

Un cadre **politique** pour les intermédiaires et le contenu Internet

Janvier 2025

Synthèse

Sans intermédiaires pour acheminer le trafic Internet vers et depuis les points de terminaison (y compris les particuliers, les serveurs, les prestataires de services et bien d'autres), et sans les nombreux autres types de fonctions qui rendent ce trafic possible, il n'y aurait pas d'Internet.

Les intermédiaires sont essentiels à l'existence d'Internet. Ce document fournit un cadre pour comprendre les rôles des intermédiaires Internet et élaborer une politique concernant la responsabilité du contenu en ligne sans nuire à la capacité des individus à utiliser Internet pour créer du contenu et communiquer entre eux.

Nous nous concentrons sur les fonctions assurées par les intermédiaires Internet pour faciliter la communication en ligne, telles que la transmission, le routage, le stockage, la mise en cache, l'hébergement, la sécurisation, la curation et la modération de contenu. Cette approche prend en compte le fait que de nombreux intermédiaires exercent plusieurs fonctions qui soulèvent des enjeux politiques variés et que bon nombre d'entre eux remplissent des fonctions fondamentalement équivalentes même si leurs services peuvent sembler très différents.

Notre objectif dans ce document est d'aider les décideurs politiques à comprendre ces fonctions et à élaborer des politiques appropriées. Des politiques bien conçues peuvent améliorer la disponibilité, la diversité, la sécurité et la confidentialité de la participation individuelle en ligne. Cependant, des politiques mal conçues peuvent affaiblir la sécurité d'Internet, nuire à la concurrence, restreindre la communication en ligne, élargir la fracture numérique et fragmenter Internet.

L'objectif n'est pas d'exonérer les intermédiaires de leur responsabilité, mais de souligner le rôle essentiel des protections en matière de responsabilité pour favoriser la participation individuelle sur Internet. Des politiques axées sur les intermédiaires mal conçues peuvent avoir des effets néfastes sur Internet et la communication. De meilleures alternatives, telles que les lois existantes en matière de confidentialité, de protection des consommateurs et de discrimination, sont souvent disponibles.

Dans ce document, nous traitons de **l'élaboration de protections en matière de responsabilité des intermédiaires** et de la motivation qui les sous-tend, en commençant par le texte de loi « Section 230 » des États-Unis, la loi brésilienne « Marco Civil da Internet » et la directive sur le commerce électronique et le règlement DSA (Digital Services Act) de l'UE. Nous expliquons pourquoi ces lois et d'autres lois similaires ont été cruciales pour la croissance de l'Internet et la capacité des individus à participer en ligne.

Nous mettons également en évidence **certaines tendances en matière d'élaboration de politiques axées sur les intermédiaires**, telles que les régimes de notification et de retrait, la modération des téléchargements et les exigences spécifiques à l'âge. Nous constatons que ces approches risquent de nuire à Internet en compromettant ses opérations techniques et sa fiabilité, en affaiblissant la sécurité et la confidentialité, en réduisant la concurrence, en bloquant excessivement les contenus légaux et en excluant les utilisateurs de la participation à Internet.

Voici plusieurs principes importants en matière d'élaboration de politiques :

1. **Effectuez une évaluation de l'impact sur Internet**
pour comprendre si une politique proposée – relative aux intermédiaires ou plus générale – pourrait avoir un effet négatif sur Internet et son fonctionnement.
2. **Évaluez soigneusement toute stratégie proposée** par rapport à l'intermédiaire précis causant un tort politique. Soyez attentif aux dommages collatéraux potentiels. Évitez d'affecter un ensemble trop vaste de fonctions et d'entités.
3. **Protégez les intermédiaires de toute responsabilité concernant le contenu créé par des tiers**, y compris le « contenu généré par les utilisateurs ». Les entités exerçant des rôles d'intermédiaires doivent être protégées de toute responsabilité concernant le contenu créé par des tiers qu'elles transmettent, reçoivent, hébergent, affichent, filtrent ou traitent de toute autre manière. Cela garantit que les utilisateurs peuvent continuer à communiquer et à partager du contenu en ligne.

4. **Protégez les rôles des intermédiaires liés à la curation et à la modération du contenu généré par les utilisateurs.** Les entités qui hébergent du contenu généré par les utilisateurs ont le droit légitime de définir les « règles de conduite » pour leurs services et doivent être protégées de toute responsabilité liée à l'application de leurs propres règles et à la suppression de contenu répréhensible.
5. **Pour répondre aux préoccupations concernant le contenu en ligne, les décideurs politiques peuvent utiliser les lois existantes ou nouvelles** axées sur la confidentialité et la sécurité, la non-discrimination, l'accessibilité, les droits de l'homme, la concurrence, le choix et le contrôle des utilisateurs, la transparence et l'ouverture, entre autres.

Nous mettons en avant plusieurs **points importants** sur les considérations politiques pour des secteurs en ligne spécifiques, notamment les réseaux sociaux, les réseaux fédérés, les jeux en ligne, la réalité augmentée/réalité virtuelle, la publicité, ainsi que les modèles commerciaux de contenu payant, la gestion de la liberté d'expression, le droit d'auteur et l'intelligence artificielle (IA).

L'**annexe** à la fin de ce document passe en revue la vaste gamme d'**intermédiaires** qui permettent les communications sur Internet. Elle fournit une **liste** et une description complètes des rôles des intermédiaires et inclut des considérations techniques et pratiques pour l'élaboration des politiques ainsi que des recommandations stratégiques pour chaque rôle.

Table des matières

Un cadre politique pour les intermédiaires et le contenu Internet	1
Synthèse	1
1 Introduction	8
1.1 Enjeux politiques concernant les intermédiaires.....	9
1.2 Internet a transformé les communications avec de fortes répercussions sociales et économiques positives.....	10
1.3 Internet favorise les communications individuelles actives.....	11
1.4 Le rôle des intermédiaires dans la communication sur Internet	13
1.5 Comparaison entre la responsabilité du contenu généré par le site et du contenu généré par les utilisateurs	15
2 Internet et la responsabilité des intermédiaires	17
2.1 Les défauts majeurs du modèle de communication à « commutation de circuits » du XIXe siècle, antérieur à Internet.....	17
2.2 Comprendre le mode de fonctionnement du réseau Internet	18
2.3 Le rôle des intermédiaires	20
Fournisseurs de services intermédiaires.....	22
3 Protections en matière de responsabilité des intermédiaires	23
3.1 Le développement initial des lois sur la protection des intermédiaires : mise en contexte	23
3.2 Les premières lois sur la responsabilité des intermédiaires Internet : section 230 des États-Unis	25
3.3 Protections initiales des intermédiaires en Europe	29
3.4 Le « Marco Civil da Internet » au Brésil.....	30
3.5 Mise à jour des mesures de protection des intermédiaires en Europe	31

3.6 Mesures de protection des intermédiaires dans d'autres contextes nationaux et internationaux.....	33
3.7 Tendances récentes en matière de responsabilité des intermédiaires et risques pour Internet.....	36
3.8 Hétérogénéité des pays	40
4 Principes d'élaboration des politiques pour les intermédiaires Internet.....	42
4.1 Principes généraux pour une politique prudente concernant Internet.....	43
4.2 Principes spécifiques concernant la protection des intermédiaires en matière de responsabilité	45
4.3 Principes juridiques et politiques spécifiques pouvant être appliqués aux rôles des intermédiaires sans porter atteinte aux communications sur Internet.....	47
5 Pleins feux sur : les considérations politiques relatives à des intermédiaires spécifiques	51
5.1 Pleins feux sur : les considérations politiques relatives aux plateformes de « réseaux sociaux » qui hébergent, organisent et modèrent le contenu généré par les utilisateurs	51
5.2 Pleins feux sur : les considérations politiques relatives aux « réseaux fédérés » permettent d'élaborer de nouvelles stratégies visant à renforcer l'engagement des utilisateurs.	54
5.3 Pleins feux sur : les considérations politiques relatives à l'écosystème du jeu interactif en ligne	56
5.4 Pleins feux sur : les considérations politiques relatives aux systèmes de réalité virtuelle et de réalité augmentée connectés à Internet	57
5.5 Pleins feux sur : les considérations politiques relatives aux intermédiaires qui permettent la publicité sur Internet	58
5.6 Pleins feux sur : les considérations politiques relatives aux paiements et autres compensations économiques pour le « contenu généré par les utilisateurs » couvert par les principes des intermédiaires Internet.....	60
5.7 Pleins feux sur : l'impact des différents niveaux nationaux de protection de la liberté d'expression	61

5.8 Pleins feux sur : la distinction entre la protection en matière de responsabilité des intermédiaires et les lois et politiques relatives au droit d’auteur.....	63
5.9 Pleins feux sur : l’intelligence artificielle.....	64
6 Conclusion	66

Annexe A – Rôles des intermédiaires 68

1 Transmission de paquets de données	69
1.1 Support de communication (filaire et sans fil)	69
1.2 Chemins de communication IP.....	70
1.3 Dorsale et réseaux de transit.....	72
1.4 Échange de trafic.....	73
1.5 Accès Internet du dernier kilomètre	75
2 Routage et fonctions annexes facilitant les communications Internet	77
2.1 Attribution d’adresse IP	77
2.2 Attribution de numéros de système autonome	79
2.3 Enregistrement et gestion DNS	80
2.4 Publication DNS.....	82
2.5 Recherche DNS	83
2.6 Services DNSSEC.....	85
2.7 Services de certificats TLS	86
3 Services d’hébergement et de mise en cache.....	88
3.1 Hébergement Web.....	88
3.2 Hébergement de messagerie électronique	90
3.3 Autres services d’hébergement.....	91
3.4 Services de mise en cache et de diffusion de contenu	92
3.5 Diffusion de contenu d’interface de programmation d’application (API).....	94

3.6 Curation, modération et affichage du contenu	95
4 Communications interpersonnelles.	97
4.1 Communications interpersonnelles (one-to-one).....	97
4.2 Communications de groupe (one-to-many).....	99
4.3 Communications de masse (many-to-many).....	101
5 Recherche.	103
5.1 Recherche sur le Web	103
5.2 Recherche intégrée	104
5.3 Recherche spécifique	105
5.4 Recherche interne au site	107
6 Protection de la cybersécurité, protection de la vie privée et contrôles du contenu utilisateur	108
6.1 Protection du trafic à l'échelle du réseau.....	108
6.2 Filtres et outils de contenu contrôlés par l'utilisateur	110
6.3 Protection du trafic axée sur l'utilisateur.....	112
7 Applications, logiciels, leur développement et leur distribution	114
7.1 Logiciel du système d'exploitation	114
7.2 Logiciel de navigation et de diffusion Web	116
7.3 Logiciels de messagerie électronique	119
7.4 Logiciels de messagerie	120
7.5 Autres logiciels utilisés pour l'envoi, la réception et l'affichage des communications Internet	121
7.6 Développement et distribution de logiciels/d'applications	123
8 Environnements complexes	125
8.1 Réseaux sociaux.....	125
8.2 Réseaux fédérés	127
8.3 Environnements de jeu	130
8.4 Environnements de réalité virtuelle et augmentée.....	131

1 Introduction

Ce document fournit un cadre pour comprendre les rôles des intermédiaires Internet et développer une stratégie concernant la responsabilité du contenu en ligne. Les intermédiaires Internet facilitent la diffusion et l'affichage de contenu ou de communications sur Internet. Les fournisseurs d'accès à Internet (FAI), les sites de réseaux sociaux, les hébergeurs Web, les services de streaming et les services de messagerie électronique sont tous des exemples d'entités exerçant des rôles d'intermédiaires. Notre objectif est d'encourager les décideurs politiques à élaborer des politiques qui préservent ce que nous considérons comme les caractéristiques les plus importantes d'Internet : être ouvert, connecté à l'échelle mondiale, sécurisé et digne de confiance.

Nous présentons une vue d'ensemble d'Internet et de certains rôles d'intermédiaires importants pour aider les décideurs politiques travaillant dans le domaine du contenu en ligne. Nous discutons de l'impact des politiques Internet sur les rôles des intermédiaires et les interactions des utilisateurs, et, comment dans certains cas, elles peuvent porter atteinte à la sécurité, à la fiabilité et à d'autres qualités fondamentales d'Internet. Enfin, nous formulons des recommandations spécifiques à l'intention des décideurs politiques cherchant à atteindre des objectifs sociaux et stratégiques par le biais de politiques qui affectent les rôles des intermédiaires Internet et les entités qui les exercent.¹

En quoi consistent les politiques et comment sont-elles mises en œuvre ?

Les politiques ayant un impact sur Internet peuvent revêtir diverses formes, notamment : des obligations légales, des protections légales, des réglementations administratives, des accords internationaux, des incitations fiscales, des rabais, des systèmes de certification, des exigences en matière d'approvisionnement et même des décisions de **ne pas légiférer** ou de ne pas réglementer.

¹ Dans le cadre des régimes de protection de la responsabilité des intermédiaires applicables à Internet, l'accent est mis sur les intermédiaires qui prennent en charge la création, la découverte, la recherche, la curation, la diffusion ou l'affichage de contenu. Cela peut inclure des e-mails, des tweets et d'autres messages publiés par des particuliers, ainsi que des textes, des fichiers audio ou des vidéos hébergés et affichés sur des sites Web et les principales plateformes en ligne. Ces régimes de responsabilité ne couvrent généralement pas les autres types d'entités qui fournissent un service « intermédiaire », comme le transfert d'argent d'une personne à une autre, et ce document n'aborde pas ce type de services non axés sur le contenu.

1.1 Enjeux politiques concernant les intermédiaires

Comme expliqué ci-dessous dans la section 2, un large éventail de fonctions intermédiaires sont essentielles au fonctionnement d'Internet. Par conséquent, les politiques qui s'appliquent aux entités intermédiaires d'Internet ou aux fonctions qu'elles exercent pourraient également affecter de manière significative la capacité des individus à créer du contenu et à communiquer entre eux.

L'influence des politiques peut être positive et constructive. Nous pensons que la plupart des décideurs politiques reconnaissent la valeur d'Internet dans leur travail. Les politiques peuvent améliorer la manière dont les individus et les communautés utilisent Internet, par exemple en encourageant les services à sécuriser les données et à protéger la confidentialité de leurs utilisateurs, et elles peuvent exploiter le pouvoir d'Internet comme une force positive dans la société.

Cependant, la prise de décisions politiques peut également entraîner des conséquences négatives considérables : affaiblissement de la sécurité et de la confidentialité sur Internet, éviction des petits concurrents et découragement des nouveaux entrants, paralysie de la capacité des utilisateurs à communiquer en ligne, élargissement de la fracture numérique et fragmentation d'Internet. Nous pensons que les décideurs politiques souhaitent éviter ces conséquences négatives, et c'est l'une des raisons pour lesquelles l'Internet Society publie ce document.

Pour les décideurs qui envisagent des politiques applicables à Internet, il est essentiel de prendre en compte les nombreux et divers types de rôles intermédiaires essentiels à la communication sur Internet. En outre, il est important de se rappeler que les entités elles-mêmes exerçant des rôles d'intermédiaires sont extrêmement diverses : des FAI ruraux aux petites et grandes sociétés d'hébergement Web, en passant par les services de dorsale Internet et les énormes sites de partage de vidéos et de réseaux sociaux. Cette diversité signifie qu'il est crucial que toutes les obligations proposées ciblent aussi étroitement que possible le rôle précis des intermédiaires.

Nous reconnaissons que tous les contenus sur Internet ne sont pas légaux et bénéfiques pour la société et que les pays recherchent des moyens efficaces pour limiter la propagation de la désinformation, des contenus préjudiciables et des activités criminelles en ligne. À cet égard, les

intermédiaires peuvent constituer une cible politique attrayante en raison de leur interaction étendue avec le contenu généré par les utilisateurs. Nous ne prétendons pas que les entités exerçant des rôles intermédiaires « ne peuvent pas » ou « ne devraient pas » être soumises à une politique d'une manière ou d'une autre. Notre objectif est de montrer que les politiques affectant les intermédiaires peuvent avoir des conséquences imprévues importantes et être préjudiciables à Internet ou à la capacité des gens à communiquer sur Internet et, par conséquent, devraient être évitées. Nous mettons également en avant divers outils politiques, tels que des lois strictes sur la confidentialité, dont les gouvernements disposent pour répondre aux problèmes sociaux en ligne.

1.2 Internet a transformé les communications avec de fortes répercussions sociales et économiques positives

Internet a radicalement transformé la façon dont les gens communiquent. Avant l'ère Internet, le téléphone et le courrier postal étaient les principaux outils disponibles pour la communication interpersonnelle. Les communications de masse telles que les journaux, la télévision et la radio offraient aux individus peu de possibilités de s'exprimer et de participer.

Contrairement aux journaux, à la radio et à la télévision, Internet permet aux individus de participer à la conversation, en temps réel et partout dans le

Internet favorise la participation

L'objectif de l'Internet Society en rédigeant ce document est d'expliquer pourquoi les intermédiaires permettant et facilitant la communication de contenus générés par les utilisateurs devraient être exonérés de toute responsabilité. Nous souhaitons également souligner qu'il existe d'autres outils politiques disponibles pour répondre de manière constructive aux préoccupations concernant les services en ligne et le contenu de leurs utilisateurs. Notre intention n'est pas de conseiller les décideurs politiques sur la manière de réglementer Internet, mais de leur suggérer comment élaborer une politique en faveur des communications individuelles, l'une des plus grandes réussites d'Internet.

« Une caractéristique essentielle d'Internet, qui le différencie de tous les autres moyens de communication, est qu'il a été conçu pour être accessible à tout le monde. Les gens peuvent s'exprimer, discuter, créer, inventer et interagir avec d'autres, qu'ils soient près de chez eux ou à l'autre bout du monde. » (Déclaration devant le Congrès d'Andrew Sullivan, PDG de l'Internet Society, le 8 mars 2023)

monde. La gamme d'options disponibles sur Internet comprend les communications interpersonnelles (p. ex., les applications de messagerie cryptées), les communications de groupe (p. ex., la publication d'un site Web) et les communications de masse (p. ex., les plateformes de réseaux sociaux). Au cours de ses premières années d'existence, Internet permettait les communications via des tableaux d'affichage, des listes de diffusion, des groupes de discussion, des blogs et une myriade d'autres formes d'engagement des utilisateurs.

La possibilité pour les individus d'utiliser Internet pour communiquer, transmettre et recevoir des informations d'autres personnes, que ce soit dans leur ville ou à l'autre bout du monde, génère également des bénéfices directs : des bénéfices qui profitent aux individus, à leurs communautés et à leurs pays. Les gens utilisent Internet pour créer de nouvelles opportunités sociales et économiques pour eux-mêmes et pour les autres. Les entrepreneurs peuvent développer des produits et des services qui répondent aux besoins de leurs communautés. Les gouvernements peuvent communiquer avec leurs citoyens de façon plus efficace, plus rapide et à moindre coût. Les communications rendues possibles par Internet contribuent à l'enrichissement des connaissances mondiales et des opportunités économiques. Au-delà de ces avantages, Internet a clairement créé des opportunités économiques pour les nations, les entreprises, les organisations et les personnes du monde entier.²

1.3 Internet favorise les communications individuelles actives

Grâce à Internet, les individus ne sont plus des consommateurs passifs de contenu majoritairement produit par des entreprises ou validé par le gouvernement. Les gens participent activement à la création de contenu et à la manière dont ce contenu peut être mis à disposition des personnes du monde entier. Dans ce document, nous utilisons le terme « **contenu généré par les utilisateurs** » pour désigner tout ce qui est publié ou partagé en ligne par un utilisateur, plutôt que par le propriétaire d'un site.

Le concept de **contenu généré par les utilisateurs** apparaît souvent dans les affaires juridiques et les débats politiques sur la question de savoir qui

2 Comme l'indique le rapport 2010 de l'OCDE sur le rôle économique et social des intermédiaires Internet, la croissance des entités assurant des fonctions d'intermédiaire Internet a contribué à la croissance économique et à la productivité, à l'investissement dans les infrastructures, à l'augmentation de l'emploi et de l'entrepreneuriat, à l'innovation, à l'autonomisation des utilisateurs, à la confiance et à la confidentialité. Voir <https://doi.org/10.1787/5kmh79zszs8vb-en>.

devrait être légalement responsable de ce contenu. Le **contenu généré par les utilisateurs** peut être une œuvre originale créée par l'utilisateur qui la publie sur Internet, ou il peut avoir été créé par quelqu'un d'autre et publié, avec ou sans l'autorisation du créateur original.

La principale caractéristique qui définit le **contenu généré par les utilisateurs** est qu'il a été créé ou publié sur un site ou partagé en ligne par une personne autre que le propriétaire du site ou du service. Il se distingue du « **contenu original du site** », c'est-à-dire du contenu créé par les employés, les sous-traitants et les services de développement de contenu du propriétaire du site, pour lequel le propriétaire du site a une responsabilité juridique claire.

Le spectre du contenu généré par les utilisateurs est vaste. Il peut s'agir de contenu publié par des particuliers, mais également de contenu publié par une organisation ou une entreprise. Il existe une gamme illimitée de types de **contenu généré par les utilisateurs** : publications sur les réseaux sociaux, e-mails, messages, vidéos longues ou courtes, critiques de produits, poésie, musique ou données d'observation collectées par des citoyens scientifiques. Le **contenu généré par les utilisateurs** peut être sérieux, farfelu, artistique, exact, erroné, intelligent, offensant, harcelant, profond, utile, inutile, c'est-à-dire tout ce qui fait partie de l'étendue infinie des idées et des expressions humaines. Mais, bien sûr, certains contenus peuvent être nuisibles, diffamatoires, trompeurs, menaçants ou même illégaux.

Comparaison entre le contenu original du site et le contenu généré par les utilisateurs

Si un constructeur automobile décide de créer un site Web de base pour afficher les nouveaux modèles de voitures disponibles à l'achat, le contenu de ce site Web sera créé par le constructeur, ses employés et ses sous-traitants. Tout comme le constructeur automobile est responsable du contenu d'une brochure ou d'un autre document imprimé, il est également responsable du contenu qu'il publie en ligne. Nous appelons ce contenu le **contenu original du site**. En principe, le fabricant serait clairement responsable et pourrait être juridiquement responsable du contenu qu'il a créé et mis en ligne.

Si le constructeur automobile choisit d'ajouter des fonctionnalités interactives au site Web et de permettre aux visiteurs individuels de publier des commentaires sur les modèles automobiles, ces

commentaires seront du **contenu généré par les utilisateurs**.

Le site Web comporterait un mélange de contenu original du site et de contenu généré par les utilisateurs.

En revanche, un site Web de réseaux sociaux destiné aux passionnés d'automobile contiendrait probablement principalement du contenu **généré par les utilisateurs** : les visiteurs individuels du site publient du contenu long et court et interagissent avec d'autres visiteurs. Il se pourrait que le site contienne du **contenu original** créé par ses propriétaires, comme des informations de support et des conditions d'utilisation.

La question de la responsabilité et des obligations légales des entités exerçant des rôles d'intermédiaires pour faciliter la communication de **contenu généré par les utilisateurs** est un sujet central abordé dans ce document.

1.4 Le rôle des intermédiaires dans la communication sur Internet

L'Internet n'existerait pas sans les entités qui exercent des rôles intermédiaires. Son architecture décentralisée et distribuée, essentielle pour les bénéfices sociaux et économiques d'Internet, dépend des centaines de milliers d'entités qui exercent des rôles d'intermédiaires.

Les rôles des intermédiaires Internet comprennent la transmission, la sécurisation, l'hébergement et la facilitation des communications sur Internet. Pour mieux comprendre les rôles des intermédiaires sur Internet, une comparaison avec les services postaux peut être utile : les services postaux utilisent de nombreux intermédiaires différents pour distribuer le courrier : des transporteurs qui récupèrent et distribuent le courrier, des camions et des avions pour transporter le courrier, des agents de sécurité pour protéger le courrier, des boîtes aux lettres pour stocker le courrier, des bureaux de poste pour tout administrer, et d'autres. Toutes ces entités sont des agents du service postal.

Internet dispose d'entités intermédiaires qui exécutent des services et des fonctions analogues, mais avec une différence essentielle : les rôles des intermédiaires Internet sont exercés par des entités indépendantes et il n'existe pas de bureau central de coordination contrôlant la diffusion des communications. Les services postaux contrôlent la manière dont le courrier est distribué à partir du moment où il est reçu ; sur Internet,

il n'existe pas d'entité unique contrôlant la manière dont le contenu est distribué ou qui est responsable de chaque étape du processus. De plus, contrairement au service postal, le contenu sur Internet est presque toujours fragmenté en parties qui sont transmises séparément et peuvent circuler via différents réseaux indépendants. De plus, contrairement au service postal, de nombreuses pages de sites Web sont constituées de composants dynamiques créés et hébergés par différentes entités. Les protocoles techniques Internet ouverts et interopérables permettent à une grande diversité de communications, y compris des pages Web composées de manière dynamique, de circuler sans contrôleur central.

Mais, dans les deux cas, le service postal et ses agents, ainsi que les différents intermédiaires impliqués dans les communications sur Internet, communiquent du contenu généré par les utilisateurs. Pourtant, les rôles des intermédiaires sont différents.

Dans ce document, nous avons choisi de nous concentrer sur les « rôles » des intermédiaires (tels que « fournir un accès à Internet ») plutôt que sur les types d'entités (tels que « fournisseur d'accès Internet » ou site de « réseaux sociaux »). Nous pensons que cette approche apporte plus de rigueur et de précision lors de la définition des politiques, car de nombreuses entités exercent plusieurs fonctions intermédiaires différentes, et ces différentes fonctions soulèvent des problèmes politiques différents.

Par exemple, un fournisseur d'accès Internet (FAI), en plus de fournir un accès Internet aux ménages, peut exécuter des fonctions intermédiaires supplémentaires telles que la téléphonie VoIP, la recherche DNS, l'hébergement de courrier électronique et le filtrage de contenu ou de logiciels malveillants. Une plateforme de réseaux sociaux, en plus de fournir à ses membres la possibilité de publier et de réagir au contenu, peut exécuter d'autres fonctions intermédiaires telles que la messagerie individuelle, l'hébergement de sites Web et la conférence audio/vidéo en direct. En outre, certains services en ligne peuvent intégrer des fonctions intermédiaires identiques ou équivalentes. L'introduction de politiques ou de règles, par exemple, concernant l'utilisation de contenu intégré sur les sites de réseaux sociaux pourrait affecter involontairement l'utilisation de contenu intégré sur Internet par tous les utilisateurs.

Nous nous concentrons sur les rôles des intermédiaires Internet qui sont d'une manière ou d'une autre impliqués dans l'affichage, la découverte, la curation ou la diffusion de *contenu **créé par d'autres***, c'est-à-dire du contenu généré par les utilisateurs.

1.5 Comparaison entre la responsabilité du contenu généré par le site et du contenu généré par les utilisateurs

Un point de départ pour la comparaison est que la personne qui crée du contenu en ligne en est responsable et n'est pas un intermédiaire pour ce contenu. Cependant, si elle transmet, affiche, héberge ou facilite de toute autre manière le contenu créé *par d'autres*, elle sera considérée comme un intermédiaire et ne sera généralement pas légalement responsable de ce contenu.

Pour certaines entités, *tout* le contenu de leurs sites Web ou de leurs services est créé « par d'autres ». Les sites Web d'autres entités peuvent contenir un mélange de contenu créé « par d'autres » (méritant ainsi des protections de responsabilité des intermédiaires) et de contenu qu'elles ont elles-mêmes créé (donc sans protection de responsabilité). Voici trois exemples permettant d'illustrer cette distinction :

- Pour un fournisseur d'accès à Internet résidentiel, *tout* le contenu transmis vers et depuis ce domicile est créé par une entité distincte du FAI. Le FAI ne crée aucun contenu ; il est uniquement responsable de sa transmission. Le FAI n'exerce généralement qu'un rôle d'intermédiaire pour le contenu qu'il gère entre l'utilisateur final et le reste d'Internet. Du point de vue de la responsabilité, le FAI n'est pas responsable du contenu qu'il transmet.
- Pour un constructeur automobile disposant d'un site Web qui décrit ses produits, mais qui permet *également* aux utilisateurs de publier des avis ou de commenter le contenu, l'entreprise est responsable de la majeure partie du contenu du site Web et n'est pas considérée comme exerçant un rôle d'intermédiaire pour ce contenu particulier. Cependant, l'entreprise **exerce** un rôle d'intermédiaire concernant les commentaires des clients publiés sur le site Web de l'entreprise. En effet, ces commentaires ont été créés par quelqu'un d'autre que l'entreprise. Le constructeur automobile est légalement responsable du contenu qu'il a créé et publié, mais le contenu publié par d'autres nécessite une approche différente en matière de responsabilité.
- Pour l'hébergeur Web indépendant qui exploite les serveurs et l'infrastructure utilisés par le constructeur automobile, la

fonction est purement intermédiaire : tout le contenu du site Web (créé par le constructeur automobile avec les commentaires des clients) est un contenu généré par les utilisateurs. Comme le FAI, l'hébergeur Web ne doit pas être tenu responsable du contenu publié par d'autres sur les sites Web qu'il héberge.

Importance du rôle des intermédiaires dans la capacité des individus à utiliser Internet et à partager du contenu

Au niveau local, les gens comptent sur des intermédiaires (les FAI et les réseaux communautaires) pour se connecter à Internet. Une fois la connexion établie, *chaque* communication sur Internet requiert l'intervention de nombreuses entités indépendantes exerçant des fonctions intermédiaires pour transmettre, héberger, sécuriser et délivrer des milliards de communications chaque jour.

Chacun utilise Internet pour des raisons différentes, mais chaque utilisation nécessite que les gens, souvent inconsciemment, accèdent et se fient à des dizaines, des centaines, voire plus d'entités exerçant des fonctions intermédiaires chaque heure passée en ligne. Cette dépendance vis-à-vis des intermédiaires est fondamentale pour le fonctionnement quotidien d'Internet. C'est pourquoi les politiques qui affectent les intermédiaires doivent être élaborées avec le plus grand soin afin de ne pas nuire au fonctionnement d'Internet.

2 Internet et la responsabilité des intermédiaires

Cette section passe brièvement en revue certains aspects techniques d'Internet et présente quelques caractéristiques importantes qui font partie de ce que nous appelons « le mode de fonctionnement du réseau Internet ». Nous décrivons également le rôle essentiel que jouent les intermédiaires dans toutes les communications Internet.

2.1 Les défauts majeurs du modèle de communication à « commutation de circuits » du XIXe siècle, antérieur à Internet

Avant Internet, le principal système de communication interpersonnelle était le système téléphonique à « commutation de circuits », dans lequel des commutateurs étaient utilisés pour créer un circuit électrique dédié entre l'émetteur d'un appel téléphonique et le destinataire. Il y a soixante ans, pour permettre un appel téléphonique de New York à Johannesburg, la compagnie de téléphone américaine utilisait les câblages locaux pour créer un circuit menant à un câble sous-marin, lequel se connectait à la compagnie de téléphonie sud-africaine, qui à son tour établissait un circuit de l'autre côté pour acheminer les voix à travers l'océan. Une fois l'appel terminé, le circuit était déconnecté, et les ressources employées pour cet appel étaient libérées pour être utilisées pour un autre appel. Pendant la majeure partie du XXe siècle, la plupart des appels téléphoniques au sein d'un pays étaient gérés par une seule compagnie de téléphone monopolistique qui contrôlait le réseau, facturait les appels et était responsable de la maintenance et de l'extension du réseau. Dans certains pays, les entreprises étaient détenues ou exploitées par l'État.

L'approche à commutation de circuits de la téléphonie traditionnelle est extrêmement inefficace. La réservation de ressources pour un appel téléphonique impliquait qu'un foyer ou une communauté avec une seule

ligne téléphonique ne pouvait avoir qu'une seule conversation à la fois et devait parfois patienter jusqu'à ce que les lignes vers le destinataire soient libres. Le réseau devait être conçu de manière à supporter les charges des périodes de pointe, ce qui entraînait des coûts considérables. Aux périodes de pointe, comme pendant les fêtes de Noël et de Nouvel An, la capacité était souvent insuffisante. L'utilisation d'un circuit dédié pour un seul appel téléphonique était inefficace en soi, car les câbles pouvaient transporter plus de contenu qu'un seul appel. L'inefficacité technique et économique de la téléphonie traditionnelle a été un facteur déterminant dans le développement des réseaux à « commutation de paquets », base de l'Internet d'aujourd'hui.

La téléphonie à commutation de circuits comportait d'autres risques et coûts. Un réseau descendant et contrôlé de manière centralisée est vulnérable aux perturbations causées par des défaillances des principaux centres de commandement ou de certaines parties du réseau.³ La compagnie nationale de téléphone, en situation de monopole, n'ayant aucune incitation à mettre sur le marché de nouveaux produits et services, avait tendance à étouffer l'innovation dans les services aux consommateurs par une réglementation onéreuse ou des coûts inabordables. Il est possible qu'une concurrence accrue dans le domaine de la téléphonie à commutation de circuits aurait conduit à davantage d'innovation, mais la centralisation intrinsèque de la commutation de circuits a signifié qu'à un moment donné, chaque réseau est passé sous le contrôle exclusif d'une entité, qui avait peu d'intérêt économique à investir dans de nouveaux services.

Ces inconvénients et d'autres ont conduit les chercheurs des années 1960 et 1970 à développer et à perfectionner la « commutation par paquets » et, finalement, à développer ce qui est devenu Internet.

2.2 Comprendre le mode de fonctionnement du réseau Internet

Souvent appelé « réseau de réseaux », Internet est un réseau connecté constitué de réseaux qui ont choisi de se connecter les uns aux autres. Les premiers concepteurs d'Internet ont reconnu les avantages d'une conception flexible pour permettre l'émergence de nouvelles technologies et la connexion de nouveaux réseaux. Ils ont également reconnu que la meilleure façon de déployer un très grand réseau distribué était de tirer parti des réseaux existants, en les reliant entre eux à l'aide de technologies simples, peu coûteuses et facilement accessibles.

3 En comparaison, Internet est largement décentralisé, ce qui améliore sa fiabilité, sa robustesse et sa capacité à contourner les problèmes de réseau.

Contrairement à la téléphonie à commutation de circuits, les communications Internet circulent sur ce réseau de réseaux à l'aide de la commutation par paquets⁴ : chaque communication est divisée en petits « paquets » et chaque paquet circule indépendamment. Par exemple, chaque e-mail est divisé en plusieurs paquets plus petits, qui peuvent emprunter, et le font souvent, des chemins différents sur Internet pour atteindre le destinataire prévu. À leur arrivée, la destination les réassemble de manière fluide avant de remettre l'e-mail à l'utilisateur final. Cela a été une grande innovation dans la manière dont le contenu était communiqué à travers les réseaux.

Internet est lui-même composé de près de 76 000 réseaux indépendants qui utilisent les mêmes protocoles techniques et choisissent de fonctionner ensemble. La plupart de ces réseaux sont privés, mais certains sont détenus ou contrôlés par des gouvernements. Chaque réseau prend des décisions indépendantes sur la manière d'acheminer le trafic vers ses voisins en fonction de ses propres besoins, de son modèle commercial et des exigences locales. En outre, il existe des centaines de milliers d'autres entités, telles que les fournisseurs d'hébergement Web, les services de messagerie électronique, les services de domaine, les services d'identité et les fournisseurs de sécurité, qui jouent un rôle clé dans la prise en charge et la facilitation des communications sur Internet. Il n'existe aucun contrôle ou coordination centralisée des réseaux ou des entités de soutien.⁵

Cette conception distribuée et décentralisée est fondamentale pour le succès d'Internet. Internet s'est répandu à travers le monde et a atteint une telle envergure grâce à ce principe de conception fondamental. À mesure que de nouveaux besoins, de nouveaux domaines d'activité ou de nouvelles inventions apparaissent, de nouveaux réseaux rejoignent Internet facilement et à moindre coût. Grâce à cette conception, même les réseaux de petite taille ou situés dans des régions reculées peuvent se connecter à Internet pour un coût relativement modeste, généralement sans nécessiter de négociations ou d'accords complexes, hormis avec les prestataires locaux.

4 Pour une description de la commutation de paquets, voir <https://www.internetsociety.org/fr/blog/2022/04/pratiques-courantes-dinterconnexion-et-de-facturation-des-reseaux-internet/> ; voir également https://en.wikipedia.org/wiki/Packet_switching.

5 Un article de l'Internet Society, « Le mode de fonctionnement du réseau Internet : définition des propriétés essentielles d'Internet », Internet Society, 9 septembre 2020, <https://www.internetsociety.org/fr/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>, identifie les propriétés essentielles qui définissent Internet en tant que tel et qui soutiennent sa croissance et son adaptabilité. Ce document s'inscrit dans un projet plus vaste intitulé « The Internet Way of Networking », avec des ressources complémentaires disponibles sur <https://www.internetsociety.org/action-plan/internet-way-of-networking/>.

Internet est fondamentalement différent des réseaux de communication à commutation de circuits du passé, et ces différences dans son fonctionnement distribué et sa conception décentralisée sont essentielles à sa santé et à sa croissance continues.

2.3 Le rôle des intermédiaires

Les entités qui assurent des fonctions intermédiaires jouent un rôle essentiel, non seulement en fournissant une connectivité mondiale et en permettant le partage de contenu, mais aussi en garantissant la sécurité, la sûreté, la confidentialité et l'accessibilité. Internet dépend d'une série d'intermédiaires pour fonctionner.

L'Internet moderne repose sur un large éventail d'intermédiaires. Certains peuvent être familiers aux utilisateurs et aux décideurs politiques, tels que les FAI, les « fournisseurs de transit » qui connectent d'autres réseaux entre eux, les services d'hébergement qui prennent en charge le contenu Web et le courrier électronique, les moteurs de recherche et les services de réseaux sociaux. D'autres types d'intermédiaires peuvent être moins connus, notamment la mise en cache de contenu, la défense réseau et cybernétique, la résolution du « système de noms de domaine » (DNS) et l'enregistrement de domaine.⁶ Même certains types de logiciels, comme les navigateurs Web, exercent des fonctions intermédiaires en recevant du contenu d'Internet et en l'affichant à un utilisateur final (souvent avec un blocage de sécurité des sites Web malveillants).

Sans intermédiaires pour acheminer le trafic Internet vers et depuis les points de terminaison (notamment les particuliers, les serveurs, les prestataires de services et bien d'autres), et sans les nombreux autres types de fonctions qui rendent ce trafic possible, il n'y aurait pas d'Internet.

Les utilisateurs peuvent choisir d'interagir directement avec certains intermédiaires, tels que leur FAI pour accéder à Internet, leur outil de recherche préféré et leur navigateur pour afficher et parfois filtrer le contenu. Le fait de disposer d'une variété d'options disponibles permet également à l'utilisateur un plus grand choix et un plus grand contrôle. Par exemple, les utilisateurs peuvent choisir d'utiliser des fonctions intermédiaires axées sur la protection de la vie privée ou qui offrent des expériences en ligne « adaptées aux familles ».

6 L'annexe du présent document fournit une liste plus longue d'intermédiaires, couvrant des dizaines de types, ainsi que des recommandations spécifiques à l'intention des décideurs politiques, avec des conseils sur les pièges à éviter concernant chaque type d'intermédiaire.

Cependant, la plupart des utilisateurs ne connaissent pas ou ne comprennent même pas la vaste gamme d'intermédiaires qui rendent leur communication possible. Les utilisateurs peuvent, par exemple, ne pas savoir ce qu'est une recherche DNS, qui exerce cette fonction pour leurs recherches Web, ni qui ou quoi prend en charge le transit de leurs paquets une fois qu'ils ont quitté leur FAI. En outre, bon nombre des entités exerçant des fonctions intermédiaires n'ont peut-être aucune relation (légale ou autre) avec l'utilisateur à l'origine de la communication, ni avec le destinataire, ni entre elles. Bien que de nombreuses entités soient commerciales, certaines fonctions d'intermédiaires sur Internet sont assurées par des communautés à but non lucratif ou bénévoles. Les entités peuvent se trouver dans des juridictions différentes de celles de l'expéditeur et du destinataire. Cette approche décentralisée et distribuée est « une fonctionnalité, pas un bug ». Il serait irréalisable d'avoir des relations directes entre chaque entité pour toutes les fonctions intermédiaires à l'échelle d'Internet. L'approche décentralisée d'Internet offre flexibilité, résilience et capacité d'évolution à la hausse ou à la baisse selon les besoins.

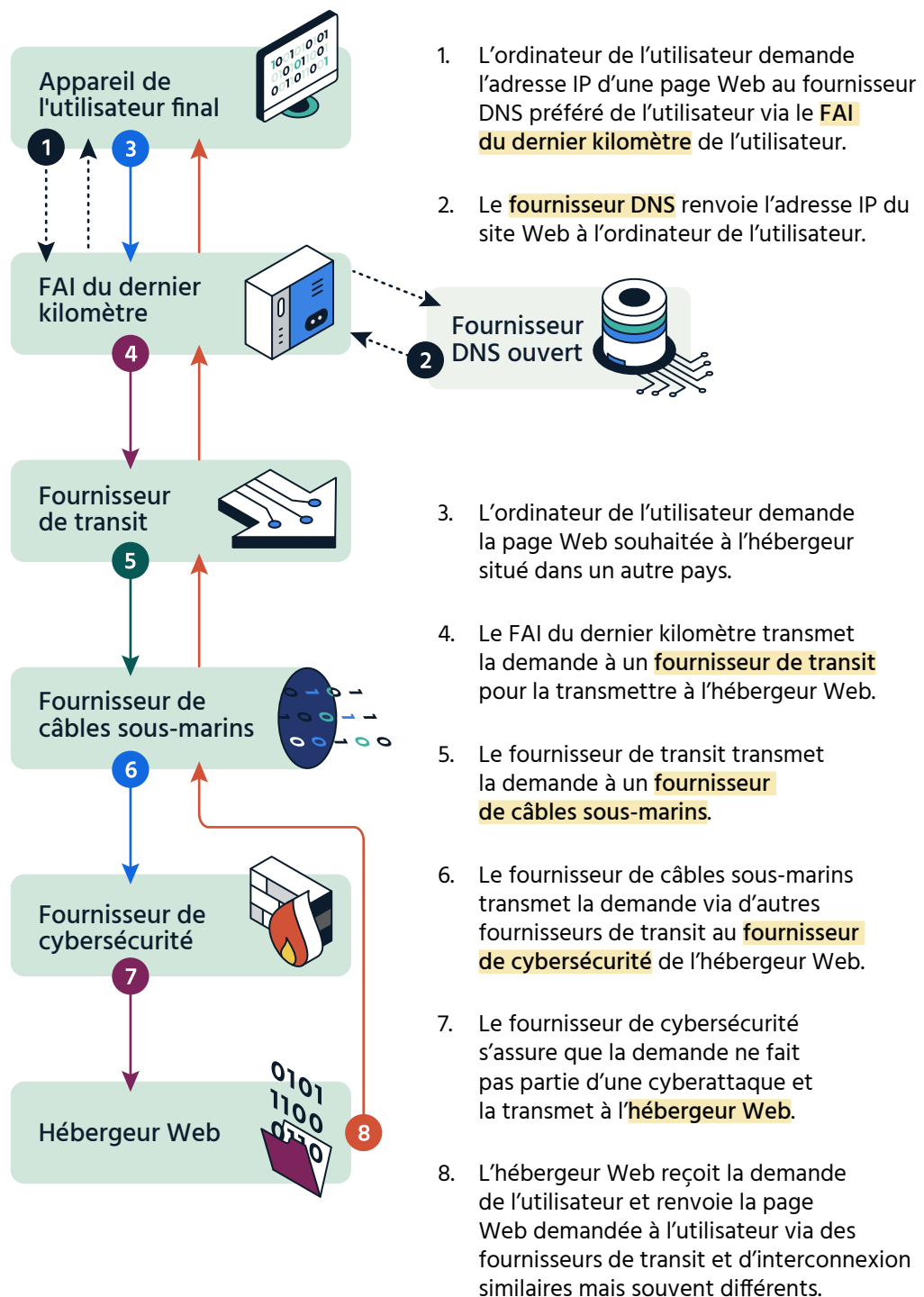
Les entités qui font fonctionner Internet et aident les utilisateurs à y accéder (parfois appelées vaguement « intermédiaires d'infrastructure ») ne sont généralement pas conscientes du contenu spécifique qui est communiqué.⁷ En revanche, les entités qui aident les utilisateurs à interagir avec le contenu sur Internet (p. ex., une plateforme de partage de vidéos ou une plateforme de réseaux sociaux) sont généralement directement impliquées dans la manière dont le contenu est affiché, organisé, partagé, etc. Cependant, il n'existe pas toujours une distinction nette entre ces entités, et toutes les « plateformes » ne sont pas informées du contenu transmis aux utilisateurs.⁸

7 Les intermédiaires d'infrastructure non seulement ne se soucient pas du contenu spécifique communiqué, mais ne peuvent pas non plus voir le contenu en raison de l'utilisation croissante du cryptage de bout en bout sur Internet.

8 Par exemple, la plupart des services de messagerie en ligne comme WhatsApp et Signal utilisent le cryptage de bout en bout, ce qui rend leur contenu transmis opaque et illisible.

Fournisseurs de services intermédiaires

Vue très simplifiée de certains des **fournisseurs de services intermédiaires** impliqués lorsqu'un utilisateur demande une page Web..



3 Protections en matière de responsabilité des intermédiaires

Cette section aborde les protections en matière de responsabilité, en commençant par un bref historique des origines et des éléments clés du texte de loi « Section 230 » des États-Unis. Nous décrivons également le « Marco Civil da Internet » du Brésil de 2014, ainsi que la Directive sur le commerce électronique de l'Europe de 2000 et le règlement DSA (Digital Services Act) de 2022, avant de passer à l'examen d'autres approches nationales ou régionales connexes.

Nous terminerons par une discussion sur les tendances récentes des politiques concernant les fonctions des intermédiaires, en identifiant certains risques spécifiques que ces approches peuvent engendrer pour Internet et ses utilisateurs.

3.1 Le développement initial des lois sur la protection des intermédiaires : mise en contexte

Internet a été développé dans les années 1970 grâce à un financement fourni par le gouvernement des États-Unis. Initialement utilisé à des fins de collaboration et de recherche par un petit groupe de chercheurs universitaires, gouvernementaux et commerciaux, il a commencé comme un réseau exclusivement américain, mais s'est rapidement développé pour inclure des connexions vers l'Europe, l'Asie et l'Océanie. Les interdictions de circulation personnelle et commerciale ont été progressivement supprimées dans les années 1990. En 1995, le gouvernement américain a transféré formellement le réseau au secteur privé, permettant ainsi à des millions de personnes d'accéder à Internet.

Alors que de plus en plus de personnes pouvaient s'exprimer publiquement sur Internet, des questions se sont rapidement posées sur la manière dont la responsabilité des contenus préjudiciables ou illégaux serait attribuée dans le contexte en ligne. Aux États-Unis, des poursuites ont été intentées, arguant que les entreprises qui autorisaient les gens à publier en ligne devaient être légalement responsables des propos publiés par ces personnes. Dans les années 1990, deux décisions judiciaires américaines fondamentales ont décidé que les hébergeurs de contenu en ligne – les intermédiaires – **seraient** responsables des propos publiés par leurs utilisateurs *si ces hébergeurs avaient pris des mesures pour modérer le discours en ligne et supprimer le contenu sexuel, offensant ou autre*.⁹

Ces décisions de justice ont créé deux scénarios irréalisables et peu attrayants pour l'Internet émergent.

D'un côté, si les entreprises prenaient des mesures pour « modérer » les discours en ligne de leurs utilisateurs, elles seraient alors responsables de ce contenu, mais ces entités¹⁰ n'avaient pas le personnel ou les ressources nécessaires pour examiner, bloquer ou supprimer tout contenu susceptible d'entraîner une responsabilité.¹¹

D'un autre côté, les entreprises pouvaient éviter toute responsabilité si elles ne prenaient aucune mesure pour supprimer le contenu sexuel, offensant ou autrement répréhensible publié par les utilisateurs. Mais un tel environnement aurait donné lieu à des conversations en ligne et à des publications inondées de contenu répréhensible. Au lieu de devenir une plateforme utile pour l'interaction sociale et civique ainsi que la croissance économique, Internet aurait perdu son utilité en tant qu'outil de communication, d'expression et de commerce individuels.

Ces décisions de justice ont engendré une incertitude importante et une responsabilité potentiellement dévastatrice pour le contenu généré par les utilisateurs dans le contexte de l'Internet en développement.

9 Dans l'affaire *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), il a été jugé qu'un fournisseur de services en ligne ne pouvait pas être tenu responsable des propos tenus par un participant sur un forum en ligne, mais *uniquement* parce que le fournisseur n'avait modéré aucun contenu. Ensuite, dans l'affaire *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), un fournisseur de services en ligne a été jugé responsable des propos tenus par les participants parce qu'il exerçait une certaine surveillance et une certaine réglementation du contenu.

10 Si les grands sites de réseaux sociaux d'aujourd'hui en sont un exemple évident, Internet des années 1990 comptait moins de « méga-sites » et il n'y avait souvent pas d'intermédiaire clairement défini qui avait le droit ou la responsabilité de modérer le contenu. Lorsqu'un modérateur était identifié, il s'agissait le plus souvent d'un particulier offrant bénévolement de son temps plutôt que d'une entreprise privée.

11 Même dans un environnement où les ressources sont abondantes, certains types de modération, comme celle des contenus diffamatoires, sont eux-mêmes problématiques, car la question de savoir si un contenu est diffamatoire ou non est souvent impossible à déterminer pour un modérateur individuel.

3.2 Les premières lois sur la responsabilité des intermédiaires Internet : section 230 des États-Unis

Face à ce défi posé au potentiel d'Internet et à la capacité des individus à s'engager en ligne, le Congrès des États-Unis a décidé, de 1995 à 1996, d'affronter la réalité selon laquelle les régimes de responsabilité existants ne fonctionnaient pas pour Internet :

- La responsabilité des éditeurs qui s'appliquait aux journaux hors ligne conduirait soit à une responsabilité potentielle massive qui paralyserait la parole individuelle sur Internet, soit à un Internet sur lequel les sites ne pourraient pas faire respecter les règles de comportement et de courtoisie.
- Le régime de transport public applicable au service téléphonique de base ne pouvait s'appliquer ni aux réseaux d'accès Internet, qui présentaient certains aspects des opérateurs de communications, mais pas suffisamment pour correspondre à ce modèle, ni aux hébergeurs de contenu, qui fonctionnent de manière complètement différente des opérateurs publics.
- Le régime de responsabilité qui s'appliquait à la radio, à la télévision et à la vidéo par câble, reposant sur des accords contractuels négociés individuellement entre les réseaux et les sociétés fournissant le contenu, ne pouvait pas s'appliquer à un monde comptant des millions, voire des milliards, d'utilisateurs en ligne.

Nous avons besoin d'une nouvelle approche de la responsabilité.

C'est dans ce contexte que le Congrès américain a examiné et promulgué la loi « Internet Freedom and Family Empowerment Act », qui est devenue la section 230 du Code des États-Unis (souvent intitulée simplement « Section 230 »).¹² L'un des objectifs explicites du Congrès pour la Section 230 était de « promouvoir le développement continu d'Internet et d'autres

¹² Le texte qui a donné naissance à la section 230 était à l'origine issu d'une proposition de loi de la Chambre des Représentants, intitulée « Internet Freedom and Family Empowerment Act ». Lors de la conférence entre la Chambre et le Sénat visant à concilier la législation relative à la loi sur les télécommunications, le texte de la section 230 a été placé immédiatement après et dans la même section statutaire que le projet de loi du Sénat, connu sous le nom de « Communications Decency Act ». Des informations supplémentaires sur le contexte de la nouvelle loi sur les télécommunications sont disponibles dans les articles « What's in a Name » (<https://www.lawfaremedia.org/article/whats-name-quite-bit-if-youre-talking-about-section-230>), « Section 230: An Overview » (par le Congressional Research Service, <https://crsreports.congress.gov/product/pdf/R/R46751>), entre autres. Le texte final peut être consulté sur <https://www.congress.gov/bills/104th-congress/senate-bill/652>.

services informatiques et médias interactifs ».¹³ Le Congrès a reconnu que les services informatiques interactifs en général, et Internet en particulier – même à ses débuts lorsque le texte de loi « Section 230 » a été promulgué – offraient une plateforme profondément différente pour la communication interactive entre individus.

Le Congrès américain a observé dans la loi que « Internet et d'autres services informatiques interactifs offrent un forum pour une véritable diversité de discours politique, des opportunités uniques de développement culturel et une myriade de voies pour l'activité intellectuelle ».¹⁴ Le Congrès a conclu que ces communications interactives, qui favorisent le débat public, devaient être encouragées. Contrairement aux formes de communication de masse « publiées » antérieures, Internet transforme l'individu d'un récepteur passif de produits créés principalement par les entreprises en un participant actif à l'élaboration de la communication et du contenu. Le Congrès a reconnu que cette « interactivité » individuelle était un attribut essentiel de l'Internet émergent qui méritait d'être protégé.

Texte clé de la Section 230 :

§ 230(c)(1) : **Traitement de l'éditeur ou de l'interlocuteur.**

Aucun fournisseur ou utilisateur d'un service informatique interactif ne doit être considéré comme l'éditeur ou l'interlocuteur d'informations fournies par un autre fournisseur de contenu informationnel.

§ 230(c)(2) : **Responsabilité civile.** Aucun fournisseur ou utilisateur d'un service informatique interactif ne peut être tenu responsable :

(A) d'une action volontairement entreprise de bonne foi pour restreindre l'accès ou la disponibilité de matériel que le fournisseur ou l'utilisateur considère comme obscène, lascif, sale, excessivement violent, harcelant ou autrement répréhensible, que ce matériel soit ou non protégé par la Constitution ; ou

(B) de toute action entreprise pour permettre ou mettre à la disposition des fournisseurs de contenu d'information ou d'autres les moyens techniques permettant de restreindre l'accès au matériel décrit au paragraphe ([A]).

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

¹⁴ 47 USC § 230(a)(3).

§ 230(f) : Définitions.

(2) Service informatique interactif

Le terme « service informatique interactif » désigne tout service d'information, système ou fournisseur de logiciel d'accès qui fournit ou permet l'accès informatique par plusieurs utilisateurs à un serveur informatique, y compris spécifiquement un service ou un système qui fournit un accès à Internet et de tels systèmes exploités ou services offerts par des bibliothèques ou des établissements d'enseignement.

(3) Fournisseur de contenu informationnel

Le terme « fournisseur de contenu informationnel » désigne toute personne ou entité responsable, en tout ou en partie, de la création ou du développement d'informations fournies via Internet ou tout autre service informatique interactif.

(4) Fournisseur de logiciels d'accès

Le terme « fournisseur de logiciels d'accès » désigne un fournisseur de logiciels (y compris des logiciels clients ou serveurs) ou d'outils d'activation qui effectuent une ou plusieurs des opérations suivantes :

- (A) filtrer, trier, autoriser ou interdire le contenu ;
- (B) sélectionner, choisir, analyser ou digérer du contenu ; ou
- (C) transmettre, recevoir, afficher, transférer, mettre en cache, rechercher, créer des sous-ensembles, organiser, réorganiser ou traduire du contenu.

Le texte de loi « Section 230 » des **États-Unis** contient trois éléments essentiels :

1. Les services informatiques interactifs (terme statutaire utilisé dans la section 230 qui fait essentiellement référence aux entités qui exercent des fonctions intermédiaires) sur Internet ne sont pas légalement responsables du contenu que d'autres entités (particuliers, sociétés et autres fournisseurs de contenu) publient sur Internet. C'est plutôt la personne ou l'entité qui a créé ou publié le contenu qui en reste légalement responsable. Cet élément permet aux FAI, aux services d'hébergement Web et à bien d'autres de transmettre ou d'héberger du contenu sans craindre une responsabilité potentiellement massive.

2. Les services informatiques interactifs ne sont pas responsables s'ils décident de bloquer ou de supprimer du contenu indésirable sur leurs plateformes. Cet élément garantit que les hébergeurs et plateformes en ligne sont protégés s'ils suppriment le contenu haineux, offensant ou autrement répréhensible de leurs sites. Si, par exemple, une personne publie du contenu sexuellement explicite sur une plateforme en ligne, elle ne pourrait pas poursuivre la plateforme si cette dernière supprimait ou bloquait ce contenu. Ainsi, les intermédiaires sont protégés pour leurs décisions de modération.
3. Les entreprises qui développent des outils technologiques permettant aux utilisateurs de filtrer et de bloquer les contenus indésirables sur Internet ne peuvent être tenues responsables de la création de cette capacité de blocage. Si, par exemple, un site Web contenant du contenu haineux et malveillant est bloqué par un logiciel installé par un parent sur un ordinateur personnel, le site Web ne peut pas poursuivre le fabricant du logiciel pour avoir bloqué son contenu. Cet élément encourage le développement d'outils permettant aux *utilisateurs* de choisir de limiter les types de contenus légaux auxquels ils (et leur famille) peuvent accéder.

Toutes les protections ci-dessus s'étendent très largement à tout service informatique interactif impliqué dans la transmission, le transport, l'hébergement, la conservation, l'affichage ou toute autre forme de facilitation de la transmission ou de l'affichage de contenu créé par d'autres, et pas seulement au service où le contenu a été publié ou partagé.

La section 230 n'utilise pas les termes « intermédiaire » ou « fonction intermédiaire » ; la loi emploie plutôt une définition large du concept « services informatiques interactifs » pour faire référence aux fonctions de base d'accès à Internet, de transit, d'hébergement, de recherche et de services connexes. Ensuite, la section 230 applique les protections de responsabilité ci-dessus à tout « fournisseur ou utilisateur d'un service informatique interactif ».

Il convient de noter que même les utilisateurs individuels sont protégés par la section 230 dans les cas où, par exemple, ils transmettent une publication en ligne à un autre destinataire.

La section 230 est considérée comme l'une des raisons essentielles pour lesquelles la liberté d'expression individuelle s'est développée sur Internet aux États-Unis.¹⁵ Parallèlement, le Congrès américain cherchait

¹⁵ Jeff Kossseff, un juriste américain, a même écrit un ouvrage complet, « The Twenty-Six Words that Created the Internet », faisant référence à la section 230 comme étant en grande partie responsable de la prospérité de l'industrie Internet américaine. Voir également <https://www.propublica.org/article/nsu-section-230> pour plus de contexte.

également à protéger et à encourager le potentiel économique d'Internet. Les avantages économiques et sociaux combinés d'Internet dont ont bénéficié les États-Unis ont conduit d'autres grands gouvernements à adopter des règles similaires.

Les États-Unis ont été la première nation à adopter des mesures de protection juridique en matière de responsabilité des intermédiaires Internet. D'autres nations et régions ont adopté des protections similaires, mais avec quelques différences importantes.

3.3 Protections initiales des intermédiaires en Europe

En 2000, l'**Union européenne** (UE) a adopté la directive sur le commerce électronique (2000/31/CE),¹⁶ ou « E-Commerce Directive », pour traiter des questions liées à la protection des intermédiaires. D'un point de vue pratique, la directive sur le commerce électronique a adopté une approche très similaire à la section 230, mais avec trois différences importantes :

- La directive de l'UE a divisé les intermédiaires en catégories de base : (a) simples transporteurs, (b) fournisseurs de mise en cache et (c) fournisseurs d'hébergement.
- La directive ne définit pas les types d'entités couvertes, mais aborde plutôt des types spécifiques d'« activités » qui bénéficieraient d'une protection en matière de responsabilité (tout comme ce document se concentre sur les « fonctions » des intermédiaires plutôt que sur les catégories d'intermédiaires).
- Plus important encore, la directive de l'UE exige que les intermédiaires qui ont connaissance d'un contenu présumé illégal prennent des mesures pour supprimer ce contenu dans un délai raisonnable.¹⁷

La directive sur le commerce électronique a régi les questions de protection des intermédiaires dans l'Union européenne pendant plus de 20 ans, jusqu'à ce qu'elle soit modifiée et complétée par le règlement DSA (Digital Services Act) et d'autres actions décrites ci-dessous.

¹⁶ Voir <https://eur-lex.europa.eu/eli/dir/2000/31/oj> ; https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000.

¹⁷ Le régime de « notification et retrait » créé par la directive sur le commerce électronique contraste avec l'approche en vigueur aux États-Unis, où le premier amendement de la Constitution américaine interdit généralement (en dehors du contexte du droit d'auteur) les mandats légaux visant à supprimer un contenu sans une détermination judiciaire spécifique selon laquelle le contenu est illégal.

3.4 Le « Marco Civil da Internet » au Brésil

Dès 2009, un large groupe de parties prenantes au **Brésil**, comprenant le gouvernement, les universitaires, la société civile et l'industrie, a lancé un projet collaboratif pour développer un ensemble de lois concernant Internet. Grâce à la participation de plusieurs parties prenantes, cet effort a fait l'objet de nombreux commentaires et contributions, et des projets ont été élaborés et peaufinés. La législation qui en a résulté a été promulguée en 2014 sous le nom de « Marco Civil da Internet », loi fédérale brésilienne n° 12.965/2014.¹⁸ Le gouvernement brésilien déclare que le Marco Civil « établit les principes, les garanties, les droits et les devoirs pour l'utilisation d'Internet au Brésil ».¹⁹

La Section III du Marco Civil énonce clairement la protection de la responsabilité des intermédiaires, tout en prévoyant des mesures supplémentaires permettant la suppression de contenu par décision judiciaire et la protection de la vie privée sous réserve de notification. Les principales clauses des dispositions sur les intermédiaires sont les suivantes :

Article 18. Le fournisseur de connexion Internet ne sera pas civilement responsable des dommages résultant de contenus générés par des tiers.

Article 19. Afin de garantir la liberté d'expression et d'empêcher la censure, les fournisseurs d'applications Internet ne peuvent être civilement responsables des dommages résultant de contenus générés par des tiers que si, après décision de justice spécifique, ils ne prennent pas de dispositions pour, dans la mesure et les limites techniques de leur service et dans le délai indiqué, rendre indisponible le contenu identifié comme contrefaisant, sous réserve par ailleurs des dispositions légales applicables.

...

Artigo 20. Si le fournisseur d'une application Internet dispose des informations de contact de l'utilisateur directement responsable du contenu visé à l'article 19, il appartiendra au fournisseur de

¹⁸ Voir <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6> ou la version officielle anglaise de la loi sur <https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180> et <https://www.daniel-ip.com/en/articles/the-brazilian-internet-bill-of-rights-and-online-infringement-of-ip-rights/>.

¹⁹ Version anglaise du Marco Civil, disponible sur http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf.

communiquer à l'utilisateur les raisons et les informations liées à l'indisponibilité du contenu, avec des informations permettant la défense contradictoire et complète devant le tribunal, sauf disposition légale expresse ou décision de justice expresse contraire.

...

Artigo 21. Les fournisseurs d'applications Internet qui mettent à disposition des contenus générés par des tiers seront tenus subsidiairement responsables de la violation de la vie privée résultant de la divulgation, sans l'autorisation des participants, d'images, de vidéos ou d'autres matériels contenant de la nudité ou des actes sexuels à caractère privé lorsque, après réception de la notification par le participant ou son représentant légal, ils ne parviennent pas à promouvoir avec diligence, dans les limites techniques de leur service, l'indisponibilité de ce contenu.

L'approche brésilienne a été considérée dans la région comme une voie vers la protection des intermédiaires tout en normalisant une voie judiciaire pour répondre aux préoccupations du gouvernement et des citoyens concernant les contenus illégaux ou préjudiciables.

3.5 Mise à jour des mesures de protection des intermédiaires en Europe

En 2022, l'**Union européenne**, motivée par des préoccupations concernant la sécurité en ligne, la propagation de la désinformation et des discours de haine, ainsi que d'autres comportements illicites ou nuisibles sur les grandes plateformes et les services largement utilisés, a adopté une mise à jour et une extension importantes de la directive sur le commerce électronique de 2000, poursuivant son approche générale consistant à s'adresser aux services (dont beaucoup englobent les « fonctions intermédiaires » évoquées ici), plutôt qu'aux entreprises. Elle reconnaît que certaines entités peuvent exercer des fonctions intermédiaires différentes et donc avoir droit à différents types de protection ou avoir des obligations différentes selon la fonction spécifique exécutée.

L'objectif principal du *règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement DSA (Digital Services Act))*²⁰ est de fournir un marché unique pour les services en ligne dans l'UE. Le règlement DSA (Digital Services Act) prévoit des protections

20 Voir <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> ainsi que la FAQ fournie par la Commission européenne sur https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 et les informations récapitulatives sur https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

en matière de responsabilité pour le contenu généré par les utilisateurs (sauf lorsque le fournisseur de services sait qu'il est illégal), mais les associe à des exigences de « diligence raisonnable ». Ces obligations rendent les fournisseurs plus responsables de ce qui se passe dans leurs services. Plutôt que d'imposer une responsabilité, le règlement DSA (Digital Services Act) utilise des amendes pour dissuader et punir le non-respect de ces obligations.

S'inspirant de la directive sur le commerce électronique, le règlement DSA (Digital Services Act) s'applique à un sous-ensemble de « services de la société de l'information » définis comme trois catégories de « services intermédiaires » :²¹

1. Un service de « simples transporteurs », consistant en la transmission dans un réseau de communication d'informations fournies par un destinataire du service, ou en la fourniture d'un accès à un réseau de communication.
2. Un service de « mise en cache », consistant en la transmission dans un réseau de communication d'informations fournies par un destinataire du service, impliquant le stockage automatique, intermédiaire et temporaire de ces informations, effectué dans le seul but de rendre plus efficace la transmission ultérieure des informations à d'autres destinataires à leur demande.
3. Un service d'« hébergement » consistant à stocker des informations fournies par et à la demande d'un destinataire du service.

En outre, le règlement impose des obligations particulières à deux catégories de services : les fournisseurs de très grands moteurs de recherche (TGM) et les fournisseurs de très grandes plateformes en ligne (TGP) (ayant plus de 45 millions d'utilisateurs européens par mois). Notamment :

- Un point de contact pour les autorités et les utilisateurs de l'UE.
- Des conditions générales conviviales.
- Transparence concernant la publicité, les systèmes de recommandation et les décisions de modération du contenu.
- Une évaluation basée sur les risques de leur service et des mesures d'atténuation appropriées.
- Audit indépendant.
- Partage de données avec les autorités à des fins de conformité et avec des chercheurs agréés pour comprendre les risques systémiques.

21 Ibid., article 3, « Définitions » du règlement DSA (Digital Services Act).

- L'obligation de fournir une option de système de recommandation non basée sur le profilage des utilisateurs.²²

3.6 Mesures de protection des intermédiaires dans d'autres contextes nationaux et internationaux

Au début des années 2000, plusieurs pays ont également adopté une législation nationale axée sur Internet, prévoyant différents niveaux de protection pour les intermédiaires.

Par exemple, en 2000, l'**Inde** a adopté la loi sur les technologies de l'information (Information Technology Act 2000), qui prévoyait que les intermédiaires ne seraient pas responsables du contenu de tiers disponible s'ils pouvaient prouver que l'infraction ou la contravention avait été commise à leur insu ou qu'ils avaient exercé toute la diligence requise pour empêcher la commission de cette infraction ou de cette contravention.²³ La loi autorise également les directives gouvernementales visant à supprimer certains contenus en ligne.

Au **Nigéria**, en 2003, les Lignes directrices pour la fourniture de services Internet publiées par la Commission nigériane des communications prévoyaient que les fournisseurs de services Internet agissant en tant que simples transporteurs (c.-à-d. hébergeurs ou services de mise en cache) ne seraient pas responsables du contenu et des communications générés par les utilisateurs, sous certaines conditions : ils doivent agir sans délai pour supprimer ou désactiver l'accès aux informations dès réception de tout avis de retrait, ou lorsqu'ils prennent connaissance que les informations à la source initiale de la transmission ont été supprimées ou désactivées.²⁴

L'Afrique du Sud, dans sa loi de 2002 sur les communications et transactions électroniques, a adopté une approche similaire, mais a subordonné les limitations de responsabilité à l'appartenance du prestataire de services à un organisme représentatif et à son obligation de respecter le code de conduite de cet organisme, reconnu par le ministre, ainsi qu'à un processus de notification et de retrait.²⁵

22 Voir les orientations de la Commission européenne sur <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.

23 Voir l'article 79 de la loi sur les technologies de l'information de 2000 (Inde), disponible sur <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf>.

24 Lignes directrices pour la fourniture de services Internet publiées par la Commission nigériane des communications en 2003 conformément à l'article 70(2) de la loi nigériane sur les communications de 2003, disponibles sur <https://ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file>.

25 Loi sur les communications et transactions électroniques de 2002 (Afrique du Sud) disponible sur https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

La loi néo-zélandaise sur les communications numériques préjudiciables de 2015 protège les « hébergeurs de contenu en ligne » de toute responsabilité, à condition qu'ils se conforment au processus de plainte légal. La loi prévoit notamment l'obligation pour l'hébergeur de contenu en ligne d'informer la personne déposant une plainte et peut impliquer l'obligation de retirer ou de désactiver le contenu.²⁶

L'Australie progresse activement en 2024 vers l'adoption d'un régime de protection de la responsabilité des intermédiaires axé sur les réclamations légales pour diffamation.²⁷ Les dispositions proposées pour l'amendement type sur la diffamation (intermédiaires numériques) de 2023 modifieraient les lois australiennes « uniformes » sur la diffamation, entrées en vigueur en 2006, afin d'harmoniser les lois sur la diffamation dans toute l'Australie. Les nouvelles dispositions visent à clarifier la position juridique des intermédiaires face aux contenus numériques diffamatoires. Elles prévoient des exemptions de responsabilité pour diffamation pour les intermédiaires numériques fournissant des services de mise en cache, de transport, de stockage et de recherche.²⁸ Toutefois, ces exemptions ne seront pas disponibles si l'intermédiaire numérique, entre autres, a sélectionné l'un des destinataires ou a promu le contenu diffamatoire. Il n'est pas certain que cela couvre la promotion de contenu auprès des utilisateurs via des algorithmes de recommandation. L'exemption pour les moteurs de recherche ne s'appliquerait pas aux « résultats de recherche sponsorisés », c'est-à-dire « les résultats [qui] sont promus ou priorisés par le fournisseur du moteur de recherche en raison d'un paiement ou d'un autre avantage accordé au fournisseur par ou au nom d'un tiers ».

Outre les lois contraignantes adoptées par les gouvernements, plusieurs organisations multilatérales ou multipartites ont publié des déclarations de soutien aux protections en matière de responsabilité des intermédiaires. Ces accords et déclarations internationaux reflètent un consensus croissant sur la valeur de telles protections. Nous fournissons un résumé de certaines de ces déclarations dans le tableau ci-dessous.

26 Loi de 2015 sur les communications numériques préjudiciables (Nouvelle-Zélande) disponible sur <https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM6512504>.

27 Voir <https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf> ou <https://www.parliament.nsw.gov.au/bill/files/18503/Passed%20by%20both%20Houses.pdf> (version Nouvelle-Galles du Sud).

28 Annexe 1, sections 10C et 10D des dispositions de 2023 relatives à la modification du modèle de diffamation (intermédiaires numériques), disponible sur <https://pcc.gov.au/uniform/2023/pcc-584-d40.pdf>.

Déclarations multilatérales et multipartites sur les protections en matière de responsabilité des intermédiaires

2011

Le Rapporteur spécial des Nations Unies (ONU) sur la liberté d'opinion et d'expression, le Représentant de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias, le Rapporteur spécial de l'Organisation des États américains (OEA) sur la liberté d'expression et le Rapporteur spécial de la Commission africaine des droits de l'homme et des peuples (CADHP) sur la liberté d'expression et l'accès à l'information²⁹ ont publié une déclaration commune appelant à la protection des intermédiaires « simple transport » et d'autres fonctions intermédiaires, exprimant l'avis qu'ils ne devraient pas être tenus de surveiller le contenu généré par les utilisateurs et ne devraient pas être soumis à des règles de retrait extrajudiciaire de contenu qui ne parviennent pas à assurer une protection suffisante de la liberté d'expression.

2013

Lors du Forum africain sur la gouvernance d'Internet, une initiative panafricaine visant à promouvoir les normes des droits de l'homme et les principes d'ouverture dans la formulation et la mise en œuvre des politiques Internet en Afrique, la Déclaration africaine des droits et libertés de l'Internet a été publiée,³⁰ qui contient un principe de protection intermédiaire très simple : « Nul ne devrait être tenu responsable du contenu sur Internet dont il n'est pas l'auteur. »³¹

2014

L'Organisation de coopération et de développement économiques (OCDE) a publié des orientations générales sur la limitation de la responsabilité des intermédiaires.³²

Limiter la responsabilité des intermédiaires Internet.

Des limitations appropriées de responsabilité pour les

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

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

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

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

intermédiaires Internet jouent un rôle fondamental dans la promotion de l'innovation et de la créativité, la libre circulation de l'information, les incitations à la coopération entre les parties prenantes et la croissance économique. Les intermédiaires Internet, comme d'autres parties prenantes, jouent également un rôle important dans la lutte contre les activités illégales, les fraudes et les pratiques trompeuses et déloyales menées via leurs réseaux et services. La proportionnalité et le respect des protections relatives à l'ensemble des droits fondamentaux applicables sont des éléments importants dans ce contexte.

Bien que les principes ne soient pas contraignants, ces orientations de l'OCDE reflètent une large reconnaissance par de nombreux gouvernements du fait que les protections en matière de responsabilité des intermédiaires jouent un rôle important pour faciliter l'expression et l'engagement créatif en ligne.

2018

En 2018, le Conseil de l'Europe a adopté la Recommandation du Comité des Ministres aux États membres sur les rôles et responsabilités des intermédiaires Internet (CM/Rec(2018)2),³³ appliquant une approche fondée sur les droits de l'homme aux responsabilités des États et des intermédiaires Internet, laissant de côté les questions de responsabilité.

3.7 Tendances récentes en matière de responsabilité des intermédiaires et risques pour Internet

Les protections accordées aux intermédiaires sont considérées comme ayant joué un rôle déterminant dans la croissance d'Internet et dans l'épanouissement de la liberté d'expression individuelle sur Internet. Certains pays, conscients des bienfaits des garanties pour les intermédiaires, ont intégré la protection de la responsabilité dans leur législation. Dans d'autres pays, l'absence de lois protégeant les intermédiaires peut conduire à des protections élaborées par les tribunaux ou à un traitement plus problématique des fonctions des intermédiaires.

³³ <https://rm.coe.int/1680790e14>.

Dans cette section, nous identifions certaines approches récemment proposées pour l'élaboration de politiques relatives aux fonctions des intermédiaires Internet. Selon la mise en œuvre exacte, ces approches peuvent créer des risques importants pour Internet et ses utilisateurs, notamment :

- Porter atteinte au fonctionnement technique et à la fiabilité d'Internet.
- Affaiblir la sécurité et la confidentialité sur Internet.
- Réduire la concurrence sur Internet dans un pays en raison des contraintes ou des responsabilités imposées au FAI.
- Limiter la capacité des individus à partager leurs opinions et autres discours sur Internet.
- Bloquer de manière excessive le contenu légal.
- Exclure injustement des segments de la population de l'accès à Internet.

Nous recommandons d'évaluer soigneusement les risques énumérés ci-dessus et les autres impacts potentiels sur Internet lors de l'examen de ces approches d'élaboration de politiques pour les fonctions des intermédiaires. Dans les sections suivantes de ce document, nous fournissons des conseils généraux et spécifiques aux décideurs politiques sur la manière d'éviter ces risques et d'autres.

Notification et retrait : tous les régimes réglementaires n'ont pas adopté la même approche en matière de responsabilité des intermédiaires. Dans une variante courante, les intermédiaires peuvent être tenus responsables, voire redevables, du contenu de leurs utilisateurs s'ils ne prennent pas certaines mesures. Par exemple, certaines juridictions ont une approche de « notification et retrait », qui exige qu'un intermédiaire supprime le contenu à la réception d'une notification légalement autorisée par un tribunal ou une agence gouvernementale autorisée. Il est important de noter qu'il n'existe généralement aucune obligation générale pour les intermédiaires de surveiller le contenu.³⁴

Connaissance : d'autres ont exigé des intermédiaires qu'ils suppriment les contenus illégaux ou préjudiciables lorsqu'ils en ont connaissance, avec différents niveaux de « connaissance » requis, le plus strict étant la « connaissance réelle³⁵ ».

34 Toutefois, les amendements apportés à la loi zimbabwéenne de 2021 sur la cybersécurité et la protection des données au Code de procédure pénale et aux preuves prévoient qu'un fournisseur d'hébergement doit, s'il « prend connaissance de toute information illégale stockée, informer rapidement l'autorité compétente pour lui permettre d'évaluer la nature de l'information et, si nécessaire, émettre une ordonnance de suppression ». Texte disponible sur <https://www.law.co.zw/download/cyber-and-data-protection-act-chapter-1207/>.

35 Voir, par exemple, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE) (Espagne), disponible sur <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758>.

Ces modifications (notification et retrait, et connaissance) de l'approche générale s'appliquent après que le contenu a été téléchargé ou partagé par un utilisateur.

Modération des téléchargements : on s'intéresse de plus en plus à la nécessité de demander aux intermédiaires, en particulier aux intermédiaires hébergeurs de contenu, de filtrer certains types de contenus avant qu'ils ne soient partagés, comme les contenus d'abus sexuels sur mineurs (CSAM, Child Sexual Abuse Material). On parle parfois de « modération des téléchargements » et, dans certaines propositions, on souhaite imposer cette obligation même aux applications de messagerie cryptées de bout en bout.³⁶

Ces types de responsabilités liées au contenu préalable à la publication commencent à être qualifiées de responsabilités de « diligence raisonnable » ou de « devoir de diligence ». Parfois, il s'agit également d'approches de « responsabilité conditionnelle », dans lesquelles un intermédiaire ne sera pas tenu responsable **à condition** qu'il fasse quelque chose ou empêche quelque chose.

Exigences spécifiques à l'âge : certains pays ont fait pression pour imposer de plus grandes responsabilités aux entités intermédiaires afin d'exclure certains groupes d'âge de leurs services ou de modifier les services ou le contenu qu'ils affichent pour ces utilisateurs. Le non-respect de ces mesures peut entraîner l'interdiction ou le blocage du service intermédiaire ou rendre l'entité intermédiaire responsable en fonction de la manière dont la politique est mise en œuvre.

Par exemple, les intermédiaires peuvent être protégés de toute responsabilité concernant le contenu généré par les utilisateurs en Indonésie s'ils s'assurent que leurs systèmes ne contiennent pas ou ne facilitent pas la diffusion de contenu interdit. Ils doivent également disposer d'un cadre de gouvernance pour le contenu généré par les utilisateurs, qui comprend les droits, les obligations, les rapports, les plaintes, la responsabilité, et fournir des informations sur les utilisateurs qui effectuent des téléchargements interdits et répondent aux « notifications de retrait ».³⁷

³⁶ De toute évidence, si un intermédiaire fournissant des messages cryptés de bout en bout est tenu de modérer le contenu envoyé entre les utilisateurs, alors les messages ne peuvent plus être qualifiés de cryptés de bout en bout.

³⁷ Règlement du ministre des Communications et de l'Information, République d'Indonésie, numéro 5 de 2020 sur les opérateurs de systèmes électroniques privés, voir article 11, disponible sur https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

Cette approche politique suscite un intérêt pour les mécanismes techniques permettant de vérifier l'âge et l'identité d'un utilisateur avant qu'il puisse utiliser des services ou accéder à du contenu. Les mécanismes actuellement disponibles suscitent toutefois de sérieuses inquiétudes quant à leur efficacité, leur confidentialité, leur sécurité et la prévention de l'accès à des contenus en ligne légaux.³⁸

Exigences en matière de traçabilité : une autre approche qui a émergé consiste à exiger des intermédiaires qu'ils soient en mesure d'identifier qui a publié du contenu, même lorsqu'une communication est cryptée de bout en bout. À titre d'exemple, en Inde, les grands intermédiaires de messagerie sur les réseaux sociaux doivent être en mesure d'identifier l'auteur initial d'un message lorsque cela est requis par une décision de justice.³⁹

Suppression des protections de responsabilité des intermédiaires : les réactions aux premières expériences avec des politiques spécifiques à Internet ont inspiré des propositions radicales. Aux États-Unis, par exemple, les inquiétudes concernant les plus grandes plateformes ont donné lieu à des propositions trop larges visant à supprimer *toutes* les protections intermédiaires de *toutes* les entités protégées par la loi pertinente, la section 230. De même, au Brésil, des questions ont été soulevées quant à la validité actuelle de l'approche adoptée dans le Marco Civil da Internet en matière de responsabilité des intermédiaires. De telles propositions visant à modifier ou à abroger les protections intermédiaires, même au stade de la proposition, ont pour conséquence directe de menacer l'existence des opérations d'Internet en créant une incertitude et la menace d'une responsabilité illimitée pour le contenu produit par d'autres.

Codes industriels obligatoires : certaines juridictions imposent des codes ou des normes industrielles exécutoires⁴⁰ pour créer de nouvelles

38 Voir Internet Society, « La loi texane sur la vérification obligatoire de l'âge affaiblira la confidentialité et la sécurité sur Internet », 23 septembre 2024, disponible sur <https://www.internetsociety.org/blog/2024/09/texas-mandatory-age-verification-law-will-weaken-privacy-and-security-on-the-internet/>.

39 Disponible sur le site Web de MeitY à l'adresse <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf>. Au moment de la rédaction du présent document, la constitutionnalité de ces règles fait l'objet de diverses procédures judiciaires.

40 Voir, par exemple, le registre des codes et normes de l'industrie australienne de la sécurité en ligne, disponible sur <https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards>.

obligations légales (telles que la sécurité dès la conception, les évaluations des risques et l'application des conditions de service) pour les catégories d'intermédiaires, par exemple les réseaux sociaux, les moteurs de recherche, en particulier dans le contexte de la sécurité en ligne.

Nous observons que les politiques dans chaque juridiction sont souvent élaborées de manière très générale. Parfois, c'est intentionnel, une façon de pouvoir suivre l'évolution de la technologie et des utilisations d'Internet. Toutefois, ces politiques générales ont souvent de graves conséquences sur Internet et sur la capacité des individus à s'exprimer en ligne.

3.8 Hétérogénéité des pays

Ce document vise à fournir des orientations politiques utiles aux pays du monde entier, qu'ils aient des niveaux élevés de pénétration d'Internet et des industries Internet bien développées ou qu'ils travaillent encore à améliorer l'accès et à développer leurs économies numériques.

Nous reconnaissons qu'il existe de vastes différences en matière de droit, de culture, d'économie, de politique, de valeurs et même d'objectifs politiques concernant le contenu sur Internet. Nous pensons que nos recommandations seront utiles à tout décideur politique envisageant une réglementation qui s'appliquerait aux intermédiaires. Le document commence par se concentrer sur l'approche politique visant à protéger les intermédiaires de toute responsabilité et sur les raisons pour lesquelles cette approche a été importante pour permettre aux individus de participer en ligne. Nous proposons également des recommandations constructives pour répondre à une grande variété de préoccupations politiques.

Nous constatons que les systèmes juridiques diffèrent dans la manière dont ils abordent le contenu problématique en ligne : certains se concentrent principalement sur la personne qui publie le contenu, tandis que d'autres s'intéressent aux intermédiaires qui hébergent ou transmettent ce contenu. En outre, alors que la plupart des pays disposent de procédures judiciaires publiques et privées pour traiter les contenus problématiques en ligne, certains ont davantage de procédures judiciaires privées que d'autres. Ces différences ont pu amener les pays à traiter la question de la responsabilité des intermédiaires avec des priorités différentes. Dans toutes les situations, cependant, il est essentiel d'éviter de faire peser la responsabilité, civile ou pénale, sur les intermédiaires en raison du contenu publié par un utilisateur ou un tiers. Si une telle

responsabilité était imposée, elle porterait atteinte à la capacité des internautes à s'exprimer et à publier du contenu en ligne. Toutefois, comme mentionné dans la section 4, les gouvernements disposent de nombreuses manières constructives de répondre aux préoccupations politiques concernant les fournisseurs de services en ligne.

Il est également important, lors de l'élaboration des politiques, de comprendre que les entités exerçant des fonctions intermédiaires varient en termes de taille, de revenus, de marges bénéficiaires et de modèle économique. Certaines sont à but non lucratif et d'autres, selon le pays et l'environnement commercial, peuvent également être gérées par les gouvernements. Certaines n'offrent qu'une seule fonction restreinte, tandis que d'autres sont fortement intégrées à une variété d'activités connexes. Cela conduit à des intérêts très divers et parfois opposés au sein d'un même secteur, ainsi qu'à des différences significatives dans leur capacité à contribuer efficacement à l'élaboration des politiques dans ce domaine.

La juridiction sur les fournisseurs de services en ligne peut également varier d'un pays à l'autre. Selon l'endroit où se trouve l'entité exerçant une fonction intermédiaire, les questions de juridiction peuvent s'avérer complexes. Il peut être plus facile pour les pays d'exercer leur juridiction lorsqu'une entité assurant des fonctions intermédiaires dispose de bureaux commerciaux ou d'infrastructures dans ce pays. Lorsque le contenu est hébergé à l'extérieur du pays, la question de la juridiction peut s'avérer plus complexe, en particulier lorsque les pays parviennent à des conclusions différentes quant à la nature légale du même contenu.

Les questions de juridiction sont déterminantes, car l'incompatibilité des lois et les revendications de juridiction extraterritoriale rendent difficile et coûteux, voire impossible, d'exercer des fonctions d'intermédiaire Internet à l'échelle mondiale. Nous exhortons les décideurs politiques à éviter de créer des lois ayant des effets extraterritoriaux et à prendre en compte les risques pour Internet à l'échelle mondiale.

4 Principes d'élaboration des politiques pour les intermédiaires Internet

Cette section présente trois ensembles de principes qui, selon l'Internet Society, seront utiles aux décideurs qui envisagent des politiques affectant les services Internet :

1. Principes généraux applicables à toute politique concernant Internet ou son utilisation.
2. Principes spécifiquement axés sur la protection des intermédiaires en matière de responsabilité.
3. Des exemples plus généraux de principes juridiques et politiques pouvant être appliqués aux fonctions d'intermédiaires sans nuire aux protections des intermédiaires en matière de responsabilité.

L'annexe du présent document va au-delà de ces principes et fournit des recommandations politiques détaillées sur un large éventail de **fonctions des intermédiaires Internet**. Dans l'annexe, nous discutons également des considérations techniques et pratiques pour chacune des fonctions des intermédiaires. Les informations contenues dans l'annexe sont regroupées par type de fonction d'intermédiaire, allant des fonctions bien connues comme l'hébergement et la diffusion de contenu, jusqu'aux fonctions essentielles permettant de communiquer des données, de localiser des contenus et de sécuriser les communications sur Internet.

4.1 Principes généraux pour une politique prudente concernant Internet

Les principes suivants devraient guider les actions politiques concernant Internet en général, et les fonctions des intermédiaires en particulier :

- A. **Impliquez les parties prenantes dans l'élaboration des politiques :**
les politiques seront plus efficaces et plus faciles à mettre en œuvre si les décideurs politiques impliquent d'autres parties prenantes tout au long du processus d'élaboration des politiques. Une implication étroite des parties prenantes garantira que l'expertise et les points de vue pertinents sont pris en compte. Nous recommandons vivement aux gouvernements d'assurer une large participation de toutes les parties prenantes concernées dans l'élaboration des politiques qui touchent à Internet.
- B. **Effectuez une évaluation de l'impact sur Internet :** l'architecture technique et le fonctionnement d'Internet peuvent être directement, et souvent involontairement, affectés par les politiques, les réglementations ou les lois appliquées au contenu d'Internet ou aux fonctions des intermédiaires permettant la communication sur Internet. Nous recommandons vivement aux décideurs politiques de réaliser une évaluation de l'impact sur Internet pour toute nouvelle proposition de politique, même si celle-ci semble spécifiquement adaptée, afin de comprendre si elle pourrait avoir un effet négatif sur Internet et son fonctionnement. L'Internet Society a analysé les propriétés et les facteurs critiques indispensables à l'existence et au développement d'Internet et a élaboré une boîte à outils d'évaluation de l'impact sur Internet pour aider les décideurs politiques dans ce processus.⁴¹
- C. **Veillez à ce que toute régulation ou loi proposée soit précisément adaptée** aux fonctions spécifiques des intermédiaires qui causent un préjudice politique : il existe un risque d'inclure un ensemble trop large de fonctions, en particulier lorsque la préoccupation en matière de politique sociale est soulevée par un ensemble très restreint d'entreprises ou d'intermédiaires. Par exemple, s'il existe une préoccupation concernant des types particuliers de contenu hébergés par un groupe de sites Web, une proposition

41 Voir Internet Society, Le mode de fonctionnement du réseau Internet : définition des propriétés essentielles d'Internet, 9 septembre 2020, disponible sur <https://www.internetsociety.org/fr/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>; Internet Society, Boîte à outils pour l'évaluation de l'impact sur Internet, 8 novembre 2021, disponible sur <https://www.internetsociety.org/fr/resources/doc/2020/internet-impact-assessment-toolkit/introduction/>.

d'élaboration de politique devrait cibler étroitement ce type de contenu et ce groupe spécifique de sites Web. Étant donné que les intermédiaires sont essentiels au fonctionnement de base d'Internet et à la capacité des individus à s'exprimer en ligne, toute politique doit être soigneusement ciblée pour éviter d'affecter un ensemble trop large de fonctions et d'entités intermédiaires.

- D. **N'utilisez pas les protections des intermédiaires comme une menace ou un argument de négociation** : les protections des intermédiaires sont si fondamentales pour le fonctionnement d'Internet qu'elles ne doivent pas être utilisées comme moyen de pression dans un débat de politique publique ni comme sanction dans la réglementation ou la loi. Un législateur ne devrait pas, par exemple, adopter un projet de loi qui stipule que si un ensemble d'entreprises ne se conforme pas à une exigence particulière, elles perdraient leurs protections en tant qu'intermédiaires. La capacité des individus à s'exprimer en ligne ne doit pas être l'otage d'autres objectifs politiques. Les décideurs politiques devraient réglementer ou légiférer directement pour atteindre leur objectif sans mettre en danger les protections des intermédiaires ni nuire au fonctionnement d'Internet.
- E. **Les politiques doivent promouvoir l'ouverture** : l'accès à Internet, aux services, aux applications, aux sites et au contenu facilite la participation individuelle. L'accès libre améliore l'expérience utilisateur et le potentiel d'Internet à stimuler l'innovation, la créativité et le développement économique. Les décideurs politiques doivent éviter de limiter ou de bloquer la disponibilité des intermédiaires qui donnent accès à Internet, à ses applications et à ses services.
- F. **Les interventions politiques doivent viser directement le préjudice** : ainsi, il y a moins de risques de nuire aux autres internautes et à Internet si elles se concentrent sur le contenu problématique et son origine. Par exemple, plutôt que d'essayer de bloquer l'accès au contenu via l'adresse IP ou le blocage DNS (ce qui pourrait également empêcher l'accès au contenu légitime et perturber le trafic Internet), la personne qui publie le contenu pourrait être obligée de le supprimer.

4.2 Principes spécifiques concernant la protection des intermédiaires en matière de responsabilité

Les quatre principes suivants se concentrent sur différents aspects des opérations et du travail des entités qui exercent des fonctions d'intermédiaires, ainsi que sur la nécessité de fournir des protections pour ces tâches :

- G. **Protéger les intermédiaires assurant les communications sur Internet de la responsabilité liée au « contenu généré par les utilisateurs », c'est-à-dire le contenu créé par d'autres :** sans protection en matière de responsabilité, l'infrastructure Internet, ainsi que les outils de base que les gens utilisent pour accéder et interagir avec le contenu, seraient paralysés par un potentiel illimité d'actions en justice. Sans protections pour ces fonctions d'intermédiaires, Internet ne pourrait tout simplement pas fonctionner. Nous recommandons vivement que les entités assurant ces fonctions intermédiaires sur Internet soient protégées de toute responsabilité pour le contenu créé par des tiers qu'elles transmettent, reçoivent, mettent en cache, filtrent ou traitent de toute autre manière.
- H. **Protéger les intermédiaires qui hébergent, facilitent et optimisent la diffusion du « contenu original du site » (c'est-à-dire le contenu créé par le propriétaire du site) :** les entités qui hébergent plus d'un milliard de sites Web sur Internet doivent être protégées de toute responsabilité concernant le contenu que leurs clients mettent en ligne. Si les hébergeurs étaient rendus responsables du contenu mis en ligne par leurs clients, la plupart ne pourraient pas continuer à proposer ce service. Cela affecterait particulièrement les hébergeurs Web de petite et moyenne taille, entraînant une hausse des coûts, étouffant la concurrence et réduisant la disponibilité et la diversité du contenu en ligne. Les propriétaires de sites doivent rester responsables et potentiellement redevables du contenu de leurs sites Web, tandis que les entités assurant des fonctions intermédiaires telles que l'hébergement Web, les moteurs de recherche et la mise en cache ne doivent pas être responsables.
- I. **Protéger les intermédiaires qui hébergent et affichent le contenu généré par les utilisateurs :** les entités assurant des fonctions d'intermédiaires pour héberger le contenu généré par les utilisateurs doivent être protégées de toute responsabilité concernant ce

contenu. Sans cette protection, ces intermédiaires ne pourraient pas continuer à diffuser le contenu. Cela aurait un impact négatif considérable sur la capacité des individus à publier du contenu et à engager des conversations et des débats avec d'autres internautes. Les intermédiaires sont nécessaires pour que les individus puissent transmettre leurs mots, leurs opinions, leurs créations artistiques et leurs discussions avec d'autres. Les protections des intermédiaires doivent être accordées aux entités qui hébergent du contenu généré par les utilisateurs, afin de permettre à ces derniers de continuer à s'exprimer et à partager leur contenu en ligne.

- J. **Protéger les intermédiaires qui organisent et modèrent le contenu des utilisateurs** : une entité qui héberge du contenu généré par les utilisateurs doit être en mesure de définir des « règles de conduite » pour les types de discussions, d'œuvres créatives ou d'autres contenus qu'elle souhaite héberger. Par exemple, si une entité hébergeant du contenu généré par les utilisateurs choisit de ne pas héberger de contenu « pour adultes » ou choisit de définir des règles pour le comportement des utilisateurs, l'entité doit être libre de le faire. Ces entités, qui remplissent des fonctions intermédiaires d'hébergement de contenu utilisateur, doivent également être protégées de toute responsabilité en cas de suppression de contenu non pertinent ou répréhensible. Étant donné la quantité massive de contenu généré par les utilisateurs téléchargé et partagé chaque minute, la curation est souvent d'une importance cruciale pour aider les utilisateurs à trouver un contenu particulier ou de type spécifique. La curation de contenu implique généralement l'utilisation d'un ou plusieurs algorithmes, depuis un algorithme simple qui présente le contenu dans l'ordre dans lequel il est reçu jusqu'à des algorithmes plus sophistiqués qui présentent le contenu en fonction du profil d'un utilisateur et de ses interactions avec le service. Le filtrage et les « règles de conduite » permettent aux services de contenu hébergé et à leurs utilisateurs d'éviter d'être submergés par du contenu non pertinent, nuisible et malveillant qui noie le contenu légitime et décourage la participation individuelle sur Internet. Les régimes de protection des intermédiaires doivent protéger les entités de toute responsabilité juridique liée à l'application de leurs propres règles de conduite ou à la suppression de contenus répréhensibles.

4.3 Principes juridiques et politiques spécifiques pouvant être appliqués aux rôles des intermédiaires sans porter atteinte aux communications sur Internet

Les intermédiaires sont essentiels pour tout contenu transmis, hébergé ou traité d'une autre manière, et ces fonctions nécessitent une protection en matière de responsabilité liée au traitement de ce contenu. Mais cela *ne signifie pas* que les entités qui assurent ces fonctions ne peuvent pas être réglementées. Il existe un large éventail de politiques, de réglementations et de lois qui s'appliquent déjà, ou peuvent s'appliquer, aux entités qui exercent des fonctions d'intermédiaires, y compris, par exemple, les lois sur la concurrence et la protection des consommateurs. Vous trouverez ci-dessous quelques principes politiques qui pourraient contribuer à répondre à certaines des préoccupations politiques suscitées par les fonctions des intermédiaires sur Internet :

Confidentialité et sécurité des utilisateurs

- La confidentialité et la sécurité sont essentielles pour protéger la vie privée, l'intégrité et la confidentialité des communications des individus.
- Les politiques doivent appliquer des règles strictes pour protéger la confidentialité et améliorer la sécurité des communications Internet.
- Les entités assurant des fonctions d'intermédiaires sur Internet doivent également s'efforcer d'intégrer la « sécurité dès la conception » et la « confidentialité dès la conception », en adoptant les bonnes pratiques du secteur et en innovant pour améliorer les fonctionnalités de confidentialité et de sécurité de leurs fonctions.

Contrôle et choix des utilisateurs

- Offrir aux utilisateurs la possibilité de choisir et de contrôler le contenu qu'ils consomment leur permet de se protéger en filtrant les contenus et les sources non pertinents et indésirables.
- Les politiques doivent s'efforcer d'améliorer le choix et le contrôle des utilisateurs sur les services en ligne qu'ils utilisent et sur le contenu qu'ils choisissent de consulter.

Accessibilité Web

- Internet doit être accessible à tout le monde.
- Les politiques qui favorisent une meilleure accessibilité peuvent aider à concevoir et mettre en place des fonctions d'intermédiaires permettant aux personnes ayant des besoins d'accessibilité particuliers de participer à la communication en ligne.⁴²
- Les entités exerçant des fonctions d'intermédiaires sur Internet doivent également s'efforcer de fournir du contenu et des contrôles en ligne qui interagissent de manière prévisible et réussie avec la technologie d'assistance.

Droits des utilisateurs

- Internet permet aux utilisateurs d'exercer leurs droits en ligne. Les intermédiaires d'Internet sont essentiels pour permettre l'exercice des droits comme la liberté d'expression, la liberté d'association et l'accès à l'information en ligne. L'ingérence du gouvernement dans les activités des intermédiaires risque d'empêcher ou de nuire à l'exercice des droits des individus.
- Les décideurs politiques doivent évaluer, et éviter ou minimiser, l'impact potentiel que toute politique proposée concernant les intermédiaires a sur l'exercice des droits de l'homme par les individus.

Compétences numériques des utilisateurs

- Les compétences numériques (également appelées littératie numérique) permettent aux utilisateurs d'être plus sélectifs dans le contenu qu'ils consomment, de reconnaître le contenu qui peut être de la désinformation, de gérer les paramètres de confidentialité et de sécurité pour protéger leurs données personnelles et de signaler le contenu indésirable.
- Les politiques doivent promouvoir les compétences numériques pour tous les utilisateurs, quels que soient leur âge et leurs besoins, par exemple en soutenant l'éducation numérique dans les écoles, les bibliothèques publiques, les programmes financés par le gouvernement et les initiatives menées par la communauté.

⁴² Voir les directives d'accessibilité du contenu Web du W3C 2.2 Comprendre les documents sur <https://www.w3.org/WAI/WCAG22/Understanding/intro>.

Non-discrimination des utilisateurs

- Les individus ont le droit d'être traités de manière égale, sans distinction de race, de couleur, de sexe, de nationalité, de langue, de religion ou d'origine ethnique, nationale ou sociale.⁴³
- Les politiques doivent empêcher toute discrimination à l'encontre d'utilisateurs individuels ou de groupes d'utilisateurs sur la base de catégories et de caractéristiques légalement protégées dans la fourniture de services Internet.

Connaissances des utilisateurs

- L'accès aux informations sur les conditions de service associées à l'hébergement, à la curation et à la modération du contenu généré par les utilisateurs permet aux utilisateurs de faire des choix éclairés sur les services qu'ils utilisent.
- Les politiques doivent encourager la transparence sur la manière dont le contenu sera hébergé, organisé et modéré.

Accès des utilisateurs à des services compétitifs

- Internet a toujours été un formidable moyen pour les petits innovateurs et entrepreneurs de démarrer et de créer des entreprises.
- Les décideurs politiques chargés d'appliquer la politique de concurrence doivent veiller à ne pas affaiblir les protections des intermédiaires.

Risques pour les utilisateurs

- De nouvelles fonctions d'intermédiaires ou l'application de fonctions connues à de nouvelles situations peuvent avoir des conséquences inattendues pour les utilisateurs et entraîner des risques pour la sécurité, la sûreté et la confidentialité des utilisateurs ainsi que pour Internet lui-même.
- Les politiques doivent encourager une approche fondée sur le risque dans l'exercice des fonctions intermédiaires, en récompensant l'atténuation des effets négatifs tout en reconnaissant qu'il n'existe pas de risque zéro.

43 La liste des classes et caractéristiques protégées peut varier selon le pays et/ou la juridiction légale. Les éléments énumérés ici sont tirés de l'article 1 de la Convention des Nations Unies sur l'élimination de toutes les formes de discrimination raciale, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>.

Signalement par les utilisateurs

- Avec la grande quantité de contenu téléchargé et partagé chaque seconde, les utilisateurs peuvent être les premiers à repérer un contenu problématique.
- Les politiques doivent encourager les entités intermédiaires qui affichent du contenu généré par les utilisateurs à fournir un moyen simple aux utilisateurs de signaler tout contenu problématique.

5 Pleins feux sur : les considérations politiques relatives à des intermédiaires spécifiques

Dans cette section, nous nous appuyons sur les considérations politiques énumérées ci-dessus. Les sections « Pleins feux sur » mettent en avant des cas qui nécessitent une discussion approfondie. De plus amples détails sur l'ensemble des fonctions des intermédiaires sont décrits dans l'annexe du présent document.

5.1 Pleins feux sur : les considérations politiques relatives aux plateformes de « réseaux sociaux » qui hébergent, organisent et modèrent le contenu généré par les utilisateurs

Une grande partie de l'attention des politiques publiques mondiales sur les entités qui hébergent du contenu généré par les utilisateurs s'est concentrée sur un petit nombre de très grandes « plateformes », en particulier les sites de réseaux sociaux qui sont utilisés par de nombreux utilisateurs dans le monde entier. Bon nombre de ces préoccupations *ne sont pas* directement liées aux protections des intermédiaires qui couvrent le contenu généré par les utilisateurs. Les décideurs politiques s'inquiètent plutôt de questions telles que la collecte et l'utilisation des données personnelles des utilisateurs par une entité, les pratiques publicitaires, la discrimination, le manque de transparence et de contrôle des utilisateurs, et les techniques permettant de conserver l'engagement continu des utilisateurs sur la plateforme, pour ne citer que quelques

sujets d'actualité. Aucune de ces préoccupations n'est en rapport avec l'objectif fondamental des protections des intermédiaires : garantir et encourager la participation individuelle sur Internet. Il n'est pas approprié de répondre à ces préoccupations en supprimant ou en soumettant les protections des intermédiaires à des conditions.

Du point de vue des protections des intermédiaires, une grande plateforme de réseaux sociaux hébergeant du contenu généré par les utilisateurs n'est fondamentalement pas différente d'un petit site Web qui héberge du contenu généré par les utilisateurs. Aucun des deux ne pourrait fonctionner s'ils étaient responsables du contenu diffamatoire, harcelant ou illégal publié par leurs utilisateurs. Il existe des moyens plus efficaces pour traiter les contenus problématiques qui évitent d'exposer les intermédiaires à la responsabilité du contenu généré par les utilisateurs (décrits dans la section 4.3 ci-dessus). Les deux types d'intermédiaires ont besoin de solides protections pour les fonctions impliquées dans l'hébergement de contenu généré par les utilisateurs. Un petit site Web ne dispose pas des ressources nécessaires pour pré-examiner tout le contenu généré par les utilisateurs et ne peut pas fonctionner avec le risque d'énormes menaces de responsabilité. Une très grande plateforme a des contraintes similaires même si elle dispose de plus de ressources en raison de la grande quantité de contenu généré par les utilisateurs (en plusieurs langues) qui est téléchargé par des millions d'utilisateurs chaque minute.

Toutefois, les protections des intermédiaires de toute responsabilité liée au contenu généré par les utilisateurs ne signifient pas que les décideurs politiques sont impuissants à répondre à d'importantes préoccupations de politique publique. Par exemple, si l'on craint qu'une plateforme organise son contenu de manière à présenter systématiquement une sélection discriminatoire de contenu aux utilisateurs, alors les lois anti-discrimination existantes ou nouvelles pourraient s'appliquer à la plateforme. Si l'on craint qu'une plateforme conçoive son interface utilisateur de manière à rendre les utilisateurs « accros » à la plateforme, alors les lois sur la santé ou la protection des consommateurs pourraient être utilisées pour protéger les utilisateurs contre l'exposition à une interface préjudiciable à leur santé ou qui les soumet à la manipulation. Si l'on craint qu'une plateforme utilise abusivement les données personnelles de ses utilisateurs, des lois sur la confidentialité et la protection des données pourraient être appliquées pour punir et décourager ces pratiques. Si l'on craint qu'une plateforme induise ses utilisateurs en erreur sur son service, des lois anti-fraude peuvent être appliquées.

Il existe des risques dans *tous* les lieux de rassemblement destinés à l'interaction sociale, qu'ils soient en ligne ou hors ligne. Malgré les meilleures intentions, les interactions sociales des enfants sur un terrain de jeu peuvent parfois inclure de l'intimidation et d'autres comportements inappropriés. Les interactions sociales entre collègues de travail peuvent parfois entraîner du harcèlement. L'écosystème en ligne peut à la fois exacerber et atténuer certains des problèmes : le manque d'interaction physique directe peut accroître le harcèlement ou l'intimidation, mais peut ouvrir des possibilités de soutien entre pairs. De plus, l'espace en ligne contient un grand nombre de lieux d'interaction sociale, de sorte que les gens peuvent quitter un espace en ligne trop toxique et rejoindre un espace plus convivial.

L'un des principaux sujets de préoccupation concerne l'utilisation d'algorithmes par les plateformes pour choisir et afficher du contenu aux utilisateurs. Les décideurs politiques ont identifié le risque que les algorithmes puissent être utilisés pour manipuler le comportement des utilisateurs avec des effets négatifs, les discriminer ou diffuser du contenu illégal ou nuisible. Cependant, les algorithmes ont toujours été utilisés par les plateformes de réseaux sociaux et par un nombre croissant d'autres sites Web, et sont essentiels à leur fonctionnement. Le volume considérable de contenu partagé sur Internet a entraîné un recours croissant aux algorithmes qui trient et affichent automatiquement le contenu. Les algorithmes recherchent du contenu erroné ou malveillant. Les algorithmes améliorent les sites de commerce électronique et gèrent le contenu affiché sur les plateformes de réseaux sociaux. Les algorithmes sont également essentiels pour accroître l'accessibilité et convertir la voix en sous-titres textuels pour les personnes malentendantes et sourdes.⁴⁴

Notre conseil aux décideurs politiques est de se rappeler que les algorithmes ne sont pas problématiques *en soi*, mais que la manière dont ils sont utilisés peut l'être. Par exemple, un algorithme qui produit systématiquement des résultats discriminatoires à l'encontre de membres de classes protégées telles que la race ou la religion est une cible légitime pour l'élaboration des politiques. L'objectif doit être d'élaborer une politique qui aborde directement le problème tout en permettant une utilisation appropriée de la modération et de la curation algorithmiques.

44 Pour une discussion plus détaillée de ces questions, veuillez vous référer au mémoire Amicus Curie de l'Internet Society dans *Gonzalez c. Google LLC*, 598 US 617 (2023), disponible sur <https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf>.

5.2 Pleins feux sur : les considérations politiques relatives aux « réseaux fédérés » permettent d'élaborer de nouvelles stratégies visant à renforcer l'engagement des utilisateurs.

Les « réseaux fédérés » ont suscité une attention croissante au cours des dernières années. Nous les mettons en lumière car ils appliquent une approche plus décentralisée à l'hébergement, au partage, à la curation et à la modération du contenu généré par les utilisateurs que les plateformes de réseaux sociaux plus traditionnelles. Plutôt que de laisser une seule entité contrôler une communauté de réseaux sociaux, par exemple, les technologies fédérées peuvent permettre à de nombreuses petites communautés de se connecter et de partager du contenu dans l'ensemble de l'écosystème fédéré. Cela crée une expérience sociale similaire mais avec une approche plus locale de la modération.

Les services « fédérés » ont fait l'actualité récemment car certains d'entre eux sont désormais en concurrence plus directe avec certaines des très grandes entreprises et plateformes de réseaux sociaux. Un exemple est Mastodon, basé sur la norme ActivityPub du World Wide Web Consortium.⁴⁵ Mastodon propose des fonctions qui ressemblent étroitement à celles de Twitter/X, notamment pour les échanges à l'échelle internationale. Une différence majeure, cependant, est que Mastodon est un ensemble de serveurs exploités par différentes entités qui ont choisi de participer au réseau fédéré, plutôt qu'un ensemble de serveurs contrôlés par une seule entreprise. Il est important de noter que chaque serveur participant au réseau fédéré Mastodon peut définir et contrôler ses propres règles de modération de contenu.⁴⁶

Bien que les réseaux sociaux fédérés soient un sujet brûlant ces derniers temps, les services fédérés ne sont pas un phénomène Internet nouveau. Par exemple, le courrier électronique sur Internet utilise un modèle fédéré : des millions d'entités exploitent leurs propres serveurs de messagerie distincts pour leur entreprise, leur organisation, leur université ou même leur foyer. Dans les coulisses, ces serveurs fédérés

⁴⁵ <https://www.w3.org/TR/activitypub/>.

⁴⁶ Mastodon a rapidement gagné en popularité après que X a radicalement modifié ses politiques de modération de contenu. Mastodon permet aux utilisateurs de mieux contrôler le contenu qu'ils voient et les autres utilisateurs avec lesquels ils interagissent. Il s'agit d'une approche décentralisée des réseaux sociaux qui permet aux petites entités et même aux particuliers d'héberger des réseaux sociaux générés par les utilisateurs et de prendre des décisions sur le contenu à autoriser ou non sur leur propre serveur et sur les autres serveurs Mastodon avec lesquels se connecter.

utilisent des protocoles de messagerie électronique pour envoyer et recevoir des courriers électroniques de manière transparente, sans aucun accord préalable.

Dans le domaine des réseaux sociaux, ces réseaux fédérés émergents ont le potentiel de démocratiser l'hébergement des réseaux sociaux. Ils permettent une curation et une modération du contenu plus précises, réalisées au plus près de l'utilisateur final. Le modèle distribué nécessite de nombreux serveurs Mastodon et a donné naissance à une nouvelle fonction intermédiaire, l'hébergement d'un serveur Mastodon, l'équivalent Mastodon d'un hébergeur Web ou d'un fournisseur de services de messagerie.⁴⁷ Fait significatif, le succès actuel des réseaux sociaux fédérés a incité Meta à envisager de permettre aux utilisateurs de Threads de partager leurs publications avec d'autres serveurs compatibles avec ActivityPub, atteignant ainsi les utilisateurs de Mastodon.⁴⁸

Nous craignons que les réseaux fédérés soient involontairement lésés par des réglementations ou des lois qui ne sont pas élaborées en tenant compte de la manière dont les réseaux fédérés modernes s'intègrent dans le paysage des « réseaux sociaux ». À titre d'exemple, si un pays devait promulguer une loi s'appliquant aux « services de réseaux sociaux » dans le but d'atteindre les plus grandes plateformes, cette terminologie pourrait bien s'appliquer à l'ensemble du réseau fédéré du système Mastodon et à ses milliers de serveurs coopérants. Une loi visant les plus grandes entreprises technologiques pourrait finir par affecter, et nuire, à un ensemble d'entités entièrement différent.

Notre conseil aux décideurs politiques qui cherchent à réglementer les plateformes de réseaux sociaux est d'être prudents et conscients de l'impact probable d'une règle ou d'un règlement proposé sur les réseaux fédérés. Sans cette attention, des conséquences néfastes imprévues pourraient survenir sur les réseaux fédérés qui offrent une alternative aux grandes plateformes de réseaux sociaux.

47 Par exemple, le fournisseur SaaS Cloudflare propose un produit : « Welcome to Wildebeest: the Fediverse on Cloudflare », The Cloudflare Blog, 2 août 2023, <https://blog.cloudflare.com/welcome-to-wildebeest-the-fediverse-on-cloudflare>.

48 Threads est entré dans le Fediverse, Engineering at Meta Blog, 21 mars 2024, <https://engineering.fb.com/2024/03/21/networking-traffic/threads-has-entered-the-fediverse/>.

5.3 Pleins feux sur : les considérations politiques relatives à l'écosystème du jeu interactif en ligne

Les jeux en ligne ont fait l'objet d'une attention particulière de la part des pouvoirs publics car nombre de leurs utilisateurs sont des enfants et des adolescents. Par exemple, en 2011, la Corée du Sud a adopté (mais abrogé par la suite) la loi de révision de la protection de la jeunesse, limitant les heures pendant lesquelles les enfants de moins de 16 ans pouvaient jouer à des jeux vidéo en ligne, bloquant l'accès entre minuit et 6 heures du matin.⁴⁹ En 2019, la Chine a restreint le temps de jeu des mineurs à 90 minutes par jour en semaine et leur a interdit de jouer en ligne entre 22h et 8h, avec des restrictions encore renforcées en 2021.⁵⁰ Les préoccupations vont de la dépendance au comportement de jeu, en passant par l'exposition à des contenus inappropriés, les contacts avec des inconnus et les violations de la vie privée.

Les jeux en ligne sont souvent interactifs avec d'autres utilisateurs et disposent souvent de fonctionnalités permettant aux utilisateurs de communiquer entre eux en temps réel. Les outils de communication de jeu les plus courants sont les capacités audios et de messagerie, mais il existe de nombreuses méthodes de communication plus subtiles : choisir et modifier des avatars, des comportements particuliers pendant le jeu, et partager des scores, des notes et d'autres réalisations. Certains jeux en ligne permettent également aux utilisateurs de télécharger et de partager des modifications apportées au jeu. Les jeux en ligne ont également inspiré de nouveaux genres d'engagement sur d'autres plateformes, telles que YouTube et Twitch, ainsi que dans le domaine de l'e-sport.⁵¹

Nous conseillons aux décideurs politiques d'être attentifs aux fonctions intermédiaires assurées par les plateformes de jeux interactifs en ligne. Aujourd'hui, la plupart des systèmes de jeux interactifs connectés à Internet, avec ou sans console matérielle, permettent un large éventail de « contenus générés par les utilisateurs », allant des simples conversations entre joueurs jusqu'aux modules complémentaires développés par les joueurs qui complètent et étendent l'environnement de jeu. Les

49 La loi a ensuite été abrogée en 2021. Voir https://en.wikipedia.org/wiki/Shutdown_law.

50 La Chine limite à 1 heure par jour le temps consacré aux jeux en ligne pour les enfants, Associated Press, Zen Soo, 19 janvier 2023, <https://apnews.com/article/gaming-business-children-00db669defcc8e0ca1fc2dc54120a0b8>.

51 Pour plus d'informations sur l'eSport, consultez Wikipédia sur <https://en.wikipedia.org/wiki/Esports>.

plateformes de jeux interactifs remplissent des fonctions intermédiaires, et les principaux régimes de protection des intermédiaires s'appliquent également à l'écosystème du jeu.

Toutefois, comme nous l'avons souligné plus haut dans « Pleins feux sur les plateformes de réseaux sociaux », les décideurs politiques ne sont pas impuissants face aux pratiques néfastes. Par exemple, si l'on craint que certaines « loot boxes » dans un jeu constituent des pratiques trompeuses ou des jeux de hasard illégaux, les lois sur la protection des consommateurs ou les jeux de hasard illégaux devraient être directement applicables à de tels comportements.

5.4 Pleins feux sur : les considérations politiques relatives aux systèmes de réalité virtuelle et de réalité augmentée connectés à Internet

Les produits de réalité virtuelle (RV) et de réalité augmentée (RA) sont de plus en plus présents dans l'écosystème Internet. Les objectifs de la RV et de la RA sont divers, mais ils sont souvent utilisés dans le cadre d'un système de communication interactif.⁵² Pour certains systèmes, des équipements spécialisés, comme des lunettes, des gants ou un casque, sont nécessaires, tandis que d'autres peuvent être utilisés directement avec un smartphone.

Comme dans l'écosystème du jeu, les systèmes RV et RA connectés à Internet prennent généralement en charge le « contenu généré par les utilisateurs », y compris une large gamme de communications d'utilisateur à utilisateur.⁵³ Ainsi, comme pour les jeux, la plupart des principaux régimes de protection des intermédiaires pourraient s'appliquer aux systèmes RV et RA.

52 Une vision de la façon dont la réalité virtuelle pourrait être utilisée est le « métavers », décrit pour la première fois dans le roman de science-fiction « Snowcrash » de Neal Stephenson, paru en 1992. Dans sa vision, le métavers est un espace de réalité virtuelle dans lequel les utilisateurs peuvent interagir les uns avec les autres à l'aide d'un avatar dans un environnement tridimensionnel géré par ordinateur.

53 De par leur nature, les systèmes RV et RA peuvent prendre en charge un vaste ensemble d'outils de communication : écrits, parlés et non verbaux tels que les mouvements de la tête et des mains, les expressions faciales, l'orientation du corps, la proximité et la posture.

D'un point de vue politique, les systèmes de réalité virtuelle (RV) et de réalité augmentée (RA) présentent des similitudes importantes avec les réseaux sociaux et d'autres services de communication individuels ou de groupe. Cependant, la réalité virtuelle et la réalité augmentée posent des défis politiques supplémentaires, tels que :

- La mise en place et l'utilisation d'avatars représentatifs pourraient créer, au moins en termes de perception, un lien plus étroit entre l'identité réelle de l'individu et son identité dans la réalité virtuelle.
- Certains systèmes RA peuvent être utilisés n'importe où dans l'espace physique, superposant des éléments virtuels dans l'environnement physique. Ces systèmes pourraient théoriquement entraîner des dommages directs dans le monde physique, tels que des accidents de la circulation ou des blessures corporelles.⁵⁴
- Les systèmes RA pourraient permettre aux personnes qui ne sont pas en ligne et qui n'ont pas donné leur consentement d'entrer dans l'environnement augmenté.

Comme pour les réseaux sociaux et les jeux en ligne, nous conseillons aux décideurs politiques de mieux résoudre les problèmes politiques liés à la confidentialité, à la dépendance des utilisateurs et à la sécurité personnelle en utilisant les lois existantes dans ces domaines plutôt qu'en modifiant les protections des intermédiaires ou en essayant de construire un nouvel ensemble de politiques spécifiques à la RV et à la RA.

5.5 Pleins feux sur : les considérations politiques relatives aux intermédiaires qui permettent la publicité sur Internet

Le contenu publicitaire est un type particulier de contenu en ligne. Bien qu'il soit souvent associé à du contenu généré par les utilisateurs, il n'est généralement pas fourni par des particuliers. Certaines publicités peuvent être considérées comme du contenu original du site, comme une publicité pour un dîner spécial du Nouvel An sur le site Web d'un restaurant. Cependant, la grande majorité du contenu publicitaire affiché sur Internet est du contenu créé par des entités autres que les propriétaires de sites Web à des fins publicitaires spécifiques et est placé pour obtenir des revenus publicitaires. Ce contenu est généralement intégré et dynamique.

54 Voir, par exemple, le Pokémon Go Death Tracker sur <https://pokemongodeathtracker.com/>.

La possibilité d'afficher du contenu publicitaire sur Internet a permis aux entreprises d'offrir leurs services pour un coût minime, voire nul, et aux particuliers de gagner de l'argent grâce à des sites de partage de contenu généré par les utilisateurs. Certains soutiennent que le système publicitaire devrait être protégé de toute responsabilité car sans la publicité pour « payer les factures », Internet aurait beaucoup moins de services et de fonctionnalités et une participation individuelle réduite. Sans revenus publicitaires, davantage de services imposeraient des frais d'utilisation, augmentant ainsi la fracture numérique.

D'autres pensent que le système publicitaire, en particulier le système publicitaire comportemental, est très problématique et devrait être considérablement restreint. Ils affirment que la publicité ciblée exploite des protections de confidentialité insuffisantes, permettant aux services en ligne et à l'industrie de tirer profit financièrement du contenu généré par les utilisateurs et des interactions en ligne.

En raison de la nature mondiale d'Internet, la portée et l'impact de la publicité en ligne peuvent être bien plus importants que ceux de la publicité dans les journaux, à la télévision et à la radio. Les publicités en ligne peuvent être adaptées et ciblées sur un utilisateur individuel ou sur de très petits groupes de personnes en termes de temps, de localisation physique et de contexte. Les annonceurs et l'écosystème d'entreprises qui soutiennent la publicité en ligne suivent les utilisateurs sur tous les appareils et même dans le monde réel.

Au-delà des débats sur le système publicitaire existant, celui-ci s'appuie incontestablement sur des protections en matière de responsabilité des intermédiaires dans certains contextes.⁵⁵ À l'extrémité visible des systèmes publicitaires (les sites Web et les services sur lesquels les publicités sont affichées), des protections des intermédiaires pourraient bien entrer en jeu. Dans la plupart des services, le contenu des publicités affichées à côté du contenu généré par l'utilisateur échappe au contrôle de l'utilisateur et n'est généralement même pas contrôlé par le propriétaire du site Web. Techniquement, le contenu publicitaire affiché via un site Web n'est généralement *pas* hébergé sur l'infrastructure du service mais est hébergé sur un serveur géré par le réseau publicitaire.

⁵⁵ Le fonctionnement interne des systèmes de publicité en ligne est assez opaque, avec de multiples entités interconnectées et indépendantes travaillant ensemble, de manière explicite et implicite. Démêler ces systèmes pour comprendre comment les protections en matière de responsabilité des intermédiaires pourraient s'appliquer dépasse largement le cadre de ce document.

Nous conseillons aux décideurs politiques de faire preuve de prudence dans l'élaboration de la réglementation de l'écosystème publicitaire en raison de l'équilibre difficile entre les avantages escomptés et les préjudices potentiels. L'écosystème de la publicité en ligne joue un rôle important dans le soutien d'un large accès à la parole, mais en même temps, il soulève des préoccupations politiques concernant la confidentialité, le ciblage inapproprié et la désinformation. Mais, comme pour toute autre fonction intermédiaire, cela ne signifie pas qu'un gouvernement ne peut pas réglementer directement les systèmes publicitaires. Par exemple, dans l'Union européenne, la première directive sur le commerce électronique imposait directement certaines exigences spécifiques en matière de transparence sur les publicités en ligne, et le règlement DSA (Digital Services Act), plus récent, a considérablement élargi ces exigences de transparence et interdit certaines techniques de conception visant à manipuler ou à tromper les utilisateurs.

5.6 Pleins feux sur : les considérations politiques relatives aux paiements et autres compensations économiques pour le « contenu généré par les utilisateurs » couvert par les principes des intermédiaires Internet

Le système de publicité sur Internet soulève une question beaucoup plus vaste : les protections des intermédiaires sont-elles appropriées pour couvrir le contenu pour lequel de l'argent ou une autre forme de valeur économique a changé de mains dans le cadre du placement de contenu sur un site Web ? La question peut se poser dans de nombreux cas différents :

- Si un site Web publie des articles écrits par des utilisateurs, mais ne le fait que si un utilisateur paie le site Web pour publier l'article, le site Web devrait-il être protégé de toute responsabilité du contenu pour lequel il a été payé ? La protection devrait-elle toujours s'appliquer si le montant payé est faible ? Et s'il est important ?
- Si un site Web paie un fournisseur de contenu (comme un « influenceur » bien connu ou une autre personnalité) pour publier du contenu sur le site Web, le site Web devrait-il avoir une responsabilité légale pour le contenu qu'il a payé et qu'il a ensuite hébergé ? Le montant des paiements ferait-il une différence dans l'analyse ?

- Si un site Web partage les revenus publicitaires avec le fournisseur de contenu, cela change-t-il la relation et la responsabilité du site Web ?⁵⁶
- Si la relation commerciale entre les annonceurs et les sites Web supprime les protections et rend l'opérateur du site Web responsable du contenu des publicités, quel effet cela aurait-il sur le système publicitaire ? Cela nuirait-il aux sites Web qui reçoivent un revenu modeste provenant d'un faible niveau de publicité ?
- Si les protections en matière de responsabilité étaient supprimées pour les fonctions intermédiaires d'hébergement de contenu généré par les utilisateurs et produit contre rémunération, cela entraînerait-il des impacts économiques, sociaux ou techniques sur le marché du contenu ? Les entreprises créeraient-elles des alternatives artificielles ou moins responsables pour éviter d'être tenues responsables ?⁵⁷
- Si le marché du contenu payant est dominé par quelques entités fortement intégrées horizontalement et verticalement dans les services en ligne, comment cela nuit-il au paysage concurrentiel du contenu ?

Dans le contexte des États-Unis, les paiements pour le contenu dans un sens ou dans l'autre n'ont généralement pas d'impact sur les protections des intermédiaires.⁵⁸ Les questions que nous soulevons ci-dessus contribuent à montrer les complexités, les avantages et les inconvénients qui découlent du fait de se concentrer sur la compensation économique.

5.7 Pleins feux sur : l'impact des différents niveaux nationaux de protection de la liberté d'expression

Pour comprendre et créer des politiques relatives aux protections des intermédiaires en matière de responsabilité, il est important de reconnaître l'influence que les protections juridiques nationales de la

56 Par exemple, YouTube dispose d'un système largement ouvert à tous ses utilisateurs qui publient des vidéos sur le site. En échange de l'autorisation de publier des publicités à côté des vidéos d'un utilisateur, YouTube partagera une partie des revenus publicitaires provenant des publicités placées. Si les vidéos de l'utilisateur sont très populaires, il recevra des revenus provenant des publicités, parfois une somme substantielle. Certains créateurs de contenu gagnent désormais leur vie ou complètent considérablement leurs revenus grâce aux paiements de YouTube. Si YouTube était responsable des vidéos pour lesquelles les utilisateurs étaient payés, YouTube pourrait-il continuer à proposer des paiements ?

57 Par exemple, chercheraient-ils à éviter toute responsabilité en rémunérant certains créateurs de contenu pour « avoir un compte » plutôt que pour le contenu qu'ils produisent, ou offriraient-ils d'autres services et abonnements gratuitement ?

58 Les propositions visant à supprimer les protections prévues par la loi américaine pour certains types de publicités payantes n'ont pas été couronnées de succès.

liberté d'expression et de parole auront sur les politiques qui pourraient affecter la capacité des individus à communiquer en ligne, que ce soit en partageant leur propre contenu ou celui d'autres personnes.

Les protections accordées à la parole et à la liberté d'expression diffèrent considérablement d'un pays à l'autre, et ces différences affectent les choix politiques disponibles au sein d'un pays. Certains pays établissent un droit à la liberté d'expression dans leur constitution, notamment le Brésil,⁵⁹ l'Équateur,⁶⁰ le Japon,⁶¹ le Pérou⁶² et les États-Unis.⁶³ D'autres pays et juridictions imposent moins de contraintes à la capacité du gouvernement, par exemple, d'obliger les entreprises privées à prendre des mesures pour restreindre ou empêcher certains types de discours. D'autres pays peuvent donner la priorité à d'autres objectifs politiques, tels que la vie privée plutôt que la liberté d'expression ou la cohésion sociale plutôt que les droits individuels. Les différents régimes nationaux peuvent expliquer en partie les différentes approches nationales en matière de protection de la responsabilité des intermédiaires. Un exemple d'approches différentes dictées par les lois constitutionnelles ou nationales sont les régimes de « notification et retrait », utilisés par l'Union européenne et certains autres pays pour exiger la suppression de contenus en ligne. Ce type de contrainte serait confronté à de sérieux défis constitutionnels s'il était mis en œuvre dans des pays où la liberté d'expression ou de parole est garantie, comme les États-Unis.⁶⁴

Nous conseillons aux décideurs politiques de bien comprendre toutes les contraintes imposées par les lois constitutionnelles et statutaires nationales, ainsi que par les conventions et accords internationaux applicables en matière de liberté d'expression.

59 Voir l'article 5 de la Constituição da República Federativa do Brasil, disponible sur https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

60 Voir l'article 66 section 6 de la Constitución del Ecuador, disponible sur https://www.gob.ec/sites/default/files/regulations/2018-11/constitucion_de_bolsillo.pdf.

61 Voir l'article 21 de la Constitution du Japon, disponible sur https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

62 Voir l'article 2 section 4 de la Constitución Política del Perú, disponible sur <https://www.congreso.gob.pe/constitucion/reglamento/>.

63 Voir le premier amendement de la Constitution des États-Unis, disponible sur <https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say>.

64 Les régimes de « notification et retrait » ont également été notoirement sujets à des abus et à des utilisations abusives. Voir, p. ex., "Warning: repressive regimes are using DMCA takedown demands to censor activists," 13 janvier 2023, disponible sur <https://www.accessnow.org/dmca-takedown-demands-censor-activists/>; "Notice and Takedown Mechanisms: Risks for Freedom of Expression Online," 7 septembre 2020, disponible sur https://www.eff.org/files/2020/09/04/mcsherry_statement_re_copyright_9.7.2020-final.pdf; "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech," septembre 2010, disponible sur https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf.

Au-delà de ces questions, si un pays veut soutenir la capacité de ses citoyens à participer à des conversations en ligne et à lancer des efforts entrepreneuriaux pour créer de nouveaux services en ligne, il doit adopter une protection des intermédiaires pour garantir que les services Internet puissent transmettre la parole des utilisateurs sans risques de responsabilité significatifs.

5.8 Pleins feux sur : la distinction entre la protection en matière de responsabilité des intermédiaires et les lois et politiques relatives au droit d'auteur

Dans de nombreux pays et régions, notamment aux États-Unis⁶⁵ et dans l'Union européenne⁶⁶, il existe des approches juridiques distinctes qui couvrent les protections de la responsabilité des intermédiaires pour le « contenu généré par les utilisateurs » différemment de « l'utilisation par des tiers de contenu protégé par le droit d'auteur ». Dans le cas de contenu généré par les utilisateurs, la question juridique est de savoir si le contenu lui-même est illégal ou s'il a causé un préjudice. Dans le cas du droit d'auteur, les questions juridiques pertinentes sont de savoir si l'auteur du contenu (a) détient le droit d'auteur, (b) dispose d'une licence pour publier le contenu ou (c) est autrement protégé par un « usage équitable » ou d'autres limitations de la loi sur le droit d'auteur. Ce document se concentre sur le premier scénario, et non sur les contenus portant atteinte au droit d'auteur.

De nombreuses lois spécifiques au droit d'auteur contiennent des exigences de notification et de retrait en vertu desquelles un titulaire de droit d'auteur peut informer une société d'hébergement du contenu qu'il prétend être protégé par le droit d'auteur. Suite à la notification, l'hébergeur dispose d'un certain délai pour supprimer le contenu spécifié. L'approche axée sur le droit d'auteur, qui ne nécessite généralement pas

65 Voir Digital Millennium Copyright Act, 17 U.S. Code § 512, disponible sur <https://www.law.cornell.edu/uscode/text/17/512>.

66 Voir l'article 17 de la directive européenne sur le droit d'auteur (la directive sur le droit d'auteur dans le marché unique numérique), disponible sur https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ:L:2019:130:TOC.

d'ordonnance judiciaire, a parfois conduit à des abus, certaines personnes utilisant des notifications de retrait de droits d'auteur pour empêcher des discours légaux.⁶⁷ En revanche, comme mentionné dans la section 3.5, les quelques pays qui ont adopté une approche de notification et de retrait pour les contenus problématiques générés par les utilisateurs ont généralement exigé une décision de justice.

5.9 Pleins feux sur : l'intelligence artificielle

Suite au lancement de services d'IA génératifs axés sur le consommateur,⁶⁸ une question courante s'est posée parmi les décideurs politiques : si et dans quelle mesure les protections des intermédiaires s'appliquent aux services qui utilisent « l'intelligence artificielle » (IA). L'IA est un terme très large qui englobe tout, depuis des algorithmes assez simples jusqu'aux réseaux neuronaux artificiels. Les outils d'IA peuvent effectuer des tâches spécifiques (par exemple, reconnaître des images), réagir à des situations spécifiques (par exemple, filtrer le spam, augmenter l'efficacité du routage) et apprendre et adapter les réponses (par exemple, interagir avec les utilisateurs en tant que chatbots). L'IA est déjà présente dans tout l'écosystème Internet, du routage du trafic Internet à la recherche et à la localisation de pages Web, en passant par la gestion de milliards de contenus.

Dans le contexte du contenu en ligne, il y a au moins trois aspects de l'IA qui méritent d'être soulignés. Le premier concerne l'utilisation de l'IA dans la fourniture de services en ligne. Différents types d'IA sont utilisés pour fournir des services en ligne depuis de nombreuses années. Par exemple, la technologie utilisée pour sélectionner et organiser le contenu à afficher aux utilisateurs inclut des aspects de l'IA depuis au moins 2006.⁶⁹ L'utilisation de l'IA dans la recherche en ligne remonte encore plus loin.⁷⁰ Comme indiqué ci-dessus dans le présent document et dans l'annexe, les lois sur la protection des intermédiaires protègent généralement les activités qui incluent la curation de contenu, le filtrage, le tri, le choix

67 Parfois qualifié de « censure par le droit d'auteur ». Pour quelques exemples, voir Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Speech (2010), Center for Democracy & Technology, disponible sur https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf; Copyright shouldn't be a tool of censorship (2017) de Daniel Nazer et Mitch Stoltz, Electronic Frontier Foundation, disponible sur <https://www.eff.org/deeplinks/2017/01/copyright-shouldnt-be-tool-censorship>.

68 Pour une explication de l'IA générative, voir Wikipédia sur https://en.wikipedia.org/wiki/Generative_artificial_intelligence.

69 Voir Cait McNamara, "The Evolution of AI on Social Media," mai 2024, disponible sur <https://favola.co.uk/the-evolution-of-ai-on-social-media/>.

70 Voir Dan Katcher, "The Evolution of AI Search: Past, Present, Future," 12 février 2024, disponible sur <https://www.rocketfarmstudios.com/blog/the-evolution-of-ai-search-past-present-future/>.

et la recherche de contenu. Ces protections s'appliquent probablement indépendamment du fait que la technologie comprenne ou non un composant d'IA.

Un deuxième aspect, plus récent, concerne les réponses générées par l'IA aux recherches d'informations des utilisateurs : la question de savoir si les résultats de l'IA qui ont été formés sur de vastes quantités de contenu généré par les utilisateurs doivent eux-mêmes être considérés comme du « contenu généré par les utilisateurs ». Les points de vue divergent quant à savoir dans quels cas le contenu généré par l'IA doit être qualifié de « contenu créé par d'autres » et, par conséquent, couvert par des protections des intermédiaires en matière de responsabilité. Bien que certains résultats de ces services d'IA puissent contenir du contenu spécifique généré par l'utilisateur, la totalité des résultats pourrait être considérée comme un nouveau contenu créé par le service.

Un troisième aspect de l'IA qui fait l'objet de discussions actives est de savoir si les services d'IA qui produisent du texte, des images, du son ou des vidéos en réponse aux demandes des utilisateurs devraient être tenus responsables de la production de contenu illégal ou illicite. Ces types de services d'IA favorisent indéniablement la créativité des utilisateurs, mais on peut également les considérer comme des co-créateurs du contenu généré.

Nous ne cherchons pas à résoudre ces questions dans ce document ni à fournir des recommandations politiques détaillées sur le traitement des services basés sur l'IA. Il n'est pas facile de répondre à ces questions, et il faudra probablement du temps et une analyse minutieuse pour élaborer des approches politiques appropriées. L'IA offre un potentiel énorme de progrès dans les domaines médicaux, scientifiques et même créatifs, et des protections pour les services basés sur l'IA peuvent être appropriées. Mais certains services d'IA peuvent créer des risques importants pour la société et pourraient justifier une prise en compte réglementaire.

Comme pour tous les autres types d'élaboration de politiques abordés dans ce document, l'Internet Society recommande que les interventions politiques visant à lutter contre l'IA soient soigneusement définies et ciblées. Sans cette précaution, des réglementations ou des restrictions trop larges sur l'IA pourraient avoir un impact négatif sur d'autres utilisations, notamment les fonctions intermédiaires permettant la communication des individus sur Internet.

6 Conclusion

Ce document fournit un cadre pour comprendre les rôles des intermédiaires Internet et développer une stratégie concernant la responsabilité du contenu en ligne. Notre objectif est de fournir des informations aux décideurs politiques afin qu'ils puissent élaborer des politiques qui préservent ce que l'Internet Society considère comme les caractéristiques les plus importantes d'Internet : être ouvert, connecté à l'échelle mondiale, sécurisé et digne de confiance. Internet est de plus en plus important pour la vie des gens et pour la prospérité économique et sociale. Alors que les décideurs politiques sont aux prises avec des préoccupations sociétales légitimes concernant le contenu en ligne, il est essentiel que les politiques garantissent qu'Internet puisse continuer à être une ressource positive pour la communication, l'éducation et le discours à l'échelle mondiale.

La responsabilité du contenu généré par les utilisateurs est un problème qui s'est accru à mesure qu'Internet s'est développé, devenant un moyen de communication essentiel pour les sociétés modernes. Il reste nécessaire d'élaborer des approches politiques qui offrent une protection en matière de responsabilité pour les différents types d'intermédiaires permettant la communication sur Internet pour préserver la santé d'Internet. Parallèlement, il existe toute une gamme d'outils politiques permettant de répondre aux préoccupations en ligne sans nuire à la participation individuelle sur Internet.

Selon nous, cinq stratégies principales devraient être suivies par les décideurs lorsqu'ils élaborent des politiques spécifiques à Internet :

1. Établir soigneusement la portée de l'élaboration des politiques pour atteindre les objectifs. Appliquer des politiques aussi spécifiques que possible pour résoudre et atténuer directement le problème.
2. Dans la mesure du possible, utiliser les outils politiques existants pour répondre à des préoccupations spécifiques. Les lois sur la confidentialité, la lutte contre la discrimination, la protection des consommateurs et autres offrent déjà des moyens de protéger les utilisateurs et d'améliorer la responsabilité en ligne.
3. Maintenir, ou lorsqu'elles n'existent pas encore, mettre en place des protections en matière de responsabilité pour les fonctions qui permettent les communications sur Internet. Cela est particulièrement important pour les fonctions essentielles au bon

fonctionnement d'Internet, mais aussi pour celles qui interagissent le plus directement avec les communications des utilisateurs, comme l'hébergement et l'affichage de contenu. Sans ces protections, Internet ne peut pas continuer à être un moyen de communication.

4. Protéger de toute responsabilité les entités qui assurent les fonctions de curation et de modération du contenu généré par les utilisateurs. La dimension d'Internet impose des mécanismes de curation et de modération du contenu. À condition d'assurer une transparence adéquate, une entité hébergeant du contenu créé par les utilisateurs devrait être en mesure d'appliquer des mécanismes de curation et de modération, qu'ils soient automatisés ou manuels, sans craindre d'engager sa responsabilité.
5. Travailler avec les parties prenantes d'Internet (notamment la société civile, les communautés universitaires et techniques, les entreprises et les citoyens) pour mener une « évaluation de l'impact sur Internet » de toute politique proposée afin d'aider à comprendre les conséquences ou effets imprévus possibles sur Internet ou ses utilisateurs.

L'Internet Society s'efforce de collaborer avec les gouvernements du monde entier pour élaborer des politiques qui répondent aux préoccupations sociétales tout en soutenant Internet. Nous œuvrons pour soutenir le développement d'Internet en tant qu'infrastructure technique mondiale, ressource destinée à enrichir la vie des gens et force du bien dans la société. Nous accueillons favorablement les discussions sur les opportunités, les défis et les préoccupations auxquels sont confrontés les décideurs politiques dans l'écosystème Internet et sur les moyens d'y répondre.

Annexe A – Rôles des intermédiaires

La présente annexe au « Cadre stratégique pour les intermédiaires Internet » (« Cadre stratégique ») décrit en détail les rôles des intermédiaires nécessaires à la circulation des communications sur Internet. Pour chacun de ces rôles, nous proposons des approches stratégiques.

Notre objectif principal est la protection de la responsabilité des intermédiaires. Cependant, comme indiqué dans la section 4.3 du Cadre stratégique,¹ il existe également d'autres approches stratégiques qui peuvent être appliquées pour répondre aux préoccupations politiques concernant les rôles des intermédiaires, telles que les lois sur la protection de la vie privée et des consommateurs.

Pour faciliter l'organisation de ces approches stratégiques recommandées, nous avons regroupé les rôles des intermédiaires concernés en huit sections distinctes (comme indiqué dans la table des matières).

¹ Cadre stratégique Section 4.3, Principes juridiques et politiques spécifiques qui peuvent être appliqués aux fonctions intermédiaires sans porter atteinte aux communications Internet.

1 Transmission de paquets de données

Cette section décrit le rôle le plus basique des intermédiaires impliqués dans la transmission des communications Internet : la transmission de données filaire ou sans fil.

- **La section 1.1** décrit la fonction permettant de fournir un support de communication pour les communications Internet.
- **La section 1.2** décrit la fonction permettant de fournir un chemin de communication sur un support de communication.
- **La section 1.3** décrit la fonction permettant de fournir des services de dorsale ou de transit afin que les fournisseurs d'accès Internet (également appelés fournisseurs de services Internet) puissent envoyer et recevoir du trafic sur Internet.
- **La section 1.4** décrit la fonction permettant aux fournisseurs d'accès Internet d'échanger leur trafic localement plutôt que de recourir à des fournisseurs de dorsale ou de transit.
- **La section 1.5** décrit la fonction permettant de fournir un accès Internet à un point de terminaison (l'appareil d'un utilisateur).

1.1 Support de communication (filaire et sans fil)

Description de la fonction : fournir les supports de communication pour prendre en charge la transmission de paquets IP (Internet Protocol). Les supports de communication sont présents partout sur Internet, depuis la connexion à un domicile ou un appareil mobile, jusqu'aux réseaux dorsaux et aux câbles sous-marins. Ce rôle d'intermédiaire est essentiel même pour les communications Internet les plus élémentaires.

Considérations techniques et pratiques : les paquets IP peuvent être transmis via un réseau filaire, par voie hertzienne et même dans l'espace à l'aide de divers protocoles réseau spécifiques au support de communication. Les supports de communication peuvent appartenir à un fournisseur ou être loués à celui-ci pour un chemin de communication basé sur le protocole Internet (voir 1.2 ci-dessous) et pourraient transporter un trafic autre que de simples paquets IP. Par exemple, la

capacité d'un câble à fibre optique sous-marin pourrait être utilisée en partie pour le trafic IP et en partie pour d'autres protocoles de transmission de données propriétaires. Voici des exemples de supports de communication : câbles sous-marins ; cuivre, câble coaxial, fibre jusqu'au domicile ; sans fil sur un spectre radio autorisé ou non.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de supports de communication ne doivent pas être tenus responsables du contenu qui transite par leurs supports.	Sans protection en matière de responsabilité, les fournisseurs de supports de communication craindraient d'être tenus responsables du contenu transitant par leurs supports de communication. Ils pourraient restreindre l'accès à leurs supports au contenu provenant d'un petit nombre de sources pré-contrôlées. Cela réduirait considérablement les sources et le type de contenu transmis via les supports de communication et entraverait la capacité des individus à interagir en ligne. Cela fragmenterait également Internet en différents réseaux de contenu.

1.2 Chemins de communication IP

Description de la fonction : envoi et réception de paquets IP (Internet Protocol) via un système de commutation de paquets réseau au moyen d'un ou de plusieurs supports de communication. Cette fonction inclut l'accès au dernier kilomètre (abordé ci-après dans la section 1.5). Sur Internet, les communications entre points de terminaison sont réalisées en traversant des chemins de communication interconnectés (passant d'un réseau à un autre). Tout comme les supports de communication (décrits ci-dessus), les chemins de communication IP sont utilisés dans toutes les parties d'Internet. Un réseau IP délivre du trafic IP sans que son client sache nécessairement quels chemins de communication seront

ou sont utilisés. Ce rôle d’intermédiaire consistant à fournir le chemin de communication IP est essentiel même pour la communication Internet la plus élémentaire.

Considérations techniques et pratiques : les principaux chemins de communication IP entre les grands réseaux informatiques interconnectés stratégiquement et les routeurs centraux sur Internet sont collectivement connus sous le nom de dorsale Internet (décrite dans la section 1.3 ci-après). Ces chemins (également appelés itinéraires) utilisent principalement des câbles à fibre optique pour une bande passante élevée, une vitesse élevée et une atténuation limitée du signal. Les réseaux qui participent à la dorsale Internet ont souvent des accords de peering sans règlement avec les réseaux voisins pour s’interconnecter et acheminer le trafic. Certains réseaux, notamment ceux qui sont plus proches de l’utilisateur final, pourraient devoir payer le transit pour que leur trafic soit acheminé vers Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de chemins de communication IP (services de réseau IP) ne doivent pas être tenus responsables du contenu qui transite par leurs réseaux.	Sans protection en matière de responsabilité, les fournisseurs de services de réseau IP craindraient d’être tenus responsables du contenu transitant par leurs réseaux. Par conséquent, ils pourraient restreindre l’accès à leurs chemins de communication au contenu provenant d’un petit nombre de sources pré-contrôlées. Dans une situation extrême, l’absence de protection en matière de responsabilité pourrait limiter l’utilisation d’Internet au contenu diffusé par un petit nombre d’entreprises et empêcher les individus de partager leur propre contenu. Cela porterait gravement atteinte au caractère ouvert et connecté à l’échelle mondiale d’Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de chemins de communication IP ne doivent pas être tenus de surveiller et d’intercepter le contenu du trafic des utilisateurs.	La surveillance ou l’interception du contenu du trafic sur les chemins de communication IP (réseaux IP) est susceptible de dégrader gravement la vitesse et la fiabilité des communications sur ces chemins. Cela violerait également les attentes des utilisateurs en matière de confidentialité, de sécurité et de respect de la vie privée. L’Internet Engineering Task Force considère la surveillance omniprésente ² des réseaux IP comme une attaque, quelle qu’en soit la motivation.

1.3 Dorsale et réseaux de transit

Description de la fonction : fournir un type spécifique de chemin de communication IP connu sous le nom de dorsale ou réseaux de transit. Ces réseaux interconnectent et regroupent le trafic provenant d’autres réseaux IP, tels que les fournisseurs d’accès du dernier kilomètre. Ce faisant, ils permettent au flux de trafic IP de se connecter à toutes les autres parties d’Internet. Ce rôle d’intermédiaire est essentiel même pour les communications Internet les plus élémentaires.

Considérations techniques et pratiques : les fournisseurs de services de dorsale ou de réseaux de transit sont généralement situés dans des zones géographiques où la demande est la plus forte et où il est plus efficace de regrouper le trafic. Ces réseaux sont essentiels pour acheminer le trafic Internet vers et depuis les FAI d’origine et autres points de terminaison vers les FAI et les points de terminaison de destination.

2 « La surveillance omniprésente est une attaque », Internet Engineering Task Force, Best Current Practice 188, RFC 7258, mai 2024, disponible sur <https://datatracker.ietf.org/doc/html/rfc7258>.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de dorsale ou de réseaux de transit ne doivent pas être tenus responsables du contenu qui transite par leurs réseaux.	Sans protection en matière de responsabilité, ces fournisseurs craindraient d’être tenus responsables du contenu transitant par leurs réseaux. Par conséquent, ils pourraient restreindre l’accès à un petit nombre de réseaux seulement. Cela entraverait l’accessibilité mondiale et réduirait la capacité des individus à communiquer en ligne.
Les fournisseurs de services de dorsale et de réseaux de transit ne doivent pas être tenus de surveiller ou d’intercepter le contenu du trafic des utilisateurs.	La fonction de fourniture de services de dorsale ou de réseaux de transit consiste à acheminer de grands volumes de trafic Internet aussi efficacement que possible. Internet ne serait ni fiable ni sûr si les fournisseurs de ces services surveillaient ou interceptaient le contenu du trafic qu’ils transportent.

1.4 Échange de trafic

Description de la fonction : fournir un emplacement physique où plusieurs réseaux IP et réseaux de diffusion de contenu peuvent échanger des paquets. Ce rôle d’intermédiaire est essentiel pour un Internet efficace, robuste, fiable et sécurisé. Avec un point d’échange Internet, les FAI peuvent échanger du trafic localement plutôt que de s’envoyer du trafic via un fournisseur de services de dorsale ou de réseaux de transit.

Considérations techniques et pratiques : les IXP sont les emplacements physiques et généralement neutres où différents réseaux locaux se connectent pour échanger du trafic entre eux, ainsi qu’avec les fournisseurs de services de dorsale ou de réseaux de transit impliqués dans l’IXP, selon les besoins. Les IXP créent des itinéraires plus courts, plus rapides et plus directs pour le trafic Internet. Ils offrent une alternative plus abordable et à faible latence au routage du trafic local via des réseaux internationaux. L’échange de trafic au niveau des IXP raccourcit et optimise le chemin de transit, réduisant ainsi la latence et les coûts.

Approches stratégiques recommandées	Raisons de cette approche
Les IXP ne doivent pas être tenus responsables du contenu qui transite par l'échange.	Sans protection en matière de responsabilité, personne ne serait probablement disposé à exploiter ou à se connecter à un point d'échange de trafic Internet. Le trafic emprunterait des chemins inefficaces et plus lents, les coûts augmenteraient et Internet serait moins abordable, moins résilient et moins durable.
Sauf à des fins de gestion efficace du trafic, les points d'échange ne doivent pas surveiller ou intercepter le trafic qui transite par eux.	L'exploitation d'un point d'échange Internet est souvent partagée par plusieurs fournisseurs de chemins de communication IP ou fournisseurs de services de réseau IP. Il est essentiel que les réseaux qui exploitent un IXP puissent être sûrs que le contenu de leur trafic n'est pas surveillé ou intercepté. Dans le cas contraire, ils pourraient être réticents à utiliser le point d'échange, car leurs clients ne souhaitent pas que leurs communications soient surveillées.
Les points d'échange Internet ne doivent pas être tenus d'intercepter, de filtrer ou de surveiller le trafic transitant par le point d'échange.	Exiger des IXP qu'ils inspectent ou analysent un contenu spécifique découragerait les FAI de participer et porterait atteinte à la sécurité des communications et à la confidentialité des utilisateurs. Une telle approche porterait atteinte à la confiance dans Internet et entraverait l'échange efficace du trafic Internet.

1.5 Accès Internet du dernier kilomètre

Description de la fonction : fournir aux utilisateurs finaux (et à leurs appareils) un accès à Internet, souvent appelé « accès du dernier kilomètre ». Il s’agit d’un type spécifique de chemin de communication IP (décrit dans la section 1.2 ci-dessus). Cette fonction, qui comprend l’acheminement du trafic IP vers et depuis l’utilisateur final, est essentielle même pour les communications Internet les plus élémentaires.

Considérations techniques et pratiques : l’accès à Internet peut être fourni aux utilisateurs finaux par un ou plusieurs moyens, notamment les connexions DSL, par câble, sans fil, mobiles, par fibre optique et par satellite. L’accès à Internet est souvent fourni par un fournisseur d’accès Internet (FAI) commercial, mais certains utilisateurs finaux accèdent à Internet via un réseau communautaire. D’un point de vue technique, l’accès au dernier kilomètre n’est pas différent des autres chemins de communication IP, mais il est souvent traité différemment dans certaines juridictions en raison de la réglementation locale des fournisseurs de services de communication aux utilisateurs finaux.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs d’accès Internet aux utilisateurs finaux ne doivent pas être tenus responsables du contenu qui transite par leurs réseaux.	Sans protection en matière de responsabilité, ces fournisseurs craindraient d’être tenus responsables du contenu que leurs clients envoient et reçoivent. Par conséquent, ils pourraient limiter le contenu que les utilisateurs finaux peuvent consulter ou transmettre sur Internet. Ils pourraient tenter d’imposer des filtres de téléchargement qui porteraient atteinte à la sécurité et à la confidentialité de l’utilisation d’Internet par leurs clients. De plus, pour réduire le risque de responsabilité, les fournisseurs bloqueraient probablement trop de contenu, empêchant les utilisateurs finaux de partager du contenu légal en ligne. Sans ces protections, l’Internet ouvert, connecté à l’échelle mondiale, sécurisé et digne de confiance serait compromis.

Approches stratégiques recommandées	Raisons de cette approche
Sauf pour des raisons de sécurité et de gestion efficace du trafic, les fournisseurs d'accès Internet aux utilisateurs finaux devraient être dissuadés de surveiller ou d'intercepter le contenu du trafic des utilisateurs.	Un principe fondamental de l'accès à Internet (souvent décrit comme la « neutralité du réseau ») est que les fournisseurs d'accès à Internet doivent fournir un accès à Internet sans tenir compte du contenu diffusé sur leurs réseaux. Si les fournisseurs d'accès Internet aux utilisateurs finaux ne suivent pas ce principe et appliquent un accès différent en fonction du contenu, cela violerait une propriété essentielle d'Internet, à savoir qu'il s'agit d'un réseau à usage général (voir le mode de fonctionnement du réseau Internet, définition des propriétés essentielles d'Internet³). Les utilisateurs finaux pourraient également restreindre la manière dont ils communiquent en ligne, craignant que leurs communications soient surveillées.

3 Internet Society, « Le mode de fonctionnement du réseau Internet : définition des propriétés essentielles d'Internet », <https://www.internetsociety.org/wp-content/uploads/2020/10/IWN-Defining-the-critical-properties-of-the-Internet-FR.pdf>.

2 Routage et fonctions annexes facilitant les communications Internet

Cette section décrit les différents rôles des intermédiaires impliqués dans l'adressage et le routage, qui sont essentiels pour un Internet efficace, robuste, fiable et sécurisé.

2.1 Attribution d'adresse IP

Description de la fonction : attribution d'adresses IP uniques aux réseaux et aux utilisateurs. Ce rôle d'intermédiaire est essentiel même pour les communications Internet les plus élémentaires, car chaque chemin de communication Internet nécessite un point de départ et une destination, ainsi que des « sauts » intermédiaires, chacun identifié par une adresse IP unique.

Considérations techniques et pratiques : les adresses IPv4 et IPv6 (également appelées ressources de numéros Internet) sont attribuées par l'Internet Assigned Numbers Authority (IANA) aux registres Internet régionaux ([RIR⁴](https://www.nro.net/about/rirs/)) pour une répartition équitable dans les régions des RIR. Au sein d'une région, les RIR attribuent des adresses IP aux fournisseurs de réseaux IP et aux organisations d'utilisateurs finaux. Dans certains pays, les RIR attribuent également des adresses IP aux registres Internet nationaux. L'IANA et les RIR sont des organisations à but non lucratif régies par des processus multipartites pour les réseaux et les utilisateurs du monde entier. Les cinq RIR comprennent le Registre Internet régional pour l'Afrique ([Afrinic⁵](https://www.afrinic.net/)), le centre d'information du réseau d'Asie-Pacifique

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

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

([APNIC](https://www.apnic.net/)⁶), le registre américain des adresses Internet ([ARIN](https://www.arin.net/)⁷), le registre d’adresses d’Internet pour l’Amérique latine et les Caraïbes ([LACNIC](https://www.lacnic.net/)⁸) et le centre de coordination de réseaux RIPE ([RIPE NCC](https://www.ripe.net/)⁹).

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d’attribution d’adresses IP ne doivent pas être tenus responsables du contenu communiqué à l’aide des adresses IP qu’ils ont attribuées.	Sans protection en matière de responsabilité, les fournisseurs de services d’attribution d’adresses IP, craignant d’être tenus responsables du contenu transmis via les adresses IP qu’ils ont attribuées, pourraient considérablement restreindre à qui ils attribuent des adresses IP et dans quelles conditions. Cela limiterait Internet et empêcherait de nombreux utilisateurs de pouvoir échanger en ligne.
Les services d’attribution d’IP ne doivent pas être tenus de contrôler les contenus illégaux ou indésirables sur Internet.	Les adresses IP sont souvent partagées par plusieurs utilisateurs finaux et peuvent être réattribuées à d’autres utilisateurs dans le même pays ou dans un autre pays. De même, les adresses IP sont souvent partagées par plusieurs hébergeurs de contenu. L’interférence avec l’attribution d’adresses IP ou l’utilisation d’adresses IP pour contrôler le contenu risque d’empêcher directement les utilisateurs de partager du contenu légal, ainsi que d’empêcher les hébergeurs de contenu de rendre le contenu légal disponible sur Internet.

6 <https://www.apnic.net/>.
7 <https://www.arin.net/>.
8 <https://www.lacnic.net/>.
9 <https://www.ripe.net/>.

2.2 Attribution de numéros de système autonome

Description de la fonction : attribuer des numéros uniques à un groupe de réseaux IP exploités par un ou plusieurs opérateurs de réseau (fournisseurs de chemins de communication IP, décrits dans la section 1.2 ci-dessus) qui ont une politique de routage externe unique et clairement définie. Un tel groupe de réseaux est appelé système autonome (AS) et le numéro unique qui l’identifie est son numéro de système autonome (ASN). Cette fonction est similaire à la fonction d’attribution d’adresse IP (décrite ci-dessus). Il s’agit d’un élément essentiel du système de routage du trafic Internet qui permet d’identifier les chemins de communication utilisés pour acheminer le trafic Internet.

Considérations techniques et pratiques : les ASN sont attribués par l’Internet Assigned Numbers Authority (IANA) aux registres Internet régionaux (RIR) afin d’être alloués dans leurs régions respectives. Les RIR attribuent des ASN à la fois aux fournisseurs de réseaux IP et aux organisations d’utilisateurs finaux. Voir la section 2.1 ci-dessus « Considérations techniques et pratiques » pour plus d’informations sur l’IANA et les RIR. Il existe une grande variété d’ASN. Certains sont très complexes, composés de plusieurs réseaux et utilisateurs indépendants, et d’autres sont plus simples.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d’attribution d’ASN ne doivent pas être tenus responsables du contenu communiqué à l’aide des ASN qu’ils ont attribués.	Sans protection en matière de responsabilité, les fournisseurs de services d’attribution d’ASN pourraient être disposés à n’allouer des ASN qu’à un très petit nombre de grands fournisseurs de services réseau bien établis, limitant ainsi la croissance et la diversité des réseaux sur Internet. Cela aurait probablement des effets graves, négatifs et imprévisibles sur Internet et son accès.

Approches stratégiques recommandées	Raisons de cette approche
Les services d'attribution d'ASN ne doivent pas être tenus de contrôler les contenus illégaux ou indésirables sur Internet.	Toute interférence dans l'allocation d'un ASN est susceptible d'entraver le routage fiable et efficace du trafic Internet, de nuire à la participation des réseaux à Internet et de bloquer l'accès et le partage de contenus légaux par un grand nombre d'utilisateurs.

2.3 Enregistrement et gestion DNS

Description de la fonction : simplifier l'enregistrement, le renouvellement et la gestion des noms de domaine pour leur publication dans le Système des Noms de Domaine (DNS). Ce rôle d'intermédiaire est essentiel pour les communications Internet impliquant l'utilisation de noms de domaine. Les noms de domaine sont les adresses « lisibles par l'homme » des réseaux, serveurs, sites Web et autres points de terminaison sur Internet.

Considérations techniques et pratiques : les noms de domaine sont importants car ils permettent aux humains de naviguer sur Internet, au lieu de mémoriser des adresses IP telles que « 192.0.2.1 ». L'enregistrement et la gestion DNS incluent l'enregistrement des noms de domaine auprès de bureaux d'enregistrement accrédités, garantissant l'intégrité de la zone DNS et la maintenance des informations du service d'annuaire des données d'enregistrement (RDDS, historiquement appelé WHOIS). Une gestion efficace consiste à garantir le respect des politiques, notamment les politiques de consensus définies par la communauté travaillant par l'intermédiaire de l'Internet Corporation for Assigned Names and Numbers (ICANN) pour les « gTLD » (« domaines génériques de premier niveau ») et les politiques définies par les organismes nationaux pour les « ccTLD » (« domaines de premier niveau de code de pays ») qui sont contrôlés par chaque pays.¹⁰ Cette fonction est assurée par plusieurs organisations travaillant en collaboration, notamment les registres DNS (qui gèrent les domaines de premier niveau gTLD et ccTLD) et les bureaux d'enregistrement (qui gèrent l'enregistrement des noms de domaine auprès de particuliers ou d'entités afin qu'ils puissent utiliser le nom de domaine sur Internet).

¹⁰ Les pays peuvent définir leur propre politique en matière de ccTLD. L'exploitation de certains ccTLD a été déléguée par le pays à une entité externe qui attribue les domaines sur une base commerciale.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d'enregistrement et de gestion DNS ne doivent pas être tenus responsables du contenu communiqué à l'aide des noms de domaine qu'ils enregistrent ou gèrent.	L'absence de protection en matière de responsabilité des fournisseurs de services d'enregistrement et de gestion DNS pour les contenus hébergés sous des noms de domaine particuliers aurait probablement un effet dissuasif sur la capacité des gens à s'exprimer en ligne. Sans protection en matière de responsabilité, les fournisseurs limiteraient probablement considérablement les personnes autorisées à enregistrer des noms de domaine et la manière dont ces derniers peuvent être utilisés. Cela pourrait même chasser les petits concurrents du marché du DNS, diminuant ainsi la concurrence et augmentant le coût d'enregistrement des noms de domaine.
Les services d'enregistrement et de gestion DNS ne doivent pas être tenus de contrôler le contenu illégal ou indésirable sur Internet.	Les noms de domaine sont un élément essentiel de la manière dont les gens interagissent avec Internet. Alourdir le système d'enregistrement DNS en l'obligeant à faire partie des contrôles de contenu conduirait à limiter le nombre de personnes pouvant enregistrer des noms de domaine et à quelles fins, réduisant ainsi considérablement la capacité des gens à utiliser Internet.

2.4 Publication DNS

Description de la fonction : rendre les données DNS enregistrées accessibles sur les serveurs DNS faisant autorité afin que les informations disponibles pour la recherche DNS (abordée dans la section 2.5 ci-après) puissent être consultées par tout le monde sur Internet. Ce rôle d'intermédiaire est essentiel pour les communications Internet impliquant l'utilisation de noms de domaine. Cette fonction couvre également (a) le fonctionnement des « serveurs racines » qui fournissent des informations sur la manière d'atteindre le serveur DNS faisant autorité pour chaque domaine gTLD ou ccTLD de premier niveau, et (b) la fourniture de copies des informations du serveur DNS faisant autorité pour la résilience, la fiabilité et des réponses de recherche DNS plus efficaces.

Considérations techniques et pratiques : le DNS est un système hiérarchique. Pour chaque domaine de premier niveau (tel que .com), il existe un intermédiaire qui publie les informations faisant autorité sur ce domaine sur un serveur DNS appelé « [serveur racine](https://root-servers.org/)¹¹ ». Ces intermédiaires sont souvent appelés « opérateurs de serveur racine ». Il s'agit généralement du registre DNS auquel l'ICANN a délégué la fonction de gestion de ce domaine de premier niveau. Pratiquement toutes les communications Internet dépendent du bon fonctionnement de la fonction de publication DNS pour garantir que le trafic est acheminé vers le bon emplacement sur Internet. L'intégrité et la fiabilité du système de serveur DNS sont essentielles au fonctionnement d'Internet. Des copies d'informations DNS faisant autorité sont utilisées pour améliorer l'efficacité et la vitesse du système DNS.

¹¹ <https://root-servers.org/>.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de publication DNS ne doivent pas être tenus responsables du contenu communiqué à l'aide des noms de domaine qu'ils publient.	La perturbation des services d'enregistrement et de gestion DNS porterait directement atteinte au fonctionnement d'Internet en empêchant les utilisateurs de localiser les serveurs où sont hébergés les contenus et autres ressources. Si les fournisseurs de services de publication DNS devaient assumer la responsabilité des contenus associés aux noms de domaine qu'ils publient, ils pourraient cesser d'assurer la fonction de publication DNS ou le faire uniquement pour les domaines pré-contrôlés. Cela aurait des conséquences graves, négatives et imprévisibles sur les communications Internet.
Les services de publication DNS ne doivent pas être tenus de contrôler le contenu illégal ou indésirable sur Internet.	Un accès fiable et rapide à des données DNS publiées sûres et dignes de confiance est essentiel pour le bon fonctionnement d'Internet. Empêcher la publication DNS ou déterminer quels domaines peuvent être publiés et dans quelles conditions fragiliserait Internet et le rendrait peu fiable.

2.5 Recherche DNS

Description de la fonction : traduire les noms de domaine en leurs adresses numériques IPv4 ou IPv6 actuellement correctes (ainsi que d'autres informations). En règle générale, les utilisateurs utilisent des noms de domaine pour localiser les sites Web et autres ressources sur Internet auxquels ils souhaitent accéder. Les noms de domaine doivent être convertis en adresse IP correcte pour permettre aux réseaux, aux serveurs et aux utilisateurs finaux (appareils) de se connecter les uns

aux autres. Cette fonction est assurée par des serveurs spécialisés appelés serveurs de noms de domaine récursifs (serveurs DNS récursifs) qui obtiennent leurs informations DNS auprès de serveurs DNS faisant autorité (voir section 2.4 ci-dessus). Ils stockent la correspondance entre les noms de domaine et les adresses IP, et répondent aux demandes de recherche de noms de domaine et de renvoi d’adresses IP (ou d’autres informations demandées).

Considérations techniques et pratiques : les serveurs DNS récursifs sont situés dans de nombreuses parties différentes d’Internet. Pour accélérer le système de noms de domaine, la plupart des ordinateurs des utilisateurs finaux ne communiquent pas avec des serveurs DNS faisant autorité. Ils demandent des informations DNS aux serveurs DNS récursifs. Certains serveurs récursifs sont proposés au monde entier (souvent appelés « serveurs DNS ouverts »). D’autres sont exploités par des fournisseurs d’accès Internet (FAI), d’autres opérateurs de réseau et des entreprises privées principalement pour l’usage de leurs utilisateurs. Parfois, des particuliers exploitent leurs propres serveurs récursifs pour un usage personnel. Ils le font sur leurs propres ordinateurs, généralement pour leur usage personnel. Bien que la fonction principale, la recherche DNS, puisse être la même, de nombreux utilisateurs choisissent un fournisseur DNS spécifique pour des raisons de sécurité et de confidentialité.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de recherche DNS ne doivent pas être tenus responsables du contenu communiqué à l’aide des réponses qu’ils fournissent aux requêtes de recherche DNS.	Sans protection en matière de responsabilité, les fournisseurs de services de recherche DNS limiteraient probablement la capacité des utilisateurs à utiliser le système DNS pour accéder au contenu Internet. Le contenu serait inaccessible sans la connaissance de l’adresse IP spécifique du site Web ou d’une autre ressource Internet. Cela aurait un impact grave et négatif sur les communications Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les services de recherche DNS ne doivent pas être tenus de contrôler le contenu illégal ou indésirable sur Internet.	Le blocage de l'accès aux noms de domaine via des services de recherche DNS (serveurs DNS récur­sifs) crée des risques importants de blocage excessif du contenu, d'empêchement de l'accès et de fragmentation d'Internet. Les tentatives d'imposer un filtrage de contenu via des serveurs DNS récur­sifs compromettent l'intégrité du DNS et le rendront peu fiable.

2.6 Services DNSSEC

Description de la fonction : fournir une authentification pour les enregistrements de noms de domaine stockés sur des serveurs DNS faisant autorité. Cette fonction est assurée en fournissant des signatures cryptographiques à clé publique pour ces enregistrements. L'objectif de cette fonction est de protéger l'intégrité des enregistrements de noms de domaine et de fournir un mécanisme permettant de valider que l'adresse IP (ou d'autres informations) renvoyée par une requête DNS correspond à ce que l'opérateur du domaine avait l'intention de fournir. Le protocole DNSSEC est un intermédiaire essentiel pour garantir qu'aucune falsification n'a été effectuée sur l'enregistrement du nom de domaine.

Considérations techniques et pratiques : DNSSEC, un protocole de sécurité développé par l'Internet Engineering Task Force (IETF), permet de prévenir une série d'attaques de cybersécurité sur les communications Internet. Sans DNSSEC, un attaquant pourrait, par exemple, corrompre les données DNS en transit en modifiant l'adresse IP correspondant au site Web auquel un utilisateur souhaite accéder, le dirigeant ainsi vers le site Web de l'attaquant. Lorsqu'il est déployé correctement, DNSSEC sécurise tous les enregistrements DNS relatifs à un nom de domaine. Ces enregistrements peuvent être utilisés pour localiser des services tels que la messagerie instantanée et le courrier électronique, ainsi que pour prendre en charge les mesures antispam qui dépendent du DNS.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services DNSSEC ne doivent pas être tenus responsables du contenu communiqué à l'aide de domaines protégés par DNSSEC.	DNSSEC protège l'intégrité des résultats DNS quel que soit le contenu sous-jacent. Sans protection en matière de responsabilité, les fournisseurs de services DNSSEC réduiraient directement l'utilisation de DNSSEC. Cela aurait pour effet de diminuer considérablement la sécurité des communications sur Internet.

2.7 Services de certificats TLS

Description de la fonction : création, stockage et émission de certificats TLS (Transport Layer Security) signés cryptographiquement pour créer des connexions sécurisées à un serveur sur Internet. Les certificats TLS sont généralement émis par une autorité de certification (« AC »). Une utilisation courante des certificats TLS est la sécurisation du trafic Web pour empêcher les écoutes clandestines et les falsifications. L'émission de certificats TLS est une fonction intermédiaire essentielle, nécessaire à un Internet fiable et sécurisé.

Considérations techniques et pratiques : un certificat TLS est signé numériquement et émis par une autorité de certification, et contient des informations telles que le nom de domaine, l'entité (personne, organisation ou appareil) pour laquelle il a été émis, le nom de l'autorité de certification émettrice et sa période de validité. Les certificats TLS protègent l'intégrité et l'authenticité des clés publiques cryptographiques utilisées pour établir des sessions HTTP cryptées (HTTPS) afin de sécuriser le trafic Web contre les écoutes clandestines et les falsifications. TLS est un outil essentiel pour sécuriser les communications sur le Web.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des certificats TLS ne doivent pas être tenues responsables du contenu sécurisé à l'aide de ces certificats TLS.	TLS est destiné à protéger le trafic sur Internet, quel que soit son contenu. Imposer la responsabilité du contenu aux fournisseurs de certificats TLS porterait atteinte à la sécurité des communications sur Internet. Si les entités fournissant des certificats TLS devaient assumer la responsabilité du contenu transmis à l'aide de leurs certificats, elles seraient réticentes à délivrer des certificats TLS, en particulier aux particuliers et aux petites entités, rendant Internet moins sûr pour tous les internautes.

3 Services d'hébergement et de mise en cache

Les deux premiers groupes de fonctions (décrits dans les sections ci-dessus) permettent les communications sur Internet. Cette troisième section décrit les fonctions qui permettent de rendre le contenu disponible sur Internet, y compris le contenu généré par les utilisateurs et créé par des particuliers et des entités plus petites.

3.1 Hébergement Web

Description de la fonction : fournir et exploiter des serveurs et autres ressources nécessaires pour héberger des sites Web ou d'autres ressources et applications Web, et les rendre accessibles sur Internet. Ce rôle d'intermédiaire permet aux particuliers et à d'autres de partager du contenu avec d'autres utilisateurs via le World Wide Web.

Considérations techniques et pratiques : l'hébergement d'un site Web implique l'exploitation de serveurs qui (a) stockent les fichiers, les bases de données, les logiciels et le code d'un site Web ou d'une application Web, et (b) reçoivent et répondent aux demandes des utilisateurs pour accéder au contenu du site. Les entités qui fournissent un hébergement peuvent également fournir d'autres services connexes, notamment une assistance technique, des solutions de sauvegarde et de sécurité. De nombreux particuliers, entreprises, organismes à but non lucratif et gouvernements s'appuient sur des services d'hébergement Web tiers plutôt que d'agir comme leur propre hébergeur Web. Ces services d'hébergement Web offrent généralement un hébergement de sites Web plus sécurisé, moins cher et plus fiable.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d'hébergement Web ne doivent pas être tenus responsables du contenu de leurs clients directs ou du contenu fourni par les utilisateurs des sites Web de leurs clients.	Si les entités fournissant des services d'hébergement Web devaient assumer la responsabilité du contenu des sites Web de leurs clients, les fournisseurs de services seraient réticents à proposer des services d'hébergement Web, notamment aux particuliers et aux petites organisations. Sans protection en matière de responsabilité, les fournisseurs de services d'hébergement peuvent restreindre sévèrement qui peut publier du contenu en ligne et quel contenu ils peuvent publier, limitant ainsi considérablement la capacité des individus à communiquer sur Internet.
Les fournisseurs de services d'hébergement Web ne doivent pas être tenus d'inspecter ou de supprimer le contenu placé par leurs clients.	Le fait d'obliger les fournisseurs à inspecter et à supprimer du contenu porterait atteinte à leur capacité à fonctionner en tant qu'hébergeurs de sites Web, en particulier les petits fournisseurs. Ils pourraient restreindre leurs services à du contenu pré-approuvé provenant d'un petit nombre de sites Web et les utilisateurs auraient des options limitées pour rendre leur contenu disponible sur Internet.
Les fournisseurs de services d'hébergement Web ne doivent pas être tenus de contrôler le contenu illégal ou indésirable.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a publié le contenu, et non au fournisseur de services hébergeant le contenu.

3.2 Hébergement de messagerie électronique

Description de la fonction : fournir et exploiter des serveurs de messagerie pour envoyer, recevoir, stocker, transférer et gérer les services de messagerie sur Internet. Ce rôle d’intermédiaire est essentiel pour le courrier électronique, outil majeur de communication sur Internet.

Considérations techniques et pratiques : l’hébergement de courrier électronique implique l’exploitation de serveurs qui envoient, reçoivent, stockent, transfèrent et gèrent les courriers électroniques. Les fournisseurs d’hébergement de messagerie peuvent également fournir d’autres services connexes, tels que le support technique, l’archivage, le filtrage du spam et le support de conformité. La plupart des internautes, qu’il s’agisse de particuliers ou d’organisations, s’appuient désormais sur l’hébergement de messagerie tiers. En règle générale, les fournisseurs tiers peuvent proposer des services de messagerie plus sûrs, moins chers et plus fiables que ceux que de nombreux particuliers et entreprises pourraient proposer eux-mêmes.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de messagerie ne doivent pas être tenus responsables du contenu des courriers électroniques envoyés ou reçus par leurs utilisateurs.	Si les entités fournissant des services de messagerie électronique devaient assumer la responsabilité du contenu des courriers électroniques envoyés ou reçus par leurs clients, les fournisseurs de services seraient réticents à proposer des services de messagerie électronique, surtout aux particuliers et aux petites entités. Sans protection en matière de responsabilité, les fournisseurs de services de messagerie électronique pourraient être contraints de chercher à surveiller et à censurer les messages électroniques. Par conséquent, le courrier électronique ne serait plus un outil utile pour les communications interpersonnelles.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs ne doivent pas être tenus de supprimer du contenu ou de bloquer la capacité des utilisateurs à utiliser leurs services.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a transmis le contenu, et non au fournisseur d'hébergement de messagerie ou à d'autres fournisseurs facilitant la transmission de courriers électroniques. Imposer une telle contrainte au fournisseur d'hébergement porterait atteinte à la capacité des petits fournisseurs à opérer sur le marché et pourrait nuire à la confiance, à l'intégrité et à la fiabilité du courrier électronique.

3.3 Autres services d'hébergement

Description de la fonction : fournir et exploiter des serveurs qui hébergent du contenu, des fichiers, des bases de données, des logiciels et du code, ainsi que d'autres ressources qui permettent à d'autres d'exploiter une vaste gamme d'applications, de sites et de services pour envoyer et recevoir des communications sur Internet. Étant donné que la grande majorité des applications et des offres sur Internet, en particulier celles proposées par les startups et les petites et moyennes entreprises, utilisent des services d'hébergement, ce rôle d'intermédiaire est essentiel pour la disponibilité d'un ensemble diversifié de services et d'applications sur Internet.

Considérations techniques et pratiques : l'hébergement implique l'exploitation de serveurs qui (a) stockent le contenu, les fichiers, les bases de données, les logiciels et le code qui composent un service ou une application en ligne (b) permettent aux utilisateurs d'interagir avec le service ou l'application. Les fournisseurs de la fonction d'hébergement peuvent également fournir d'autres services connexes, notamment le support technique, les solutions de sauvegarde, la sécurité et l'accès à Internet. De nombreux utilisateurs font appel à des services d'hébergement tiers, car ces fournisseurs peuvent offrir un hébergement plus sûr, moins cher et plus fiable que celui que de nombreux particuliers et entreprises pourraient fournir eux-mêmes.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d'hébergement ne doivent pas être tenus responsables du contenu de leurs clients ou des utilisateurs de leurs clients.	Si les entités fournissant des services d'hébergement devaient assumer la responsabilité du contenu envoyé ou reçu par les clients ou les utilisateurs des clients, les fournisseurs de services seraient réticents à proposer cette fonction, surtout aux particuliers et aux petites entités. Sans protection en matière de responsabilité, l'innovation sur Internet diminuerait et l'hébergement de contenu serait limité à un petit nombre de grands fournisseurs.
Les fournisseurs de services d'hébergement ne doivent pas être tenus de contrôler le contenu illégal ou indésirable sur Internet.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a transmis le contenu, et non au fournisseur qui héberge le contenu. Imposer une telle contrainte au fournisseur d'hébergement porterait atteinte à la capacité des petits fournisseurs à opérer sur le marché et les utilisateurs auraient des options plus limitées pour rendre leur contenu disponible en ligne.

3.4 Services de mise en cache et de diffusion de contenu

Description de la fonction : stockage temporaire de copies de contenu plus près de l'utilisateur final pour réduire la latence et les coûts du contenu fréquemment consulté. Les services de mise en cache sont un type particulier de service d'hébergement, impliquant généralement le stockage temporaire de copies d'autres contenus plus proches de l'utilisateur final. Les réseaux de diffusion de contenu (CDN) utilisent des centres de données et des réseaux géographiquement dispersés pour

diffuser plus rapidement le contenu de leurs clients aux utilisateurs finaux. En général, leurs clients sont de grands distributeurs de contenu tels que des services de streaming. Ces services de mise en cache et de diffusion de contenu sont essentiels au fonctionnement efficace d’Internet.

Considérations techniques et pratiques : certaines fonctions de mise en cache sont fournies par les navigateurs (abordées ci-après), cependant, sur Internet, la principale fonction de mise en cache est généralement proposée par un CDN, qui exploite un réseau de serveurs distribués. La fonction de mise en cache peut également être proposée par les fournisseurs d’accès Internet pour accélérer l’accès au contenu pour les clients du FAI. Dans les deux cas, les serveurs de mise en cache stockent des copies temporaires de contenus populaires, tels que des pages Web, des vidéos ou des images. Étant donné que ces serveurs sont répartis sur différents réseaux sur Internet, cela signifie que les copies du contenu souhaité peuvent être plus proches des utilisateurs et accessibles plus rapidement. Cela réduit la distance que le contenu doit parcourir, ce qui diminue le temps de chargement et la latence, et améliore l’expérience utilisateur. La mise en cache réduit également le coût de distribution du contenu en évitant la retransmission répétée du même contenu. Les décisions concernant le contenu à mettre en cache et pendant combien de temps sont généralement automatisées en fonction d’algorithmes de mise en cache spécifiques.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de mise en cache et de diffusion de contenu ne doivent pas être tenus responsables du contenu mis en cache.	Si les entités fournissant des services de mise en cache ou de diffusion de contenu devaient assumer la responsabilité du contenu temporairement stocké sur leurs serveurs, les fournisseurs de services seraient réticents à proposer les services, ce qui augmenterait les coûts, réduirait directement l’efficacité et affecterait négativement l’expérience utilisateur.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de mise en cache ne doivent pas servir de points de contrôle pour le contenu illégal ou indésirable sur Internet.	Si les fournisseurs de services de mise en cache étaient tenus de contrôler le contenu, ils ne mettraient en cache que le contenu connu et contrôlé. Cela augmenterait les coûts pour les petits fournisseurs de contenu et les rendrait moins attractifs pour les internautes en raison de la qualité réduite de l'expérience utilisateur. Les utilisateurs perdront l'accès à une grande diversité de contenus, et le contenu local sera probablement celui qui en souffrira le plus.

3.5 Diffusion de contenu d'interface de programmation d'application (API)

Description de la fonction : héberger et diffuser du contenu via une API, ou interface de programmation d'application, qui est un ensemble de règles ou de protocoles permettant aux serveurs informatiques de communiquer des informations d'une machine à une autre. Les API sont des outils très courants utilisés dans un large éventail de contextes pour envoyer et recevoir des informations sur Internet, et dans certains de ces contextes, elles sont utilisées pour transmettre du contenu généré par les utilisateurs. Dans un cas d'utilisation courant, par exemple, les API peuvent permettre l'affichage de publications de blog ou de réseaux sociaux intégrées à d'autres pages Web.

Considérations techniques et pratiques : cette fonction est très similaire à l'hébergement général de contenu Web décrit ci-dessus, mais utilise parfois des protocoles ou des capacités techniques différents pour demander et envoyer le contenu.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services API ne doivent pas être tenus responsables du contenu utilisateur fourni via leurs services.	Si les entités fournissant des services API devaient assumer la responsabilité du contenu utilisateur fourni via leurs services, elles seraient réticentes à proposer de tels services, réduisant ainsi la capacité des personnes à publier et à recevoir du contenu légal sur Internet.
Les services API ne doivent pas être utilisés pour contrôler le contenu illégal ou indésirable sur Internet.	Les API sont des outils fondamentaux dans tout l'écosystème Internet, et toute tentative de les utiliser comme moyen de contrôler le contenu en ligne risque de cloisonner le contenu au sein des services, réduisant ainsi considérablement l'interopérabilité et l'innovation.

3.6 Curation, modération et affichage du contenu

Description de la fonction : organiser et, dans certains cas, sélectionner le contenu à afficher aux utilisateurs. Cette fonction se distingue de l'hébergement Web, décrit précédemment dans la section 3.1, par les services supplémentaires fournis, comme la curation ou la modération de contenu. Elle est très souvent présente sur les sites Web proposant du contenu généré par les utilisateurs. Cette fonction peut être assurée aussi bien de manière automatisée à l'aide d'algorithmes et d'automatisations que parfois de manière manuelle par des particuliers.

Considérations techniques et pratiques : la fonction de curation de contenu est généralement fournie par les hébergeurs de contenu généré par les utilisateurs, qui doivent gérer et organiser un vaste volume de soumissions. Il existe de nombreuses raisons de proposer cette fonction. Par exemple, les hébergeurs peuvent filtrer le contenu qui enfreint leurs conditions de service. Ils présenteront probablement aussi le contenu aux

utilisateurs en fonction de leurs intérêts et préférences, de leur historique de visionnage ou d'autres critères. Ces fonctions permettent la gestion pratique du contenu sur les sites de contenu généré par les utilisateurs. Les décisions de curation et de modération ont plus de chances d'être pertinentes et compréhensibles pour les utilisateurs si elles intègrent des aspects culturels, linguistiques et autres éléments contextuels.

Approches stratégiques recommandées	Raisons de cette approche
Les organisations fournissant des fonctions de curation, de modération et d'affichage de contenu aux utilisateurs devraient pouvoir le faire sans craindre d'être tenues responsables de ce contenu.	Si les entités fournissant des fonctions de curation et de modération devaient assumer la responsabilité du contenu ou de ces fonctions, elles seraient réticentes à les proposer. Sans curation ni modération, le contenu généré par les utilisateurs serait désorganisé et non trié. Il serait difficile pour les utilisateurs de partager du contenu avec leur public et de localiser le contenu qu'ils souhaitent.
L'accès à la curation et à la modération ne devrait pas être limité.	Sans curation ni modération, qui sont essentielles pour bloquer le spam et le contenu non pertinent et pour fournir du contenu intéressant aux utilisateurs, les sites d'hébergement de contenu deviendraient probablement ingérables pour les opérateurs et indésirables pour les visiteurs du site.

4 Communications interpersonnelles

Cette section comprend un quatrième groupe de fonctions axé sur différents modes de communication qui permettent aux gens d'échanger sur Internet. Ces fonctions sont essentielles pour que les particuliers, ainsi que les petites organisations et entreprises, puissent interagir sur Internet.

Certains aspects de ces fonctions sont similaires à d'autres rôles d'intermédiaires présentés dans cette annexe. Il est toutefois important de les décrire séparément, car il s'agit de fonctions fondamentales qui reviennent sans cesse dans les nouveaux services fournis sur Internet. Par exemple, les applications de messagerie sont une innovation relativement récente qui combine les fonctions de communication de type one-to-one (communication interpersonnelle) et one-to-many (communication de groupe).

4.1 Communications interpersonnelles (one-to-one)

Description de la fonction : fournir un moyen fiable d'envoyer, de recevoir, d'afficher, d'acheminer et de prendre en charge des communications discrètes, en temps réel (de manière synchrone) ou pour une livraison ultérieure (de manière asynchrone) entre un expéditeur et un destinataire. Cette fonction peut, dans certains cas, être couplée à une fonction « découverte » permettant de rechercher d'autres utilisateurs d'un service particulier (par exemple, par nom ou numéro de téléphone) pour permettre aux utilisateurs de se connecter avec d'autres utilisateurs.

Considérations techniques et pratiques : cette fonction permet aux individus (et aux organisations) de communiquer entre eux de manière étendue. Cette fonction fait partie d'une large gamme de services, notamment le courrier électronique, la messagerie texte, le chat, la messagerie directe et d'autres outils. Elle peut inclure des communications interpersonnelles dans un large éventail d'environnements, tels que les sites Web, la vidéoconférence, les jeux,

les réseaux sociaux et d’autres contextes. Certains environnements peuvent également permettre à un interlocuteur de diffuser le même contenu à plusieurs destinataires en même temps (similaire à la fonction de communication de groupe abordée dans la section 4.2). Certains de ces services offrent une sécurité et une confidentialité renforcées comme caractéristique distinctive, basées sur le cryptage de bout en bout (E2EE), la décentralisation ou d’autres technologies.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de communications interpersonnelles ne doivent pas être tenus responsables du contenu envoyé ou reçu par leurs utilisateurs.	Si les entités fournissant des services de communications interpersonnelles devaient assumer la responsabilité du contenu des communications de leurs utilisateurs, elles seraient réticentes à proposer ces services, notamment aux particuliers et aux petites entités. Sans protection en matière de responsabilité, les fournisseurs pourraient être contraints de cesser d’offrir le service ou de surcensurer les messages, y compris les discours légitimes, pour éviter toute responsabilité. Le résultat serait une réduction de la capacité des gens à communiquer en ligne.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de communications interpersonnelles ne doivent pas être tenus responsables du traitement du contenu problématique envoyé ou reçu par les clients	La responsabilité du contenu problématique devrait être imputée à la personne ou à l'entité qui a transmis le contenu, et non au fournisseur de services qui héberge ou diffuse le contenu. Imposer aux fournisseurs de services de communications interpersonnelles des contraintes de révision du contenu pourrait bien les pousser à la faillite (en particulier les plus petits) et ainsi réduire la capacité des utilisateurs à communiquer individuellement. Cela pourrait également les amener à supprimer des protections essentielles en matière de confidentialité et de sécurité, telles que le cryptage de bout en bout.

4.2 Communications de groupe (one-to-many)

Description de la fonction : fournir un moyen fiable d'envoyer, de recevoir, d'afficher, d'acheminer et de prendre en charge des communications discrètes, en temps réel (de manière synchrone) ou pour une livraison ultérieure (de manière asynchrone) d'un expéditeur à un groupe **précis** de destinataires (qui *peuvent* ou *non* être définis ou contrôlés par l'expéditeur). Les destinataires pourraient ou non avoir la capacité de répondre et d'engager une conversation au sein du groupe plus large.

Considérations techniques et pratiques : cette fonction permet aux personnes (et aux organisations) de communiquer de façon plus étendue avec des groupes de destinataires. Cette fonction fait partie d'une large gamme de services, allant des services de listes de diffusion par courrier électronique vieux de plusieurs décennies aux services de webinaires vidéo plus modernes. Certains de ces services peuvent offrir une sécurité

et une confidentialité renforcées comme caractéristique distinctive, comme le cryptage de bout en bout (E2EE) ou la décentralisation. En général, les participants aux communications de groupe ont la possibilité de quitter ou de « se désinscrire » du groupe, ou de bloquer les communications provenant d'expéditeurs particuliers.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de communications de groupe ne doivent pas être tenus responsables du contenu envoyé ou reçu par leurs utilisateurs.	Si les entités fournissant des services de communication de groupe devaient assumer la responsabilité du contenu des communications de leurs utilisateurs, elles seraient réticentes à proposer ces services. Sans protection en matière de responsabilité, les fournisseurs pourraient être contraints de cesser d'offrir le service ou de surcensurer les messages, y compris les discours légitimes, pour éviter toute responsabilité. Le résultat serait une réduction de la capacité des gens à communiquer en ligne.
Les fournisseurs de services de communication de groupe ne doivent pas être tenus responsables du contrôle ou du filtrage des contenus problématiques échangés par leurs utilisateurs.	La responsabilité du contenu problématique devrait être imputée à la personne ou à l'entité qui a transmis le contenu, et non au fournisseur de services qui héberge ou diffuse le contenu. Si les fournisseurs étaient tenus de surveiller de manière proactive le forum pour détecter tout contenu indésirable, cette contrainte réduirait probablement la capacité des fournisseurs (en particulier les plus petits) à héberger un tel forum. Les fournisseurs doivent être protégés s'ils choisissent de supprimer ou de bloquer un utilisateur qui viole les conditions de service ou les normes du groupe.

4.3 Communications de masse (many-to-many)

Description de la fonction : fournir un moyen fiable d'envoyer, de recevoir, d'afficher, d'acheminer et de prendre en charge les communications, en temps réel (de manière synchrone) ou pour une livraison ultérieure (de manière asynchrone) par les expéditeurs/créateurs de contenu à tous les utilisateurs d'un service ou à un autre groupe large et indéfini de destinataires non contrôlés par l'expéditeur. Les destinataires ou les participants peuvent ou non avoir la possibilité de répondre et d'engager une conversation au sein du groupe plus large.

Considérations techniques et pratiques : cette fonction donne aux personnes (et aux organisations) la possibilité de communiquer largement avec le public ou d'autres grands groupes de personnes (comme tous les utilisateurs d'un service particulier). Cette fonction fait partie d'une large gamme de services, parmi lesquels des sites « wiki » collaboratifs, des sites de développement de contenu/logiciel collaboratif, des sites de partage d'images/vidéos préenregistrées, des services de streaming vidéo en direct et des sites de réseaux sociaux. Certains de ces services pourraient offrir aux utilisateurs la possibilité de limiter la distribution de leurs publications ou de leur contenu à un groupe défini de personnes (similaire à la fonction de communication de groupe décrite au point 4.2 ci-dessus). Certains fournisseurs de services de communications de masse offrent aux utilisateurs la possibilité de bloquer les communications provenant d'expéditeurs particuliers ou de se désinscrire du groupe.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de communications de masse ne doivent pas être tenus responsables du contenu envoyé ou reçu par leurs utilisateurs.	Si les entités fournissant des services de communication de masse devaient assumer la responsabilité du contenu des communications de leurs utilisateurs, elles seraient réticentes à proposer ces services. Sans protection en matière de responsabilité, les fournisseurs peuvent être contraints de cesser d'offrir le service ou de surcensurer les messages, y compris les discours légitimes, pour éviter toute responsabilité. Le résultat serait une réduction de la capacité des gens à communiquer en ligne.
Les fournisseurs de services de communication de masse ne doivent pas être tenus responsables du contrôle ou du filtrage des contenus problématiques échangés par leurs utilisateurs.	La responsabilité du contenu problématique devrait être imputée à la personne ou à l'entité qui a transmis le contenu, et non au fournisseur de services qui héberge ou diffuse le contenu. Si les fournisseurs étaient tenus de surveiller de manière proactive le forum pour détecter tout contenu indésirable, cette contrainte réduirait probablement la capacité des fournisseurs (en particulier les plus petits) à héberger des communications de masse. Les fournisseurs doivent être protégés s'ils choisissent de supprimer ou de bloquer un utilisateur qui viole les conditions de service ou les normes du groupe.

5 Recherche

Cette section couvre un cinquième groupe de fonctions comprenant les principales méthodes utilisées par les internautes pour localiser du contenu. Les fonctions de recherche sont utilisées à la fois parce que les gens veulent accéder à de nouvelles informations ou à de nouveaux contenus, et parce qu'ils veulent revisiter des contenus précédemment consultés.

De nombreux outils et techniques de recherche affichent une partie du contenu de la ressource suggérée en réponse à une requête de recherche.¹² Par conséquent, la fonction de recherche comprend non seulement la localisation du contenu, mais également l'affichage du contenu généré par les utilisateurs. Les fonctions de recherche sont essentielles pour permettre aux utilisateurs de découvrir et d'accéder au contenu sur Internet.

5.1 Recherche sur le Web

Description de la fonction : répondre aux requêtes de recherche en offrant les moyens de connecter l'utilisateur au contenu et, souvent, en affichant une partie du contenu. La recherche est le plus souvent effectuée par des « moteurs de recherche », qui sont des services tiers permettant aux utilisateurs de rechercher des ressources pertinentes sur le World Wide Web en fournissant des mots-clés, une question ou en téléchargeant ou en créant un lien vers une image.

Considérations techniques et pratiques : fournir cette fonction de recherche implique généralement (a) l'indexation du contenu sur Internet à l'aide d'algorithmes qui évaluent et enregistrent des informations telles que la pertinence des mots clés, le type de contenu, la clarté du contenu, l'engagement de l'utilisateur et la qualité de la page, et (b) l'identification, la fourniture d'un lien d'accès et l'affichage des résultats suggérés (souvent avec des « extraits » du contenu) en réponse à une requête de recherche de l'utilisateur à l'aide d'algorithmes qui évaluent des facteurs tels que l'emplacement de l'utilisateur, la langue de l'utilisateur, l'historique de recherche précédent et le type d'appareil.

¹² Bien que certains outils de recherche fournissent désormais des résumés de contenu générés par l'IA en réponse aux requêtes de recherche. Pour une discussion de ces questions, voir la section 5.9 du Cadre stratégique, Pleins feux sur : l'intelligence artificielle.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de recherche ne doivent pas être tenus responsables des contenus Internet créés par des tiers et affichés aux utilisateurs en réponse à leurs requêtes.	Si les moteurs de recherche étaient tenus responsables du contenu généré par les utilisateurs, ils cesseraient probablement d'indexer la plupart du contenu du Web. Cela aurait pour conséquence concrète de rendre une grande partie d'Internet inaccessible aux utilisateurs du monde entier.
Les fournisseurs de services de recherche ne doivent pas être tenus responsables du traitement du contenu problématique affiché dans les résultats de recherche.	La recherche est une fonction intermédiaire essentielle à la communication sur Internet, car elle facilite l'accès des utilisateurs au <i>contenu créé par d'autres</i> en les aidant à trouver et à localiser du contenu « pertinent » sur Internet. Sans recherche, les utilisateurs devraient connaître à l'avance l'URL ou l'adresse IP de chaque site Web ou autre ressource en ligne à laquelle ils souhaitent accéder, ce qui est impossible à l'échelle d'Internet.

5.2 Recherche intégrée

Description de la fonction : fournir des résultats de recherche intégrés, spécifiques à un site, comme service aux sites Web et autres entités n'ayant pas les ressources techniques ou les capacités financières pour créer leurs propres outils de recherche dédiés.

Considérations techniques et pratiques : en confiant la fonction de recherche interne à un moteur de recherche tiers, un site Web peut proposer la recherche directement à ses utilisateurs. Cette fonction est souvent, mais pas exclusivement, proposée par les moteurs de recherche qui proposent eux-mêmes des recherches axées sur le Web (comme abordé ci-dessus). Les résultats de la recherche peuvent être adaptés aux besoins du site Web spécifique qui utilise la recherche intégrée.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de recherche intégrés ne doivent pas être tenus responsables du contenu Internet géré par le site Web sous-jacent qui utilise le service pour une fonction de recherche intégrée.	Si les fournisseurs de services de recherche intégrés étaient tenus responsables du contenu affiché dans les résultats de recherche, ils cesseraient probablement d'offrir ce service, en particulier aux petits sites Web et aux entreprises ou organisations moins établies, ce qui aurait un impact direct sur l'expérience des internautes, car les sites manqueraient de bonnes fonctions de recherche.
Les fournisseurs de services de recherche intégrés ne doivent pas être tenus responsables du traitement du contenu problématique affiché dans les résultats de recherche intégrés.	Si les fournisseurs de moteurs de recherche intégrés étaient tenus de surveiller le contenu du site, le service deviendrait probablement trop coûteux pour les petits sites Web et les entreprises ou organisations moins établies. Cela entraverait directement la capacité des petits sites Web à rivaliser avec les sites plus grands.

5.3 Recherche spécifique

Description de la fonction : fournir des résultats de recherche axés sur des médias ou des sujets spécifiques (tels que, par exemple, des services audios inversés ou des outils de recherche de podcasts ou d'images) à partir de sites exploités par des tiers autres que le fournisseur de recherche. Cette fonction augmente la capacité des utilisateurs à localiser le contenu qui les intéresse sur Internet, en particulier le contenu qui n'est pas facilement consultable à l'aide d'un moteur de recherche général.

Considérations techniques et pratiques : les outils de recherche généraux sont souvent trop vastes, et une gamme d'outils de recherche plus ciblés est donc apparue pour permettre aux utilisateurs d'Internet

de rechercher des types de contenu particuliers de manière plus efficace et plus efficiente. Les résultats de la recherche peuvent être adaptés aux types de médias ou de contenu.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de recherche spécifique ne doivent pas être tenus responsables des contenus Internet créés par des tiers et affichés aux utilisateurs en réponse à leurs requêtes.	Si les fournisseurs de services de recherche spécifique étaient tenus responsables du contenu affiché dans leurs résultats de recherche, ils ne pourraient probablement pas continuer à fonctionner et les internautes perdraient ainsi des outils indispensables à la découverte de contenu en ligne important.
Les fournisseurs de services de recherche spécifique ne doivent pas être tenus responsables du traitement du contenu problématique affiché dans les résultats de recherche.	Tout comme la recherche sur le Web est un outil essentiel qui a permis à Internet de devenir une énorme ressource d'information, les outils de recherche spécifiques ont offert une valeur similaire pour des contenus moins couverts par les moteurs de recherche généraux. Le fait d'imposer de telles contraintes aux fournisseurs pourrait probablement conduire certains d'entre eux à éliminer ou à restreindre ce type d'outil de recherche précieux.

5.4 Recherche interne au site

Description de la fonction : fournir une recherche de contenu au sein du site. Certains grands services en ligne (en particulier ceux qui hébergent du contenu généré par les utilisateurs, comme les services de réseaux sociaux) proposent leurs propres outils de recherche internes, adaptés à leur service, pour permettre aux utilisateurs de découvrir du contenu sur leurs sites.

Considérations techniques et pratiques : fournir des outils permettant aux utilisateurs de localiser du contenu est une fonction de base des sites qui prennent en charge le contenu généré par les utilisateurs. Les résultats de la recherche peuvent être adaptés aux types particuliers de contenu pris en charge par le site et/ou à l'utilisateur individuel.

Approches stratégiques recommandées	Raisons de cette approche
Les opérateurs de sites qui fournissent leurs propres outils de recherche pour localiser le contenu du site ne doivent pas être tenus responsables du contenu créé par d'autres, car ils proposent un outil de recherche au sein du site pour permettre la découverte de ce contenu.	Si ces sites n'étaient pas autorisés à fournir des outils de recherche sur leurs sites, les utilisateurs seraient privés d'outils locaux efficaces pour localiser du contenu.

6 Protection de la cybersécurité, protection de la vie privée et contrôles du contenu utilisateur

Cette section couvre un sixième groupe de fonctions qui :

- (a) visent à lutter contre les cyberattaques sur Internet et qui sont essentielles pour un Internet sécurisé, robuste, fiable et efficace,
- (b) permettent aux utilisateurs individuels de prendre des mesures pour protéger la sécurité et la confidentialité de leurs propres communications Internet, et
- (c) permettent aux utilisateurs d'exercer un contrôle sur les catégories de contenu qu'ils peuvent recevoir.

Remarque : certaines lois de protection de la responsabilité des intermédiaires étendent explicitement leurs protections aux logiciels et services qui permettent aux utilisateurs de contrôler le contenu qu'ils reçoivent sur Internet. Par exemple, les fournisseurs de logiciels de filtrage contrôlés par les utilisateurs et axés sur la famille peuvent être protégés contre les poursuites judiciaires intentées par les sites bloqués par le logiciel. Voir, par exemple, le Code statutaire des États-Unis, 47 U.S.C. §§ 230(f)(2) et (4).na Internet.

6.1 Protection du trafic à l'échelle du réseau

Description de la fonction : protection des réseaux, des services en ligne, des sites Web et d'autres ressources Internet contre un large éventail de trafic malveillant, y compris les attaques par déni de service distribué

(DDoS) et d'autres menaces de cybersécurité. Cette fonction fait partie d'un effort global de collaboration en matière de cybersécurité¹³ visant à sécuriser les communications sur Internet.

Considérations techniques et pratiques : les protections à l'échelle du réseau impliquent l'utilisation de techniques différentes et en constante évolution (telles que les bases de données de signatures, la détection d'anomalies et l'intelligence artificielle) et d'infrastructures dédiées pour se défendre contre les cyberattaques et atténuer l'impact du trafic malveillant sur la disponibilité, l'accessibilité ou la fiabilité des réseaux, des services en ligne, des sites Web et d'autres ressources Internet. Certaines de ces techniques nécessitent que les communications passent par un réseau exploité par un fournisseur de cybersécurité avant d'atteindre le réseau prévu. Ainsi, il arrive parfois que les réseaux des fournisseurs de services de cybersécurité véhiculent sur Internet du « contenu généré par les utilisateurs » et d'autres types de contenu « créé par d'autres ».

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de protection du trafic à l'échelle du réseau ne doivent pas être tenus responsables du contenu qui transite par leurs réseaux.	Sans protection en matière de responsabilité, les fournisseurs craindraient d'être tenus responsables du contenu circulant sur leurs réseaux ou qu'ils examinent à des fins de sécurité. Ils pourraient retirer ou restreindre la protection des réseaux ou d'autres ressources sur Internet, ce qui augmenterait considérablement le risque de cyberattaques nuisibles sur Internet.

13 Internet Society, « Sécurité collaborative : une approche pour résoudre les problèmes de sécurité Internet », avril 2015, disponible sur <https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf>.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de protection du trafic à l'échelle du réseau ne doivent pas être tenus responsables de la gestion du contenu problématique envoyé ou reçu par les réseaux, les services en ligne, les sites Web et les autres ressources Internet protégés.	La protection du trafic à l'échelle du réseau est un processus hautement dynamique et itératif visant à répondre aux cyberattaques en constante évolution. Imposer des contraintes supplémentaires et sans rapport pour tenter de bloquer certains types de contenu compromettrait l'efficacité de la protection cybernétique globale. Cela pourrait également encourager les fournisseurs à exiger de leurs clients qu'ils autorisent le décryptage lorsque le trafic transite par leurs systèmes. Cela porterait atteinte à la confidentialité, à l'intégrité et à la sécurité des communications des internautes. Toute tentative de recherche d'un contenu spécifique nécessiterait de tenter de rassembler au milieu du réseau tous les paquets de données distincts qui composent l'élément de contenu (afin de pouvoir déterminer quel contenu est transmis), et cela serait très difficile à faire de manière cohérente pour un fournisseur de services.

6.2 Filtres et outils de contenu contrôlés par l'utilisateur

Description de la fonction : fournir à l'utilisateur des outils pour bloquer ou limiter la diffusion de certains types de contenu sur ses appareils. Différents types d'outils sont disponibles. Par exemple, des outils de filtrage de contenu contrôlés par l'utilisateur peuvent être utilisés pour réduire la livraison de courriers indésirables, bloquer la livraison de code malveillant par un site Web ou chercher à empêcher la visualisation de contenu Web indésirable tel que de la pornographie par un foyer ou l'appareil d'un utilisateur.

Considérations techniques et pratiques : les filtres et outils contrôlés par l'utilisateur offrent des protections importantes (comme contre le spam et les logiciels malveillants sur les pages Web) et des options de protection familiale (comme contre la pornographie ou d'autres contenus). Ces outils utilisent des méthodes techniques diverses, et ne sont pas toujours totalement efficaces (mais peuvent néanmoins s'avérer très utiles). Ils sont parfois fournis en tant que service supplémentaire par un fournisseur d'accès Internet, mais aussi généralement sous forme de logiciel à installer sur les ordinateurs et appareils des utilisateurs. La loi américaine sur la protection de la responsabilité des intermédiaires, Section 230, reconnaissant la valeur de ces outils pour permettre aux utilisateurs de décider quel contenu bloquer, inclut spécifiquement des protections pour les entités fournissant ces outils. Voir, par exemple, le Code statutaire des États-Unis, 47 U.S.C. §§ 230(f)(2) et (4).

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de filtres et d'outils contrôlés par l'utilisateur ne doivent pas être tenus responsables du contenu qui transite par leurs outils, ni de la décision de bloquer un contenu spécifique.	Sans protection en matière de responsabilité, les fournisseurs seraient probablement incapables de poursuivre leurs activités, privant ainsi les internautes d'importantes protections en matière de cybersécurité et de spam, ainsi que d'outils de filtrage de contenu.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de filtres et d'outils contrôlés par les utilisateurs ne doivent pas être tenus responsables du traitement du contenu problématique envoyé ou reçu par leurs utilisateurs.	L'objectif de ces filtres et outils est de permettre aux <i>utilisateurs</i> de décider à quel contenu ils souhaitent accéder et quel contenu ils préfèrent bloquer. L'instauration d'une obligation pour les fournisseurs de <i>bloquer</i> le contenu problématique avant qu'il n'atteigne les utilisateurs rendrait l'outil plus complexe (et cela pourrait en outre ne pas être réalisable). Une telle obligation porterait atteinte à l'autonomie des utilisateurs dans le contrôle du contenu qu'ils reçoivent et leur ferait craindre que leurs communications Internet soient surveillées. Ainsi, ils seront probablement réticents à utiliser de tels outils pour sécuriser leurs interactions en ligne, ce qui entraînera une diminution de la cybersécurité globale sur Internet.

6.3 Protection du trafic axée sur l'utilisateur

Description de la fonction : permettre aux utilisateurs individuels de protéger leur trafic Internet contre les cyberattaques, la surveillance (par des entités privées et des gouvernements) et la censure.

Considérations techniques et pratiques : les protections du trafic axées sur l'utilisateur sont celles qui peuvent être appliquées à la discrétion de l'utilisateur pour diriger son trafic Internet sur des chemins et des protocoles réseau fiables. Ces protections peuvent également aider les utilisateurs à masquer leur identité ou leur localisation et ainsi améliorer leur confidentialité et leur sécurité. Ces services de protection du trafic

emploient différentes méthodes techniques, telles que les réseaux privés virtuels (VPN), les services de routage en oignon (notamment le réseau Tor), ainsi que d’autres approches. Dans la plupart des cas, les fournisseurs de ces services ne savent pas — et souvent ne peuvent pas savoir — quel contenu circule sur leurs réseaux.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de protection du trafic axée sur l'utilisateur ne doivent pas être tenus responsables du contenu qui transite par leurs réseaux.	Sans protection en matière de responsabilité, les fournisseurs seraient probablement incapables d'exercer leurs activités, privant ainsi les internautes d'un outil de cybersécurité important les protégeant des cyberattaques, du vol d'identité, de la surveillance et de la censure.
Les fournisseurs de protection du trafic axée sur l'utilisateur ne doivent pas être tenus responsables du traitement du contenu problématique envoyé ou reçu par leurs utilisateurs.	Inspecter et potentiellement bloquer un trafic particulier serait en totale contradiction avec l'intention des fournisseurs de services de protection du trafic axés sur l'utilisateur. Cela nuirait à l'efficacité de ces services, réduisant la confidentialité et augmentant les risques de sécurité pour les utilisateurs.

7 Applications, logiciels, leur développement et leur distribution

Le septième groupe de fonctions intermédiaires comprend les applications informatiques, les programmes et les bibliothèques de logiciels les plus courants utilisés pour l'envoi, la réception et l'affichage des communications Internet. Cette section aborde également les fonctions intermédiaires de distribution d'applications et de logiciels. Les applications et logiciels décrits dans cette section peuvent également inclure des fonctionnalités qui ne sont pas liées aux communications Internet.

En raison du rôle primordial des logiciels dans la facilitation, l'affichage, la protection et le filtrage du contenu sur Internet, certaines lois de protection de la responsabilité des intermédiaires incluent spécifiquement dans leur protection les créateurs et les distributeurs des logiciels utilisés dans les communications Internet. *Voir, par exemple*, le Code statutaire des États-Unis, 47 U.S.C. §§ 230(f)(2) et (4).

Les fonctions de cette section (telles que le développement de logiciels Web et de messagerie électronique) sont étroitement liées aux fonctions décrites dans les sections 3 et 4 ci-dessus (y compris par exemple l'hébergement Web et les communications interpersonnelles). Cette section, cependant, se concentre sur le développement et la distribution du logiciel sous-jacent utilisé pour offrir les services mentionnés ci-dessus, ce qui peut justifier des protections pour les intermédiaires indépendamment de la fourniture des services.

7.1 Logiciel du système d'exploitation

Description de la fonction : fourniture d'un logiciel d'appareil qui permet (1) à l'appareil de se connecter à Internet et d'envoyer ou de recevoir des communications sur Internet, (2) aux utilisateurs de l'appareil de saisir du

contenu à transmettre sur Internet, et (3) aux utilisateurs de l'appareil de recevoir et de visualiser du contenu transmis sur Internet. Ces fonctions font partie des nombreuses autres tâches qu'un système d'exploitation exécute sur un appareil.

Considérations techniques et pratiques : le système d'exploitation d'un appareil exécute des fonctions essentielles qui permettent la transmission, la réception et l'affichage des communications vers et depuis Internet. Pratiquement tous les appareils informatiques disposent d'un système d'exploitation sous-jacent, depuis les appareils grand public comme les ordinateurs, les téléphones mobiles et les téléviseurs jusqu'aux routeurs, commutateurs, serveurs et autres appareils essentiels au fonctionnement d'Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des systèmes d'exploitation ne doivent pas être tenues responsables du contenu Internet transmis, reçu ou affiché via le système d'exploitation.	Les systèmes d'exploitation sont essentiels pour les communications sur Internet et pour Internet lui-même. Imposer la responsabilité du contenu Internet créé ou transmis par les utilisateurs ou d'autres personnes aux fournisseurs de systèmes d'exploitation limiterait considérablement, voire éliminerait, la capacité des utilisateurs à communiquer sur Internet.
Les systèmes d'exploitation ne doivent pas être contraints de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique sur Internet.	La sécurité, la stabilité, la fiabilité et l'intégrité des systèmes d'exploitation sont essentielles à l'accès à Internet et à l'informatique en général. Les contraintes imposées aux systèmes d'exploitation de surveiller ou de bloquer l'accès au contenu porteraient atteinte à la rapidité, à la sécurité et à la fiabilité des fonctions des systèmes d'exploitation.

7.2 Logiciel de navigation et de diffusion Web

Description de la fonction : fournir des logiciels permettant de demander, d'envoyer, de recevoir et d'afficher du contenu à l'aide de protocoles du World Wide Web. Ces actions sont effectuées par deux grands types de logiciels : les logiciels « serveur » Web (qui reçoivent et répondent aux demandes des clients Web pour du contenu en ligne) et les logiciels « clients », le plus souvent des navigateurs Web, qui permettent aux utilisateurs de demander, de recevoir et de visualiser un large éventail de contenus Web. Cette fonction intermédiaire inclut également les « applications » (logiciels exécutés sur les smartphones, les ordinateurs et d'autres appareils) qui récupèrent du contenu à l'aide des protocoles du World Wide Web. Une grande quantité de contenu Internet est distribuée aux utilisateurs grâce aux fonctions des logiciels de serveur Web et de client Web, qui constituent une méthode essentielle pour accéder au contenu en ligne.

Considérations techniques et pratiques : le Web s'appuie sur l'interopérabilité offerte par les protocoles du World Wide Web, le plus souvent le langage de balisage hypertexte, ou HTML, pour le formatage du contenu, et le protocole Hypertext Transfer Protocol Secure, ou HTTPS, pour la demande et la diffusion sécurisées du contenu. Cette interopérabilité constitue l'un des avantages fondamentaux d'Internet : la possibilité pour tout le monde de créer, formater et lier du contenu accessible par des personnes du monde entier. De nombreux sites Web intègrent du contenu provenant de plusieurs sources (par exemple, une vidéo intégrée provenant d'un service de streaming ou une photo provenant d'un service de partage de photos qui apparaît au milieu de la page Web). Les navigateurs Web sont un outil courant pour accéder au contenu Internet et offrent à l'utilisateur un riche ensemble d'options pour contrôler le contenu qui lui est présenté et, dans une certaine mesure, pour protéger sa propre confidentialité et sa sécurité.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des logiciels clients et serveurs Web ne doivent pas être tenues responsables du contenu transmis, reçu ou affiché via le logiciel.	Les logiciels de navigation et de service Web sont essentiels pour permettre aux individus d'accéder au contenu sur Internet. Sans protection en matière de responsabilité, les entités offrant ces fonctions intermédiaires essentielles risqueraient d'être tenues responsables du contenu traité par leur logiciel. Elles pourraient restreindre l'utilisation de leurs outils pour limiter leur responsabilité, par exemple en limitant l'utilisation aux ressources Web qu'elles ont inspectées ou qui ont accepté de les indemniser en cas d'action en justice. Les sites Web et les ressources Web modernes contiennent généralement du contenu dynamique qui peut changer fréquemment et sans préavis. Il est donc pratiquement impossible pour quiconque d'évaluer si le contenu que les utilisateurs souhaitent envoyer ou recevoir pourrait entraîner une responsabilité. Le risque de responsabilité limiterait probablement considérablement le contenu disponible sur le Web et entraverait la capacité des individus à communiquer en ligne.

Approches stratégiques recommandées	Raisons de cette approche
Les logiciels de navigation Web ne doivent pas être contraints de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique sur Internet.	Les contraintes imposant aux logiciels de serveur ou de client Web de surveiller ou de bloquer l'accès au contenu risqueraient de nuire à la rapidité, à la sécurité, à la confiance et à la fiabilité d'Internet. Par exemple, si les navigateurs filtrent ou bloquent le contenu d'une manière incontrôlable et ingérable par l'utilisateur, celui-ci utilisera des outils alternatifs pour modifier ou remplacer son navigateur (ce qui pourrait l'exposer à des logiciels malveillants et à des vols d'identité).
Les logiciels de navigation Web ne doivent pas être contraints de réduire la sécurité pour permettre à des tiers d'examiner et de bloquer le contenu problématique sur Internet.	Des politiques ont été proposées qui obligent les navigateurs à réduire la sécurité globale pour permettre à des tiers d'examiner et de bloquer le trafic qui serait autrement crypté entre le navigateur Web et le serveur Web. Par exemple, l'obligation d'installer des certificats racines contrôlés par le gouvernement¹⁴ permettrait ce type de blocage, mais porterait également atteinte à la sécurité, à la confiance et à la fiabilité d'Internet.

14 Internet Society, « L'île Maurice ne doit pas tomber dans le piège de la surveillance de masse », 28 mai 2021, disponible sur <https://www.internetsociety.org/fr/blog/2021/05/lile-maurice-ne-doit-pas-tomber-dans-le-piege-de-la-surveillance-massive/>.

7.3 Logiciels de messagerie électronique

Description de la fonction : fournir un logiciel pour l’envoi, la réception, le stockage et l’affichage des courriels. Ces actions sont effectuées par deux grands types de logiciels : les logiciels serveurs de messagerie et les logiciels clients de messagerie. Le logiciel serveur exécute les fonctions « back-end » de transmission, de réception et de stockage des courriels, tandis que le logiciel client permet aux utilisateurs d’envoyer, de recevoir, de transférer et d’afficher les courriels. Le courrier électronique est un mécanisme de communication largement utilisé, basé généralement sur un modèle asynchrone, fédéré et de stockage et de transfert, avec des serveurs de messagerie ou des systèmes indépendants transmettant et recevant des courriels pour le compte des expéditeurs et des destinataires.

Considérations techniques et pratiques : l’interopérabilité des serveurs et des clients de messagerie utilisant des protocoles de messagerie acceptés à l’échelle mondiale signifie que les expéditeurs et les destinataires peuvent échanger des courriels quel que soit le logiciel de messagerie ou les fournisseurs de services qu’ils utilisent. Des technologies de cryptage telles que S/MIME et PGP sont disponibles pour sécuriser les courriels de bout en bout pour les utilisateurs qui choisissent de crypter leurs courriels.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des logiciels clients et serveurs ne doivent pas être tenues responsables du contenu transmis, reçu ou affiché via le logiciel.	Les logiciels de messagerie client et serveur sont des outils essentiels pour la communication sur Internet. Sans protection en matière de responsabilité, les développeurs de logiciels risquent d’arrêter de fournir des services de messagerie à de larges groupes d’utilisateurs, limitant ainsi la capacité des utilisateurs à communiquer par courriel sur Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les logiciels de messagerie ne doivent pas être contraints de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique sur Internet.	Les contraintes imposées aux logiciels de messagerie électronique de surveiller ou de bloquer l'accès au contenu porteraient atteinte à la sécurité, à la confidentialité et à la fiabilité du courrier électronique. Cela découragerait également les fournisseurs de messagerie électronique d'offrir à leurs clients la possibilité de sécuriser leurs communications électroniques avec un cryptage de bout en bout.

7.4 Logiciels de messagerie

Description de la fonction : fournir des logiciels pour une large gamme d'outils permettant d'envoyer, de recevoir, de stocker et d'afficher des messages. Ces actions sont effectuées par deux grands types de logiciels : les logiciels « serveur » de messagerie (qui exécutent des fonctions « back-end » de routage des messages et peuvent également recevoir, transmettre et stocker des messages) et les logiciels « client » (qui permettent aux utilisateurs d'envoyer, de recevoir et de visualiser des messages, et peuvent également les stocker). Comme le courrier électronique, la messagerie est un mécanisme de communication largement utilisé.

Considérations techniques et pratiques : il existe une grande variété de systèmes de messagerie, et beaucoup d'entre eux ne sont pas interopérables entre eux (et l'architecture interne des différents systèmes peut être très différente). Certains systèmes de messagerie sont basés sur des normes Internet largement développées, tandis que d'autres ont développé à la fois les logiciels clients et les logiciels serveurs pour prendre en charge la messagerie. Certains systèmes de messagerie prennent en charge la messagerie cryptée de bout en bout, ce qui peut fournir des protections essentielles pour garantir la confidentialité et la sécurité des messages.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des logiciels de messagerie, y compris des logiciels clients et serveurs, ne doivent pas être responsables du contenu transmis, reçu ou affiché via le logiciel.	Les logiciels de messagerie sont un outil de communication essentiel sur Internet, notamment pour une communication sécurisée et privée de bout en bout. Sans ces protections, les fournisseurs de logiciels pourraient craindre d'être tenus responsables du contenu partagé par leurs utilisateurs. Par conséquent, ils pourraient cesser de fournir cette fonction ou se sentir obligés d'affaiblir la sécurité et la confidentialité des communications de leurs utilisateurs en désactivant le cryptage de bout en bout ou en analysant les communications de leurs utilisateurs.
Les logiciels de messagerie ne doivent pas être contraints de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique sur Internet.	Les contraintes imposées aux logiciels de messagerie de surveiller ou de bloquer l'accès au contenu porteraient atteinte à la sécurité, à la confidentialité et à la fiabilité de la messagerie.

7.5 Autres logiciels utilisés pour l'envoi, la réception et l'affichage des communications Internet

Description de la fonction : fournir à une application ou à un programme une fonction secondaire qui offre la possibilité d'envoyer, de recevoir et d'afficher du contenu et des communications. Par exemple, une application qui fournit des informations sur les sentiers de randonnée dans une région géographique pourrait également permettre aux utilisateurs de publier des commentaires sur les sentiers, qui seront envoyés à d'autres utilisateurs.

Considérations techniques et pratiques : il existe une grande diversité de programmes et d'applications qui permettent aux utilisateurs de publier ou d'envoyer du contenu et de recevoir du contenu d'autres personnes.

Approches stratégiques recommandées	Raisons de cette approche
Les entités qui fournissent des applications permettant aux utilisateurs de publier, de transmettre ou de recevoir du contenu ou des communications ne doivent pas être responsables du contenu généré par les utilisateurs qui est transmis, reçu ou affiché via l'application.	Étant donné qu'un grand nombre d'applications permettent aux utilisateurs de transmettre du contenu et des communications, des réglementations formulées de manière générale pourraient facilement englober des centaines, voire des milliers d'applications, dont beaucoup proviennent de start-ups et de petits fournisseurs. Sans protection en matière de responsabilité pour le contenu généré par les utilisateurs, les développeurs et les fournisseurs de telles applications seraient peu enclins à proposer des fonctionnalités de communication supplémentaires dans le cadre de leur service, compromettant ainsi la capacité des individus à communiquer via ces applications et limitant l'innovation et les nouveaux produits sur Internet. Cela pourrait également pousser certains fournisseurs, notamment les plus petits, à quitter le marché.

Approches stratégiques recommandées	Raisons de cette approche
Les applications ne doivent pas être contraintes de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique généré par les utilisateurs sur Internet.	Les contraintes imposant aux entités fournissant des fonctions de communication dans le cadre de leurs logiciels de programme et d'application de surveiller ou de bloquer l'accès au contenu généré par les utilisateurs risqueraient de limiter les communications légitimes et de nuire à la sécurité, à la confidentialité, à la confiance et à la fiabilité d'Internet.

7.6 Développement et distribution de logiciels/d'applications

Description de la fonction : développer et faciliter la distribution de logiciels et d'applications qui prennent en charge la communication de contenu sur Internet. Cette fonction comprend, par exemple, des applications, des logiciels, des bibliothèques de logiciels et des plug-ins logiciels qui transmettent, reçoivent, affichent, transmettent, mettent en cache, recherchent, créent des sous-ensembles, organisent, réorganisent, traduisent, filtrent, autorisent, interdisent, sélectionnent, choisissent, analysent, digèrent du contenu ou facilitent de toute autre manière la communication de contenu sur Internet. Cette catégorie de logiciels et d'applications, ainsi que leur distribution, peut être fournie aux utilisateurs finaux, aux fournisseurs d'infrastructures Internet ou à d'autres participants de l'écosystème Internet. Étant donné que peu de personnes disposent aujourd'hui des connaissances techniques nécessaires pour créer leurs propres applications client et serveur Internet, la capacité de localiser et de récupérer des logiciels écrits par d'autres est une fonction essentielle au fonctionnement d'Internet.

Considérations techniques et pratiques : le développement et la distribution d'outils logiciels permettant aux utilisateurs d'accéder à Internet et de communiquer via celui-ci sont des fonctions essentielles. La fonction de développement et de distribution prend une large gamme de formes, notamment des référentiels de logiciels open source (qui

fournissent certains des logiciels les plus fondamentaux sur lesquels fonctionne Internet), des espaces de travail de développement de logiciels collaboratifs (souvent utilisés pour développer des logiciels open source), des « magasins d'applications » disponibles pour les utilisateurs, des « magasins » dans les navigateurs et d'autres logiciels pour permettre aux utilisateurs d'ajouter des modules complémentaires tiers (par exemple, pour prendre en charge le filtrage du trafic Web, la mise à jour et la correction des logiciels installés) et d'autres approches.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de développement et de distribution de logiciels ne doivent pas être tenus responsables du contenu que les utilisateurs envoient et reçoivent à l'aide du logiciel développé ou distribué.	Sans ces protections en matière de responsabilité, les fournisseurs risqueraient de ne pas être en mesure de fournir ces fonctions en raison de préoccupations concernant la responsabilité potentielle pour le contenu traité par le logiciel développé ou distribué. Cette responsabilité mettrait en péril le fonctionnement d'Internet et nuirait particulièrement aux développeurs de logiciels open-source.¹⁵
Les développeurs et les fournisseurs de logiciels ne doivent pas être contraints de bloquer ou d'interférer de quelque autre manière que ce soit avec le contenu problématique généré par les utilisateurs sur Internet.	De telles contraintes nuiraient à la connectivité mondiale et à l'accès des particuliers aux outils de communication de contenu en ligne. Les contributions aux logiciels open source diminueraient probablement et les logiciels critiques ne seraient pas maintenus, ce qui conduirait à un Internet beaucoup moins sûr et moins fiable.

¹⁵ Internet Society, « La proposition de loi sur la cyber-résilience de l'UE portera préjudice à l'écosystème open source », 24 octobre 2022, disponible sur <https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/>.

8 Environnements complexes

Cette dernière section aborde les sites et services pouvant être perçus comme fournissant une fonction unique et distincte (comme une fonction de « réseau social ») ou comme combinant les fonctions décrites dans les sections précédentes afin de créer un environnement plus riche pour les interactions des utilisateurs. En fin de compte, l'analyse stratégique est très similaire : les entités gèrent du contenu créé par d'autres personnes et, par conséquent, imposer une responsabilité aux entités soulève des préoccupations importantes non seulement pour cette catégorie de fonctions, mais également pour d'autres fonctions intermédiaires critiques d'Internet.

8.1 Réseaux sociaux

Description de la fonction : fournir un environnement de réseautage social qui permet aux utilisateurs de se connecter avec d'autres utilisateurs, ainsi que de créer, partager, échanger, recevoir et interagir avec du contenu créé par d'autres. La section 5.1 du Cadre stratégique¹⁶ aborde plus en détail les réseaux sociaux.

Considérations techniques et pratiques : les sites de réseaux sociaux facilitent la communication, le réseautage et la découverte de contenu entre les utilisateurs, souvent grâce à une combinaison de texte, d'images, de vidéos et de liens. Les fonctions supplémentaires exécutées par les sites de réseaux sociaux incluent la gestion des comptes utilisateurs, l'hébergement et la diffusion de contenu, les algorithmes de recommandation et de personnalisation de contenu, ainsi que les outils d'interaction avec les utilisateurs tels que les « j'aime », les commentaires et les partages. La fonction consistant à offrir un environnement de réseau social peut être appliquée à un éventail très large de sites, et ne se limite pas aux grandes plateformes de réseaux sociaux connus. Par exemple, de nombreux sites offrent aux utilisateurs la possibilité d'interagir les uns

¹⁶ Cadre stratégique Section 5.1, Pleins feux sur : les considérations politiques relatives aux plateformes de « réseaux sociaux » qui hébergent, organisent et modèrent le contenu généré par les utilisateurs.

avec les autres, d'échanger du contenu et des idées et de développer des relations directes avec d'autres utilisateurs. Les fonctions de « réseau social » pourraient facilement s'appliquer à des services de réseaux sociaux destinés à un public restreint ou de niche, ainsi qu'à des sites qui se concentrent sur des communautés d'intérêt spécifiques, comme les coureurs de marathon, les jardiniers, les fans d'une équipe sportive particulière ou les membres d'un parti politique ou d'un club.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de réseaux sociaux ne doivent pas être tenus responsables du contenu créé, publié, envoyé ou reçu par leurs utilisateurs.	Si les entités fournissant des services de réseaux sociaux étaient tenues responsables du contenu généré par les utilisateurs (voir la section 1.5 du Cadre stratégique¹⁷ pour une discussion sur le contenu généré par les utilisateurs), elles pourraient réduire de manière significative les possibilités pour les individus de s'engager dans des échanges en ligne et risqueraient de surcensurer les messages, y compris les discours légitimes, de leurs utilisateurs. L'absence de protections en matière de responsabilité pourrait amener les fournisseurs à restreindre sévèrement la publication de contenu en ligne, limitant ainsi de façon importante la capacité des individus à échanger du contenu sur Internet.

¹⁷ Cadre stratégique Section 1.5, Comparaison de la responsabilité pour le contenu généré par un site et le contenu généré par les utilisateurs.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de réseaux sociaux ne doivent pas être tenus responsables du contenu problématique créé, publié, envoyé ou reçu par leurs utilisateurs.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a publié le contenu, et non au fournisseur de services hébergeant le contenu. Attribuer la responsabilité aux fournisseurs porterait atteinte à leur capacité à diffuser des volumes importants de contenus générés par les utilisateurs.
Lorsque les préoccupations politiques portent sur les actions du fournisseur de services (et non sur le contenu des publications des utilisateurs), toute réponse politique ne doit pas entraver la liberté d'expression des utilisateurs.	Comme mentionné dans la section 5.1 du Cadre stratégique, il existe un large éventail de lois et de politiques qui peuvent être appliquées aux fournisseurs de services de réseaux sociaux sans les rendre responsables du contenu créé ou communiqué par leurs utilisateurs.

8.2 Réseaux fédérés

Description de la fonction : fournir une approche décentralisée pour l'hébergement, le partage, la conservation et la modération de contenu généré par les utilisateurs, y compris par exemple les environnements de réseaux sociaux. Plusieurs serveurs exploités indépendamment peuvent choisir de participer à un réseau fédéré, permettant aux utilisateurs d'interagir sur le réseau fédéré tandis que chaque serveur conserve le contrôle de ses propres données et communautés. Par exemple, contrairement à une communauté de réseaux sociaux contrôlée de manière centralisée, un système de réseaux sociaux fédéré peut permettre à de nombreuses petites communautés indépendantes de se connecter et de partager du contenu dans l'ensemble de l'écosystème

fédéré. Cela peut offrir une expérience similaire à celle des réseaux sociaux, mais avec une approche plus locale de la modération. La section 5.2 du Cadre stratégique¹⁸ traite plus en détail des réseaux fédérés.

Considérations techniques et pratiques : les réseaux sociaux fédérés de serveurs exploités indépendamment, utilisant des protocoles standardisés tels qu'ActivityPub, sont devenus plus populaires. Dans ce type de réseau, chaque serveur indépendant définit ses propres règles et politiques sur, par exemple, la modération, la confidentialité des données et d'autres sujets, tout en participant à un réseau plus large. Le système de messagerie électronique mondial d'Internet est un autre exemple de réseau fédéré, car un grand nombre de serveurs de messagerie gérés indépendamment échangent des courriers électroniques entre eux sans accord préalable. Le système de messagerie permet à chaque entité participante distincte de définir ses propres politiques, par exemple en matière de gestion du spam et de limites de stockage des messages. Les fournisseurs de services fédérés, dont beaucoup sont de petites entreprises ou organisations, permettent aux utilisateurs de maintenir des connexions étendues sur Internet tout en étant en mesure de sélectionner un fournisseur de services qui offre des politiques de confidentialité, de modération et autres qui répondent à leurs préférences.

18 Cadre stratégique Section 5.2, Pleins feux sur : les considérations politiques relatives aux « réseaux fédérés » permettent d'élaborer de nouvelles stratégies visant à renforcer l'engagement des utilisateurs.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services de contenu fédérés ne doivent pas être tenus responsables du contenu créé, publié, envoyé ou reçu par leurs utilisateurs.	Si ces fournisseurs étaient tenus responsables du contenu généré par les utilisateurs, ils risqueraient de ne plus pouvoir, pour des raisons techniques ou financières, continuer à proposer ces services. Les réseaux fédérés, par leur nature, attirent les petites entreprises et même les particuliers en tant que fournisseurs de services. Dans l'éventualité où ces entités ne pourraient plus opérer, les internautes se verraient privés d'outils précieux, permettant non seulement de diversifier les options face aux grandes entreprises de réseaux sociaux, mais aussi de bénéficier d'une modération de contenu plus nuancée.
Les fournisseurs de services de contenu fédérés ne doivent pas être tenus responsables du contenu problématique créé, publié, envoyé ou reçu par leurs utilisateurs.	La responsabilité du contenu problématique devrait être imputée à la personne ou à l'entité qui a publié le contenu, et non au fournisseur qui héberge le contenu. Attribuer la responsabilité au fournisseur fédéré compromettrait le potentiel positif des réseaux fédérés et limiterait considérablement leur disponibilité.

8.3 Environnements de jeu

Description de la fonction : permettre à plusieurs joueurs de se connecter et de jouer à des jeux vidéo ensemble en temps réel sur Internet, tout en leur offrant différentes façons d’interagir et de partager du contenu. La section 5.3 du Cadre stratégique¹⁹ traite plus en détail des environnements de jeu.

Considérations techniques et pratiques : la majorité, sinon la totalité, des environnements de jeu modernes sont connectés à Internet, certains étant entièrement basés en ligne. Les éléments de communication courants des environnements de jeu incluent le chat en ligne et les appels vocaux et vidéo directs entre joueurs. Les écosystèmes de jeu ne sont pas seulement des espaces où les utilisateurs peuvent participer à des jeux en ligne avec d’autres utilisateurs du monde entier : ils offrent également un environnement de réseaux sociaux.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs d’environnements de jeu ne doivent pas être tenus responsables du contenu créé, publié, envoyé ou reçu par leurs utilisateurs.	Si les fournisseurs étaient tenus responsables du contenu des communications de leurs clients, ils pourraient réduire considérablement les opportunités pour les individus d’interagir les uns avec les autres et pourraient surcensurer les messages, y compris les discours légitimes de leurs utilisateurs. L’absence de protection en matière de responsabilité pourrait restreindre considérablement la participation des utilisateurs et la publication de contenu, modifiant et limitant fortement les écosystèmes de jeu.

¹⁹ Cadre stratégique Section 5.3, Pleins feux sur : les considérations politiques relatives à l’écosystème du jeu interactif en ligne.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs d'environnements de jeu ne doivent pas être tenus responsables du contenu problématique créé, publié, envoyé ou reçu par leurs utilisateurs.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a publié le contenu, et non au fournisseur de services hébergeant le contenu. Attribuer la responsabilité à un fournisseur de jeux modifierait probablement la dynamique des jeux et compromettrait la viabilité des systèmes de jeu.

8.4 Environnements de réalité virtuelle et augmentée

Description de la fonction : permettre à plusieurs utilisateurs d'interagir et de collaborer dans un environnement de réalité virtuelle (VR) ou de réalité augmentée (AR) partagé. La section 5.4 du Cadre stratégique²⁰ traite plus en détail des environnements VR et AR.

Considérations techniques et pratiques : bien que les environnements de réalité virtuelle ou augmentée soient apparus plus récemment dans les systèmes de jeu, les systèmes AR et VR s'intègrent de plus en plus à Internet, tout comme les systèmes de jeu. De nombreux environnements VR et AR se connectent directement à Internet et permettent aux utilisateurs d'interagir les uns avec les autres en temps réel. Les environnements VR et AR peuvent, dans certains cas, créer des impacts directs sur le monde physique et sur des personnes qui ne participent pas intentionnellement à un environnement de réalité virtuelle ou augmentée.

²⁰ Cadre stratégique Section 5.4, Pleins feux sur : les considérations politiques relatives aux systèmes de réalité virtuelle et de réalité augmentée connectés à Internet.

Approches stratégiques recommandées	Raisons de cette approche
Les fournisseurs de services d'environnements de réalité virtuelle ou augmentée ne doivent pas être tenus responsables du contenu créé, publié, envoyé ou reçu par leurs utilisateurs.	Si les fournisseurs de VR et AR étaient tenus responsables du contenu des communications de leurs utilisateurs, les fournisseurs de services pourraient réduire considérablement les opportunités pour les individus d'interagir les uns avec les autres en ligne et pourraient surcensurer les messages, y compris les discours légitimes de leurs utilisateurs. Sans protection en matière de responsabilité, les fournisseurs pourraient restreindre sévèrement la publication de contenu en ligne et déterminer quel type de contenu peut être partagé, modifiant et limitant ainsi considérablement le développement continu des technologies et services de réalité virtuelle et de réalité augmentée..
Les fournisseurs d'environnements VR et AR ne doivent pas être tenus responsables du contenu problématique créé, publié, envoyé ou reçu par leurs utilisateurs.	La responsabilité du contenu problématique doit être imputée à la personne ou à l'entité qui a publié le contenu, et non au fournisseur de services hébergeant le contenu. Attribuer la responsabilité aux fournisseurs aurait probablement un impact négatif sur le développement des technologies de réalité virtuelle et augmentée.