones técnicas y prácticas: el desarrollo y la distribución de herramientas de software que permitan a los usuarios acceder a Internet y comunicarse a través de la web son funciones vitales. La función de desarrollo y distribución adopta una amplia gama de formas, incluidos los repositorios de software de código abierto (que proporcionan algunos de los software más fundacionales sobre los que funciona Internet), los espacios de trabajo de desarrollo colaborativo de software (a menudo utilizados para desarrollar software de código abierto), las “tiendas de aplicaciones” a disposición de los usuarios, las “tiendas” en navegadores y otros software que permiten a los usuarios añadir complementos de terceros (por ejemplo, para admitir el filtrado del tráfico web; la actualización y la aplicación de parches al software instalado) y otros enfoques.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de desarrollo y distribución de software no deben ser responsables del contenido que los usuarios envían y reciben con el software desarrollado o distribuido.	Sin estas protecciones contra la responsabilidad, los proveedores probablemente no podrían ofrecer estas funciones debido a la preocupación sobre la posible responsabilidad por el contenido manejado por el software que se desarrolla o distribuye. La responsabilidad pondría en peligro la capacidad de Internet para seguir funcionando y sería especialmente perjudicial para los desarrolladores de software de código abierto.¹⁵
No se debe obligar a los desarrolladores y proveedores de programas informáticos a bloquear o interferir de otro modo en el contenido problemático generado por los usuarios en Internet.	Tales obligaciones afectarían negativamente a la conectividad mundial y al acceso de las personas a las herramientas para comunicar contenido en línea. Las contribuciones al software de código abierto probablemente disminuirían y el software crítico no se mantendría, lo que llevaría a una Internet mucho menos segura y fiable.

15 Internet Society, “The EU’s Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem”, 24 de octubre de 2022, disponible en <https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/>.

8 Entornos complejos

En esta última sección se analizan los sitios y servicios que podrían considerarse como proveedores de una función única y específica (como una función de “medios sociales”) o como proveedores de una combinación de las funciones analizadas en las secciones anteriores para crear un entorno más enriquecido para la interacción de los usuarios. En última instancia, el análisis de políticas es muy similar: las entidades manejan contenido creado por otras personas y, por lo tanto, la imposición de responsabilidad a las entidades plantea importantes problemas no solo a esta categoría de funciones, sino también a otras funciones críticas de los intermediarios de Internet.

8.1 Medios sociales

Descripción de la función: proporcionar un entorno de red social que permita a los usuarios conectarse con otros usuarios, así como crear, compartir, intercambiar, recibir e interactuar con contenido creado por terceros. En la sección 5.1 del Marco de políticas¹⁶ se analizan los medios sociales con más detalle.

Consideraciones técnicas y prácticas: los medios sociales facilitan la comunicación, la creación de redes y el descubrimiento de contenido entre los usuarios, a menudo mediante una combinación de texto, imágenes, videos y enlaces. Otras funciones de los medios sociales son la gestión de cuentas de usuario, el alojamiento y distribución de contenido, los algoritmos de recomendación y personalización de contenido, y las herramientas de interacción con los usuarios, como los “me gusta”, los comentarios y las acciones compartidas. La función de proporcionar un entorno de medio social puede aplicarse a una amplia gama de sitios, no solo a los servicios de medios sociales grandes y conocidos. Por ejemplo, muchos sitios ofrecen a los usuarios la oportunidad de relacionarse entre sí, intercambiar contenido e ideas y entablar relaciones directas con otros usuarios. Las funciones de los “medios sociales” podrían aplicarse fácilmente a los servicios de medios sociales pequeños y de audiencia

¹⁶ Marco de políticas, Sección 5.1, Punto destacado: consideraciones de políticas para las plataformas de “medios sociales” que alojan, seleccionan y moderan contenido generado por el usuario.

de nicho, y también a sitios centrados en comunidades específicas de interés, como corredores de maratón, jardineros, seguidores de un equipo deportivo concreto o miembros de un partido o club político.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de medios sociales no deben ser responsables del contenido creado, publicado, enviado o recibido por sus usuarios.	Si las entidades que prestan servicios de medios sociales pudieran ser responsables del contenido generado por los usuarios (consulte la sección 1.5 del Marco de políticas¹⁷ para un análisis del contenido generado por los usuarios), podrían reducir significativamente las oportunidades de que las personas participen en el discurso en línea y podrían censurar en exceso el discurso, incluido el discurso legal de sus usuarios. Sin protecciones contra la responsabilidad, los proveedores podrían restringir considerablemente quién puede colocar contenido en línea, lo que limitaría significativamente la capacidad de las personas para comunicar contenido en Internet.
Los proveedores de medios sociales no deben ser responsables del contenido problemático creado, publicado, enviado o recibido por sus usuarios.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo publica, no en el proveedor de servicios que lo aloja. Responsabilizar a los proveedores socavaría su capacidad para transmitir cantidades significativas de contenido generados por los usuarios.

¹⁷ Marco de políticas Sección 1.5, Comparación entre la responsabilidad del contenido generado por el sitio y la responsabilidad del contenido generado por el usuario.

Enfoques de políticas recomendados	Motivos para este enfoque
Cuando las preocupaciones en materia de políticas se centran en las acciones del proveedor de servicios (y no en el contenido de las publicaciones de los usuarios), cualquier respuesta en forma de política no debería afectar la libertad de expresión de los usuarios.	Como se señala en la Sección 5.1 del Marco de políticas, existe una amplia gama de leyes y políticas que pueden aplicarse a los proveedores de servicios de medios sociales sin hacerlos responsables del contenido creado o comunicado por sus usuarios.

8.2 Redes federadas

Descripción de la función: proporcionar un enfoque descentralizado para alojar, compartir, seleccionar y moderar contenido generado por los usuarios, incluidos, por ejemplo, los entornos de medios sociales. Múltiples servidores operados de forma independiente pueden optar por participar en una red federada, lo que permite a los usuarios interactuar a través de la red federada mientras cada servidor mantiene el control sobre sus propios datos y comunidades. Por ejemplo, a diferencia de la comunidad de un medio social controlada centralmente, el sistema de un social federado puede permitir que muchas comunidades independientes más pequeñas se conecten y compartan contenido en todo el ecosistema federado. Esto puede crear una experiencia similar a la de un medio social, pero con un enfoque más local hacia la moderación. La Sección 5.2 del Marco de políticas¹⁸ trata las redes federadas con más detalle.

Consideraciones técnicas y prácticas: los medios sociales federados compuestos por servidores operados de forma independiente usando protocolos estandarizados como ActivityPub se han vuelto más populares. En este tipo de red, cada servidor independiente establece sus propias normas y políticas, por ejemplo, sobre moderación, privacidad de los datos y otros temas, sin dejar de participar en una red más amplia. El sistema mundial de correo electrónico de Internet es otro ejemplo de red federada, ya que una gran cantidad de servidores de correo administrados de forma independiente intercambian correos electrónicos entre sí sin acuerdo previo. El sistema de correo electrónico permite a cada entidad

¹⁸ Marco de políticas, Sección 5.2, Punto destacado: consideraciones de políticas para “redes federadas” que habilitan nuevos enfoques para facilitar la participación del usuario.

participante establecer sus propias políticas, por ejemplo, sobre el manejo del correo no deseado y los límites de almacenamiento de mensajes. Los proveedores de servicios federados, muchos de los cuales son pequeñas empresas u organizaciones, permiten a los usuarios mantener amplias conexiones a través de Internet y, al mismo tiempo, seleccionar un proveedor de servicios que ofrezca políticas de privacidad, moderación y otras que se ajusten a sus preferencias.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de contenido federados no deben ser responsables del contenido creado, publicado, enviado o recibido por sus usuarios.	Si estos proveedores pudieran ser responsables del contenido generado por los usuarios, es posible que no puedan (técnica o financieramente) continuar ofreciendo esos servicios. Por su naturaleza, las redes federadas atraen a pequeñas empresas e incluso a individuos como proveedores de servicios. Si estas entidades no pueden operar, los usuarios de Internet perderían valiosas herramientas que ofrecen alternativas a las grandes empresas de medios sociales y una moderación de contenido más granular.
Los proveedores de servicios de contenido federados no deben ser responsables del contenido problemático creado, publicado, enviado o recibido por sus usuarios.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que publicó el contenido y no en el proveedor de servicios que lo aloja. Poner la responsabilidad en el proveedor federado socavaría el potencial positivo de las redes federadas y restringiría en gran medida su disponibilidad.

8.3 Entornos de juego

Descripción de la función: facilitar que múltiples jugadores se conecten y jueguen juntos a videojuegos en tiempo real a través de Internet, lo que incluye facilitar una serie de métodos para que los jugadores interactúen e intercambien comunicaciones y contenido entre sí. La Sección 5.3 del Marco de políticas,¹⁹ describe los entornos de juego con más detalle.

Consideraciones técnicas y prácticas: la mayoría de los entornos de juego modernos, si no todos, están parcialmente conectados a través de Internet, y algunos están totalmente basados en Internet. Los componentes de comunicación habituales en los entornos de juego incluyen un chat dentro del juego y las conexiones directas de voz y video de persona a persona. Los ecosistemas de juego no son meros espacios para que los usuarios participen en juegos en línea con otros usuarios de todo el mundo: también proporcionan un entorno de medios sociales.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de entornos de juego no deben ser responsables del contenido creado, publicado, enviado o recibido por sus usuarios.	Si los proveedores pudieran ser responsables del contenido de las comunicaciones de sus clientes, podrían reducir significativamente las oportunidades de que las personas se relacionen entre sí, y podrían censurar en exceso el discurso, incluido el discurso legal, que sus usuarios tratan de comunicar. Sin protecciones contra la responsabilidad, se podría restringir severamente quién puede participar y qué contenido puede publicarse, lo que alteraría y limitaría significativamente los ecosistemas de juego.

¹⁹ Marco de políticas, Sección 5.3, Punto destacado: consideraciones de políticas para el ecosistema de juegos interactivos en línea.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de entornos de juego no deben ser responsables del contenido problemático creado, publicado, enviado o recibido por sus usuarios.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo ha publicado, no en el proveedor de servicios que lo aloja. Responsabilizar a un proveedor de juegos probablemente alteraría la dinámica de los juegos y socavaría la viabilidad de los sistemas de juego.

8.4 Entornos de realidad virtual y aumentada

Descripción de la función: permitir que múltiples usuarios interactúen y colaboren en un entorno compartido de realidad virtual (RV) o realidad aumentada (RA). La Sección 5.4 del Marco de políticas²⁰ analiza con más detalle los entornos de RV y RA.

Consideraciones técnicas y prácticas: aunque los entornos de realidad virtual o aumentada surgieron más recientemente que los sistemas de juego, los sistemas de RA y RV, al igual que los sistemas de juego, se integran cada vez más con Internet. Muchos entornos de RV y RA se conectan directamente a Internet y permiten a los usuarios interactuar entre sí en tiempo real. En algunos casos, los entornos de RV y RA pueden tener impactos directos en el mundo físico y en personas que no participan intencionadamente en estos entornos.

²⁰ Marco de políticas, Sección 5.4, Punto destacado: consideraciones de políticas para los sistemas de realidad virtual y realidad aumentada conectados a Internet.

Enfoques de políticas recomendados	Motivos para este enfoque
Los proveedores de servicios de entornos de realidad virtual y aumentada no deben ser responsables del contenido creado, publicado, enviado o recibido por sus usuarios.	Si los proveedores de RV y RA pudieran ser responsables del contenido de las comunicaciones de sus usuarios, podrían reducir significativamente las oportunidades de que las personas participen en discursos en línea y podrían censurar en exceso el discurso, incluido el discurso legal, que sus usuarios tratan de comunicar. Sin protecciones contra la responsabilidad, los proveedores podrían restringir severamente quién puede colocar contenido en línea y qué contenido pueden colocar, lo que alteraría y limitaría significativamente el desarrollo de las tecnologías y los servicios de RV y RA.
Los proveedores de entornos de realidad virtual y realidad aumentada no deben ser responsables del contenido problemático creado, publicado, enviado o recibido por sus usuarios.	La responsabilidad del contenido problemático debe recaer en la persona o entidad que lo ha publicado, no en el proveedor de servicios que lo aloja. Responsabilizar a los proveedores probablemente repercutiría negativamente en el desarrollo de tecnologías de realidad virtual y aumentada.