

## Splinternet

### Description

Contraction des mots « *split* » et « internet », le splinternet désigne l'internet fragmenté, morcelé. Le mot au pluriel – des splinternets – signifie des fragments d'internet en tant que réseaux non interopérables. Le terme a été inventé en 2001 par Clyde Wayne Crews, chercheur auprès du Cato Institute – think tank libertarien basé à Washington –, pour décrire « *des internets parallèles, gérés comme des univers distincts, privés et autonomes* ». En français, l'expression « balkanisation d'internet » a été utilisée un temps. Aujourd'hui, le terme « fragmentation », à la polysémie plus large, l'emporte. « *Le splinternet est l'opposé d'internet* » résume l'Internet Society (ISOC), association fondée par deux pionniers de l'internet, Vint Cerf et Bob Kahn, qui soutient le développement du réseau dans le monde. Le splinternet évoque la possibilité d'une mutation de l'internet mondial, maillage de réseaux ouverts et connectés les uns aux autres, en un ensemble de réseaux nationaux, somme d'intranets ou juxtaposition de réseaux fermés, déconnectés les uns des autres et contrôlés par des États ou par des entreprises. Deux événements majeurs de l'actualité internationale, la guerre en Ukraine déclenchée en février 2022 et la révolte du peuple iranien depuis la mi-septembre 2022, incitent à parler des internets plutôt que d'internet au singulier.

D'un accès ouvert, sans restriction, et avec un langage commun (les protocoles internet de formatage, de nommage, d'adressage, de routage) permettant à des systèmes et à des machines de communiquer, l'internet comme passage obligé de l'ensemble des activités de vie économique et sociale constitue ce que l'on appelle un « bien commun ». Pour comprendre l'opposition entre splinternet(s) et internet, il faut revenir aux principales caractéristiques de ce dernier, comme le rappelle l'Internet Society :

1. Une infrastructure accessible dotée d'un protocole commun ;
2. Une architecture ouverte, aux composantes interopérables et réutilisables ;
3. Une gestion décentralisée et un système unique de routage distribué ;
4. Des identifiants mondiaux communs ;
5. Un réseau technologiquement neutre et à usage général.

« *L'internet est global par nature, ce qui fait sa résilience. Sa redondance explique sa robustesse. L'image d'une toile d'araignée permet de comprendre ce terme technique : si un fil est coupé, d'autres prennent le relais pour transporter les flux de données* », résume Constance Bommelaer de Leusse, vice-présidente de l'Internet Society. Privé de ces caractéristiques, un splinternet généralisé deviendrait une dystopie, avec des réseaux informatiques à accès et usages contrôlés, empêchant la libre circulation de l'information. Au-delà de cette caricature, la notion de « splinternet » renvoie à la question de souveraineté numérique, la fragmentation des réseaux pouvant servir une forme de protectionnisme alors que l'unité de l'internet sous-entend la mondialisation.

Si l'internet se fragmente, les splinternets ne sont pas tous de même nature, comme le démontre le rapport « *Splinternets* » : *Addressing the renewed debate on internet fragmentation* », publié en juillet 2022 par le Parlement européen. Il fait référence notamment aux travaux de Milton Mueller, professeur à l'Institut de technologie de Géorgie (États-Unis) et cofondateur de l'Internet Governance Project, qui choisit le mot « alignement » pour qualifier cette partition du cyberspace calquée sur les frontières géopolitiques : « *L'alignement de l'internet peut être alimenté par des efforts visant à filtrer les contenus pour les rendre conformes aux lois locales ; à exiger des entreprises qu'elles stockent les données de leurs utilisateurs dans les juridictions locales ; à maintenir le routage de l'internet à l'intérieur des frontières des États ; à exiger des gouvernements ou des utilisateurs qu'ils fassent appel à des entreprises locales plutôt qu'étrangères pour les équipements et les services ; à lier la cybersécurité à la sécurité nationale.* »

Nombreux sont encore les pays où la liberté sur internet n'existe pas ou de façon très partielle, avec un accès limité et un filtrage des contenus ([voir La rem n°59, p.66](#)). Des régimes autoritaires comme la Chine, l'Iran et la Russie ont érigé leurs frontières numériques, jusqu'à reproduire leur politique liberticide dans une version nationale de l'internet. Cependant, le principe d'un internet comme infrastructure mondiale unifiée et ouverte est aujourd'hui débattu, même au sein des démocraties. Au fur et à mesure que l'économie numérique se déploie et, avec elle, la richesse des nations, le principe de la « souveraineté numérique » se retrouve au centre des ambitions. L'Union européenne doit faire face à l'hégémonie des groupes internet américains, la collecte et le contrôle des données étant devenus un facteur essentiel de développement. Au jeune monde numérique en pleine croissance, où les messageries, les réseaux sociaux, les sites web et autres applications traversent les frontières en toute transparence, s'imposent ainsi progressivement des visions politiques et défensives de la souveraineté numérique. Les tracés des splinternets dessinent des enjeux nationaux, politiques, technologiques et commerciaux.

### **Avant le web, les premiers « splinternets »**

Si l'origine la plus évidente de la fragmentation de l'internet reste politique, d'autres enjeux d'ordre juridique ou économique expliquent les possibles divisions du réseau mondial. Ainsi, à l'aube des années 1990, des fournisseurs privés de services en ligne tels que les américains Prodigy, CompuServe, AOL et MSN commercialisaient un « jardin clos » (*walled garden*) de services et de contenus destinés au grand public. N'offrant aucune interconnexion, ces systèmes propriétaires fermés constituaient, en raison de leur

---

modèle économique, un splinternet avant l'heure. Ils n'ont pas survécu à l'avènement en 1993 du World Wide Web avec sa navigation illimitée.

### **Splinternet et autocratie**

Dans la brève histoire de l'internet, la première référence mondiale en matière de splinternet reste, bien sûr, la Chine. Un décret de février 1996, qui lui donne tout pouvoir sur la conception de l'internet, permet au gouvernement chinois de réaliser les deux conditions nécessaires à l'isolement : séparer le pays du reste du monde et couper l'accès de l'intérieur. Afin de créer son propre modèle de l'internet, la Chine a largement investi dans des équipements utiles à la censure : 20 milliards de dollars par an indiquait en 2001 le Centre international des droits de l'homme et du développement démocratique, cité par le magazine *Wired*. Le résultat en est la grande muraille numérique, puissant pare-feu qui filtre tout élément entrant et bloque tout contenu indésirable. Un milliard d'internautes en Chine surfent non pas sur l'internet mondial, mais sur une version gouvernementale de l'internet dont ils doivent se satisfaire : un véritable splinternet.

Contrairement à la Chine, la Russie dispose d'une infrastructure internet qu'elle surveille, certes, mais qui demeure relativement ouverte, notamment parce qu'elle est restée tributaire d'entreprises étrangères pour fonctionner. Avec plus de 3 000 fournisseurs d'accès qui appliquent, chacun à sa façon, les consignes émises par l'autorité de régulation russe Roskomnadzor, la censure s'en trouve trop décentralisée pour être totalement efficace, comme l'explique au magazine *Wired* Doug Madory, spécialiste de la surveillance sur internet. Conformément à la loi nationale sur l'internet de novembre 2019 dans laquelle sont inscrits les grands chantiers numériques, le RuNet, l'internet souverain annoncé par le chef du Kremlin, a pu être déconnecté une première fois avec succès du réseau mondial le 24 décembre 2019. Puis, en mars 2021, la Russie est parvenue à restreindre l'accès à Twitter par une solution centralisée de filtrage du trafic internet. Le conflit avec l'Ukraine pourrait encourager Vladimir Poutine à isoler la population russe du reste du monde et de ses contestations. Depuis la loi du 4 mars 2022 qui verrouille l'information, les Russes n'ont plus accès à Twitter : cette nouvelle opération de censure centralisée démontrerait, selon les experts, que le pays serait bientôt prêt à faire fonctionner son internet « souverain ». Tandis que Twitter riposte en installant une version accessible sur Tor (le réseau qui rend toute connexion anonyme), le 4 et le 7 mars 2022, Cogent Communications et Lumen Technologies, deux entreprises américaines gestionnaires de réseau – qui assurent le trafic entre les fournisseurs de contenus et les fournisseurs d'accès – quittaient le pays, déconnectant délibérément leurs clients russes. Le 6 avril 2022, les États-Unis, l'Union européenne et le G7 prenaient l'engagement que les entreprises qui fournissent un accès internet seraient exemptées des sanctions prises contre la Russie.

Comme la Chine, l'Iran dispose déjà d'un intranet national. Opérationnel depuis 2012, le RNI, réseau national de l'information, assure la continuité des services de messagerie, de moteur de recherche, d'applications et des sites web sélectionnés par le régime islamique (néanmoins soumis à une intense surveillance) quand le pays tout entier est coupé de l'internet mondial. Ce fut le cas dix jours en 2019, après la répression meurtrière des manifestations populaires contre la hausse du prix de l'essence. Depuis le 16 septembre 2022, jour de la mort de Mahsa Amini, 22 ans, tuée par la police des mœurs en raison de son

---

voile « mal mis », la population iranienne subit les conséquences d'un décrochage de l'internet mondial aux heures où se déroulent les manifestations, entre 16 heures et minuit, le but étant d'empêcher la circulation de l'information à l'intérieur et vers l'extérieur du pays. Le débit internet est maintenu faible et intermittent le reste du temps, ou nul dans certaines régions – notamment au Kurdistan, région d'origine de la victime. Déjà privée de Twitter et de Facebook (Meta) depuis 2009, ainsi que de la messagerie Telegram, la population n'a désormais plus accès à Instagram ni à WhatsApp, derniers réseaux sociaux étrangers encore tolérés. Communiquer de façon confidentielle et sécurisée par VPN (*virtual private network*) n'est plus garanti depuis que les autorités disposent d'une technique pour les traquer et les déconnecter. En réaction, les États-Unis ont annoncé le 23 septembre 2022 que certaines interdictions de commerce avec l'Iran portant sur la fourniture de technologies d'accès à internet pourraient être levées, et qu'une dérogation particulière serait accordée à Starlink, le service de connexion internet par satellite lancé par Elon Musk.

Selon l'ONG américaine Freedom House, la liberté sur internet diminue dans le monde en 2022 et ce, pour la douzième année consécutive. La Chine se maintient à la dernière place du classement et la Russie atteint son plus bas niveau historique.

### Splinternet et géopolitique

Aux États-Unis, la fin de l'unité de l'internet a été en quelque sorte proclamée. En août 2020, le président Donald Trump a signé deux décrets afin que soient interdites dans le pays deux applications d'origine chinoise, TikTok et WeChat. Il les accuse de récupérer les données personnelles des Américains au profit du régime de Pékin. « *Les États-Unis, pays qui a financé les premiers développements d'internet, considèrent maintenant des stratégies qui vont le fracturer en morceaux* », alerte l'Internet Society. Tandis que des multinationales comme Ford, Walmart ou Disney s'inquiètent des conséquences pour leur commerce avec la Chine, celui-ci passant notamment par la super app WeChat ([voir La rem n°60, p.71](#)). Un plan baptisé Clean Network, présenté par le secrétaire d'État Mike Pompeo, va jusqu'à proposer d'expulser hors du territoire américain les services de cloud computing des chinois Alibaba, Tencent et Baidu. « *Cela signale pour tous les pays, et pas seulement pour la Chine, que tout service web basé à l'étranger, y compris les services américains, devrait être considéré comme une menace de sécurité nationale. C'est l'abandon complet des principes de l'OMC pour les services et équipements des télécommunications* », écrit le professeur Milton Mueller cité dans *Les Échos*. La même année, le gouvernement indien ira, quant à lui, jusqu'à bannir TikTok de son territoire, à la suite d'un conflit militaire à la frontière avec la Chine. Sous la présidence de Jo Biden, les décrets Trump ont été annulés et les États-Unis ont lancé, en avril 2022, une « Déclaration pour l'avenir de l'internet » qui mobilise une soixantaine de pays – à l'exception, parmi les démocraties, de l'Inde, de l'Afrique du Sud et du Brésil – afin de combattre « *la montée de l'autoritarisme numérique* », de soutenir un internet « *ouvert, libre, mondial, interopérable, fiable et sûr* », et de « *résister aux efforts pour fragmenter l'internet mondial* ».

De son côté, la Commission européenne tente de rattraper son retard par rapport aux États-Unis et à la Chine en présentant en mars 2021 son plan pour une souveraineté numérique d'ici à 2030. L'un des principaux objectifs est la maîtrise des données des pays de l'Union européenne, dont 90 % sont stockées et

---

traitées par des entreprises américaines. Se soustraire à la dépendance vis-à-vis des groupes internet américains n'est plus un sujet de débat : « *Les enjeux sont autant économiques que stratégiques, et maintenant géopolitiques, mais aussi éthiques et démocratiques, ils sont au moins aussi importants pour notre avenir que les enjeux énergétiques* », selon Michel Paulin, directeur général d'OVHcloud, cité par *Le Monde*. En attendant, la Cnil (Commission nationale de l'informatique et des libertés) et la Cour de justice de l'Union européenne ont recommandé au gouvernement de changer de prestataire pour l'hébergement de la plateforme centralisant les principales bases de données médicales françaises (Health Data Hub) ; il s'agit, en effet, de l'américain Microsoft qui est donc soumis aux lois extraterritoriales américaines permettant l'accès aux données par les autorités des États-Unis.

### **Splinternet et monopole**

Le phénomène de consolidation de l'internet, conséquence d'un petit nombre d'entreprises qui contrôlent à la fois les services et les infrastructures, contribue également au risque de fragmentation de l'internet. Le rapport « Splinternets » du Parlement européen décrit de nombreux cas de figure illustrant la contradiction possible entre le maintien de l'unité de l'internet et les intérêts commerciaux des acteurs dominants : leurs décisions génèrent « *des modèles de fragmentation du point de vue de l'utilisateur final* ».

Ainsi, outre ses nombreux services internet, Google – qui possède déjà ses câbles sous-marins et ses centres de données – pourrait, en y ajoutant ses propres protocoles, achever de construire sa propre infrastructure fournissant exclusivement ses clients. Le rapport mentionne aussi deux décisions d'Apple : en 2010, celle de ne plus recourir à la technologie Adobe Flash, entraînant sa disparition en 2020 ; et, en 2016, celle de retirer la possibilité de se connecter à un VPN *via* le protocole PPTP (Point-to-Point Tunneling Protocol), protocole conçu par Microsoft à la fin des années 1990. Un autre exemple illustre le pouvoir de décision des grands acteurs internet au sein des organismes de normalisation, en l'occurrence l'IETF (Internet Engineering Task Force), qui influe sur la rapidité du déploiement d'une technique. Inventé par Google afin de réduire le temps de latence et améliorer la performance de ses propres services, le protocole de transport QUIC a été présenté à l'IETF en 2013 et il est devenu une norme en 2021. « *Le déploiement de QUIC sur certaines des plus grandes plateformes internet souligne la capacité de Google à proposer et à défendre des protocoles conformes à ses propres impératifs économiques et techniques. En effet, une latence réduite dans l'accès aux sites web avait été identifiée comme une opportunité très rentable, étant donné l'effet observé de la latence sur les revenus des sites web* », selon les auteurs du rapport pour le Parlement européen.

À plusieurs reprises, Google a été accusé, notamment par Microsoft, de bloquer ou de dégrader l'accès à ses services web Google Earth ou YouTube à la concurrence. Ainsi, en 2018, Google a procédé à une mise à jour de Blink, un composant (appelé « moteur de rendu ») de son navigateur Chrome, et en a assuré la compatibilité avec l'interface de YouTube, entraînant une dégradation significative de la vitesse de chargement du site de vidéos sur les navigateurs n'étant pas basés sur Blink, notamment Firefox. Ainsi peut-on lire dans le rapport du Parlement européen que « *les composants techniques peuvent être utilisés comme des outils stratégiques par les entreprises technologiques pour contrôler les marchés numériques, et participer à l'élaboration d'un internet moins interopérable et plus fragmenté. Indirectement, ces incompatibilités peuvent aussi conduire à l'obsolescence programmée de protocoles, de dispositifs ou*

---

---

*d'applications, et donc favoriser encore plus la fragmentation ».*

Compte tenu de l'importance majeure du choix des éléments techniques, programmes et protocoles, pour l'interconnexion et l'interopérabilité dans l'évolution du fonctionnement du réseau de réseaux, l'un des défis à relever concernant la fragmentation de l'internet réside, selon les auteurs, dans la maîtrise du rôle prédominant des groupes internet monopolistiques au sein des organismes de normalisation tels que le World Wide Web Consortium (W3C) ou l'Internet Engineering Task force (IETF), d'autant qu'apparaissent les futurs marchés liés à l'intelligence artificielle, à la 5G/6G et à l'internet des objets.

Proposées par des opérateurs télécoms, les offres de connexion à l'internet appelées « *zero rating* » sont un autre exemple de fragmentation « économique » du cyberspace. Forfait limité avec un accès gratuit à un nombre restreint de services, cette formule commerciale constitue une violation du principe de la neutralité du Net. Pour cette raison, le service Free Basics de Facebook (Meta) – qui offre aux pays émergents un internet gratuit mais bridé, avec accès au seul réseau social et à quelques services choisis, quand les concurrents sont payants – a été interdit par l'Agence indienne de régulation des télécoms (TRAI) en décembre 2015.

### **Splinternet et technologie**

Le plus souvent pour cause d'incompatibilité, des normes et des protocoles peuvent être des facteurs de fragmentation de l'internet. Leur obsolescence peut participer également aux divergences de connectivité. Enclenché afin de remédier au manque d'adresses internet, ou adresses IP (une série de chiffres identifiant chaque machine connectée directement au réseau), le passage du protocole IPv4 au protocole IPv6, dont les spécifications ont été définies en 1998, est un bon exemple de « concurrence des normes » selon les auteurs du rapport « Splinternets ». Sur cette question, l'Europe a été en avance par rapport aux États-Unis, qui disposaient d'une large réserve d'adresses IPv4.

Dans une volonté délibérée des gouvernements de ne pas coordonner leurs stratégies, le lent déploiement de l'IPv6 en plus de vingt ans a eu pour conséquence principale le maintien de la prédominance de l'IPv4 au niveau mondial. Le premier frein vers l'IPv6 réside donc dans les coûts engendrés par cette transition pour les opérateurs télécoms et les entreprises, qui doivent assurer le fonctionnement des deux protocoles en parallèle. Le second frein est le recours généralisé au procédé de traduction d'adresse réseau ou NAT (Network Address Translation) par les entreprises et les fournisseurs d'accès. Afin de pallier l'augmentation du nombre de machines à connecter, cette fonction NAT permet d'attribuer une adresse IP publique unique (visible sur internet) à plusieurs adresses IP privées d'un intranet, d'un VPN ou simplement d'une box internet ([voir La rem n°60, p.36](#) et [n°40, p.24](#)). « *La possibilité d'un éclatement de portions de l'internet, reposant exclusivement soit sur IPv4, soit sur IPv6, reste cependant aussi peu probable. Cela signifie néanmoins que la permanence du NAT et des plans de numérotation privés restera une menace pour l'unité de l'internet dans un avenir proche* », écrivent les auteurs. Et, d'un point de vue plus général, ils soulignent l'importance des protocoles techniques comme « *instruments de pouvoir, et leur déploiement une occasion de contester la domination des concurrents commerciaux* ».

Une autre situation où la technologie devient un facteur de fragmentation est lié à l'absence de reconnaissance au niveau mondial des noms de domaine internationalisés (IDN), ces noms de domaine qui sont enregistrés dans des langues aux caractères non latins comme l'arabe, l'hindi, le chinois ou le cyrillique. En effet, nombreuses sont les langues qui utilisent des caractères différents du American Standard Code for Information Interchange (ASCII), langage standard des ordinateurs, et pourtant l'internet mondial n'est pas encore multilingue en l'absence d'un traitement uniforme des noms de domaine en caractères locaux aux différents niveaux du Domain Name System (le DNS traduit les noms de domaine en adresse IP). En 2021, environ 2,5 % de tous les noms de domaine étaient des IDN selon l'IDN World Report, cité dans le rapport du Parlement européen. D'après une étude récente de l'ICANN (Internet Corporation for Assigned Names and Numbers) portant sur une sélection de sites web populaires, seuls 8 % autorisaient l'utilisation d'adresses électroniques internationalisées.

### **Splinternet et démocratie**

Afin de nourrir la réflexion sur le phénomène de fragmentation, le rapport de recherche destiné au Parlement européen décrit quatre scénarios, illustrant chacun une option stratégique pour l'Union européenne : le statu quo, accepter la fragmentation, s'y opposer systématiquement ou bien déterminer les fragmentations qui seraient inévitables.

Inapplicable si l'on tient compte des débats actuels sur la souveraineté, notamment celui portant sur le cadre légal du transfert des données personnelles entre l'Europe et les États-Unis : « *le premier scénario repose sur l'hypothèse que l'internet et le marché numérique sont structurés de manière à éviter la fragmentation. La gouvernance de l'internet resterait essentiellement un processus multipartite, et l'UE interviendrait rarement directement dans les questions relatives aux normes* », ceci à la condition que la question de la fragmentation ne soit pas considérée « *comme une priorité, un risque probable ou un problème public* ».

Accepter la fragmentation : ce deuxième scénario envisage les splinternets comme une caractéristique intrinsèque de l'internet, correspondant aussi bien aux intérêts des États qui souhaitent veiller à leur souveraineté numérique qu'aux intérêts des acteurs privés qui protègent la maîtrise de leurs écosystèmes. Dans le cadre de l'Union européenne, un splinternet représentant les contours de sa souveraineté pourrait, en « *limitant ou interdisant les transferts de données vers des pays tiers, [...] contribuer à limiter considérablement la surveillance étrangère publique ou privée sur les données européennes, y compris les données personnelles ou celles contenant des informations sur des secrets industriels ou commerciaux. En outre, en écartant du marché intérieur les acteurs et services étrangers qui ne respectent pas les règles européennes, de nouveaux services pourraient émerger et être en mesure de rivaliser* ». En revanche, cette fragmentation pourrait par exemple « *entraîner des interruptions de service pour les utilisateurs européens, si les fournisseurs de services, d'équipements ou de logiciels clés qui ne sont pas produits en Europe, comme les navigateurs web, décident de quitter le marché européen* ».

Si elle s'opposait systématiquement au phénomène de la fragmentation comme le prévoit le troisième scénario, l'Union européenne devrait alors revoir certaines de ses réglementations, afin d'encourager le fonctionnement de l'internet ouvert avec des mesures plus strictes en matière d'interopérabilité, ou au contraire des mesures plus souples en matière de transfert de données personnelles et de localisation des données non personnelles. Elle interdirait notamment la pratique du géoblocage (limiter un service à une zone géographique) et soutiendrait des projets open source. Le rapport européen d'ajouter : « *D'une manière générale, ce scénario peut impliquer de s'abstenir d'utiliser la législation pour imposer une conception technique spécifique ou l'utilisation de protocoles spécifiques plutôt que d'autres, et de laisser les acteurs du marché prendre leurs décisions sur la base de la disponibilité de normes ouvertes mondiales.* »

Le quatrième et dernier scénario consiste à envisager la fragmentation comme une exception au principe de l'unité de l'internet, principe qui résulterait des droits fondamentaux et serait par conséquent lié à la liberté d'accès à l'information et la liberté d'expression. Ainsi, les auteurs du rapport reprenant l'expression de la Cour européenne des droits de l'homme (CEDH) formulent le postulat qu'une fragmentation de l'internet, à l'instar d'une limite à la liberté d'expression, ne peut être justifiée que si elle est « *nécessaire dans une société démocratique* ». En vertu de l'article 11 de la Charte des droits fondamentaux de l'Union européenne consacrant la liberté d'expression et d'information, ainsi que l'article 19 de la Déclaration universelle des droits de l'homme affirmant le droit à la liberté d'opinion et d'expression, les auteurs requièrent que « *toute tentative directe de couper l'accès à certaines parties de l'internet apparaît donc comme une limitation de la liberté d'expression* ». Ils considèrent que reconnaître l'unité de l'internet

comme un droit numérique fondamental exige de le placer, à la fois juridiquement et politiquement, au-dessus des lois et règlements. Ainsi, la proposition d'introduire « *la protection d'un internet neutre et ouvert où les contenus, les services et les applications ne sont pas bloqués ou dégradés de manière injustifiée* » dans la future déclaration européenne sur les droits et principes numériques, présentée par la Commission européenne en janvier 2022, constitue pour les auteurs du rapport « *un pas dans la bonne direction* ».

« *Un splinternet n'est pas ce que les optimistes avaient en tête. C'est vrai. Mais c'est ce que nous obtenons. Les États découpent lentement l'internet. L'internet universel, à mon avis, dépendait en fin de compte d'un haut niveau de domination géopolitique et technologique des États-Unis, et je ne vois aucune raison de penser que cette domination se reproduira ou qu'un internet universel peut être réalisé par d'autres moyens. Ce que nous devons faire maintenant, c'est déterminer comment préserver les aspects universels de l'internet qui doivent et peuvent être préservés, et comment faire face en même temps à l'affirmation croissante des États* », analyse l'ancien journaliste devenu consultant Scott L. Malcomson, auteur en 2016 de *Splinternet : How Geopolitics and Commerce Are Fragmenting the World Wide Web*.

Sources :

- « The Web in the World », an interview with Scott L. Malcomson, author of *Splinternet : How Geopolitics and Commerce Are Fragmenting the World Wide Web*, OR Books, orbooks.com, March 17, 2016.
- « TikTok : l'offensive des États-Unis accélère le morcellement d'internet », Florian Dèbes, *Les Échos*, 17 août 2020.
- « La Commission européenne fixe des objectifs pour atteindre la souveraineté numérique d'ici à 2030 », Samuel Stolton, euractiv.fr, 9 mars 2021.
- « Il faut sauver l'internet mondial de la guerre en Europe », Constance Bommelaer de Leusse, Internet Society, lesechos.fr, 9 mars 2022.
- « Ukraine : les réseaux sociaux passent en mode « guerre » », Raphaël Balenieri, Fabio Benedetti Valentini, lesechos.fr, 11 mars 2022.
- « Experts say Russia's war on Ukraine is accelerating the « splinternet ». But what is the splinternet », Sophie Mellor, fortune.com, March 22, 2022.
- « Qu'est-ce que le Splinternet ? Et les raisons pour lesquelles il faut s'y intéresser », Dan York, internetsociety.org, 23 mars 2022.
- « Russia Inches Toward Its Splinternet Dream », Chris Stokel-Walker, wired.com, April 1, 2022.
- « Internet : les États-Unis rassemblent une soixantaine de pays dans une coalition contre la « montée de l'autoritarisme numérique » », Corine Lesnes, lemonde.fr, 28 avril 2022.
- « « Splinternets » : Addressing the renewed debate on internet fragmentation », Clément Perarnaud (Brussels School of Governance – Vrije Universiteit Brussel), Julien Rossi (COSTECH – Université de technologie de Compiègne and PREFICS – Université Rennes 2), Francesca Musiani (CIS – CNRS), Lucien Castex (IRMECCEN – Université Sorbonne Nouvelle), report commissioned and published by the Panel for the Future of Science and Technology (STOA), European Parliamentary Research Service (EPRS), European Parliament, europarl.europa.eu/thinktank, July 11, 2022.

- « À la traîne des Chinois et des Américains, l'Europe rêve de souveraineté numérique », Sophy Caulier, *Le Monde*, 11 septembre 2022.
- « Washington annonce des mesures pour faciliter l'accès des Iraniens à internet », AFP, tv5monde.org, 23 septembre 2022.
- « Les autorités iraniennes limitent massivement l'accès à internet », G.Go, *Le Monde*, 8 octobre 2022.
- « La Russie fait plonger la liberté sur internet dans le monde », AFP, tv5monde.org, 18 octobre 2022.

## Categorie

1. A retenir

### **date créée**

11 janvier 2023

### **Auteur**

francoise