

# Les politiques comptent

Glossaire de 75 termes clés pour comprendre les politiques relatives à Internet—2025

Les questions et débats politiques qui aboutissent à des décisions et des lois peuvent sembler trop complexes, trop techniques, dépendantes du contexte ou trop éloignés de la vie quotidienne. Pourtant, les résultats qui en découlent influencent la façon dont nous utilisons Internet et notre capacité à nous connecter, à créer et à nous épanouir en ligne.

Voilà pourquoi tout le monde devrait comprendre les politiques liées à Internet, pas seulement les spécialistes. Avec la bonne approche, chacun peut comprendre ces concepts et faire la différence.

Ce glossaire fournit des explications simples et directes des principaux termes employés dans les politiques liées à Internet, avec une liste de mots en français.

Ce glossaire contribue non seulement à assurer la cohérence et la compréhension dans toutes les langues, mais il permet aussi aux internautes comme vous d'intervenir, de façon proactive ou réactive selon la situation, pour participer à la définition des politiques liées à Internet. Des sources fiables sont mises en lien lorsque nécessaire, afin de fournir un contexte détaillé et une synthèse complète.

Internet est pour tout le monde, et les politiques s'y rapportant concernent tout et chacun. En comprenant ce qui est en jeu et en y prêtant attention, nous sommes mieux préparés à contribuer à façonner, protéger, soutenir, influencer l'avenir d'Internet et du monde numérique qui nous entoure, afin d'en faire une force positive au service de tout le monde, partout au monde.

## A

### TERME

### DÉFINITION

#### Acceptation universelle

Un principe d'internationalisation et d'accessibilité lié à l'avènement d'un Internet multilingue. L'utilisation de l'alphabet latin ne devrait pas être un critère préalable à l'utilisation d'Internet.

**Accès**

La possibilité pour chacun d'accéder à Internet, de rester connecté et de s'en servir comme ressource publique afin de promouvoir le développement économique, social et culturel. Cela comprend, par exemple, l'accès à la connexion, à des contenus adaptés, ainsi qu'aux langues et alphabets locaux.

Plus de deux milliards de personnes n'ont toujours pas accès à Internet de manière fiable et abordable. Voilà pourquoi la communauté mondiale de [l'Internet Society](#) œuvre à [connecter les personnes dépourvues d'accès à Internet](#) afin de combler la fracture numérique.

**Accès universel**

L'une des facettes du droit universel à la liberté d'expression pour les personnes consiste à avoir un accès à Internet inclusif, équitable et abordable, indépendamment de leur lieu de résidence ou de leur origine.

Découvrez l'[histoire inspirante](#) de la communauté reculée d'Ulukhaktok, qui a mis en place le premier réseau communautaire de l'Arctique au cœur de la pire saison des feux de forêt du Canada. Le réseau renforce la résilience locale d'Internet et aide à éviter que les habitants perdent l'accès à Internet lorsqu'ils en ont le plus besoin.

**Accessibilité**

La conception et la régulation des espaces numériques (ainsi que de leurs produits et services) de manière à ce que chacun, y compris les personnes en situation de handicap, les personnes âgées et celles ayant des compétences limitées en lecture ou en numérique, puisse y accéder et les utiliser efficacement.

Comprendre ce qu'est l'accessibilité vous aide à reconnaître quand un espace numérique peut être utilisé par tout le monde. Cela permet aussi de soutenir la conception inclusive et de défendre de meilleurs outils et services, afin que toutes les personnes puissent participer pleinement au monde numérique.

**Adresse de protocole Internet (adresse IP)**

Un identifiant unique attribué à chaque ordinateur et appareil (p. ex. imprimante, routeur, appareil mobile, etc.) connecté à Internet. Il sert à localiser et identifier le nœud lors de la communication avec d'autres nœuds du réseau, afin de permettre aux appareils de communiquer sur Internet.



**Algorithme**

Un ensemble de règles ou d'instructions mathématiques qu'un ordinateur suit pour résoudre un problème ou exécuter une tâche. Il s'agit d'une liste d'opérations simples, précises et univoques appliquées de manière automatique et systématique à une série de signes ou d'objets (définition de l'OCDE). Dans le cas des réseaux sociaux, il s'agit des règles propres à chaque plateforme servant à filtrer, définir et déterminer ce que vous voyez en ligne—actualités, publicités, vidéos et résultats de recherche.

Il est important de comprendre le rôle des algorithmes, car ils façonnent discrètement ce que nous voyons en ligne chaque jour, souvent sans que nous le remarquions, et en savoir plus à leur sujet nous permet de mieux questionner et orienter notre expérience numérique.

**Analyse côté client (CSS)**

[Méthode](#) consistant à faire analyser par des appareils, comme votre ordinateur ou votre téléphone, le contenu avant qu'il ne soit crypté et envoyé, afin de détecter des contenus illégaux.

Cela compromet le cryptage sous prétexte de sécurité et peut transformer votre appareil personnel en outil de surveillance à votre insu.

**Approche du spectre**

Dans le contexte des réseaux communautaires, il s'agit d'une stratégie flexible qui permet différentes façons d'accéder aux signaux et de les gérer, afin que des projets locaux et pilotés par la communauté puissent également créer et maintenir leurs propres réseaux.

Soutenir la promotion d'une approche plus équitable du spectre permet aux habitants des zones éloignées ou mal desservies de créer un Internet local et abordable, plutôt que d'attendre l'arrivée des grandes entreprises.



## TERME

## DÉFINITION

### Approche multipartite

Modèle de gouvernance qui implique la participation et la collaboration de diverses parties prenantes issues de différents secteurs de la société dans les processus décisionnels liés à la gouvernance et à la gestion d'Internet.

Ces parties prenantes comprennent, par exemple, les gouvernements, la communauté technique, la société civile, le milieu universitaire et les utilisateurs finaux. Contrairement aux modèles traditionnels de gouvernance, qui se caractérisent par des structures hiérarchiques descendantes et un contrôle centralisé, l'approche multipartite met l'accent sur l'inclusion, la transparence et la collaboration entre les différents groupes de parties prenantes.

Voici [pourquoi l'approche multipartite fonctionne](#).

### Approches d'octroi de licences (réseaux communautaires)

L'octroi de licences fait référence à l'autorisation légale nécessaire pour exploiter certaines parties d'un réseau communautaire. Chaque pays a ses propres règles, certains offrant davantage de flexibilité aux réseaux communautaires ou proposant des licences abordables, permettant ainsi aux communautés de créer leur propre réseau lorsque les fournisseurs de services ne le font pas. Un octroi de licences favorable permet aux citoyens de s'impliquer, de mettre en place une connectivité abordable et de connecter leurs communautés à Internet.

[Découvrez les approches d'octroi de licences qui contribuent à réduire la fracture numérique.](#)

## B

## TERME

## DÉFINITION

### Blocage de contenu

Il s'agit d'une tendance mondiale et croissante où les gouvernements ou les fournisseurs de services empêchent les internautes d'accéder à certains contenus en ligne, souvent pour des raisons telles que la protection des enfants ou la sécurité nationale. Même si le blocage vise parfois des contenus illégaux, comme ceux liés aux abus sur enfants, il y a peu de consensus international sur ce qui doit ou ne doit pas être bloqué.

Bien que le [blocage de contenu](#) puisse sembler être une solution rapide, il ne supprime pas réellement le contenu d'Internet. Il peut également bloquer involontairement des sites et services légitimes, affectant à la fois les utilisateurs et les entreprises. Ceux qui essaient de contourner les blocages à l'aide d'outils comme les VPN peuvent voir leur confidentialité ou leur sécurité compromises, rendant leur navigation sur Internet moins sûre.



## TERME

## DÉFINITION

### Botnets

Un ensemble d'ordinateurs connectés à Internet (bots) infectés par un logiciel malveillant (malware), permettant à un opérateur (bot herder) de les contrôler à distance via un serveur de commande et contrôle (C&C) pour exécuter des tâches automatisées, comme le vol d'informations ou le lancement d'attaques sur d'autres ordinateurs.

Pour en savoir plus, consultez notre [Fiche sur les politiques publiques : les botnets](#), qui présente les enjeux, les points de vigilance et les principes directeurs.

## C

## TERME

## DÉFINITION

### Confiance en ligne

La confiance que les utilisateurs ont dans le fait qu'Internet—ainsi que les systèmes, plateformes et services qui y sont construits—fonctionnera de manière sécurisée, fiable et en respectant leurs droits, leur confidentialité et leurs données.

Renforcer la confiance par la transparence, la responsabilité, des technologies sécurisées et des règles équitables est essentiel pour garantir que les individus et les entreprises continuent de bénéficier d'Internet.

[En savoir plus sur la nécessité de la confiance et les moyens de l'instaurer.](#)

### Confidentialité

Votre droit de contrôler qui peut voir vos informations personnelles en ligne. La confidentialité signifie également respecter les personnes en traitant leurs données personnelles de manière équitable et transparente, en limitant les informations collectées et utilisées, et en garantissant une gestion responsable et la sécurité des données.

[Consultez les bonnes pratiques en matière de confidentialité et les ressources associées.](#)



**Confidentialité des données**

La protection des données personnelles contre tout accès, utilisation ou divulgation non autorisés. Il s'agit de garantir que les individus contrôlent la manière dont leurs données sont collectées, stockées, traitées et partagées par les organisations ou les entités.

Il existe de nombreux outils en ligne utiles en matière de protection de la confidentialité. Utilisez-les pour protéger votre confidentialité en ligne et pour savoir quelles informations vous partagez lorsque vous naviguez sur Internet.

Tutoriels de l'Internet Society sur l'identité, la confidentialité et la gestion de vos empreintes numériques :

- [Comprendre l'identité numérique et la confidentialité](#)
- [Comprendre vos empreintes numériques](#)

Chaque fois que vous utilisez une application ou un site Web, être conscient de la collecte de vos données et de vos droits vous permet de limiter les risques et de reprendre le contrôle sur vos informations.

**Contenus locaux**

Les contenus générés localement, pertinents et adaptés aux réalités locales d'un pays donné. Ces contenus stimulent la croissance de l'Internet local, régional ou national car ils sont pertinents pour les communautés et les économies de ce pays spécifique.

**Coupe d'Internet**

Perturbation intentionnelle des communications basées sur Internet dans une zone géographique spécifique, rendant les services en ligne inaccessibles ou effectivement indisponibles pour une population spécifique. Cela comprend les tentatives des gouvernements de contrôler le flux d'informations lors d'élections ou d'exams nationaux.

**Cryptage**

Processus qui protège les données contre tout accès non autorisé en les rendant incompréhensibles pour quiconque ne possède pas la clé permettant de les déchiffrer. Une personne non autorisée peut toujours accéder aux données cryptées, mais celles-ci apparaîtront comme des données aléatoires et incompréhensibles.

Vous devriez utiliser et appliquer le [cryptage](#) pour protéger vos données stockées comme vos données transmises. Le cryptage joue un rôle essentiel pour protéger vos activités numériques quotidiennes, comme la banque en ligne ou les achats, en garantissant que vos messages privés restent confidentiels.

Ressource supplémentaire : [Guide du cryptage à l'usage des parents](#).



**Cryptage de bout en bout (E2EE)**

Processus consistant à crypter les données au point de transmission et à ne les décrypter qu'au point de réception.

L'objectif de l'E2EE est de garantir qu'aucun intermédiaire (tel que les serveurs de courrier électronique ou de messagerie) ne puisse accéder au contenu de la communication, même s'il joue un rôle légitime dans la transmission des données entre l'expéditeur et le destinataire.

**Cybercriminalité**

Crimes commis en ligne, tels que le piratage ou les arnaques en ligne.

Selon des chercheurs en sécurité, la cybercriminalité continue de croître avec le nombre d'appareils connectés et l'importance des activités réalisées en ligne. Cela implique des mesures de prévention et de lutte, comme l'application systématique de mesures de sécurité de base (mises à jour et correctifs réguliers), une coopération internationale renforcée en matière de cybercriminalité et l'adoption de lois sur la cybersécurité plus strictes dans de nombreux pays.

**Cyberharcèlement**

Un phénomène en croissance qui touche les enfants et les jeunes. Des études ont montré qu'environ 43 % des enfants sont victimes de cyberharcèlement, et que les filles sont deux fois plus susceptibles d'être ciblées. Les élèves victimes de cyberharcèlement connaissent une baisse de leurs résultats scolaires et présentent davantage de pensées suicidaires que ceux qui n'ont jamais été confrontés à ce type d'agression entre pairs. Il existe un lien entre le cyberharcèlement, la victimisation et l'abandon scolaire, entraînant un risque accru de niveau d'instruction faible et de consommation de substances à l'âge adulte.

La prévention du cyberharcèlement à l'école est essentielle pour protéger les élèves contre cette nouvelle forme de violence.

**Cybersécurité**

Pratique consistant à protéger la sécurité et la confidentialité des réseaux et des programmes contre les attaques numériques en utilisant des solutions techniques et technologiques.

Les cyberattaques visent généralement à accéder à des informations sensibles, à les modifier ou à les détruire, à extorquer de l'argent aux utilisateurs par le biais de ransomwares ou à interrompre les processus commerciaux normaux.

Tous les crimes commis sur Internet ne relèvent pas du terme cybersécurité.



# D

TERME	DÉFINITION
<b>Désinformation</b>	<p>La désinformation consiste en des informations fausses créées volontairement pour tromper les gens. Elle se distingue de la mésinformation, qui désigne des informations fausses partagées par erreur, sans intention de nuire.</p>
<b>Données</b>	<p>Toute information collectée, stockée, traitée ou transmise en ligne, comme votre localisation, vos clics, vos photos ou vos messages.</p> <p>Dans de nombreuses juridictions, il existe une exigence selon laquelle les données doivent être stockées de manière spécifique ou dans certaines zones géographiques, souvent appelée localisation des données, afin de protéger la confidentialité, la sécurité ou de se conformer aux lois locales.</p> <p>Traiter et partager les données sensibles de manière réfléchie est essentiel, d'où l'importance de suivre les bonnes pratiques de <a href="#">gestion responsable des données</a>.</p>
<b>Données à caractère personnel</b>	<p>Toute information qui, associée à d'autres informations, peut être utilisée pour identifier une personne en particulier.</p>
<b>Droit à l'oubli</b>	<p>Le droit légal d'une personne de demander que des informations spécifiques la concernant soient dissociées de son nom, afin d'empêcher toute recherche en ligne. (Par exemple, rechercher « John Smith scandale de fraude » ne permettrait pas de retrouver l'information en question).</p>
<b>Doxing</b>	<p>Pratique consistant à révéler publiquement des informations personnelles ou sensibles sur quelqu'un en ligne (comme le nom complet, l'adresse personnelle ou des détails sur la famille), souvent dans l'intention de nuire ou de harceler.</p> <p>C'est inquiétant, car tout le monde peut être visé, et cela entraîne de vraies répercussions pour la personne concernée. Avoir conscience des conséquences sur la vie privée peut nous aider à réduire considérablement le partage de nos données personnelles, à exiger de meilleures protections numériques et à prendre des mesures actives pour protéger nos données en ligne.</p>



# E

## TERME

## DÉFINITION

### Empreinte numérique

La trace de données laissée par l'activité en ligne d'un individu. Elle comprend toutes les interactions et informations numériques associées à une personne sur diverses plateformes et services en ligne, y compris les réseaux sociaux, les achats en ligne, l'historique de navigation sur le Web, l'utilisation d'applications et les données de localisation. Nos empreintes numériques incluent de plus en plus des données collectées de manière passive par des systèmes tels que la reconnaissance des plaques d'immatriculation, les caméras de surveillance urbaines, les trackers de fitness, les réseaux de téléphonie mobile, et ainsi de suite. Notre empreinte numérique englobe des données qui ne résultent pas simplement de notre propre activité en ligne délibérée.

Bien qu'il soit impossible de n'avoir aucune empreinte numérique, vous pouvez prendre [des mesures simples pour réduire votre empreinte numérique](#).

### Équité numérique

Le concept selon lequel chaque personne devrait avoir une chance égale d'accéder aux technologies numériques, y compris Internet.

# F

## TERME

## DÉFINITION

### Filtrage de contenu

Une pratique consistant à restreindre l'accès des internautes à certains contenus en ligne, généralement illégaux, conformément aux exigences des gouvernements.

Les autorités nationales peuvent adopter des politiques publiques visant à restreindre ou à empêcher l'accès à des contenus tels que des contenus pédopornographiques, des contenus qui violent les lois sur la propriété intellectuelle, menacent la sécurité nationale ou sont interdits pour diverses raisons culturelles ou politiques.



## TERME

## DÉFINITION

**Fondation Internet Society**

C'est la branche philanthropique de l'Internet Society qui finance des initiatives dans le monde entier pour contribuer à rendre Internet ouvert, sûr et accessible à tout le monde.

Elle soutient la communauté Internet mondiale, composée de chercheurs, de développeurs, d'organisations à but non lucratif, d'éducateurs et d'autres acteurs, par le biais d'une douzaine de programmes de subventions qui encouragent l'utilisation d'Internet comme infrastructure technique essentielle, afin d'apporter aux communautés une meilleure éducation, des soins de santé améliorés et davantage d'opportunités économiques, entre autres domaines prioritaires.

**Fracture numérique**

L'écart entre ceux qui ont accès à Internet et ceux qui n'en ont pas.

La fracture numérique est multifacette et englobe de nombreux facteurs contribuant au manque d'accès, tels que la connectivité physique, l'accessibilité financière, la qualité du service et la pertinence.

**Fragmentation**

Division de l'Internet mondial unifié et ouvert en réseaux plus petits et isolés, soumis à des règles, réglementations et normes techniques différentes, qui peuvent ne pas être en mesure de s'interconnecter ou d'interopérer de manière fluide.

Il s'agit d'un enjeu majeur, car la fragmentation d'Internet entraîne le blocage de sites qui affecte votre expérience en ligne. En savoir plus sur les raisons pour lesquelles il faut s'y intéresser.

**G**

## TERME

## DÉFINITION

**Gestion responsable des données**

Les principes éthiques de transparence, d'équité et de respect appliqués au traitement des données sensibles. Elle peut protéger notre confidentialité et notre autonomie, tout en renforçant la confiance nécessaire pour que l'innovation numérique prospère au bénéfice de tout le monde.

[En savoir plus sur les raisons, les enjeux et les bonnes pratiques.](#)



## TERME

## DÉFINITION

**Gouvernance de l'Internet**

Les politiques, règles et processus décisionnels qui déterminent la manière dont Internet est géré et utilisé. Cela implique des acteurs clés tels que les gouvernements, les entreprises privées, la communauté technique et les organisations de la société civile.

La manière dont [Internet est gouverné](#) influence directement son fonctionnement, l'accès qu'en ont les utilisateurs, ainsi que son ouverture, sa sécurité et son inclusivité.

Consultez le [Bilan des 20 ans du Forum sur la gouvernance de l'Internet](#) pour découvrir comment Internet est efficacement gouverné grâce au modèle consultatif et multipartite.

**Gouvernance des données**

Ensemble de règles régissant la collecte, l'utilisation et la protection des données.

L'Internet Society plaide en faveur de cadres de gouvernance des données transparents et responsables, qui protègent la confidentialité et les données personnelles. Pour garantir que les politiques de données soient conçues de manière à protéger les droits des utilisateurs tout en favorisant l'innovation et la confiance dans l'écosystème numérique, elle soutient les normes ouvertes pour la gestion des données et défend l'utilisation du cryptage et d'autres technologies renforçant la sécurité des données. Elle encourage également la coopération internationale pour développer des lois de protection des données, afin de préserver l'intégrité des données tout en assurant l'interopérabilité numérique à l'échelle mondiale.

# H

## TERME

## DÉFINITION

**Hameçonnage**

Une attaque visant à voler votre argent ou votre identité en vous faisant révéler vos informations personnelles, telles que vos numéros de carte de crédit, vos informations bancaires ou vos mots de passe, sur des sites Web qui se font passer pour légitimes.



**Inclusion numérique**

Une approche globale visant à assurer un accès équitable aux services et technologies numériques pour tout le monde (par exemple, les jeunes, les femmes, les personnes âgées, les minorités et les personnes en situation d'handicap).

**Internet**

Un « réseau de réseaux » composé de près de 70 000 réseaux indépendants qui utilisent les mêmes protocoles techniques et décident de collaborer et de se connecter entre eux.

Explorez davantage les bases du [fonctionnement d'Internet, qui gère Internet](#), ainsi que les comportements souhaitables sur Internet et ceux qui sont limités par des contraintes techniques. Faire d'Internet un espace sûr et une force positive est une responsabilité collective et collaborative.

**Internet des Objets (IdO)**

Les objets du quotidien connectés à Internet et dotés de puissantes capacités d'analyse de données, qui promettent de transformer notre façon de travailler, de vivre et de jouer. L'IdO fait l'objet de vifs débats, car il suscite des inquiétudes en matière de surveillance et de respect de la confidentialité (par exemple, les appareils ménagers et électroniques intelligents).

**Internet ouvert**

Un Internet libre, accessible et non contrôlé par un seul groupe.

L'une des principales caractéristiques opérationnelles d'Internet est qu'il est conçu comme une plateforme ouverte favorisant l'innovation et le partage d'idées.

**Internet Society (ISOC)**

Une organisation caritative mondiale dont la mission est de promouvoir et de développer [un Internet ouvert, sûr et digne de confiance pour tout le monde](#).

L'[Internet Society](#) soutient et promeut le développement de certains aspects d'Internet : une infrastructure technique mondiale, une ressource pour enrichir la vie des personnes et une force positive pour la société.

**Internet Society Pulse**

[Pulse](#) est un site Web central qui regroupe des données fiables et précises sur Internet provenant de nombreuses sources, offrant un aperçu de sujets tels que l'impact des coupures d'Internet et la résilience du réseau d'un pays. Il fournit des informations de base et un contexte aux journalistes qui couvrent les questions liées à Internet dans le monde entier.



**Les portes dérobées**

Toute méthode qui permet à un tiers d'accéder à des données cryptées, créant ainsi une vulnérabilité majeure qui affaiblit la sécurité des informations personnelles des utilisateurs et d'Internet dans son ensemble.

[Les portes dérobées](#) peuvent sembler être un outil de sécurité, mais elles peuvent aussi ouvrir discrètement la voie aux abus, à la surveillance ou au piratage. Connaître ce mécanisme vous permet de choisir en connaissance de cause les outils et plateformes auxquels vous faites confiance.

**Lignes d'action (SMSI)**

Lors du Sommet mondial sur la société de l'information (SMSI) des Nations Unies, tenu entre 2003 et 2005, une liste de « lignes d'action » a été établie. Il s'agit d'un ensemble de domaines prioritaires, tels que l'accès, les compétences, la sécurité en ligne et la diversité culturelle, destinés à guider les pays et les organisations dans la construction d'un monde numérique plus inclusif.

Il est utile de les connaître, car elles transforment de grands objectifs mondiaux en étapes concrètes, facilitant la collaboration entre gouvernements, organisations et communautés pour que chacun puisse utiliser et profiter d'Internet.

Cette année, l'Assemblée générale des Nations Unies examinera les progrès réalisés dans la mise en œuvre des lignes d'action du SMSI, faisant de 2025 une étape charnière pour Internet. Découvrez comment [relever au mieux les défis actuels avec une vision tournée vers l'avenir, en prenant appui sur le cadre du SMSI](#).

**Littératie numérique**

Acquérir des compétences numériques et techniques pour utiliser de manière sûre et efficace les technologies numériques, les outils de communication et les réseaux afin de naviguer dans le monde numérique.

Ces compétences permettent aux individus d'utiliser la technologie avec confiance et responsabilité pour atteindre divers objectifs, qu'il s'agisse d'apprendre, de travailler, d'accéder à des services ou de s'engager au sein des communautés.

## TERME

## DÉFINITION

**Localisation des données**

Exigence de stockage des données sur le territoire national.

Les exigences de localisation des données n'améliorent pas la sécurité ; au contraire, elles fragmentent Internet et compliquent la protection des données contre les menaces de cybersécurité.

Les États et le public doivent promouvoir la sécurité et la confidentialité des données par la coopération internationale et des normes de cybersécurité strictes, tout en rejetant les mesures protectionnistes qui isolent les pays, pénalisent les entreprises et limitent la libre circulation de l'information.

**Localisation forcée des données**

Le terme « localisation forcée des données » fait référence aux exigences gouvernementales relatives au contrôle du stockage et des flux de données, et visant à conserver celles-ci au sein d'une juridiction spécifique. Les lois sur la localisation des données, parfois appelées « résidence des données » ou « souveraineté sur les données », visent généralement à conserver les données personnelles ou les données sur des transactions financières au sein d'un pays, où elles sont soumises à la réglementation locale et peuvent être consultées.

Les mesures de localisation forcée des données vont d'une simple obligation de conserver physiquement les données dans leur pays d'origine à une restriction, ou même une interdiction, de les transférer vers d'autres pays. Voici un exemple concret pour illustrer [ce que cela implique pour le Mode de fonctionnement du réseau Internet](#).

# M

## TERME

## DÉFINITION

**Mésinformation**

Des informations fausses ou trompeuses résultant d'une simple erreur dans les faits.

Cela diffère de la désinformation, qui est une information fausse créée et diffusée délibérément dans le but de tromper ou de manipuler, souvent à des fins politiques, financières ou idéologiques.

**Mode de fonctionnement du réseau Internet**

La base d'un Internet fort et prospère qui fonctionne comme il le fait grâce aux [cinq propriétés essentielles](#) qui, combinées, déterminent son fonctionnement et son évolution.



## TERME

## DÉFINITION

**Modération de contenu**

Le processus par lequel des entreprises privées comme Facebook, TikTok ou YouTube surveillent, examinent, suppriment ou signalent du contenu sur leurs plateformes selon leurs propres règles (règles communautaires ou conditions d'utilisation).

Cela affecte ce que vous pouvez publier et consulter en ligne, tout en manquant souvent de transparence et de responsabilité.

# N

## TERME

## DÉFINITION

**Neutralité du réseau**

Également appelée neutralité du Net, il s'agit du principe selon lequel toutes les données en ligne doivent être traitées de manière égale. Bien que les opérateurs de réseau puissent utiliser des techniques de gestion du trafic pour maintenir les performances, il existe des inquiétudes quant au fait que ces pratiques puissent être utilisées pour favoriser certaines données, bloquer des contenus concurrents ou accorder un avantage déloyal, notamment lorsqu'elles sont motivées par des objectifs de revenus.

Ces actions risquent de compromettre le caractère ouvert et transparent d'Internet et de nuire aux utilisateurs finaux.

**Normes open source**

Règles ou directives accessibles au public que tout et chacun peut utiliser, partager ou exploiter librement.

Dans le domaine de la gouvernance d'Internet, ce dernier repose fondamentalement sur l'existence de ces normes ouvertes et non propriétaires. Ces normes sont essentielles pour permettre aux appareils, aux services et aux applications de collaborer sur un réseau vaste et dispersé de réseaux.

Informez-vous [sur les organisations à l'origine des normes ouvertes d'Internet](#), qui veillent à ce que ces normes disposent de spécifications librement accessibles, ne soient pas entravées, bénéficient d'un développement ouvert et évoluent en permanence.



# O

## TERME

## DÉFINITION

### Open Source

Modèle de développement logiciel décentralisé qui encourage la collaboration ouverte en rendant le code source librement accessible pour toute modification ou amélioration par les pairs.

# P

## TERME

## DÉFINITION

### Pacte numérique mondial (PNM)

Une initiative des Nations unies visant à définir des principes communs pour construire un avenir numérique plus sûr, inclusif, ouvert et centré sur l'humain. Il vise à orienter la manière dont les technologies numériques, en particulier Internet, sont gouvernées à l'échelle mondiale.

Ce qui est en jeu, c'est l'avenir d'Internet, car cela pourrait affecter la connectivité numérique, la fragmentation d'Internet, la protection des données, les droits humains en ligne et la promotion d'un Internet de confiance.

### Plaidoyer

Soutenir ou promouvoir activement une cause, ou faire entendre la voix de votre communauté sur des sujets tels que les droits numériques, la sécurité en ligne ou l'accès abordable, grâce à la sensibilisation du public, à l'éducation et à l'engagement auprès des décideurs afin de contrer les menaces législatives sur Internet.

[Comprendre le plaidoyer](#) et la force de votre voix peut nous aider à créer un Internet plus ouvert et inclusif.

### Projet de loi

Une proposition formelle visant à créer une nouvelle loi ou à modifier une loi existante. En ce qui concerne les politiques liées à Internet, un projet de loi peut avoir un impact sur la confidentialité, l'accès, la liberté d'expression ou la sécurité en ligne des utilisateurs. Pour en savoir plus sur les principaux enjeux, consultez ces [fiches sur les politiques publiques](#).

En suivant attentivement les questions politiques et les projets de loi en discussion, vous pouvez intervenir et influencer les décisions avant qu'elles ne deviennent des lois. Exprimer, partager ou relayer des préoccupations, voire signer des pétitions, peut aider à tenir les décideurs responsables.



# R

TERME	DÉFINITION
<b>Rançongiciels</b>	<p>Un type d'attaque par logiciel malveillant qui permet aux pirates d'infiltrer vos données. Voici <a href="#">6 conseils pour vous en prémunir</a>.</p>
<b>Rapport d'évaluation de l'impact sur Internet</b>	<p>Rapports courts produits par l'Internet Society, les membres de notre communauté et d'autres partenaires, qui analysent comment différentes politiques ou nouvelles technologies peuvent affecter les conditions nécessaires à l'<a href="#">existence</a> et au <a href="#">développement</a> d'Internet.</p> <p>La rédaction d'un rapport d'évaluation de l'impact sur Internet vous intéresse-t-elle ? Consultez notre <a href="#">Boîte à outils pour l'évaluation de l'impact sur Internet</a> pour en savoir plus.</p>
<b>Réglementations</b>	<p>Lois ou règles établies par les autorités pour encadrer l'utilisation d'Internet ou le comportement en ligne. Bien que les réglementations visent à répondre aux risques sociaux en ligne, beaucoup d'entre elles sont mal définies ou peu pratiques, ce qui entraîne souvent des conséquences inattendues pour l'infrastructure d'Internet.</p>
<b>Régulation des contenus</b>	<p>La manière dont les gouvernements utilisent des lois, des politiques ou des directives officielles pour définir quels types de contenus sont autorisés ou interdits en ligne. Cela peut limiter l'accès des internautes à certaines informations.</p> <p>Ces questions ont récemment fait l'objet de préoccupations et de débats publics, soulignant le besoin de sensibiliser aux lois et mesures nationales pouvant mettre en danger les droits humains. La censure est la principale préoccupation.</p>



**Responsabilité des intermédiaires**

La question de savoir si les plateformes en ligne ou les prestataires de services tels qu'Amazon, Facebook, WhatsApp ou YouTube peuvent être tenus légalement responsables des contenus publiés par leurs utilisateurs. Ces plateformes ne créent pas le contenu—elles se contentent de l'héberger ou de le transmettre.

Si les plateformes craignent d'être sanctionnées pour le contenu publié par leurs utilisateurs, elles peuvent être amenées à bloquer excessivement du contenu pour se protéger, limitant ainsi ce que les utilisateurs peuvent dire, partager ou voir en ligne.

En comprenant cela, les utilisateurs peuvent soutenir des politiques et réglementations équilibrées qui protègent la liberté d'expression responsable tout en traitant les préjudices réels.

[D'autres ressources à ce sujet sont disponibles en anglais, français, espagnol, portugais et arabe.](#)

**Responsabilité des plateformes**

Réglementation qui tient les plateformes numériques, comme Facebook ou YouTube, responsables de la manière dont elles gèrent les contenus, les données des utilisateurs, les algorithmes et d'autres aspects de leurs services ayant un impact sur la société. Cela aurait un impact négatif sur trois piliers d'Internet : son architecture ouverte composée de composants interopérables et réutilisables ; sa gestion décentralisée et son routage distribué ; et son réseau neutre sur le plan technologique et à usage général.

Cela pourrait entraîner des coûts et des risques accrus pour les opérateurs ou les fournisseurs de services, conduisant à une baisse des investissements, à la réaffectation de ressources critiques à des activités non essentielles, à une limitation de l'innovation et, globalement, à un réseau moins performant. Cela pourrait influencer ce que vous voyez, partagez et croyez en ligne, ainsi que la manière dont vos données personnelles sont traitées.



# S

## TERME

## DÉFINITION

### Sécurité des données

Mesures visant à sécuriser les données en ligne, personnelles ou non, pour garantir leur confidentialité et leur disponibilité.

Cela implique l'utilisation du cryptage et le contrôle des accès pour sécuriser et protéger vos données. Pour en savoir plus : [Bonnes pratiques en matière de sécurité des données et de l'information](#).

### Sécurité des enfants en ligne

Actions légales et réglementaires destinées à assurer la protection des enfants sur Internet.

Les pays utilisent un ensemble de mesures, telles que des filtres de contenu, l'autonomisation des utilisateurs et la coopération entre parties prenantes. Bien que certains soutiennent que le cryptage freine les efforts de protection des enfants en ligne, son rôle crucial dans la protection de la confidentialité et de la sécurité des enfants est souvent négligé dans les débats politiques.

### Sécurité en ligne

Politiques, réglementations et mesures visant à protéger les individus contre des risques tels que le cyberharcèlement, les agressions, les atteintes à la confidentialité et l'exposition à des contenus nuisibles ou illégaux lors de l'utilisation d'Internet.

[La sécurité en ligne](#) a un impact sur l'expérience d'Internet de tout le monde, en particulier celle des enfants, des jeunes et des utilisateurs marginalisés. Il s'agit d'un effort collaboratif, la sécurité sur Internet étant une responsabilité partagée qu'aucune entité ne peut assurer seule.

### Solutions d'accès légal

Un mécanisme qui permet aux autorités gouvernementales d'accéder aux communications ou aux données privées, souvent par le biais de mandats ou d'ordonnances judiciaires, affaiblissant ainsi la sécurité pour tout le monde.

Si ce type d'accès n'est pas strictement encadré, avec une supervision rigoureuse, de la transparence et des limites claires, il peut menacer la confidentialité et la liberté. Il ouvre la voie à la surveillance de masse ou à l'imposition de portes dérobées au nom de termes « légaux » visant à contourner le cryptage.

### Souveraineté numérique

La capacité d'une nation à déterminer son autonomie numérique et les politiques gouvernementales qui en découlent explicitement.

Bien que les besoins et objectifs liés à Internet varient selon les pays, les politiques de [souveraineté numérique](#) incluent des efforts visant à fragmenter Internet en isolant certaines régions du réseau mondial.



## TERME

## DÉFINITION

**Spam**

Tout type de message électronique, de SMS, d'appel téléphonique ou de message indésirable que vous recevez en masse de la part de personnes ou d'entreprises qui veulent faire de la publicité pour leurs produits ou diffuser leurs opinions politiques ou sociales.

**Surveillance**

Consiste à surveiller ou suivre les actions des personnes—souvent à l'aide de caméras, d'outils en ligne ou de données—afin de recueillir des informations les concernant. Cela est souvent réalisé par les gouvernements, mais ils ne sont pas les seuls.

Il ne s'agit pas seulement de « n'avoir rien à cacher » : c'est votre droit à la confidentialité, à donner votre consentement et à contrôler votre vie numérique qui doit être protégé, d'autant plus que des risques sérieux pour la sécurité peuvent survenir en cas de mauvaise utilisation des données.

**Surveillance de masse**

Surveillance non ciblée ou généralisée du comportement ou des communications des individus. Dans le contexte d'Internet, c'est l'objectif de certaines politiques gouvernementales, en particulier dans des sociétés répressives ou autoritaires.

Quelle que soit la justification invoquée (sécurité nationale, lutte contre le terrorisme ou la maltraitance des enfants), la surveillance de masse est, par définition, disproportionnée dans une société démocratique. Cette pratique menace la liberté d'expression en ligne ainsi que la sécurité, la confidentialité et l'autonomie des citoyens.

**U**

## TERME

## DÉFINITION

**Une connectivité de qualité**

Avoir plus qu'un simple accès à Internet. Cela signifie disposer d'un accès à Internet rapide, constant, fiable et sécurisé, permettant aux personnes de participer pleinement au monde numérique pour le travail, l'éducation, la communication ou l'accès aux services.



**TERME****DÉFINITION****Usurpation d'identité**

Une problématique de confidentialité où des criminels volent des identifiants, mots de passe et informations associées afin de se faire passer pour d'autres internautes. Ce qui pousse les criminels à commettre un vol d'identité est souvent un simple gain économique : en volant vos informations et en se faisant passer pour vous, ils peuvent commander des biens et services, détourner des livraisons existantes ou transférer des fonds.

La technologie a peut-être changé, mais les motivations et méthodes de ces voleurs sont toujours les mêmes. Il existe de nombreuses protections légales, comme les lois sur la protection des consommateurs, qui peuvent également s'appliquer aux internautes, la meilleure pratique étant de trouver un équilibre entre la protection de la confidentialité, le développement économique et un Internet ouvert.

**V****TERME****DÉFINITION****Vérification de l'âge**

Le processus permettant de déterminer l'âge d'un utilisateur avant de lui donner accès à certains contenus, plateformes ou services en ligne.

L'expression « contrôle de l'âge » désigne l'ensemble des méthodes de vérification de l'âge. La vérification de l'âge est le terme le plus courant, mais désigne uniquement les contrôles reposant sur une source authentifiée, par exemple une pièce d'identité ou un compte bancaire.

Les gouvernements exigent de plus en plus la vérification de l'âge afin de limiter l'accès à certains types de contenus et de services en ligne. Bien que [ces lois](#) aient souvent pour objectif de protéger les enfants contre les contenus pour adultes, elles peuvent également engendrer des risques en matière d'accessibilité, de confidentialité et de sécurité pour les utilisateurs de tous âges..



# Z

## TERME

## DÉFINITION

### Zero-rating

Lorsque les opérateurs mobiles permettent aux utilisateurs d'accéder à certaines applications ou services sans consommer leur forfait de données. C'est souvent présenté comme un avantage pour les utilisateurs, mais cela implique généralement des accords entre les grandes entreprises technologiques et les opérateurs de télécommunications.

Bien que cela puisse réduire les coûts pour les utilisateurs, cela soulève des inquiétudes concernant la concurrence et la neutralité du Net, c'est-à-dire le principe selon lequel tous les contenus en ligne doivent être traités de manière égale. [Découvrez comment cela se manifeste.](#)

## Internet est pour tout le monde

Fondée en 1992, l'Internet Society est une organisation caritative mondiale qui estime qu'Internet est pour tout le monde. En étroite collaboration avec nos membres, nos groupes d'intérêt spécial, et plus de 120 chapitres à travers le monde, nous contribuons à défendre et à promouvoir les politiques, les normes et les protocoles Internet qui garantissent un Internet ouvert, connecté à l'échelle mondiale et sécurisé.

En savoir plus sur [InternetSociety.org](https://InternetSociety.org)



L'Internet Society est une organisation caritative enregistrée aux États-Unis sous le numéro d'identification fiscale fédérale 501(c)(3) (EIN 54-1650477), reconnue à plusieurs reprises par Charity Navigator avec sa plus haute distinction, une note de 4 étoiles.