Fiche d'orientation politique: points de vue sur le blocage de contenu Internet

Septembre 2025

Synthèse

Imaginez que l'on cherche à empêcher des personnes d'entrer dans un bâtiment en ville en fermant toute une rue. Cette rue pourrait aussi desservir des hôpitaux, des écoles et des habitations, donc la fermer couperait l'accès à de nombreux services essentiels pour beaucoup de gens, et des individus déterminés trouveront quand même d'autres moyens d'y entrer. C'est similaire à ce qui se passe lorsque les gouvernements tentent de bloquer l'accès à certains sites Web ou contenus en ligne en coupant des parties d'Internet à l'aide de méthodes de blocage d'adresses IP (Protocole Internet) ou DNS (Système de Noms de Domaine). Bien que cette approche puisse paraître rapide et simple, elle a souvent des conséquences plus importantes que prévu, perturbe d'autres services et ne résout pas le problème de fond.

Le blocage d'adresses IP et DNS est devenu la méthode la plus couramment proposée en raison de sa simplicité apparente et de sa facilité de déploiement. Les gouvernements du monde entier demandent de plus en plus aux fournisseurs d'accès à Internet (FAI) et aux résolveurs DNS de bloquer l'accès au contenu Internet qu'ils jugent illégal ou répréhensible, comme les jeux d'argent non autorisés, le matériel d'abus sur enfants, la violation du droit d'auteur et les menaces à la sécurité nationale.1 . Cependant, ces méthodes échouent souvent à traiter efficacement les causes profondes des problèmes visés et peuvent provoquer d'importantes perturbations techniques ainsi que des dommages sociétaux.

Bien que le blocage de contenu puisse sembler être une solution rapide pour empêcher l'accès à du matériel illégal, il s'avère souvent inefficace et entraîne fréquemment le blocage de services légitimes, affectant à la fois les utilisateurs et les entreprises. De plus, le blocage d'adresses IP et DNS ne supprime pas le contenu d'Internet, le rendant toujours accessible à des personnes déterminées. Les tentatives de contournement du blocage peuvent mettre en danger la confidentialité, la sécurité et la sûreté des utilisateurs.

[1] i2Coalition. *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, 3 juin 2025. Disponible sur : https://i2coalition.com/i2coalition-launches-dns-at-risk-report-and-website-to-spotlight-rising-global-internet-infrastructure-abuse/

L'Internet Society a publié une analyse technique des méthodes de blocage les plus courantes, en soulignant leurs limites et les risques potentiels. L'analyse montre que les deux techniques sont facilement contournées, imprécises et susceptibles de causer des dommages collatéraux. L'Internet Society encourage les décideurs politiques à privilégier les solutions qui s'attaquent aux contenus préjudiciables à la source, plutôt que de s'appuyer sur des mesures techniques brutales qui peuvent créer des externalités négatives sur la nature ouverte et mondiale de l'Internet.

Principaux points à considérer

Le blocage d'adresses IP et DNS, de par sa conception, interfère avec les mécanismes de base qui permettent aux utilisateurs de trouver et d'accéder à des informations sur Internet. La mise en œuvre de méthodes de blocage d'adresses IP et DNS implique bien plus qu'une simple exécution technique. Ces approches ont un impact sur le fonctionnement fondamental d'Internet et leur utilisation peut entraîner des conséquences opérationnelles, juridiques et sociétales importantes. Cette section présente les facteurs essentiels qui devraient guider toute réflexion politique sur le blocage de contenu.

Le **blocage d'adresses IP** refuse l'accès à un contenu en empêchant l'établissement de connexions TCP/IP vers des adresses IP spécifiques, coupant ainsi efficacement la communication avec les serveurs ciblés. Le **blocage DNS** quant à lui, manipule le système de noms de domaine en renvoyant des réponses fausses ou trompeuses lorsqu'un utilisateur tente d'accéder à un domaine bloqué, donnant l'impression que le contenu est inaccessible.

Les deux approches sont généralement imposées au niveau national et habituellement mises en œuvre au sein du réseau du fournisseur d'accès à Internet (FAI). Elles sont privilégiées dans les cercles politiques en raison de leur apparente simplicité et de leur évolutivité. Cependant, ces techniques peuvent manquer de précision et sont facilement contournées par les utilisateurs via des VPN (réseaux privés virtuels) ou en changeant les résolveurs DNS, tandis que les fournisseurs de contenu peuvent simplement changer l'infrastructure sur laquelle le contenu est hébergé.

Ce qui définit en fin de compte le problème, c'est l'écart entre les résultats politiques escomptés et les effets techniques réels. Ces méthodes ne suppriment pas le contenu d'Internet et ne s'attaquent pas à sa source. Au contraire, elles imposent des barrières d'accès peu fiables et sujettes à des dommages collatéraux. Ce décalage entre les objectifs des politiques et la réalité technique souligne la nécessité de réponses plus nuancées, plus efficaces et moins perturbatrices.

Défis

La mise en œuvre du blocage d'adresses IP et DNS soulève une série de défis techniques, sociaux, économiques et politiques complexes. Sur le plan technique, ces mesures sont par nature des instruments rudimentaires, incapables de distinguer efficacement un contenu illégal d'un contenu légitime lorsqu'ils sont hébergés sous la même adresse IP ou sont susceptibles d'être résolus via le même domaine. En conséquence, les services légaux sont souvent pris entre deux feux, entraînant un blocage excessif et un risque d'interruption de l'accès aux informations et aux plateformes essentielles.

Imaginez un serveur hébergeant à la fois un site de streaming pirate et un petit site de commerce électronique utilisant la même adresse IP. Un ordre de blocage de cette adresse IP bloquera également l'accès au site de commerce électronique, perturbant ainsi les opérations commerciales légitimes même si le site n'était pas impliqué dans le piratage[2]. Cela illustre comment le blocage au niveau des adresses IP peut provoquer de vastes perturbations de services, bien au-delà de l'objectif initial.

Pour tenter de récupérer l'accès, les utilisateurs peuvent se tourner vers des outils tels que les VPN ou différents résolveurs DNS. Le danger est que les utilisateurs, en cherchant à contourner le blocage de contenu, risquent de choisir involontairement des VPN ou des résolveurs DNS qui promettent l'accès, mais offrent des protections moindres en matière de sécurité et de confidentialité. Par conséquent, l'expérience Internet de ces utilisateurs peut devenir moins sûre et moins sécurisée. Des entreprises légitimes peuvent être contraintes de déplacer leurs services vers une adresse IP ou un domaine non bloqué, ou de changer de fournisseur d'hébergement.

Entre 2024 et 2025, l'Italie a déployé son système Piracy Shield, un dispositif anti-piratage agressif obligeant les FAI, les services DNS et les fournisseurs de VPN à bloquer, dans les 30 minutes suivant la demande des ayants droit, les domaines et adresses IP liés au streaming sportif illégal3. Cependant, cette politique a fréquemment entraîné un surblocage de services légitimes, y compris des domaines Google, des sites hébergés par Cloudflare et Google Drive, provoquant de larges perturbations pour les entreprises, les internautes et les services 4cloud.

Le blocage de domaines au niveau des résolveurs DNS publics peut avoir des conséquences inattendues qui vont au-delà du contrôle du contenu, affectant directement la sécurité en ligne des utilisateurs dans les pays où ces services opèrent. Par exemple, les résolveurs récursifs publics tels que Quad9[5] jouent un rôle essentiel dans la protection des utilisateurs contre les logiciels malveillants, le

[2] The i2Coalition, *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, mai 2025, p. 8, disponible sur : https://i2coalition.com/wp-content/uploads/2025/05/DNS-at-Risk-How-Network-Blocking-and-Fragmentation-Undermine-the-Global-Internet.pdf.

[3] TechRadar, *Italy's Piracy Shield may be breaching EU law…*, 10 juillet 2025

[4] DediRock, *Report Highlights Risks of Government DNS Blocking*, juin 2025

[5] Quad9. *About Quad9*. Disponible sur : https://quad9.net/about

phishing et d'autres cybermenaces en filtrant les domaines nuisibles en fonction des flux de renseignements sur les menaces mondiales.

Lorsque les gouvernements obligent ces résolveurs à détourner des ressources techniques et opérationnelles pour mettre en œuvre des blocages spécifiques au contenu, cela peut compromettre leurs fonctions de sécurité essentielles. Cela affaiblit non seulement le bouclier protecteur des particuliers et des entreprises, mais peut également réduire la cyber-résilience globale d'un pays en supprimant ou en altérant une couche d'infrastructure de confiance. Le risque est qu'en appliquant des mesures spécifiques à chaque site, les autorités érodent par inadvertance un service défensif qui profite à des millions d'utilisateurs, les laissant plus exposés à la fraude en ligne, au vol d'identité et aux attaques réseau.

D'un **point de vue économique,** les mesures de blocage d'adresses IP et DNS peuvent entraîner des coûts importants pour les fournisseurs d'accès à Internet et les opérateurs de réseau. Ces coûts comprennent les dépenses opérationnelles liées à la mise en œuvre et à la maintenance des systèmes de blocage, les pertes de revenus pour les plateformes en ligne et les entreprises touchées par le surblocage, ainsi que des impacts économiques plus importants résultant d'une confiance et d'une fiabilité réduites dans l'infrastructure Internet[6].

Principes directeurs et recommandations

L'Internet Society estime que la manière la plus appropriée de lutter contre le contenu illégal et les activités illicites sur Internet est de s'attaquer à leur source. L'utilisation du DNS ou des adresses IP pour bloquer l'accès à des contenus en ligne est probablement inefficace et susceptible de causer des dommages collatéraux touchant des internautes innocents. Pour ces raisons, ainsi que compte tenu des défis évoqués ci-dessus, nous déconseillons le blocage de contenu. Néanmoins, ces techniques sont toujours utilisées. Conscients de cette réalité, nous suggérons deux stratégies principales aux décideurs politiques préoccupés par les contenus illégaux sur Internet :

- **S'attaquer au problème à la source :** l'approche la moins dommageable pour Internet est d'attaquer les contenus illégaux et les activités illicites à leur source. La suppression du contenu illégal de sa source et la prise de mesures coercitives contre la source permettent d'éviter les effets négatifs du blocage et sont plus efficaces pour supprimer le contenu illégal. La coopération entre juridictions et parties prenantes est une condition préalable au succès, car le contenu illégal en ligne dépasse les frontières nationales et le cadre des lois nationales.
- **Prioriser et utiliser des approches alternatives,** par exemple :

[6] Analysys Mason, *The economic cost of network blocking*, report for Cloudflare, 28 juillet 2025. Disponible sur : https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/

- Une coopération efficace entre les fournisseurs d'accès, les forces de l'ordre et les autorités nationales peut fournir des moyens supplémentaires pour aider les victimes de contenus illégaux et pour prendre des mesures coercitives.
- Créer un environnement de confiance où les utilisateurs reçoivent des informations sur ce qui est légal et ce qui ne l'est pas peut améliorer l'autocontrôle. Dans certains cas (p. ex. le contrôle parental), permettre aux utilisateurs d'utiliser des filtres sur leurs propres appareils, avec leur consentement, peut être efficace et moins dommageable pour Internet.

Nous proposons les directives spécifiques suivantes pour réduire l'impact négatif du blocage de contenu :

- Écarter toutes les options autres que le blocage : en premier lieu, il faut épuiser toutes les solutions pratiques pour traiter le contenu à sa source, ou recourir à tout autre moyen alternatif au blocage. Le blocage de contenu ne doit pas être envisagé simplement parce que c'est plus facile. Il doit être nécessaire et proportionné.
- Faire preuve de transparence : il doit y avoir transparence sur le blocage, ainsi que sur l'objectif et les politiques de blocage de contenu sous-jacents. Les gouvernements doivent veiller à ce que les utilisateurs concernés puissent exprimer leurs préoccupations concernant les impacts négatifs sur leurs droits, leurs intérêts et leurs opportunités.
- Donner du pouvoir aux utilisateurs : ceux-ci doivent pouvoir filtrer eux-mêmes le contenu illégal ou indésirable sur leurs propres appareils ou réseaux, en ayant accès à des outils de sécurité en ligne et à des formations aux compétences numériques.
- Limiter la portée : bloquer le contenu autant que possible au niveau local afin de réduire l'impact à l'échelle mondiale.
- Impliquer les parties prenantes : l'élaboration et la mise en œuvre des politiques concernant le contenu en ligne devraient inclure un large éventail de parties prenantes, y compris des spécialistes des domaines technologique, économique, des droits des consommateurs et autres, afin de garantir que des mesures appropriées sont prises pour minimiser les effets secondaires négatifs des politiques visant ce contenu.
- Respecter la procédure légale : tout ordre de blocage de contenu illégal doit être fondé sur la loi, faire l'objet d'un examen indépendant et être ciblé de manière précise afin d'atteindre un objectif légitime. Les moyens les moins restrictifs disponibles pour traiter les activités illégales doivent être priorisés. Les fournisseurs d'accès à Internet ou autres intermédiaires en ligne ne doivent pas se transformer en agents de la force publique : ils ne devraient pas être tenus de déterminer quand un comportement ou un contenu est illégal.
- Limiter dans le temps : toutes les mesures de blocage doivent être temporaires. Elles doivent être supprimées dès que la raison du blocage cesse d'exister. Il est assez fréquent que le contenu illégal soit déplacé pour échapper aux mesures de blocage, alors que celles-ci restent souvent en place longtemps après le déplacement du contenu.

L'opposition de l'Internet Society au blocage d'adresses IP et DNS repose sur le fait que ces techniques compromettent les propriétés fondamentales d'Internet, telles que définies dans le mode de fonctionnement du réseau **Internet (abrégé IWN en anglais).** Ces méthodes de blocage perturbent l'architecture technique qui rend Internet ouvert, accessible à l'échelle mondiale et résilient.

L'Internet Society a élaboré une description technique de ces principes fondamentaux. Nous l'appelons « Mode de fonctionnement du réseau Internet » un cadre qui décrit ce qui rend Internet unique par rapport aux autres réseaux. Nous avons créé la boîte à outils pour l'évaluation de l'impact sur Internet[7] pour aider notre communauté d'experts techniques, politiques et autres à utiliser ce cadre. Il peut aider à identifier les domaines où les politiques, décisions commerciales, réglementations ou tendances peuvent affecter les fondements uniques d'Internet, ainsi que les bonnes pratiques qui les soutiennent.

[7] Internet Society. *Boîte à outils pour l'évaluation de l'impact sur Internet*, 2020. Disponible sur : https://www.internetsociety.org/fr/resources/internet-impact-assessment-toolkit/