Imposición de bloqueos por DNS

Consideraciones críticas

7 de noviembre de 2025

Resumen

Aunque a menudo se presenta como una solución sencilla basada en políticas, la imposición de bloqueos por DNS es una medida ineficaz, perjudicial y poco práctica. Estos bloqueos son **ineficaces** porque los usuarios pueden eludirlos fácilmente y no eliminan el contenido que se pretende bloquear, el cual suele reaparecer bajo nuevos nombres de dominio. Son **perjudiciales** porque se trata de un instrumento impreciso que no distingue entre material lícito e ilícito, lo que provoca bloqueos excesivos, fragmenta el sistema global de nombres de dominio de Internet y genera fallas en los servicios interconectados, incluidos protocolos de seguridad críticos. Por último, son **poco prácticos** porque el DNS no está limitado por la geografía, lo que significa que las órdenes de bloqueo nacionales dirigidas a resolvedores globales producen efectos extraterritoriales no deseados y generalizados. Imponer bloqueos es una herramienta equivocada para una función para la que el DNS nunca fue diseñado. Para abordar los daños en línea, las intervenciones deben enfocarse en el propio contenido y en los actores responsables, sin comprometer la universalidad, la confiabilidad y la seguridad de la infraestructura básica de Internet.

Introducción

El Sistema de Nombres de Dominio (DNS) cumple una función crítica para Internet. Permite que las personas utilicen palabras familiares como “example.com” en vez de largas direcciones numéricas para acceder a sitios web, enviar correos electrónicos y utilizar diferentes servicios en línea. Sin esta capa de nombres, Internet no sería el sistema de comunicaciones global y práctico del que todo el mundo depende hoy en día.

Como el DNS ofrece esta función, a veces se considera un lugar conveniente para hacer cumplir las políticas públicas, especialmente porque el filtrado de DNS o control parental voluntario es una práctica común. Los gobiernos y los tribunales recurren cada vez más a la imposición de bloqueos por DNS para impedir el acceso a ciertos contenidos, ya sea para combatir la explotación infantil, evitar la infracción de los derechos de autor, limitar los juegos de azar en línea o abordar material políticamente sensible o ilícito.

Este enfoque parece sencillo: si un nombre no se puede traducir a su dirección IP, no es posible acceder al contenido. Sin embargo, esta simplicidad es engañosa. El DNS fue diseñado pensando en la universalidad, la consistencia y la usabilidad, no como una herramienta para la aplicación de políticas públicas. Reutilizarlo para este fin introduce efectos secundarios técnicos y operativos, genera tensiones jurídicas y jurisdiccionales y socava importantes medidas de seguridad que protegen a los usuarios. Es importante destacar que estas intervenciones son inherentemente imprecisas: no pueden dirigirse a páginas o archivos individuales, tienden a causar daños colaterales y son fáciles de eludir. Además, la naturaleza global y descentralizada del DNS hace que sea difícil que un bloqueo basado en la ubicación se limite a una única jurisdicción.

El mensaje de este informe es simple: imponer un bloqueo por DNS puede parecer una solución técnica sencilla para hacer cumplir las políticas públicas, pero en la práctica es una medida poco precisa, costosa e incluso contraproducente. Para entender por qué, es necesario considerar el DNS como una infraestructura global compartida y reconocer el impacto cuando se le asigna una función para la que no fue diseñado.

Breve introducción al DNS

El DNS proporciona la función de nombres que, en la práctica, permite que Internet funcione. Las computadoras utilizan direcciones IP para identificarse entre sí, pero estas son difíciles de recordar y de usar para las personas. Por lo tanto, la función del DNS es ofrecer una traducción entre nombres fáciles de recordar, como “example.com”, y los identificadores numéricos que las redes requieren para entregar los datos. De esta forma, permite a las personas interactuar con Internet de una manera sencilla e intuitiva, mientras que las computadoras siguen dependiendo de los identificadores numéricos necesarios para entregar los paquetes de datos.

El proceso de traducción entre nombres y direcciones se puede comprender a través de dos componentes clave del DNS. El primero es el *resolvedor recursivo*, un servidor que recibe la solicitud del usuario para resolver un nombre de dominio determinado (por ejemplo, “example.com”) y se encarga de encontrar la dirección IP correspondiente. Para ello, el resolvedor consulta secuencialmente una serie de *servidores de nombres autoritativos*, que son los servidores que almacenan los registros oficiales de porciones específicas o “zonas” del DNS. El proceso empieza en la parte superior de la jerarquía, la llamada zona “raíz”, que indica al resolvedor dónde encontrar los servidores del siguiente nivel (por ejemplo, “.com”). A su vez, estos servidores dirigen el resolvedor a los servidores autoritativos del dominio solicitado (por ejemplo, “example.com”), que finalmente proporcionan la dirección IP.

Esto subraya dos características importantes del DNS:

- **La resolución DNS es consistente, pero no persistente:** el operador del servidor autoritativo puede actualizar los registros de manera que un dominio apunte a diferentes direcciones IP a lo largo del tiempo. De hecho, muchos dominios están configurados para devolver varias

direcciones IP en una única respuesta, lo que permite que los usuarios sean dirigidos a servidores más próximos a su ubicación. Esta flexibilidad del DNS permite redundancia, distribución del tráfico y una rápida recuperación ante interrupciones del servicio.

- **La resolución DNS se produce antes de que se solicite cualquier página web o archivo específico:** los detalles de lo que se está accediendo, como el camino específico a una página web,[1] una imagen o un archivo de video, son gestionados posteriormente por el servidor web y el navegador (o por alguna otra aplicación). Como resultado, el DNS trabaja únicamente a nivel de nombres de dominio, no a nivel de páginas individuales u otros recursos.

Resolvedores DNS recursivos privados vs. públicos

Si bien técnicamente es posible instalar el resolvedor recursivo en el dispositivo del usuario para que realice todo el proceso de resolución de nombres por su cuenta, esto es poco común y en general poco práctico.[2] En vez de ello, la mayoría de los dispositivos depende de un resolvedor recursivo separado generalmente operado por su proveedor de servicios de Internet (ISP) u otro servicio.

Tradicionalmente, el resolvedor recursivo lo proporciona el ISP del usuario o, en el caso de una red empresarial, el administrador de la red. En este modelo, conocido como *resolvedor recursivo privado*, el resolvedor opera dentro de la red de acceso y está disponible principalmente para los suscriptores o miembros de dicha red. En este caso, el resolvedor recursivo se configura automáticamente a través de la configuración de la red. Como resultado, la mayoría de los usuarios desconocen el resolvedor específico que están utilizando, ya que se proporciona automáticamente como parte de su servicio de acceso a Internet.

En los últimos años, también ha aumentado el uso de los llamados *resolvedores recursivos públicos*. Estos son gestionados por organizaciones externas, como Google (8.8.8.8), Cloudflare (1.1.1.1) y Quad9 (9.9.9.9), que ponen sus resolvedores a disposición de cualquier usuario de Internet. Los resolvedores públicos suelen promocionarse por su mayor velocidad, sus funciones de seguridad avanzadas o sus mejores prácticas en materia de privacidad. Pueden ser adoptados por usuarios que reconfiguran sus dispositivos, por desarrolladores de aplicaciones que necesitan un rendimiento DNS consistente o por redes enteras que optan por externalizar la resolución DNS en vez de operar sus propios resolvedores.[3]

---

[1] El camino de una página web es la parte de la URL que sigue al nombre de dominio e identifica un recurso específico en el servidor web. Por ejemplo, en "https://example.com/articles/2025/DNSblocking.html", el nombre de dominio es "example.com", mientras que "/articles/2025/DNSblocking.html" es el camino de la página. La resolución DNS ignora todo lo que no sea el dominio.

[2] Internet Society, *Introduction to DNS Privacy* (2018), https://www.internetsociety.org/resources/doc/2018/introduction-to-dns-privacy/.

[3] Farzaneh Badiei and Sebastian Castro, *Resolving the Future – The DNS Layer and the Power to Navigate the Internet* (Digital Medusa, 2025), https://digitalmedusa.org/wp-content/uploads/2025/04/DNS-Resolvers-2025-Final.pdf.

Las diferencias operativas y estructurales entre los resolvedores recursivos privados y públicos son significativas en varios aspectos. En particular, los resolvedores privados generalmente están tanto técnica como contractualmente vinculados con la red de acceso en la que operan, lo que los convierte en parte de la relación de servicio directa con el usuario. Por el contrario, los resolvedores públicos se ofrecen como servicios independientes que operan globalmente y pueden estar ubicados en jurisdicciones diferentes a las de sus usuarios.

Bloqueo por DNS

El bloqueo por DNS (también conocido como filtrado basado en DNS) modifica el funcionamiento normal del DNS para impedir que los usuarios accedan a determinados nombres de dominio. Como se describió anteriormente, en condiciones normales, cuando un usuario escribe un nombre de dominio (por ejemplo, "example.com") en un navegador web, su resolvedor recursivo devuelve la dirección IP correspondiente para que el navegador (u otra aplicación) pueda conectarse al servidor correcto.

Sin embargo, con el bloqueo por DNS, el resolvedor está configurado para verificar los nombres solicitados contra una lista de bloqueo antes de completar la búsqueda. Si el nombre consultado está en la lista, el resolvedor devolverá una respuesta modificada o falsa en vez de la dirección IP real.

Los formuladores de políticas suelen citar el uso de filtrado voluntario como prueba de que la imposición de bloqueos por DNS es simplemente una extensión de prácticas ya existentes. Sin embargo, esta comparación resulta engañosa. Si bien ambos enfoques implican modificar las respuestas del DNS, difieren fundamentalmente en su propósito, implementación y efectos técnicos.

En primer lugar, el filtrado voluntario es impulsado por el usuario, la organización o el proveedor de servicios de Internet (ISP), quienes seleccionan una lista de bloqueo que pueden modificar o deshabilitar en cualquier momento. Por ejemplo, los usuarios pueden habilitar filtros de control parental para bloquear contenido pornográfico o listas de seguridad para protegerse contra el malware y los sitios de phishing.[4] Por el contrario, un bloqueo por DNS impuesto es una expresión de política pública dictada por agencias gubernamentales o tribunales cuyas decisiones son vinculantes para todos los operadores dentro de su jurisdicción. De este modo, la autoridad para decidir qué nombres pueden resolverse o no se traslada del perímetro de la red a una autoridad centralizada (el estado), donde las decisiones se imponen universalmente y sin la participación del usuario.

En segundo lugar, en los sistemas voluntarios el filtrado por DNS suele implementarse cerca del usuario, por ejemplo, en routers domésticos, firewalls corporativos o resolvedores a nivel de ISP, que el usuario puede reemplazar o reconfigurar. Por lo tanto, el filtrado opera en el marco de una relación limitada y

[4] Richard Barnes et al., *RFC 7754 Technical Considerations for Internet Service Blocking and Filtering* (2016), 77, https://datatracker.ietf.org/doc/rfc7754/.

transparente.[5] En cambio, los bloqueos por DNS impuestos requieren intervención a nivel de sistema: los resolvedores de toda una jurisdicción (y potencialmente más allá) deben reconfigurarse para cumplir con una orden. En la práctica, estas medidas eliminan la posibilidad de que los usuarios o las redes elijan resolvedores DNS alternativos, transformando una decisión de gestión local en una política de alcance nacional.

Por último, ambos enfoques difieren en sus consecuencias técnicas y operativas. El filtrado voluntario suele ser limitado, transparente y administrado localmente. Por ejemplo, si se produce un bloqueo excesivo, puede ser detectado y resuelto rápidamente para limitar su impacto en la Internet en general. En cambio, un bloqueo impuesto implica el riesgo de generar efectos colaterales significativos al imponer una resolución de nombres inconsistente entre distintas jurisdicciones.

¿Por qué los bloqueos por DNS son una herramienta poco precisa?

El bloqueo por DNS no elimina el contenido de Internet, sino que únicamente impide que un resolvedor específico resuelva las direcciones IP del servidor donde se aloja dicho contenido. El contenido sigue siendo accesible a través de otros resolvedores o mediante una conexión directa siempre que la dirección IP esté disponible.

Los bloqueos por DNS son fáciles de eludir

Existen numerosas técnicas de elusión fácilmente accesibles (e incluso automatizadas) que permiten que un usuario evite un bloqueo por DNS. Esto reduce drásticamente su eficacia a largo plazo.

En primer lugar, el usuario puede simplemente cambiar de resolvedor. Dado que los bloqueos por DNS suelen implementarse en resolvedores DNS específicos, como los operados por un proveedor de servicios de Internet, a menudo el usuario puede eludir el bloqueo dirigiendo las consultas a un resolvedor diferente. La mayoría de los usuarios empieza con un resolvedor elegido por su ISP que se ha configurado automáticamente a través de los ajustes de red durante la instalación. Sin embargo, los usuarios pueden anular esta configuración y apuntar a otro resolvedor (como un resolvedor público) o incluso ejecutar un resolvedor en su propio dispositivo. Por ejemplo, durante la prohibición de Twitter en Turquía en 2014, el uso del resolvedor público de Google para eludir los bloqueos por DNS de los ISP locales se generalizó tanto que la dirección IP del resolvedor (8.8.8.8.) se pintó con aerosol en las paredes para difundir información sobre cómo sortear la censura.[6]

---

[5] Internet Society, *Policy Brief: Perspectives on Internet Content Blocking* (2025), https://www.internetsociety.org/resources/policybriefs/2025/perspectives-on-internet-content-blocking/.

[6] Aaron Souppouris, 'Turkish Citizens Use Google to Fight Twitter Ban', The Verge, 21 March 2014, https://www.theverge.com/2014/3/21/5532522/turkey-twitter-ban-google-dns-workaround.

En segundo lugar, el usuario puede utilizar una red privada virtual (VPN) o la red Tor.[7] Estas herramientas cifran y redirigen todo el tráfico de Internet (incluidas las consultas al DNS) a través de servidores ubicados en otra red (potencialmente fuera de la jurisdicción afectada). Desde la perspectiva del resolvedor del ISP, no se están realizando consultas ya que la resolución DNS se realiza a través de servidores externos. Las VPN y Tor son herramientas cada vez más comunes que permiten que usuarios sin conocimientos técnicos eludan la censura.

No eliminan el contenido objetivo

El bloqueo por DNS únicamente impide que un resolvedor traduzca un nombre de dominio bloqueado a su dirección IP correspondiente. No elimina el contenido subyacente de Internet. En la práctica, el material generalmente sigue estando disponible y puede ser accedido otra vez una vez que se vincula a un nuevo nombre de dominio. Esta dinámica es especialmente visible en contextos en rápida evolución como el phishing, los discursos extremistas o la infracción de los derechos de autor. En estos casos, los operadores pueden registrar nuevos dominios y redirigirlos a los mismos servidores casi de inmediato. Como resultado, un bloqueo aplicado a un dominio suele tener un efecto temporal hasta que el sitio reaparece bajo otro dominio.[8]

Los bloqueos por DNS provocan problemas

La resolución DNS solo traduce un nombre de dominio a la dirección IP de un servidor web, no el camino completo de un recurso. Por ejemplo, cuando un usuario ingresa "https://example.com/page1" en su navegador, el DNS solo resuelve la parte "example.com" a una dirección IP. El resto del camino, es decir, "/page1" (o cualquier imagen, video o archivo específico), se gestiona una vez que se ha establecido una conexión con el servidor web. Esto significa que el bloqueo por DNS solo se aplica a nombres de dominio completos, no a páginas o archivos individuales.[9]

Esto convierte el bloqueo por DNS en una herramienta poco precisa. Aunque solo una página de un dominio sea ilícita, el bloqueo a nivel de DNS puede impedir el acceso al resto del contenido alojado en el mismo dominio, incluso si es legítimo. El impacto puede ser particularmente significativo en plataformas compartidas como redes sociales, blogs o servicios en la nube, donde millones de usuarios diferentes dependen de un mismo nombre de dominio. Por lo tanto, un solo bloqueo puede interrumpir grandes cantidades de contenido no relacionado.

Además, los servicios en línea rara vez existen como un único sistema alojado en un solo servidor. Por el contrario, lo que un usuario percibe como un sitio web o aplicación unificada suele estar compuesto por una colección de componentes distribuidos entre múltiples servidores. Por ejemplo, la estructura

[7] ICANN SSAC, *DNS Blocking Revisited*, SAC127 (2025), https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf.

[8] Barnes et al., *RFC 7754 Technical Considerations for Internet Service Blocking and Filtering*.

[9] ICANN SSAC, *SSAC Advisory on Impacts of Content Blocking via the DNS*, SAC056 (2012), https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-056-en.pdf.

básica de una página web podría obtenerse de un servidor y las imágenes y videos de otro, la función de inicio de sesión podría depender de un servicio de autenticación externo y las funciones adicionales podrían ser obtenidas de otros proveedores externos. Estos elementos, cada uno alojado en distintos servidores, se ensamblan para ofrecer una experiencia de usuario fluida y su funcionamiento generalmente depende de los nombres de dominio para ubicar y conectar las diferentes partes.[10] Estas dependencias también implican que bloquear un dominio puede generar fallas en sitios y aplicaciones no relacionados. Si un resolvedor devuelve una respuesta alterada o inconsistente, el servicio principal puede fallar por completo, incluso si el usuario no se da cuenta de qué parte del sistema originó el problema.[11]

La práctica de los bloqueos por DNS también tiene importantes implicancias para la seguridad. Por ejemplo, la comunidad de Internet desarrolló Extensiones de Seguridad de DNS (DNSSEC) para abordar vulnerabilidades del DNS. DNSSEC permite firmar criptográficamente los registros DNS de manera que los resolvedores recursivos puedan verificar que las respuestas que reciben son auténticas y no han sido alteradas. Cuando se implementa correctamente, DNSSEC previene ataques de intermediario (*man-in-the-middle*), en los que se inyectan respuestas DNS falsas para redirigir a los usuarios hacia sitios maliciosos. Esto crea un conflicto directo con el bloqueo por DNS, ya que cualquier intento de redirigir una consulta a un dominio distinto al solicitado interfiere con el funcionamiento de DNSSEC. Si un resolvedor devuelve una dirección IP falsificada para cumplir con una orden de bloqueo, por ejemplo, enviando al usuario a una página que indica que el sitio está bloqueado, esa respuesta no puede ser firmada por el operador legítimo del dominio y sería rechazada por la validación de DNSSEC. Mientras que DNSSEC busca garantizar la autenticidad mediante la validación criptográfica, el bloqueo por DNS introduce una falta de autenticidad deliberada. El resultado es un conflicto en el que las órdenes de bloqueo por DNS socavan la adopción generalizada de DNSSEC.[12]

Los bloqueos por DNS son poco prácticos

La arquitectura de Internet no se ajusta a la geografía ni a las jurisdicciones. Si bien la transmisión de datos inevitablemente ocurre a través de infraestructuras físicas ubicadas en lugares específicos, los sistemas de direccionamiento y nombres que permiten la comunicación por Internet operan de forma independiente de las fronteras geográficas. Por ejemplo, un dominio podría haber sido registrado a través de un registrador en un país determinado, sus servidores de nombres autoritativos podrían ser operados desde otro, y su contenido podría estar alojado en servidores web en una tercera jurisdicción. Para la red, todas estas ubicaciones pueden parecer muy cercanas en términos de milisegundos, incluso cuando geográficamente estén a muchos kilómetros.

---

[10] Populating the Page: How Browsers Work - Performance | MDN', MDN Web Docs, 11 August 2025, https://developer.mozilla.org/en-US/docs/Web/Performance/Guides/How_browsers_work.

[11] ICANN SSAC, *DNS Blocking Revisited*.

[12] Steve Crocker et al., *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill* (Authors (Affiliations provided for identification only), 2011), https://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Los resolvedores recursivos introducen aún más complejidad. Por ejemplo, un resolvedor público ubicado en el país A puede atender consultas de millones de usuarios en los países B, C y D. Las políticas de bloqueo de contenido aplicadas a este resolvedor pueden afectar a usuarios mucho más allá de la jurisdicción prevista a menos que el operador pueda distinguir la ubicación del usuario de manera muy confiable y rápida (en milisegundos), lo cual se complica por las limitaciones de la geolocalización de las direcciones IP.

Desde una perspectiva técnica, los operadores pueden implementar filtros que aproximen la ubicación geográfica de un usuario a partir de su dirección IP. Sin embargo, este enfoque dista mucho de ser preciso.[13] Este tipo de filtrado basado en la ubicación es imperfecto y puede clasificar erróneamente a los usuarios, especialmente en regiones donde las direcciones IP se asignan de forma fluida, se comparten entre países o se reasignan de forma dinámica. Esto puede provocar que usuarios legítimos fuera de la jurisdicción prevista vean denegado su acceso, mientras que los usuarios objetivo puedan seguir accediendo.

Además, la incorporación de filtrado basado en la ubicación también corre el riesgo de entrar en conflicto con los compromisos de privacidad y neutralidad de muchos operadores de resolvedores públicos. Servicios como los resolvedores públicos de Cloudflare o Quad9 se promocionan explícitamente como alternativas globales, consistentes y respetuosas de la privacidad frente a los resolvedores operados por los ISP.[14] Esto incluye políticas como no registrar, elaborar perfiles ni modificar las consultas al DNS de los usuarios según quiénes sean o dónde se encuentren. Por el contrario, el filtrado basado en la ubicación obligaría a los resolvedores a recopilar o inferir este tipo de información para cada consulta, lo que socavaría tanto la neutralidad como la privacidad.

Dado que el DNS es un sistema global, las medidas de bloqueo suelen entrar en conflicto con numerosos marcos legales nacionales. Lo que puede estar prohibido en una jurisdicción puede ser lícito en otra y una orden de bloqueo dictada a nivel nacional no puede conciliarse fácilmente con estas diferencias. Este problema es particularmente grave para los resolvedores públicos que prestan servicios a usuarios de todo el mundo y más allá de las fronteras. Cuando un regulador o un tribunal nacional ordena al operador de un resolvedor público que implemente un bloqueo, en la práctica le está pidiendo que aplique leyes nacionales a usuarios en el extranjero. El operador podría entonces enfrentarse a un dilema jurídico: cumplir con la orden y arriesgarse a infringir los derechos de los

[13] 'Geolocation Accuracy', MaxMind, 12 March 2025, https://support.maxmind.com/hc/en-us/articles/4407630607131-Geolocation-Accuracy; Jon Worley, 'IP Geolocation: The Good, The Bad, & The Frustrating', 11 June 2018, https://www.arin.net/vault/blog/2018/06/11/ip-geolocation-the-good-the-bad-the-frustrating/.

[14] 'Quad9 | A Public and Free DNS Service for a Better Security and Privacy', Quad9, accessed 2 September 2025, https://quad9.net/; '1.1.1.1 Public DNS Resolver', Cloudflare Docs, 13 August 2024, https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/.

usuarios o las leyes de otra jurisdicción, o negarse y exponerse a sanciones en la jurisdicción que impone el bloqueo.[15]

Además, implementar un bloqueo por DNS puede resultar costoso tanto para los operadores como para los usuarios. Hacerlo, especialmente cuando se aplica selectivamente por jurisdicción, exige no solo cambios técnicos en la infraestructura del resolvedor sino también una inversión operativa continua. Configurar una lista de bloqueo simple de aplicación global es relativamente fácil. Sin embargo, implementar un bloqueo dirigido basado en la ubicación del usuario o la jurisdicción aumenta significativamente la complejidad y los costos. Cuanto más fragmentadas sean las reglas, mayor será la carga operativa para los operadores de DNS y mayor la probabilidad de errores por bloqueo excesivo o insuficiente. Si bien el costo incremental de implementar una regla de bloqueo adicional puede ser moderado, los costos se multiplican a medida que más jurisdicciones imponen requisitos diferentes. El resultado podría ser una consolidación del mercado donde solo los grandes operadores puedan operar a gran escala, reduciendo la competencia y la diversidad en la prestación de servicios de DNS.[16]

Desde la perspectiva del usuario, un bloqueo también conlleva el riesgo de afectar la calidad del servicio, ya que integrar verificaciones de geolocalización en la resolución DNS podría aumentar la latencia. Aunque retrasos de tan solo unos milisegundos puedan parecer insignificantes, a escala de Internet impactan la experiencia del usuario porque las páginas complejas se cargan mucho más lentamente debido a que a cada componente se accede a través del DNS y se somete, por ejemplo, a una verificación de geolocalización. Esto también puede llevar a los usuarios a cambiar de resolvedores, lo que socava tanto el cumplimiento como los objetivos comerciales.

Conclusión

Como herramienta de política pública, los bloqueos por DNS resultan ineficaces, perjudiciales y poco prácticos.

No funcionan porque se pueden eludir fácilmente y no eliminan el contenido objetivo, que sigue siendo accesible, incluso bajo un nuevo nombre de dominio. Provocan problemas ya que bloquean excesivamente contenidos legítimos, fragmentan la resolución global de nombres y provocan fallas colaterales en servicios interconectados, incluida la seguridad. Son poco prácticos porque el DNS no está limitado geográficamente y la existencia de resolvedores globales significa que las órdenes de bloqueo nacionales producen efectos extraterritoriales.

---

[15] Ernesto van der Sar, 'French Piracy Blocking Order Goes Global, DNS Service Quad9 Vows to Fight', *TorrentFreak*, 12 December 2024, https://torrentfreak.com/french-piracy-blocking-order-goes-global-dns-service-quad9-vows-to-fight-241212/.

[16] David Abecassis et al., *The Economic Cost of Network Blocking* (Analysys Mason, 2025), https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/.

Por todas estas razones, la imposición de bloqueos por DNS no es la herramienta adecuada para la aplicación de políticas públicas, una función para la que nunca fue diseñado.

Si es necesario abordar daños en línea, las intervenciones deben enfocarse en el contenido, en los actores responsables y en medidas basadas en el debido proceso y la cooperación internacional. El DNS existe para facilitar el uso de Internet, no para servir como mecanismo de control. Preservar su universalidad, confiabilidad y seguridad es fundamental para mantener una Internet abierta, resiliente y global.

Referencias

Abecassis, David, Andrew Daly, et Dalya Glickman. The Economic Cost of Network Blocking. Analysys Mason, 2025. https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/

Badiei, Farzaneh, et Sebastian Castro. Resolving the Future – The DNS Layer and the Power to Navigate the Internet. Digital Medusa, 2025. https://digitalmedusa.org/wp-content/uploads/2025/04/DNS-Resolvers-2025-Final.pdf

Barnes, Richard, Alissa Cooper, Olaf Kolkman, Dave Thaler, et Erik Nordmark. RFC 7754 Technical Considerations for Internet Service Blocking and Filtering. 2016. https://datatracker.ietf.org/doc/rfc7754/

Documents Cloudflare '1.1.1.1 Public DNS Resolver'. 13 août 2024. https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/

Crocker, Steve, David Dagon, Dan Kaminsky, Danny McPherson, et Paul Vixie. Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill. Auteurs (Affiliations fournies à des fins d'identification uniquement), 2011. https://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf

ICANN SSAC. DNS Blocking Revisited. SAC127. 2025. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf

ICANN SSAC. SSAC Advisory on Impacts of Content Blocking via the DNS. SAC056. 2012. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-056-en.pdf

Internet Society. Introduction to DNS Privacy. 2018. https://www.internetsociety.org/resources/doc/2018/introduction-to-dns-privacy/

Internet Society. Perspectives sur le blocage de contenu sur Internet : tour d'horizon. 2017. https://www.internetsociety.org/resources/doc/2017/perspectives-on-internet-content-blocking/

MaxMind. 'Geolocation Accuracy'. 12 mars 2025. https://support.maxmind.com/hc/en-us/articles/4407630607131-Geolocation-Accuracy

Documents Web MDN 'Populating the Page: How Browsers Work - Performance | MDN'. 11 août 2025. https://developer.mozilla.org/en-US/docs/Web/Performance/Guides/How_browsers_work

Quad9. 'Quad9 | A Public and Free DNS Service for a Better Security and Privacy'. Consulté le 2 septembre 2025. https://quad9.net/

Sar, Ernesto van der. 'French Piracy Blocking Order Goes Global, DNS Service Quad9 Vows to Fight'. TorrentFreak, 12 décembre 2024. https://torrentfreak.com/french-piracy-blocking-order-goes-global-dns-service-quad9-vows-to-fight-241212/

Souppouris, Aaron. 'Turkish Citizens Use Google to Fight Twitter Ban'. The Verge, 21 mars 2014. https://www.theverge.com/2014/3/21/5532522/turkey-twitter-ban-google-dns-workaround

Worley, Jon. 'IP Geolocation: The Good, The Bad, & The Frustrating'. 11 juin 2018. https://www.arin.net/vault/blog/2018/06/11/ip-geolocation-the-good-the-bad-the-frustrating/