Blocage DNS imposé

Aspects essentiels

7 novembre 2025

Résumé

Le blocage DNS imposé, souvent présenté comme une solution politique simple, est inefficace, nuisible et peu pratique. Il est **inefficace,** car il est facilement contourné par les utilisateurs et ne parvient pas à supprimer le contenu ciblé, qui réapparaît simplement sous de nouveaux noms de domaine. Il est **nuisible,** car cet instrument imprécis est incapable de distinguer un contenu illégal d'un contenu légitime, ce qui entraîne un blocage excessif, une fragmentation du système mondial de nommage d'Internet et des défaillances des services interconnectés, y compris des protocoles de sécurité essentiels. Enfin, il est **peu pratique** car le DNS n'est pas limité par des frontières géographiques, ce qui signifie que les ordres nationaux de blocage visant des modules de résolution mondiaux créent des effets extraterritoriaux involontaires et étendus. Le blocage imposé est un outil inadapté à un rôle pour lequel le DNS n'a jamais été conçu. Pour lutter contre les préjudices en ligne, les interventions doivent se concentrer sur le contenu lui-même et sur les acteurs responsables, tout en ne compromettant pas l'universalité, la fiabilité et la sécurité de l'infrastructure fondamentale d'Internet.

Introduction

Le Système de Noms de Domaine (DNS) remplit une fonction essentielle pour Internet. Il permet aux utilisateurs d'employer des mots familiers, comme « example.com », au lieu de longues adresses numériques pour accéder aux sites Web, envoyer des e-mails et utiliser des services en ligne. Sans cette couche de nommage, Internet ne serait pas le système de communication mondial et pratique dont le monde dépend aujourd'hui.

Parce que le DNS offre cette fonction, il est parfois considéré comme un point pratique pour appliquer des politiques publiques, d'autant plus que le filtrage DNS volontaire ou parental est une pratique courante. Les gouvernements et les tribunaux ont de plus en plus recours au blocage DNS imposé pour empêcher l'accès à certains contenus, que ce soit pour lutter contre l'exploitation sexuelle des enfants, la violation du droit d'auteur, restreindre les jeux d'argent en ligne ou aborder des contenus politiquement sensibles ou illicites.

Cette approche paraît simple : si un nom ne peut pas être traduit en son adresse IP, le contenu devient inaccessible. Cette apparente simplicité est cependant trompeuse. Le DNS a été conçu pour l'universalité, la cohérence et la facilité d'utilisation, et non comme un outil d'application des politiques publiques. Le réutiliser à cette fin entraîne des effets secondaires techniques et opérationnels, crée des tensions juridiques entre les juridictions et compromet les mesures de sécurité importantes qui protègent les utilisateurs. Il est important de noter que ces interventions sont intrinsèquement imprécises : elles ne peuvent pas cibler des pages ou des fichiers spécifiques, sont sujettes à des dommages collatéraux et sont facilement contournées. De plus, la nature globale et décentralisée du DNS rend difficile de limiter le blocage basé sur la localisation à une seule juridiction.

Le message de ce rapport est simple : le blocage DNS imposé peut sembler une solution technique simple pour appliquer une politique publique, mais en pratique, il est imprécis, coûteux et même contre-productif. Pour comprendre pourquoi, il faut considérer le DNS comme une infrastructure mondiale partagée et reconnaître les conséquences lorsqu'on lui confie une tâche pour laquelle il n'a pas été conçu.

Comprendre le DNS (Une brève ébauche)

Le DNS assure la fonction de nommage qui permet le fonctionnement pratique de l'Internet. Bien que les ordinateurs utilisent des adresses IP pour s'identifier entre eux, celles-ci sont difficiles à mémoriser ou à utiliser pour les humains. Ainsi, le rôle du DNS est d'assurer la traduction entre des noms compréhensibles par l'être humain, comme « example.com », en identifiants numériques dont les réseaux ont besoin pour acheminer les données. Ce faisant, il permet aux utilisateurs d'interagir avec Internet de manière simple et intuitive, tandis que les ordinateurs continuent de s'appuyer sur les identifiants numériques nécessaires à l'acheminement des paquets de données.

Le processus de traduction entre les noms et les adresses peut être compris à travers deux composants clés du DNS. Le premier est le *résolveur récursif*, qui est un serveur recevant la requête de l'utilisateur pour résoudre un nom de domaine donné (par exemple, « example.com ») et qui est chargé de trouver l'adresse IP correspondante. Pour ce faire, le résolveur interroge séquentiellement une série de *serveurs de noms faisant autorité*, qui sont les serveurs qui détiennent les enregistrements officiels pour des portions spécifiques, ou « zones », du DNS. Le processus commence au sommet de la hiérarchie, la zone dite « racine », qui indique au résolveur où trouver les serveurs du niveau suivant (comme, « .com »). Ces serveurs, à leur tour, indiquent au résolveur les serveurs faisant autorité pour le domaine demandé (comme « example.com »), qui fournit enfin l'adresse IP.

Cela met en évidence deux caractéristiques importantes du DNS :

- **La résolution DNS est cohérente, mais non persistante :** L'opérateur du serveur faisant autorité peut mettre à jour les enregistrements afin qu'un domaine pointe vers différentes adresses IP au fil du temps. En fait, de nombreux domaines sont même configurés pour

renvoyer plusieurs adresses IP dans une seule réponse, permettant ainsi aux utilisateurs d'être dirigés vers les serveurs les plus proches d'eux. Cette flexibilité du DNS favorise la redondance, la répartition du trafic et une récupération rapide en cas de panne.

- **La résolution DNS se produit avant que toute page Web ou fichier spécifique ne soit demandé :** Les détails de ce qui est consulté, comme le chemin d'une page Web spécifique[1], une image ou un fichier vidéo, sont traités ultérieurement par le serveur Web et le navigateur (ou une autre application). En conséquence, le DNS fonctionne uniquement au niveau des noms de domaine, et non au niveau des pages individuelles ou d'autres ressources.

Résolveurs récursifs DNS privés vs publics

Bien qu'il soit techniquement possible d'installer le résolveur récursif sur l'appareil de l'utilisateur pour que le résolveur effectue de manière autonome l'intégralité du processus de résolution des noms, cela reste peu fréquent et très peu pratique[2]. La plupart des appareils s'appuient plutôt sur un résolveur récursif séparé, généralement exploité par leur fournisseur d'accès à Internet (FAI) ou un autre service.

Le résolveur récursif a traditionnellement été fourni par le FAI de l'utilisateur ou, dans le cas d'un réseau d'entreprise, par l'administrateur réseau. Dans ce modèle, appelé *résolveur récursif privé,* le résolveur récursif est exploité au sein du réseau d'accès et est principalement accessible aux abonnés ou aux membres de ce réseau. Dans ce cadre, le résolveur récursif est généralement configuré automatiquement via les paramètres réseau. Par conséquent, la plupart des utilisateurs ignorent quel résolveur spécifique ils utilisent, puisqu'il leur est fourni automatiquement dans le cadre de leur service d'accès à Internet.

Ces dernières années, on a également constaté une augmentation de l'utilisation des résolveurs *récursifs dits publics.* Ils sont exploités par des organisations tierces, telles que Google (8.8.8.8), Cloudflare (1.1.1.1) et Quad9 (9.9.9.9), qui rendent leurs résolveurs accessibles à toute personne connectée à Internet. Les résolveurs publics sont souvent mis en avant pour leur vitesse améliorée, leurs fonctionnalités de sécurité avancées ou leurs pratiques de confidentialité renforcées. Ils peuvent être adoptés par des particuliers qui reconfigurent leurs appareils, par des développeurs d'applications qui ont besoin de performances DNS constantes, ou par des réseaux entiers qui choisissent d'externaliser la résolution DNS plutôt que d'exploiter leurs propres résolveurs[3].

---

[1] Le chemin d'une page Web est la partie d'une URL qui suit le nom de domaine et qui identifie une ressource spécifique sur le serveur Web. Par exemple, dans « https://example.com/articles/2025/DNSblocking.html », le nom de domaine est « example.com », tandis que « /articles/2025/DNSblocking.html » correspond au chemin de la page. La résolution DNS ne prend en compte que le domaine.

[2] Internet Society, Introduction à la confidentialité sur l'Internet (2018), https://www.internetsociety.org/resources/doc/2018/introduction-to-dns-privacy/ .

[3] Farzaneh Badiei 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.

Les différences opérationnelles et structurelles entre les résolveurs récursifs privés et publics sont importantes à plusieurs égards. Notamment, les résolveurs privés sont généralement liés, à la fois sur le plan technique et contractuel, au réseau d'accès dans lequel ils fonctionnent, ce qui en fait une partie intégrante de la relation directe de l'utilisateur avec le service. En revanche, les résolveurs publics sont proposés comme des services indépendants, fonctionnant à l'échelle mondiale et pouvant être situés dans des juridictions différentes de celles de leurs utilisateurs.

Blocage DNS

Le blocage DNS (également appelé filtrage basé sur le DNS) modifie le fonctionnement normal du DNS pour empêcher les utilisateurs d'accéder à certains noms de domaine. Tel que cela est décrit ci-dessus, dans des conditions normales, lorsqu'un utilisateur saisit un nom de domaine (par exemple, « example.com ») dans un navigateur Web, son résolveur récursif renvoie l'adresse IP correspondante afin que le navigateur (ou une autre application) puisse se connecter au serveur approprié.

Cependant, avec le blocage DNS, le résolveur est configuré pour vérifier les noms demandés par rapport à une liste de blocage avant de compléter la recherche. Si le nom demandé figure sur la liste, le résolveur renverra une réponse modifiée ou erronée au lieu de l'adresse IP réelle.

Les décideurs politiques citent parfois l'utilisation du filtrage volontaire comme preuve que le blocage DNS imposé n'est qu'une extension des pratiques existantes. Cette comparaison est cependant trompeuse. Bien que les deux approches impliquent de modifier les réponses DNS, elles diffèrent fondamentalement par leur objectif, leur mise en œuvre et leurs effets techniques.

Tout d'abord, le filtrage volontaire est dirigé par l'utilisateur individuel, l'organisation ou le fournisseur d'accès à Internet (FAI), qui choisit une liste de blocage qu'il peut modifier ou désactiver à tout moment. Les utilisateurs peuvent, par exemple, activer des filtres de contrôle parental pour bloquer la pornographie ou des listes de sécurité pour se protéger contre les logiciels malveillants et les sites d'hameçonnage[4]. En revanche, le blocage DNS imposé est l'expression d'une politique publique, émise par des agences gouvernementales ou des tribunaux, dont les décisions sont contraignantes pour tous les opérateurs relevant de leur juridiction. L'autorité ayant le pouvoir de décider ce qui peut ou ne peut pas être résolu passe ainsi de la périphérie du réseau à une autorité centralisée (l'État), où les décisions sont imposées universellement et sans intervention des utilisateurs.

Ensuite, dans les systèmes volontaires, le filtrage DNS est généralement mis en œuvre près de l'utilisateur, par exemple sur les routeurs domestiques, les pare-feux d'entreprise ou les résolveurs au niveau du FAI, que l'utilisateur peut remplacer ou reconfigurer. Le filtrage s'effectue donc dans le cadre

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

d'une relation limitée et transparente[5]. Le blocage imposé, en revanche, nécessite une intervention au niveau du système, où les résolveurs de l'ensemble d'une juridiction (et potentiellement au-delà) doivent être reconfigurés pour se conformer à un ordre. De telles mesures suppriment la possibilité pratique pour les utilisateurs ou les réseaux de choisir des résolveurs alternatifs, transformant un choix de gestion local en une politique au niveau national.

Enfin, les deux approches diffèrent par leurs conséquences techniques et opérationnelles. Le filtrage volontaire est généralement limité, transparent et géré localement. Par exemple, en cas de blocage excessif, il peut être rapidement détecté et corrigé, avec un impact limité sur le reste d'Internet. En revanche, le blocage imposé risque d'entraîner d'importants effets collatéraux en imposant une résolution des noms incohérente à travers les juridictions.

Pourquoi le blocage DNS est un outil imprécis

Le blocage DNS ne supprime pas le contenu d'Internet. Il empêche seulement un résolveur particulier de résoudre les adresses IP du serveur qui héberge le contenu. Le contenu reste accessible via d'autres résolveurs ou par connexion directe dès que l'adresse IP est connue.

Le blocage DNS est facile à contourner

Les utilisateurs déterminés disposent de nombreuses techniques de contournement facilement accessibles (et même automatisées) pour éviter le blocage DNS. Cela réduit considérablement l'efficacité du blocage DNS à long terme.

Tout d'abord, l'utilisateur peut simplement changer de résolveur. Étant donné que le blocage DNS est généralement mis en œuvre sur des résolveurs spécifiques, tels que ceux exploités par un fournisseur d'accès à Internet (FAI), un utilisateur peut souvent contourner le blocage en dirigeant ses requêtes vers un autre résolveur. La plupart des utilisateurs commencent par un résolveur choisi par leur FAI et configuré automatiquement via les paramètres réseau lors de l'installation. Cependant, les utilisateurs peuvent remplacer ce paramètre et pointer vers un autre résolveur (par exemple, un résolveur public) ou même exécuter un résolveur sur leur propre appareil. Par exemple, lors de l'interdiction de Twitter en Turquie en 2014, l'utilisation du résolveur public de Google pour contourner les blocages DNS imposés par les FAI locaux est devenue si répandue que l'adresse IP du résolveur (8.8.8.8) a été peinte sur les murs pour indiquer comment contourner la censure[6].

[5] Internet Society, Fiche d'orientation politique : points de vue sur le blocage de contenu Internet (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 mars 2014, https://www.theverge.com/2014/3/21/5532522/turkey-twitter-ban-google-dns-workaround.

Ensuite, l'utilisateur peut utiliser un réseau privé virtuel (VPN) ou le réseau Tor[7]. Ces outils chiffrent et redirigent l'ensemble du trafic Internet (y compris les requêtes DNS) via des serveurs situés dans un autre réseau (potentiellement en dehors de la juridiction concernée). Du point de vue du module de résolution du FAI, aucune requête n'est effectuée, puisque la résolution DNS est réalisée via des serveurs externes. Les VPN et Tor sont des outils de plus en plus courants, ce qui facilite le contournement même pour les utilisateurs non techniques.

Le contenu ciblé n'est pas supprimé

Le blocage DNS empêche uniquement un module de résolution de traduire un nom de domaine bloqué en son adresse IP correspondante. Il ne supprime pas le contenu sous-jacent d'Internet. En pratique, le contenu reste généralement disponible et peut être à nouveau consulté dès qu'il est associé à un nouveau nom de domaine. Cette dynamique est particulièrement visible dans des contextes rapides comme le hameçonnage, la propagande extrémiste ou la violation du droit d'auteur. Dans de tels cas, les opérateurs ciblés peuvent enregistrer de nouveaux domaines et les diriger vers les mêmes serveurs presque immédiatement. En conséquence, un blocage appliqué à un domaine ne peut affecter l'accès que temporairement, jusqu'à ce que le site réapparaisse sous un autre nom[8].

Le blocage DNS perturbe le fonctionnement

La résolution DNS ne traduit qu'un nom de domaine en adresse IP d'un serveur Web, et non le chemin complet d'une ressource. Par exemple, lorsqu'un utilisateur saisit « https://example.com/page1 » dans son navigateur Web, le DNS ne résout que la partie adresse IP de « example.com ». Le reste du chemin, c'est-à-dire la partie « /page1 » (ou toute image, vidéo ou fichier spécifique), est traité une fois qu'une connexion a été établie avec le serveur Web. Cela signifie que le blocage DNS ne peut s'appliquer qu'aux noms de domaine entiers, et non aux pages ou fichiers individuels[9].

Cela fait du blocage DNS un outil imprécis. Si une seule page d'un domaine est illégale, le blocage au niveau DNS empêche l'accès à tout le reste du contenu licite hébergé sous ce même domaine. L'impact peut être particulièrement important pour les plateformes mutualisées telles que les réseaux sociaux, les services de blogging ou les services cloud, où des millions d'utilisateurs différents peuvent dépendre du même nom de domaine. Un blocage unique peut donc perturber d'énormes quantités de contenu sans lien.

De plus, les services en ligne n'existent que rarement comme un système unique hébergé sur un seul serveur. En fait, ce qu'un utilisateur perçoit comme un site Web ou une application unifiée est généralement un ensemble de composants répartis sur plusieurs serveurs. Par exemple, la structure de

[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.

base d'une page Web peut être fournie par un serveur, tandis que les images ou les vidéos sont intégrées depuis un autre, la fonction de connexion peut dépendre d'un service d'authentification externe, et des fonctionnalités supplémentaires peuvent provenir d'autres fournisseurs tiers. Ces éléments, chacun hébergé sur des serveurs différents, sont assemblés pour offrir une expérience utilisateur fluide, et leur intégration repose généralement sur les noms de domaine pour localiser et connecter les différentes parties[10]. Ces dépendances signifient également que le blocage d'un domaine peut provoquer des dysfonctionnements sur des sites et applications sans lien entre eux. Si un module de résolution fournit une réponse modifiée ou incohérente, le service principal peut échouer complètement, même si l'utilisateur ne remarque jamais quelle partie du système a échoué[11].

La pratique du blocage DNS a également des implications importantes en matière de sécurité. Par exemple, la communauté Internet a développé les extensions de sécurité du DNS (DNSSEC) afin de remédier aux vulnérabilités du système DNS. DNSSEC permet de signer cryptographiquement les enregistrements DNS afin que les résolveurs récursifs puissent vérifier que les réponses qu'ils reçoivent sont authentiques et n'ont pas été altérées. Lorsqu'il est correctement déployé, DNSSEC empêche les attaques de type « man-in-the-middle » (soit l'attaque de l'homme du milieu) où de fausses réponses DNS sont injectées afin de rediriger les utilisateurs vers des sites malveillants. Cela crée un conflit direct avec le blocage DNS, car toute tentative de rediriger une requête vers autre chose que le domaine demandé va à l'encontre du fonctionnement prévu de DNSSEC. Si un résolveur renvoie une adresse IP falsifiée pour se conformer à une mesure de blocage, par exemple en redirigeant l'utilisateur vers une page indiquant que le site est bloqué, cette réponse ne peut pas être signée par l'opérateur légitime du domaine et serait donc rejetée par la validation DNSSEC. Lorsque DNSSEC vise à garantir l'authenticité par une validation cryptographique, le blocage DNS introduit une inauthenticité délibérée. Il en résulte un conflit dans lequel les mesures de blocage DNS compromettent l'adoption généralisée de DNSSEC.[12]

Le blocage DNS est peu pratique

L'architecture d'Internet ne correspond pas aux frontières géographiques ou aux juridictions. Alors que la transmission des données s'effectue inévitablement via des infrastructures physiques situées dans des lieux précis, les systèmes d'adressage et de nommage qui permettent la communication sur Internet fonctionnent indépendamment des frontières géographiques. Par exemple, un domaine peut être enregistré auprès d'un bureau d'enregistrement dans un pays, ses serveurs de noms faisant autorité étant exploités depuis un autre, et les serveurs Web hébergeant réellement le contenu se trouvant encore dans un autre pays. Pour le réseau, tous ces emplacements dispersés peuvent sembler très «

[10] 'Populating the Page: How Browsers Work - Performance | MDN', MDN Web Docs, 11 août 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 (Auteurs (Affiliations fournies uniquement à des fins d'identification), 2011), https://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf.

proches » en termes de millisecondes plutôt qu'en miles ou en kilomètres, même s'ils sont répartis géographiquement.

Les résolveurs récursifs ajoutent encore plus de complexité. Par exemple, un résolveur public situé dans le pays A peut traiter les requêtes de millions d'utilisateurs des pays B, C et D. Les politiques de blocage de contenu appliquées à ce résolveur peuvent donc affecter des utilisateurs bien au-delà de la juridiction visée, à moins que l'opérateur ne puisse déterminer de manière fiable et extrêmement rapide (en quelques millisecondes) la localisation de chaque utilisateur, ce qui est compliqué par les limites de la géolocalisation basée sur l'adresse IP.

D'un point de vue technique, les opérateurs peuvent mettre en place des filtres qui estiment la localisation géographique d'un utilisateur en se basant sur son adresse IP. Cependant, cette approche est loin d'être précise[13]. Ce type de filtrage basé sur la localisation est imparfait et peut entraîner des erreurs de classification des utilisateurs, en particulier dans les régions où les adresses IP sont mobiles, partagées entre plusieurs pays ou réattribuées de manière dynamique. Cela peut conduire à ce que des utilisateurs légitimes situés en dehors de la juridiction visée se voient refuser l'accès, tandis que les utilisateurs ciblés peuvent malgré tout y accéder.

De plus, l'ajout d'un filtrage basé sur la localisation risque également d'entrer en conflit avec les engagements en matière de confidentialité et de neutralité de nombreux opérateurs de résolveurs publics. Des services tels que les résolveurs publics de Cloudflare ou de Quad9 se présentent explicitement comme des alternatives globales, cohérentes et respectueuses de la confidentialité aux résolveurs gérés par les FAI[14]. Cela inclut des politiques telles que l'absence de journalisation, de profilage ou de modification des requêtes DNS des utilisateurs en fonction de leur identité ou de leur localisation. En revanche, le filtrage basé sur la localisation obligerait les résolveurs à collecter ou à déduire ce type d'informations pour chaque requête, compromettant à la fois la neutralité et la confidentialité.

Étant donné que le DNS est un système mondial, les mesures de blocage entrent souvent en conflit avec de nombreux cadres juridiques nationaux. Ce qui peut être interdit dans une juridiction peut être légal dans une autre, et un ordre de blocage émis au niveau national ne peut pas facilement tenir compte de ces différences. Ce problème est particulièrement aigu pour les résolveurs publics, qui desservent des utilisateurs à l'échelle mondiale et au-delà des frontières. Lorsqu'un organisme de réglementation national ou un tribunal ordonne à un opérateur de résolveur public de mettre en place un blocage, il demande en réalité à cet opérateur d'appliquer la législation nationale à des utilisateurs

[13] 'Geolocation Accuracy', MaxMind, 12 mars 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, consulté le 2 septembre 2025, https://quad9.net/; '1.1.1.1 Public DNS Resolver', Documents Cloudfare, 13 août 2024, https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/.

situés à l'étranger. L'opérateur se retrouve alors confronté à un dilemme juridique : se conformer à l'ordre et risquer de violer les droits des utilisateurs ou les lois d'une autre juridiction, ou refuser et s'exposer à des sanctions dans la juridiction imposant le blocage[15].

Enfin, la mise en œuvre du blocage DNS peut s'avérer coûteuse, tant pour les opérateurs que pour les utilisateurs. La mise en œuvre du blocage, en particulier lorsqu'il est appliqué de manière sélective selon la juridiction, nécessite non seulement des modifications techniques de l'infrastructure des modules de résolution, mais aussi un investissement opérationnel continu. Une simple liste de blocage appliquée à l'échelle mondiale est relativement facile à configurer, mais un blocage ciblé basé sur la localisation des utilisateurs ou la juridiction légale augmente considérablement la complexité et le coût. Plus les règles deviennent fragmentées, plus le fardeau opérationnel des opérateurs DNS est important et plus le risque d'erreurs, de blocages excessifs ou insuffisants, augmente. Bien que le coût supplémentaire pour prendre en charge une règle de blocage additionnelle puisse être modeste, les coûts se multiplient à mesure que de plus en plus de juridictions imposent des exigences différentes. Le résultat peut être une consolidation du marché, où seuls les acteurs les plus importants peuvent opérer à grande échelle, ce qui réduit la concurrence et la diversité de l'offre de services DNS.[16]

Du point de vue de l'utilisateur, le blocage risque également d'affecter la qualité du service, car l'intégration de vérifications de géolocalisation dans la résolution DNS peut augmenter la latence. Bien que des retards de seulement quelques millisecondes puissent sembler insignifiants, à l'échelle d'Internet ils ont un impact sur l'expérience utilisateur, car les pages complexes se chargent beaucoup plus lentement puisque chaque composant est atteint via le DNS et subit, par exemple, une vérification de géolocalisation. Cela peut également inciter les utilisateurs à se tourner vers des résolveurs alternatifs, ce qui compromet à la fois la conformité et les objectifs commerciaux.

Conclusion

En tant qu'outil de politique publique, le blocage DNS est inefficace, nuisible et peu pratique.

Cela ne fonctionne pas, car il peut être facilement contourné et ne parvient pas à supprimer le contenu visé, qui reste accessible, y compris sous un nouveau nom de domaine. Cela perturbe le fonctionnement en entraînant un blocage excessif de contenus licites, en fragmentant la résolution globale des noms de domaine et en provoquant des défaillances collatérales au sein de services interconnectés, y compris les services de sécurité. C'est peu pratique, puisque le DNS n'est pas limité

[15] Ernesto van der Sar, '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/.

[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/.

par la géographie, et que les modules de résolution mondiaux font que les mesures nationales de blocage produisent des effets extraterritoriaux.

Pour toutes ces raisons, le blocage DNS imposé est un outil inadapté à l'application des politiques publiques. Un rôle pour lequel il n'a jamais été conçu.

Si les préjudices en ligne doivent être traités, les interventions devraient se concentrer sur le contenu lui-même, les acteurs responsables, ainsi que sur des mesures fondées sur le respect des procédures légales et la coopération internationale. Le DNS existe pour rendre Internet utilisable, et non pour servir de mécanisme de contrôle. Préserver son universalité, sa fiabilité et sa sécurité est essentiel pour maintenir un Internet ouvert, résilient et accessible à l'échelle mondiale.

Références

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/