8 novembre 2021

Les facilitateurs d'un Internet ouvert, mondialement connecté, sécurisé et fiable

Internet Society

Table des matières

Introduction

Le potentiel d'Internet est illimité. Internet, est donc une ressource mondiale, qui est utile au commerce, aux activités récréatives, à la recherche, à l'éducation, aux loisirs et à tout le reste. Mais, avec différentes parties prenantes et une rivalité dans les demandes du réseau, sauvegarder le futur d'Internet peut sembler une mission impossible.

Cette tâche pourrait ne pas être complexe. Internet a été créé sur une base unique[1] qui autorise les utilisateurs par-delà les frontières à modeler collectivement son évolution. À maintes reprises, différents groupes et organisations[2] du monde entier, avec des points de vue différents, ont trouvé un socle commun et un ensemble d'objectifs partagés pour Internet, c'est-à-dire un réseau ouvert, mondialement connecté, sécurisé et fiable.

La mission de l'Internet Society est elle aussi basée sur ces objectifs. Malheureusement, Internet est aujourd'hui loin de réaliser ce projet ambitieux d'ouverture, de connexion mondiale, de sécurité et de fiabilité. De plus, un éventail d'évolutions commerciales et d'interventions réglementaires gouvernementales (ou leur absence) menace de nous en éloigner au lieu de nous en rapprocher. C'est pourquoi il est urgent et important de protéger l'évolution d'Internet vers ces objectifs.

Ces objectifs servent de points de repère à notre parcours collectif vers un meilleur Internet. Ils nous indiquent ce que nous voulons qu'Internet soit, maintenant et à l'avenir. En étudiant les changements proposés dans les politiques, les technologies et les applications au regard de ces objectifs, nous pouvons mieux comprendre si nous progressons effectivement vers un Internet prospère, ou si nous nous en écartons.

Des objectifs ambitieux pour un Internet prospère	
Un Internet ouvert	Un Internet ouvert permet aux individus et aux organisations de fusionner les technologies, sans autorisation nécessaire et avec un minimum de barrières. La préservation et le développement d'un Internet ouvert contribuent à encourager l'innovation et lui permet de s'adapter aux applications futures.

1 Mode de fonctionnement du réseau Internet : Définition des propriétés essentielles d'Internet https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet

2 Voir par exemple Les objectifs de l'OCDE pour la prise de décision pour Internet (https://www.oecd.org/digital/ieconomy/oecd-goals-for-internet-policy-making.pdf), la déclaration du Département d'État américain sur la gouvernance de l'Internet (https://2009-2017.state.gov/documents/organization/255010.pdf), l'Union Africaine (https://au.int/sites/default/files/newsevents/conceptnotes/31357-cn-background_note_on_the_au_declaration_on_ig_en_1.pdf), la stratégie de l'Union européenne en matière de cybersécurité (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN), le Council of Foreign Relations (https://cdn.cfr.org/sites/default/files/pdf/2013/06/TFR70_cyber_policy.pdf.pdf), CITEL (http://www.oas.org/CITEL/citel1/ult-ciberseguridad_i.asp), la Global Commission on Internet Governance (https://www.cigionline.org/publications/one-internet/).

	Un Internet ouvert est un Internet accessible. Il est facile de se connecter à un Internet ouvert et d'utiliser ses services.
Un Internet mondialement connecté	L'Internet mondialement connecté est inclusif. Il permet aux réseaux et aux utilisateurs d'être interconnectés sans restrictions géographiques. Le renforcement de la connectivité d'Internet rend celui-ci plus précieux pour chaque participant, en tant qu'outil pour les communications, l'apprentissage et le commerce.
Un Internet sécurisé	Un Internet sécurisé est résistant aux attaques contre son infrastructure, et offre un service robuste à sa communauté d'utilisateurs. Un Internet sécurisé n'engendre pas d'insécurité, comme des botnets utilisés dans les attaques par hameçonnage. Améliorer la sécurité d'Internet renforce son utilité pour tous ses participants.
Un Internet fiable	Un Internet fiable répond aux attentes de ses utilisateurs en offrant une base résiliente et digne de confiance pour les applications et les services. Améliorer la fiabilité d'Internet donne aux individus et aux organisations la possibilité de se fier à Internet en tant que ressource de communications disponibles en continu au niveau mondial.

Les facilitateurs d'un Internet ouvert, mondialement connecté, sécurisé et fiable

Pour chacun de ces objectifs d'Internet, nous avons identifié une série de caractéristiques annexes pour faire progresser Internet, ses infrastructures et son utilisation vers ses objectifs universels. Nous appelons ces caractéristiques annexes les **« facilitateurs »** : ils font progresser et rendent possible l'objectif visé.

Identifier ces facilitateurs permet de simplifier l'analyse des effets potentiels des changements proposés et leurs possibles conséquences à terme sur les objectifs. Par exemple, un Internet sécurisé exige qu'Internet permette à la fois la confidentialité et l'intégrité des données. Ces deux paramètres sont des facilitateurs : la confidentialité des données soutient l'objectif d'un Internet sécurisé, de même que l'intégrité des données. Si l'un de ces paramètres fait défaut, la sécurité d'Internet en est réduite. Puisque ces facilitateurs, et non les objectifs, sont les outils pour l'analyse des propositions, ils sont l'épicentre de ce cadre.

Ci-dessous, nous avons identifié les facilitateurs[3] qui sont liés à chacun des quatre objectifs d'Internet. Pour éclaircir pleinement la signification de chaque facilitateur, ainsi que la façon dont celui-ci permet de s'approcher d'un objectif d'Internet, nous proposons des exemples de politiques ou technologies spécifiques à un facilitateur, qui font progresser ou régresser l'objectif dans le domaine identifié.

Il est important de remarquer que les facilitateurs sont présentés dans leur forme idéale. Le fait de les considérer comme le reflet d'un état parfait nous offre un point de référence, qui nous aide à déterminer si un développement particulier fait progresser Internet vers les objectifs identifiés ou s'il le fait régresser. Ces facilitateurs peuvent aussi mettre à jour certaines des tensions qui existent entre les objectifs et rendre plus visibles les éventuels inconvénients. Par exemple, certaines des actions peuvent avoir un effet positif sur la sécurité d'Internet, mais le rendre moins ouvert.

Soutenir un Internet ouvert

Internet est pleinement ouvert quand tout le monde peut y créer, l'utiliser et le déployer à sa guise. Avec un Internet complètement ouvert, tout le monde est libre de déployer des réseaux Internet et de créer des services et applications sur Internet, de les associer de façon originale et de les déployer sans barrières, tant que cela est fait de manière interopérable. Un Internet ouvert est un Internet accessible :

3 Cette liste de facilitateurs n'a pas vocation à être une énumération exhaustive de tout ce qui contribue à un objectif. Ils sont listés pour vous aider à analyser les changements susceptibles d'avoir un effet, positif ou négatif, sur l'objectif. SI vous identifiez un aspect d'un changement qui affecte fortement un objectif, mais ne rentre pas facilement dans la liste des facilitateurs, il peut s'agir d'un nouveau facilitateur. Utilisez-le dans votre analyse et transmettez-le-nous pour que nous puissions l'ajouter aux prochaines versions de ce document. Certains des facilitateurs peuvent être liés à plusieurs objectifs d'Internet. Par exemple, « l'accès facile et sans restrictions » pourrait aussi être pris en compte dans l'objectif de la connectivité mondiale. Ce cadre est une simplification de cette réalité : puisque les facilitateurs, et non les objectifs sont les principaux outils analytiques pour l'évaluation de l'impact, un facilitateur est associé à un objectif dans le seul but d'aider à contextualiser son rôle.

les réseaux peuvent facilement le rejoindre, et les utilisateurs peuvent facilement s'y connecter et utiliser ses services.

Les tableaux ci-dessous définissent certains des facilitateurs d'un Internet ouvert. Nous fournissons aussi quelques exemples de politiques ou technologies qui font progresser ou régresser l'objectif dans le domaine identifié. Veuillez remarquer que ces exemples doivent être compris comme des illustrations de leurs effets sur les facilitateurs pour lesquels ils sont présentés : certains de nos exemples peuvent avoir des effets positifs sur un facilitateur et négatifs sur un autre[4].

Facilitateur	Accès facile et sans restrictions
Description	Il est facile de devenir une partie d'Internet, pour les réseaux comme pour les utilisateurs. Cela implique qu'Internet soit abordable pour les utilisateurs et que les services Internet soient accessibles, et que les réseaux puissent facilement intégrer Internet, sans règlement ou barrières commerciales superflus, pour les utilisateurs comme pour les réseaux.
Questions	Le changement proposé crée-t-il ou réduit-il une barrière à l'entrée, par exemple des coûts, des charges administratives ou d'autres complexités ? Ce changement restreint-il le nombre de personnes qui peuvent participer à Internet, en fermant celui-ci ? Le changement proposé entraîne-t-il inutilement des besoins de compétences particulières ou augmente-t-il les coûts ?

Exemple 1 : les directives d'accessibilité du contenu Web (WCAG) sont une recommandation du World Wide Web Consortium (W3C) pour rendre le contenu du Web plus accessible, principalement pour les personnes en situation de handicap. Par exemple, en recommandant des alternatives textuelles pour tout contenu non textuel pour qu'il puisse être converti en un autre format, comme la parole ou de grands caractères. Dans certaines juridictions, la conformité à ces directives est exigée par la loi pour protéger les droits des personnes en situation de handicap.

Il s'agit là d'un exemple d'effet positif sur un Internet ouvert pour les utilisateurs, renforçant « un accès facile et sans restrictions » en facilitant l'utilisation des services Internet par tous.

4 Pour des exemples plus détaillés d'évaluations de l'impact étudiant plusieurs facilitateurs, nous vous recommandons de visiter notre référentiel de fiches consacré à l'impact sur Internet, disponible ici : https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

Exemple 2 : l'octroi de licences pour le spectre est un procédé permettant aux agences de réglementation d'allouer des ressources peu abondantes et finies, l'accès aux ondes radio, à différents usages, dont l'usage d'Internet. Les politiques d'octroi de licences pour le spectre peuvent avoir un effet important sur l'accès à Internet dans des zones peu desservies par les infrastructures fibre et cuivre. Par exemple, en 2020, les États-Unis ont réattribué une partie du spectre pour soutenir les services 5G en récupérant des sections sous-utilisées du spectre, qui, à l'origine, avaient été allouées aux services télévisuels éducatifs dans les années 60.[5] Étant donné qu'une partie des ondes radio affectées étaient déjà utilisées pour élargir l'accès à Internet de groupes mal desservis, ce changement de politique pourrait avoir eu un effet négatif sur l'objectif d'un Internet ouvert en supprimant un accès au spectre qui était utilisé pour l'accès à l'Internet. Toutefois, ce processus de prise de décision ouvert préserve l'usage existant pour les services Internet et permet aux communautés rurales tribales d'avoir un accès prioritaire au spectre pour des réseaux communautaires, avant les intérêts commerciaux, bien qu'elles ne fassent pas le poids sur le plan économique.

Cela illustre un effet positif sur l'objectif d'un Internet ouvert pour les réseaux, renforçant « l'accès facile et sans restrictions » par des politiques qui favorisent l'accès à Internet pour les communautés et les groupes sans but lucratif.

Exemple 3 : dans certains pays, l'accès à Internet est uniquement disponible au travers de fournisseurs d'accès en situation de monopole. Cela entraîne des coûts plus élevés (du fait de l'absence de concurrence) ainsi qu'une limitation des types de services et méthodes de connexions disponibles. Ce manque de choix de fournisseurs limite concrètement l'accès global.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet ouvert aux utilisateurs et réseaux en affaiblissant un « accès facile et sans restrictions » par la restriction des options de connectivité et les coûts plus élevés.

Facilitateur	**Usage et déploiement sans restrictions des technologies Internet**
Description	Les technologies et normes Internet sont adoptables sans restrictions. Ce facilitateur s'applique aux terminaux; les technologies utilisées pour se connecter à Internet et l'utiliser n'exigent pas d'autorisation d'un tiers, d'un fournisseur de systèmes d'exploitation (OS), d'un fournisseur de réseau ou de tout autre tiers. L'infrastructure Internet est une ressource disponible pour quiconque souhaite l'utiliser. Les technologies existantes peuvent être combinées et utilisées pour créer de nouveaux produits et services qui élargissent les capacités d'Internet.

5 https://docs.fcc.gov/public/attachments/FCC-19-62A1.pdf

Questions	Le changement proposé réduit-il la façon dont les technologies d'Internet peuvent être utilisées ou déployées ? Ce changement crée-t-il une limite injuste ou discriminatoire ? Le changement proposé limite-t-il de façon déraisonnable la gestion et le contrôle par les utilisateurs finaux de leurs propres appareils ?

Exemple 1 : le système d'authentification SecurID de RSA était un système d'authentification multi-facteurs des débuts d'Internet, protégé par des brevets et secrets commerciaux. La dépendance à un seul fournisseur et les dépenses que cela entraînait étaient très rentables pour RSA, mais limitaient aussi la capacité des développeurs à inclure la technologie SecurID dans les applications d'Internet, ce qui privait les utilisateurs d'une possibilité de plus de sécurité et de protection contre l'usurpation d'identité.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet ouvert causé par la mise à mal de ce facilitateur, en restreignant l'utilisation et le déploiement de technologies.

Exemple 2 : OAuth[6] est un protocole conçu à l'origine pour résoudre le problème du partage de données d'un utilisateur privé d'une application avec une autre application, sans que l'utilisateur ne doive partager son mot de passe. Après des débuts modestes, il est devenu une solution d'authentification et d'autorisation très largement utilisée, des applications Internet aux solutions d'entreprise. La nature ouverte, collaborative et sans restrictions d'OAuth lui a permis de toucher de nombreux cas d'utilisation, ainsi que de nombreux produits et applications. L'existence d'un système sécurisé, standardisé et largement accepté pour l'authentification et l'autorisation réduit les barrières pour les innovations ultérieures et des utilisations d'Internet novatrices et sécurisées.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet ouvert, renforçant « l'utilisation et le déploiement sans restrictions de technologies d'Internet » en créant les éléments technologiques constitutifs d'une nature ouverte, collaborative et sans restrictions.

Exemple 3 : Google et Oracle se sont livrés durant neuf ans une bataille complexe[7] au sujet de l'Interface de programmation d'application Java (API) basée sur la propriété de Java par Oracle et l'utilisation par Google de l'API pour rendre son propre système d'exploitation Android compatible avec les applications Java. Oracle affirmait que l'API lui appartenait et qu'il pouvait la contrôler autant que le reste du code source Java, tandis que Google considérait que son utilisation de l'API n'était pas soumise au copyright selon la doctrine de « l'usage loyal ». Finalement, la Cour suprême américaine[8] a donné raison à Google : le

6 OAuth est développé par le Groupe de travail OAuth de l'IETF. Plus d'informations sont disponibles sur https://oauth.net/2/

7 Malgré un certain manque d'objectivité dans la description des problématiques, la description par l'EFF de l'historique du procès de *Google contre Oracle* est disponible pour ceux qui souhaiteraient une description détaillée sur https://www.eff.org/cases/oracle-v-google.

8 La décision de la Cour suprême est disponible sur https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf

copyright d'Oracle ne restreignait pas l'utilisation par Google de l'API. Les motifs de cette affaire étaient largement économiques : si Oracle avait gagné, Google aurait eu une énorme facture à payer vu l'immense popularité d'Android. Mais la question plus large de savoir si l'utilisation de l'API représentait un usage loyal affecte les innovations futures d'Internet.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet ouvert qui renforce « l'utilisation et le déploiement sans restrictions de technologies Internet », parce que la Cour suprême américaine a clairement établi que certains types d'innovation et d'utilisation ne pouvaient être restreints.

Facilitateur	**Développement, gestion et gouvernance collaboratifs**
Description	Les technologies et normes d'Internet sont développées, gérées et gouvernées d'une manière ouverte et collaborative. Cette collaboration ouverte s'étend à la construction et au fonctionnement d'Internet et des services construits sur Internet. Le processus de développement et de maintenance est basé sur la transparence et le consensus, et son objectif est l'optimisation de l'infrastructure et des services au bénéfice des utilisateurs de ces technologies.
Questions	Le changement proposé limite-t-il la collaboration durant le développement, le fonctionnement ou la gouvernance ? L'objectif de la politique proposée est-il de restreindre la collaboration ?

Exemple 1 : l'espace d'adressage d'Internet est une ressource limitée, qui exige une administration attentive. Au lieu d'une instance centralisée pour la prise de décision, chacune des grandes régions d'Internet est responsable de la gouvernance de l'espace d'adressage de sa région. Les décisions politiques relatives à l'espace d'adressage local sont basées sur un processus collaboratif conduit par la communauté de la région. Les politiques qui obtiennent un consensus sont mises en œuvre par le Registre Internet régional[9]. Cela crée un environnement au sein duquel Internet lui-même peut être « ouvert » selon un contexte adapté à la région.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet ouvert, renforçant « le développement, la gestion et la gouvernance collaboratifs » grâce à une gestion par la communauté des ressources d'Internet.

9 Vous trouverez plus d'informations sur les Registres Internet régionaux sur le site de la Number Resource Organization sur https://www.nro.net/about/rirs/

Exemple 2 : les points d'échange Internet (IXP) offrent aux opérateurs de réseaux communautaires la possibilité de se connecter et d'échanger du trafic Internet[10]. Le fait de réunir les acteurs d'Internet comme les FAI, les réseaux municipaux, et les réseaux de diffusion des données, permet que le trafic Internet local soit dirigé de manière plus efficace, et que les utilisateurs locaux bénéficient d'un meilleur accès, plus résilient au trafic régional. Les IXP incluent souvent des concurrents, qui collaborent pour leur bénéfice propre et celui de la communauté locale. De nombreux IXP ont une politique de peering ouverte et sans restrictions qui laisse chaque participant décider avec qui ils veulent faire le peering. Une politique de peering multilatérale avec tous les membres est très répandue.

Les IXP sont un exemple d'effet positif sur l'objectif d'un Internet ouvert, renforçant « le développement, la gestion et la gouvernance collaboratifs » en permettant un accès ouvert, par des politiques non-discriminatoires et la création de communautés locales.

Soutenir un Internet mondialement connecté

Avec un Internet véritablement interconnecté, quiconque voulant participer à Internet peut le faire, et échanger du trafic avec les autres participants sans restrictions. Un Internet mondialement connecté ne consiste pas simplement en une infrastructure technique, mais aussi en une infrastructure au sein de laquelle tous les obstacles à la connexion sont minimisés et où quiconque le désire peut obtenir une connexion rapide, fiable et abordable aux terminaux (utilisateurs, services ou ressources comme le stockage, le calcul, la détection et la commande), où qu'il soit situé.

Facilitateur	**Accessibilité sans restrictions**
Description	Les utilisateurs d'Internet ont accès à toutes les ressources et technologies disponibles sur Internet et sont capables de rendre eux-mêmes des ressources disponibles. Une fois une ressource rendue disponible d'une manière quelconque par son propriétaire, il est impossible de bloquer un accès ou une utilisation légitime de cette ressource par des tiers.
Questions	Le changement proposé restreint-il les ressources qu'un utilisateur utilise et auxquelles il a accès, ou restreint-il les ressources qu'un utilisateur peut mettre à disposition sur Internet ? Ce changement permet-il à un tiers de bloquer l'accès à une part importante des ressources d'Internet, ou de créer des points uniques de défaillance ?

10 Une plus longue explication des caractéristiques et bénéfices des IXP est disponible dans la série explicative de l'Internet Society « Développer Internet » sur https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/

Exemple 1 : la communauté Internet a travaillé dur pour atténuer les effets négatifs de l'utilisation largement répandue d'appareils de la Traduction d'adresse réseau (NAT)[11] entre les réseaux d'utilisateurs finaux et Internet, qui permet une utilisation plus efficace de l'espace d'adressage IPv4 public limité. Bien que la NAT soit inoffensive pour la plupart des utilisateurs d'Internet, elle peut entraîner des perturbations majeures pour certains protocoles, comme la Voix par IP (VoIP). Pour éviter les problèmes créés par la NAT, la communauté Internet a défini d'autres protocoles, notamment STUN[12], TURN[13] et ICE[14]. Pour de nombreux utilisateurs, ces protocoles et technologies permettent l'utilisation de communications de type pair-à-pair, qui seraient sans cela involontairement bloquées du fait de la NAT.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet mondialement connecté, renforçant « l'accessibilité sans restrictions » en supprimant les barrières à une connectivité de bout en bout.

Exemple 2 : dans certains pays, les services de VoIP sont bloqués parce que la politique du gouvernement est de conserver un monopole d'État sur les communications téléphoniques (pour pouvoir les taxer). Ce blocage réduit l'efficacité économique, impose des coûts plus élevés et contribue à isoler les utilisateurs de ce pays des autres utilisateurs d'Internet bénéficiant des technologies et services de VoIP.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet mondialement connecté, affaiblissant « l'accessibilité sans restrictions » en bloquant des services.

Facilitateur	**Capacité disponible**
Description	La capacité d'Internet est suffisante pour répondre à la demande des utilisateurs. Personne ne s'attend à ce que la capacité d'Internet soit infinie, mais la capacité de connexion (ports, bande passante, services) doit être suffisante pour répondre à la demande des utilisateurs.
Questions	Le changement proposé contribue-t-il à augmenter la disponibilité des ressources d'Internet, telles que la bande passante ou d'autres capacités ? Cette politique a-t-elle pour effet de limiter la croissance et la capacité, directement ou indirectement ?

11 Les lecteurs techniques peuvent souhaiter faire une distinction entre les différents types de NAT, mais, pour fluidifier la lecture, le terme « NAT » désigne ici toutes les technologies d'adresse de réseau et de traduction du port.

12 Session Traversal Utilities for NAT (STUN), RFC 5389 https://www.ietf.org/rfc/rfc5389.txt

13 Traversal Using Relays around NAT (TURN), RFC 8656 https://www.ietf.org/rfc/rfc8656.txt

14 Interactive Connectivity Establishment (ICE), RFC 5245 https://www.ietf.org/rfc/rfc5245.txt

Exemple 1 : les parties prenantes de la République démocratique du Congo se sont mises d'accord pour créer un IXP dans la capitale, Kinshasa (KINIX). Après quelques années, la communauté a ressenti le besoin d'un second IXP dans la deuxième plus grande ville, Lubumbashi. Il a été mis en service en 2019. Maintenant, au cours du troisième trimestre de 2021, la communauté lancera un 3ème IXP à Goma. L'établissement de ces IXP réduit significativement les coûts de connectivité (en 2020, les économies annuelles estimées par réseau s'élevaient à 163 000 dollars américain) et augmente la capacité de communication disponible.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet mondialement connecté, en améliorant la « capacité disponible » dans des zones peu desservies.

Exemple 3 : le projet Starlink de SpaceX vise à fournir un service Internet par le biais de satellites en orbite terrestre basse. Bien que le projet en soit à ses débuts et toujours en phase de test, il peut fournir d'importantes capacités supplémentaires dans des zones qui sont actuellement mal desservies. La façon dont les gouvernements choisissent de réguler et d'octroyer des licences pour le produit Starlink (à la fois dans l'espace et tout particulièrement pour les segments terrestres) affectera fortement l'augmentation ou non de la capacité Internet dans une zone.

Si l'obtention d'une licence, les coûts et les restrictions retenues par chaque agence de réglementation dans une zone particulière ne sont pas onéreux, Starlink aura vraisemblablement un effet positif sur l'objectif d'un Internet mondialement connecté, en augmentant la « capacité disponible ».

Exemple 3 : les réseaux qui choisissent de ne pas déployer IPv6, mais s'appuient sur la traduction d'adressage réseau de qualité téléphonique (CGNAT), qui est en résumé une version beaucoup plus large que la NAT mentionnée plus tôt, vont arriver à un point où leurs utilisateurs auront épuisé toutes les ressources disponibles. Les CGNAT restreignent de fait le nombre de connexions pouvant être utilisées simultanément par les utilisateurs individuels. Sans une CGNAT, un utilisateur individuel peut utiliser simultanément 64 000 connexions, alors que dans le pire des cas, un million de personnes utilisant une CGNAT peuvent n'avoir que 16 connexions simultanées disponibles par utilisateur individuel[15]. Ce nombre est à comparer aux 50 connexions simultanées nécessaires pour charger un site Internet standard.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet mondialement connecté. L'épuisement des adresses IPv4, conjugué à l'absence de déploiement d'IPv6, conduit à une pénurie des ressources pour les utilisateurs, ce qui amenuise « la capacité disponible ».

Soutenir un Internet sécurisé

Un Internet sécurisé est résistant aux attaques contre son infrastructure, et offre un service robuste à sa communauté d'utilisateurs. Cela signifie que ses protocoles et son infrastructure, comme le routage et le

15 Nous considérons que l'opérateur de réseau n'a que /24 d'espace d'adressage disponible, le bloc le plus large actuellement alloué par les RIR. De cette manière, les utilisateurs ont accès à 256 adresses fois 64 mille ports.

DNS, doivent présenter une base sécurisée, résistante à la fois aux attaques intentionnelles et aux accidents. Dans un Internet sécurisé, la confidentialité, l'intégrité et la disponibilité des données doivent être protégées. Idéalement, un Internet sécurisé n'engendre pas d'insécurité, comme des botnets utilisés dans les attaques par hameçonnage. Et les services et applications qui fonctionnent sur Internet doivent eux-mêmes être sécurisés et, dans la mesure du possible, offrir une défense en profondeur.

Dans ce contexte, le terme « sécurisé » complète et se rapporte au terme « fiable ». Dans l'évaluation des différentes politiques proposées par le prisme des facilitateurs, ces deux qualités seront souvent prises en compte.

Facilitateur	**Confidentialité des données des informations, des appareils et des applications**
Description	La confidentialité des données, réalisée généralement avec des outils tels que le cryptage, permet aux utilisateurs d'envoyer des informations sensibles par Internet de façon à ce que des oreilles indiscrètes ou malveillantes ne puissent pas consulter le contenu ou savoir qui communique. Permettre le transfert de données sensibles participe à la création d'un Internet sécurisé. La confidentialité des données s'applique aussi aux données statiques et à celles conservées sur les appareils. (N.B., la « non-divulgation » contribue aussi à la confidentialité, qui relève d'un Internet fiable)
Questions	Le changement proposé renforce-t-il ou affaiblit-il la capacité des utilisateurs de préserver la confidentialité de leurs informations en transit ou statiques ? Si le changement est mis en œuvre, les protocoles sous-jacents d'Internet offrent-ils une confidentialité plus forte ou plus faible ?

Exemple 1 : la Norme de sécurité des données (DSS) du secteur des cartes de paiement (PCI) est une norme mondiale qui s'applique à quiconque traite des données de cartes de paiement. La DDS du PCI exige que les communications soient cryptées, et que les données statiques soient protégées par des technologies telles que le cryptage. En créant une norme de secteur exigeant le cryptage quand les données sont envoyées sur Internet, la DSS du PCI renforce la confidentialité des données statiques et en transit dans un domaine, les transactions commerciales en ligne, qui est devenu une partie intégrante de la société numérique.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet sécurisé, en renforçant « la confidentialité des données des informations, des appareils et des applications » en exigeant un cryptage pour protéger les informations sensibles et confidentielles.

Exemple 2 : l'Île Maurice a récemment proposé que l'ensemble du trafic des médias sociaux soit décrypté, inspecté et archivé. Les motivations sont fondées sur la relative rareté de la langue locale et sur le manque de présence physique des organisations principales de médias sociaux, ce qui entraîne des réponses trop tardives aux plaintes légitimes provenant de l'Île Maurice. Si cela n'avait pas été rejeté, le changement proposé aurait nui à la sécurité d'Internet pour les personnes vivant à l'Île Maurice et leurs correspondants, en réduisant considérablement la confidentialité des informations échangées sur les réseaux sociaux. Malheureusement, de telles propositions deviennent courantes dans l'ensemble du monde.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet fiable en affaiblissant « la confidentialité des données d'information, des appareils et des applications » en exigeant la suppression de la protection des informations échangées entre des correspondants en ligne.

Exemple 3 : La plupart[16] des sites Internet ont désormais recours au cryptage pour assurer la confidentialité des données de leurs utilisateurs. Cette sécurité additionnelle est basée sur des protocoles normalisés (TLS/HTTPS) et des cadres pour asseoir le procédé de cryptage solidement en utilisant des certificats d'identité numérique et des autorités de certifications (CA) fiables. Ensemble, les certificats, les CA et tous les processus et règles qui gouvernent cet écosystème[17] sont communément appelés « la WebPKI » (pour « infrastructure de clé publique du Web »), Bien qu'il existe de nombreuses critiques légitimes sur différents aspects de la WebPKI, le résultat global est que les utilisateurs d'Internet sont capables d'utiliser facilement et de manière transparente un cryptage pour assurer une meilleure confidentialité à leurs activités sur Internet.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet fiable, renforçant « la confidentialité des données des informations, des appareils et des applications » grâce au développement d'une norme au niveau du secteur et à sa mise en œuvre par les développeurs d'applications.

Facilitateur	**Intégrité des informations, des applications et des services**
Description	L'intégrité des données envoyées sur Internet et stockées dans des applications n'est pas compromise. C'est-à-dire que les informations envoyées sur Internet ne peuvent pas être modifiées durant leur transit, à moins d'une demande d'une des parties communicantes (ex. : un bot de sous-titrage peut être utile pour convertir les mots parlés en texte). Les services Internet essentiels sous-jacents, comme le DNS et le système de routage, ne peuvent pas être manipulés ou compromis par des acteurs malveillants.

16 Plus de 90 % du trafic Web est sécurisé par HTTPS https://transparencyreport.google.com/https/overview?hl=en

17 Voir, par exemple, le CA/Browser Forum sur https://cabforum.org/ et la production du groupe de travail de l'IETF sur la PKI sur https://datatracker.ietf.org/wg/pkix/documents/.

	Les données stockées dans les applications ne peuvent être manipulées ou compromises par des tiers.
Questions	Le changement proposé renforce-t-il ou affaiblit-il l'intégrité des données ou la capacité des utilisateurs à vérifier que les données ne sont pas corrompues ? Le changement proposé renforce-t-il ou affaiblit-il l'exactitude et l'intégrité des services Internet, comme le DNS ?

Exemple 1 : l'infrastructure à clé publique de ressources (RPKI) est un ensemble de normes technologiques et de bases de données hébergées sur Internet, qui aide à accroître l'intégrité du routage sur Internet. Avec la RPKI, les détenteurs d'adresses IP peuvent publier des informations sur la façon dont leurs blocs d'adresses doivent être acheminés. Dans le même temps, les opérateurs de réseau comme les FAI peuvent utiliser les informations publiées dans le système RPKI pour valider les mises à jour de routage et éviter les comportements malveillants, comme le détournement d'espace d'adressage IP.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet sécurisé en augmentant « l'intégrité des informations, des applications et des services » dans le domaine du système de routage d'Internet.

Exemple 2 : en 2011, S.978, la « PROTECT IP Act » a été présentée au Sénat des États-Unis. Ce projet de loi contenait un éventail d'exigences techniques pour le filtrage du contenu d'Internet, y compris l'interception et la modification des demandes et réponses du DNS. La législation proposée présentait aussi une incompatibilité avec une technologie importante pour la sécurité d'Internet, les extensions de sécurité du DNS (DNSSEC), et aurait freiné le déploiement des DNSSEC. S.978 aurait accompli sa tâche, notamment au détriment de la solidité et la stabilité du DNS. (Le projet de loi n'a jamais été soumis au vote au Sénat).

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet sécurisé, en affaiblissant « l'intégrité des informations, des applications et des services » pour le système DNS.

Soutenir un Internet fiable

Contrairement à la sécurité, la fiabilité ne dépend pas seulement de l'état d'Internet, mais aussi de l'état des personnes et organisations qui l'utilisent et y participent. La mesure selon laquelle Internet peut être considéré comme fiable dépend de la base d'utilisateurs informés qui ont les outils pour évaluer la

fiabilité, en fonction de leur connaissance actuelle des vulnérabilités d'Internet et des menaces qui pèsent sur lui.[18]

Les concepts d'un Internet fiable et d'un Internet sécurisé sont étroitement liés : si Internet n'est pas sécurisé, il ne peut en aucun cas être fiable. Toutefois, un Internet complètement sécurisé peut également ne pas être digne de confiance si cela bafoue les attentes des utilisateurs ou si certains des participants ne sont pas dignes de confiance. La fiabilité n'est pas simplement une question de sécurité.

Facilitateur	**Robustesse, résilience et disponibilité**
Description	Internet est robuste quand des technologies et des procédés sont en place et permettent la distribution de services de la manière prévue. Si, par exemple, la disponibilité d'un service Internet est imprévisible, alors les utilisateurs considéreront cela comme un manque de fiabilité. Cela peut réduire la confiance non pas en un seul service, mais en Internet dans son ensemble. La résilience est liée à la robustesse : un Internet résilient conserve un niveau acceptable de service même face à des erreurs, des comportements malveillants et d'autres entraves à un fonctionnement normal.
Questions	Le changement proposé crée-t-il des variations imprévisibles de la robustesse d'Internet, d'un service ou d'un ensemble de services ? Empêchera-t-il les utilisateurs de savoir, au jour le jour, s'ils peuvent utiliser Internet et ses services ? Le changement proposé augmente-t-il ou réduit-il le niveau global de la résilience d'Internet face aux dysfonctionnements ?

Exemple 1 : statuspage.io est un produit commercial qui se concentre sur l'affichage du statut du service (fonctionne : oui, non, partiellement) pour les utilisateurs du service. En créant un produit entier autour de l'offre de cette information, l'équipe statuspage.io a fourni un outil à la communauté Internet qui remplit une niche et facilite la communication transparente du statut du service. Parce que statuspage.io est marchand, il a aussi inspiré des concurrents en open source ou marchands, ce qui a rendu ce type d'outil

18 Les lecteurs peuvent trouver que les termes « digne de confiance » et « fiable » prêtent à confusion. Ici, la fiabilité d'Internet peut être évaluée d'une façon neutre selon des éléments techniques et de politiques qui sont généralement objectifs. Toutefois, l'utilisateur peut ne pas accorder sa confiance à un réseau fiable. Un Internet qui est fiable peut ne pas être digne de confiance. Et un Internet non fiable peut quand même être digne de confiance.

de transparence encore plus largement disponible pour les opérateurs de réseau et les fournisseurs de service d'information.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet fiable, en renforçant « la robustesse, la résilience et la disponibilité » en augmentant la transparence sur la performance du service.

Exemple 2 : Les coupures délibérées d'Internet sont souvent utilisées au niveau d'un pays durant des périodes de tension, comme des élections fortement contestées ou des troubles civils. Les gouvernements en Biélorussie, en Inde et au Venezuela ont tous coupé l'Internet de leur pays récemment[19]. Le résultat de ces coupures peut être un amenuisement de la fiabilité d'Internet. La logique et la durée de ces coupures sont rarement transparentes, ce qui nuit encore plus à la confiance.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet fiable, en réduisant « la robustesse, la résilience et la disponibilité » par une interruption délibérée des services.

Facilitateur	**Responsabilité**
Description	La responsabilité concernant Internet donne aux utilisateurs l'assurance que les organisations et les institutions avec lesquelles ils interagissent opèrent directement et indirectement de manière transparente et loyale. Dans un Internet responsable, les entités, les services et les informations peuvent être identifiés et les organisations impliquées devront rendre des comptes pour leurs actes.
Questions	Le changement proposé crée-t-il des autorités opaques ou des acteurs cachés ? Ce changement a-t-il pour effet de créer des autorités anonymes ou ne rendant pas de comptes, susceptibles de nuire à la confiance que les utilisateurs ont en Internet ?

Exemple 1 : la RFC 7725[20] définit la façon dont le propriétaire d'un site Internet doit signaler à ses utilisateurs que l'information n'est pas disponible suite à une exigence légale. Les sites Internet, les FAI et les moteurs de recherche qui bloquent l'accès à des informations en raison d'une sanction peuvent utiliser le mécanisme de cette RFC pour être très transparents : « vous ne pouvez voir ce que vous recherchez car il nous est légalement interdit de vous le montrer ».

19 Voir ISOC Pulse tracker https://pulse.internetsociety.org/shutdowns pour plus d'exemples spécifiques

20 RFC 7725: An HTTP Status Code to Report Legal Obstacles at https://www.rfc-editor.org/rfc/rfc7725.txt

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet fiable en renforçant « la responsabilité » par une transparence accrue.

Exemple 2 : le Forum mondial de l'Internet contre le terrorisme[21] (GIFCT) vise à « empêcher les terroristes et les extrémistes violents d'exploiter les plateformes numériques ». Dans le cadre de cette mission, le GIFCT conserve une base de données d'images et de vidéos considérées comme des « données à caractère terroriste », qu'il met à disposition de ses membres. Quand une vidéo ou une image figurant dans cette base de données est détectée, les utilisateurs de la base de données peuvent agir sur la foi de cette information[22]. Cette base de données s'est accrue, et contient désormais plus de 300 000 images et vidéos. Parce que la base de données utilise des hachages unidirectionnels pour identifier les éléments, les vidéos et images mises en cause ne sont pas conservées. Cela entraîne un manque de transparence : les chercheurs ne peuvent pas examiner la base de données et les organismes de réglementation ne peuvent pas réaliser d'audit, ainsi que des risques significatifs pour la liberté d'expression, comme une censure de données non-anglophones. L'étendue de la base de données est aussi difficile à contrôler, puisque, dans certains cas, il est difficile d'identifier des « données à caractère terroriste » au niveau mondial.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet fiable, en affaiblissant « la responsabilité » par sa conception et le déploiement d'outils de blocage opaques, avec peu de surveillance et souvent peu de recours pour l'utilisateur.

Facilitateur	**Confidentialité**
Description	La confidentialité sur Internet est la capacité des individus et des groupes à comprendre et contrôler quelles informations les concernant sont recueillies et comment elles le sont, et à contrôler la façon dont elles sont utilisées et partagées. La confidentialité comprend souvent des aspects d'anonymisation, par la suppression de liens entre les données, les appareils, les sessions de communications et l'identité des personnes auxquelles ils se rattachent.
Questions	Le changement proposé améliore-t-il, réduit-il ou élimine-t-il la capacité des utilisateurs à comprendre ou contrôler la façon dont leurs informations sont recueillies, ou à contrôler comment ces informations sont utilisées et partagées ?

21 Voir https://gifct.org/ et plus spécifiquement https://vimeo.com/564638166. Les membres fondateurs du GIFCT comprennent Facebook, Microsoft, Twitter et YouTube.

22 « Il appartient à chaque membre du consortium de savoir comment il utilise la base de données, notamment en fonction de ses propres conditions d'utilisation, de la façon dont sa plateforme fonctionne et de la façon dont il utilise les capacités techniques et humaines. » (Citation du rapport 2020 sur la transparence du GIFCT, disponible sur https://gifct.org/wp-content/uploads/2020/10/GIFCT-Transparency-Report-July-2020-Final.pdf) Le rapport sur la transparence indique clairement que le GIFCT cherche une façon d'augmenter la responsabilité, mais n'a pas encore réussi à trouver une solution satisfaisante.

	Cela a-t-il pour effet de fournir ou d'éliminer la possibilité pour un utilisateur d'agir de manière anonyme ou en utilisant un pseudonyme ?

Exemple 1 : le projet de loi sur la sécurité en ligne de 2021 du gouvernement britannique oblige les fournisseurs à surveiller et effacer les données « légales mais préjudiciables ». Les partisans de cette loi déclarent qu'en pratique, elle obligera les fournisseurs de service à analyser les données, y compris les messages privés. La seule façon de le faire serait de casser le cryptage de bout en bout, ce qui impliquerait que les plateformes de messages « privées » soient sujettes à la surveillance par des acteurs, étatiques ou non, même sans allégation ou soupçon qu'un crime a effectivement été commis.

Il s'agit d'un exemple d'effet négatif sur l'objectif d'un Internet fiable, car cela affaiblit « la confidentialité » en créant des acteurs cachés et des actions cachées sur la base d'une surveillance omniprésente du trafic[23].

Exemple 2 : la loi California Consumer Privacy Act (CCPA) donne aux consommateurs plus de contrôle sur les informations personnelles les concernant recueillies par les entreprises. Bien que la majeure partie de la CCPA concerne les politiques et déclarations communiquées manuellement, la CCPA actuelle exige également que les entreprises tiennent compte des déclarations de refus des navigateurs Web du style « Ne pas me suivre » ; ceci donne une manière simple et facile aux utilisateurs finaux d'indiquer leurs préférences en matière de confidentialité. En encourageant les contrôles de confidentialité normalisés et automatisés, comme le Contrôle global de la confidentialité (GPC), la CCPA aide les utilisateurs à mieux gérer leur confidentialité.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet fiable, renforçant la « confidentialité » en fournissant aux consommateurs davantage de contrôle sur les informations personnelles que les entreprises recueillent.

Exemple 3 ; le RGPD de l'Union européenne est une législation de grande ampleur, qui vise à fortement améliorer la confidentialité des utilisateurs d'Internet. Bien que la mise en œuvre des exigences du RGPD ait entraîné dans de nombreux cas une expérience utilisateur sous-optimale, le règlement a des effets très positifs sur la fiabilité, en inscrivant les politiques de confidentialité et de respect de la vie privée des utilisateurs dans le modèle commercial et la conception des services actuels d'Internet, ce qui permettra de renforcer la confiance sur le long terme.

Il s'agit d'un exemple d'effet positif sur l'objectif d'un Internet fiable, car il renforce « la confidentialité » en en faisant un impératif dans les modèles commerciaux et la conception de services.

[23] RFC7258, « Pervasive Monitoring Is an Attack », https://datatracker.ietf.org/doc/rfc7258/