La Lettre Afnic

n°2

Internet made in France

Bienvenue dans la deuxième édition de La Lettre Afnic.
Cette publication trimestrielle, dédiée à la gouvernance technique de l'internet, a pour ambition de vous tenir informés des développements les plus récents, des enjeux stratégiques et des opportunités qui façonnent l'écosystème de l'internet en général, et de la gestion des noms de domaine en particulier. Nous espérons que sa lecture sera enrichissante et inspirante, nourrissant votre réflexion et votre vision de la gouvernance de l'internet.

1 QUAND LES RÉGLEMENTATIONS LOCALES ENTRENT EN CONFLIT AVEC LES RÈGLES DE GOUVERNANCE DE L'INTERNET 02

2 DÉBAT AUTOUR DU SYSTÈME DE NOMMAGE : DNS VS BLOCKCHAIN 05

3 MÉSUSAGES DES PROTOCOLES ET RISQUES DE FRAGMENTATION 07

4 LES PROCHAINS ÉVÉNEMENTS AUXQUELS L'AFNIC PARTICIPE 10

Télécharger la version accessible

Quand les réglementations locales entrent en conflit avec les règles de gouvernance de l'internet

L'exemple d'AFRINIC, le registre internet régional pour l'Afrique, montre comment une décision judiciaire locale peut mettre en péril le développement d'internet sur tout un continent.

Rappel : comment se déroule l'attribution des adresses IP ?

Parce qu'internet est transfrontalier par nature et désormais omniprésent dans tous les aspects de nos vies, qu'ils soient économiques, sociaux ou culturels, la question de sa gouvernance revêt une importance capitale. Pour qu'il reste un réseau ouvert, favorisant la libre circulation de l'information et la connectivité de tous à l'échelle mondiale, des organismes et entités ont été créés pour superviser et coordonner les éléments qui le composent – et notamment les adresses IP.

L'attribution des adresses IP dans le cadre du système d'adressage internet est une des fonctions de l'IANA *(internet Assigned Numbers Authority)*. C'est ce département de l'ICANN qui est responsable de la gestion des réserves d'adresses IP globales et de leur distribution aux registres internet régionaux (RIR).

Au nombre de cinq, ces RIR sont l'ARIN (pour l'Amérique du Nord), RIPE NCC (en Europe), APNIC (en Asie-Pacifique), LACNIC (en Amérique latine et aux Caraïbes) et AFRINIC (en Afrique). Dans leurs fonctions d'allocation des adresses IP, les RIR se voient confier des blocs d'adresses IP par l'IANA, qu'ils vont ensuite attribuer aux FAI (fournisseurs d'accès internet), aux entreprises et aux organisations dans leurs régions respectives.

Cette mission est régie par un certain nombre de règles et de procédures, que chaque RIR applique dans sa propre région pour s'assurer que les adresses IP sont utilisées de manière efficace et équitable – l'une des principales étant que les adresses IP allouées doivent être utilisées pour favoriser le développement de l'internet dans la région spécifiquement couverte par le RIR.

Mais que se passe-t-il lorsque ces règles et politiques de gouvernance de l'internet entrent en conflit avec des lois et réglementations locales ? Nous allons, dans cet article, nous appuyer sur le cas concret d'AFRINIC, le registre internet régional pour l'Afrique, en démêlés avec la justice mauricienne depuis 2021, pour comprendre les conséquences d'un tel scénario.

L'affaire AFRINIC vs. Cloud Innovation

NOTE :
Pour les besoins de l'article, il ne s'agit là que d'un résumé succinct du conflit juridique qui oppose AFRINIC à Cloud Innovation. Ce sont plutôt ses conséquences qui nous intéressent ici. Vous pouvez toutefois consulter une chronologie plus détaillée des litiges sur le site internet d'AFRINIC.

Pour mieux comprendre la situation, rappelons qu'AFRINIC, officiellement reconnu par l'ICANN en 2005, est le dernier registre internet régional à avoir été créé. Il dispose ainsi d'un nombre encore important d'adresses IPv4, en tous cas en comparaison aux autres registres dont les réserves sont épuisées ou en passe de l'être.

Nous sommes donc dans un contexte de pénurie d'adresses IPv4, alors que la demande n'en est pour autant pas affaiblie (voir notre encadré). Il n'est pas rare que des opérateurs internet s'enregistrent en Afrique dans l'unique but de récupérer des adresses IPv4 auprès d'AFRINIC, sans être parfaitement transparents sur la zone géographique où ces adresses IP seront utilisées. C'est exactement ce qu'il s'est passé avec Cloud Innovation, une entreprise basée aux Seychelles mais appartenant à un citoyen chinois.

Après avoir alloué des blocs d'adresses IP à Cloud Innovation, AFRINIC a découvert que l'entreprise ne respectait pas leur Registration Service Agreement

(RSA) : les ressources allouées n'étaient utilisées ni aux fins pour lesquelles les applications avaient été faites, ni dans la région africaine où les services étaient censés être offerts. AFRINIC a alors demandé à Cloud Innovation de remédier à ces violations et, devant leur refus, décidé de bloquer les adresses IP allouées dans le but de les récupérer. En retour, Cloud Innovation a attaqué AFRINIC en justice.

Deux corpus de règles qui s'opposent

Dans ce contentieux, AFRINIC a appliqué les règles de gouvernance de l'internet, qui ont été établies de manière transparente à l'échelle mondiale. Plus exactement, elle a voulu faire respecter le principe de besoin justifié, c'est-à-dire que les adresses IP soient utilisées de manière appropriée et conformément au besoin initialement énoncé ; et la politique de répartition, qui veut que les adresses IP bénéficient, dans le cas d'AFRINIC, au continent africain.

> « Les règles de gouvernance de l'internet font loi, mais elles ne sont pas la loi. »

Or, si les règles de gouvernance de l'internet font loi, elles ne sont pas la loi – contrairement à la loi mauricienne, régissant les relations commerciales et contractuelles des entreprises opérant sur le territoire de l'île. C'est le cadre juridique national dont dépend AFRINIC, puisque son siège social est situé sur l'Île Maurice.

C'est donc devant cette juridiction que s'est retourné Cloud Innovation, et la Cour suprême de l'Île Maurice a appliqué le droit local aux règles d'attribution des adresses IP, au même titre que n'importe quel autre contrat de vente. Cloud Innovation a obtenu non seulement la réactivation de ses adresses IP, mais également des dommages et intérêts, entraînant le gel des comptes bancaires d'AFRINIC.

Si cette saisie conservatoire a été levée au bout de deux mois et demi, les litiges opposant AFRINIC à Cloud Innovation sont toujours en cours. À ce jour, Cloud Innovation a engagé plus de 25 procédures contre AFRINIC devant la Cour suprême de l'Ile Maurice et 2 procédures devant la Cour suprême des Seychelles.

Des conséquences à court terme dévastatrices pour l'internet africain

Il est important de comprendre, dans un premier temps, les conséquences immédiates que la décision de la Cour suprême de l'Île Maurice a eu pour AFRINIC, envoyant des ondes de choc à travers le monde de l'internet.

Le temps qu'a duré la saisie conservatoire, les fonds d'AFRINIC ont été complètement gelés, paralysant ses opérations. Sans accès à ses ressources financières, AFRINIC s'est retrouvée momentanément dans l'incapacité de continuer à fonctionner normalement. Les salaires du personnel, les frais d'exploitation et les investissements nécessaires pour maintenir les services ont tous été mis en suspens, plaçant l'organisation au bord de l'effondrement. Or si l'on considère que les adresses IP sont en quelque sorte la matière première d'internet, on voit bien que l'interruption de service d'allocation sur une zone géographique représenterait une rupture de service qui aurait des conséquences systémiques.

De fait, la décision a mis en danger le principe même de toute nouvelle allocation d'adresses IP par AFRINIC. Cela signifie que le risque est réel qu'aucune nouvelle adresse IP ne puisse être, dans un avenir proche, attribuée aux opérateurs et aux entreprises qui en auraient besoin pour leurs activités en Afrique. Cette situation a entraîné l'amplification d'un marché de seconde main des adresses IPv4. Les opérateurs ont dû se tourner vers des transactions non réglementées pour acquérir des adresses IP auprès d'autres parties disposant d'excédents. Cela a ouvert la porte à des pratiques commerciales opaques et spéculatives, où les prix des adresses IP ont connu une augmentation exponentielle, rendant l'accès à ces ressources encore plus difficile pour les petites entreprises et les pays en développement. Or, l'allocation raisonnée et transparente des adresses IP par les RIR est précisément le remède à ce dévoiement anarchique que représente le second marché des adresses IP.

> « Le risque est qu'aucune nouvelle adresse IP ne puisse être attribuée aux opérateurs et aux entreprises qui en auraient besoin pour leurs activités en Afrique. »

Deux dénouements possibles aux conséquences diamétralement opposées

La bataille judiciaire n'étant toujours pas terminée, la situation entre AFRINIC et Cloud Innovation reste incertaine, avec plusieurs scénarios futurs possibles qui pourraient façonner l'avenir de l'organisation et de la distribution des adresses IP en Afrique.

Premier scénario, AFRINIC gagne son procès en appel, ce qui l'autorise à « récupérer » les adresses IP attribuées à Cloud Innovation. L'affaire fait jurisprudence, AFRINIC retrouve sa position et continue à allouer des adresses IP conformément aux règles de gouvernance de l'internet.

Second scénario, c'est Cloud Innovation qui finit par gagner le procès. La société conserve le droit d'utiliser les adresses IP qui lui ont été allouées et AFRINIC est contrainte de lui verser des dommages et intérêts. Comme il s'agit d'une organisation à but non lucratif – l'attribution d'adresses IP n'est pas un service gratuit, mais les montants facturés servent principalement à couvrir les frais de fonctionnement –, AFRINIC ne dispose pas des fonds nécessaires pour s'en acquitter.

Ici encore, deux sous-scénarios se profilent :

- Première possibilité, AFRINIC est dissoute par ses propres membres. Un nouvel organisme est créé dans un autre pays, les adresses IP gérées par AFRINIC lui sont transférées et il reprend le flambeau de leur attribution sur le continent africain.
- Seconde possibilité, la justice mauricienne déclare que les adresses IP sont des actifs d'AFRINIC et qu'à ce titre, elles peuvent être saisies pour couvrir les dommages et intérêts dus à Cloud Innovation.

Cette dernière éventualité serait la plus catastrophique. En remettant entre les mains d'un acteur privé des dizaines, voire des centaines de milliers d'adresses IPv4, cela priverait l'Afrique de ressources essentielles à son développement numérique et soulèverait, de manière plus générale, des inquiétudes quant à la privatisation d'un bien commun essentiel à l'infrastructure d'internet.

Quelle qu'en soit l'issue, cette affaire aura un impact significatif sur la distribution des adresses IP en Afrique et au-delà. Les décisions prises par les tribunaux et les parties concernées auront des répercussions durables sur la gouvernance de l'internet, la disponibilité des ressources et l'équité numérique.

Le litige opposant AFRINIC à Cloud Innovation met clairement en évidence les dangers des conflits entre les règles de gouvernance de l'internet et les lois locales. On voit ici qu'une seule entreprise, en obtenant en sa faveur une décision de justice locale en contradiction avec les règles établies à l'échelle mondiale pour la gestion d'internet, peut bousculer l'accès à internet, l'innovation et le développement économique de continents entiers. Il soulève également des questions sur la reconnaissance mutuelle des règles d'attribution des adresses IP et la nécessité d'une coordination plus étroite entre la justice, les gouvernements et les acteurs nationaux et internationaux de la gouvernance de l'internet.

La pénurie d'adresses IPv4, un facteur clé dans l'émergence des conflits

Pour mieux appréhender la situation qui a plongé l'AFRINIC dans ses affres juridiques, il est important de comprendre pourquoi les adresses IPv4 ont tant de valeur.

La version la plus récente du protocole de communication qui permet aux appareils de se connecter et de communiquer sur internet est IPv6, également connu sous le nom de protocole internet version 6. IPv6 a été développé pour remplacer progressivement IPv4, la version précédente, largement utilisée depuis les débuts d'internet.

L'une des principales raisons de la création d'IPv6 est la pénurie de plus en plus prégnante d'adresses IPv4 disponibles. Avec la croissance rapide d'internet et du nombre d'appareils connectés, le nombre limité d'adresses IPv4 n'arrive plus à suivre la demande. IPv4 utilise un format d'adresse de 32 bits, permettant ainsi la création de 2^32 (soit environ 4,3 milliards) d'adresses IP ; IPv6 utilise quant à lui un format d'adresse de 128 bits, pouvant générer 2^128, soit 340 undécillions (340 suivi de 36 zéros) d'adresses IP.

Si la transition d'IPv4 vers IPv6 est à terme inévitable, plusieurs freins subsistent aujourd'hui. On compte parmi eux :

- Une certaine forme de résistance au changement, IPv4 dominant le marché depuis des décennies ;
- Le coût et la complexité perçue de la configuration d'un réseau IPv6, qui nécessite des investissements à la fois logiciels, matériels et en formation[1].

C'est pourquoi, pour l'instant, sur de nombreux continents, IPv4 domine toujours. Les réserves d'adresses IPv4 disponibles s'amenuisant, un marché parallèle s'est même créé, où l'adresse IPv4 de seconde main se négocie parfois à prix d'or.

1. Le sujet de la transition vers IPv6 est identifié depuis de nombreuses années en France et en Europe, où une politique volontariste de déploiement d'IPv6 est mise en œuvre. En France, l'ARCEP est l'organisme de référence pour ce suivi. L'Afnic participe à ces actions et propose des formations sur le déploiement d'IPV6.

2

Débat autour du système de nommage : DNS vs Blockchain

Dans cet article, nous nous intéressons aux enjeux liés au choix d'un système de nommage, opposant l'historique DNS au challenger Blockchain. Découvrez les arguments avancés par les partisans de chaque système, notamment en termes de centralisation, de cybersécurité et d'efficacité énergétique, pour une réflexion éclairée sur l'avenir du système de nommage sur internet.

Système de nommage d'internet : sur internet, tout périphérique connecté au réseau est étiqueté par une adresse IP. Il s'agit d'un identifiant unique, qui permet de distinguer un périphérique d'un autre lors de l'envoi et de la réception de messages via le réseau.

Ces adresses IP sont constituées d'une combinaison de chiffres ni très explicite, ni très facile à retenir. Pour cette raison, les noms de domaine ont été créés pour convertir les adresses numériques en noms simples et compréhensibles. Le nom de domaine d'un site internet (par ex. *www.afnic.fr*) est en effet beaucoup plus facile à mémoriser qu'une adresse IP (192.134.5.37).

Pour résoudre un nom de domaine, c'est-à-dire trouver son adresse IP correspondante et pouvoir accéder à ses ressources, le DNS *(Domain Name System)*, le système de nommage d'internet, assure non seulement ses fonctions de mappage entre les noms de domaine et les adresses IP qu'ils représentent, mais également une gestion dynamique, évolutive et hiérarchique de son espace de noms.

Cependant, comme il s'agit d'un des protocoles les plus utilisés pour la résolution de noms de domaine, il est aussi le vecteur de nombreuses attaques sur son infrastructure et a été, à ce titre, identifié comme un point de défaillance unique (ou SPOF pour *Single Point of Failure*) d'internet, nécessitant d'être remplacé. De nombreuses tentatives ont été lancées dans ce sens ces quarante dernières années, la dernière en date étant les systèmes de nommage basés sur la blockchain.

Les arguments avancés par les partisans du remplacement du DNS par la blockchain sont-ils convaincants ? Penchons-nous sur trois des aspects incontournables d'un système de nommage, et ce que le DNS et la blockchain ont à proposer en la matière.

Un système de nommage ne peut être totalement décentralisé

Une architecture centralisée sur internet pose principalement des problèmes de vulnérabilité aux pannes et aux cyberattaques – lorsqu'un système centralisé tombe ou est compromis, c'est tout le réseau qui en pâtit –, ainsi que de risque de censure et de contrôle – lorsqu'un petit nombre d'entités ont le pouvoir de contrôler l'accès aux ressources en ligne, elles peuvent décider quels contenus sont accessibles ou non, et par qui.

Même si le DNS est conçu pour être une architecture distribuée, il suit un modèle de gouvernance hiérarchique et présente une certaine forme de centralisation, avec la racine en haut et les TLD (*Top-Level Domains* ou domaines de premier niveau comme «.fr» ou «.com») en dessous. L'ICANN et les opérateurs de registre déterminent ce qui est ajouté ou retiré du fichier racine ou des TLD.

Pour les partisans d'un système de nommage basé sur la blockchain, l'idée est notamment de se libérer de cette autorité centrale de l'écosystème DNS, comme l'ICANN, les registres et les bureaux d'enregistrement. En utilisant la blockchain, les noms de domaine et adresses IP associées sont diffusés sur un réseau décentralisé. Les mêmes informations sont répliquées sur chaque nœud du réseau, évitant ainsi toute autorité centrale.

Cette logique ne prend toutefois pas en compte que le DNS est finalement également distribué, car les données de la résolution de noms de domaine sont répliquées sur plusieurs serveurs pour des questions de répartition des tâches et de résilience du système.

Elle oublie également que les systèmes de nommage basés sur la blockchain présentent eux aussi une certaine forme de centralisation : par exemple, dans le cas d'ENS *(Ethereum Name Service)*, un équivalent du DNS pour la blockchain, Amazon héberge plus de deux tiers des nœuds du réseau, et près de 50 % d'Ethereum est hébergé aux États-Unis. Cette forme de consolidation de l'architecture peut également laisser craindre une prise de contrôle par l'une ou l'autre de ces deux parties prenantes majoritaires.

Un système de nommage doit être le plus cybersécurisé possible

C'est un fait : le DNS est victime de nombreux types d'attaques de sécurité, comme le déni de service distribué (ou DDoS pour Distributed Denial of Service), le spoofing DNS ou l'amplification. Parce qu'elles sont nombreuses et que leurs répercussions sont potentiellement énormes, on dit du DNS qu'il est un SPOF d'internet – un SPOF se traduisant par la défaillance généralisée d'un système provoquée par une seule source. Cette notion reste toutefois théorique, puisque jamais, depuis le début d'internet, le monde n'a connu de panne généralisée de la résolution DNS, même si des tentatives d'y arriver ont été documentées.

Pour répondre à ces préoccupations, la blockchain propose un stockage et une distribution des mêmes informations sur plusieurs nœuds. En répartissant ces données sur tout le réseau plutôt que dans un emplacement central, la blockchain ne peut pas être définie comme un SPOF. La falsification des données de la blockchain est également plus complexe, car si une copie de la blockchain tombe entre des mains malveillantes, seule cette copie serait compromise et non l'intégralité du réseau.

Toutefois, les extensions de sécurité du DNS, comme DNSSEC *(DNS Security)*, pourraient en grande partie limiter les attaques sur le DNS. Mais le déploiement de DNSSEC à l'échelle mondiale reste problématique, car complexe sur les plans administratifs et techniques. On estime aujourd'hui le pourcentage de validation DNSSEC, c'est-à-dire le mécanisme de sécurité qui vise à assurer l'intégrité et l'authenticité des données DNS, à environ 30 %.

Un système de nommage ne peut pas faire l'impasse sur l'efficacité énergétique

Les systèmes de nommage basés sur la blockchain ont tendance à être moins efficaces sur le plan énergétique que les systèmes de nommage DNS traditionnels.

Les systèmes de nommage basés sur la blockchain nécessitent en effet généralement un mécanisme de consensus (c'est ainsi qu'on appelle un protocole utilisé dans les systèmes distribués pour parvenir à un accord sur l'état du système), qui demande une puissance de calcul élevée et donc une consommation énergétique importante.

Des calculs complexes doivent être effectués pour valider les transactions et sécuriser le réseau, ce qui requiert des ressources énergétiques considérables.

Une unique transaction Ethereum sur ENS représenterait ainsi environ 147 kg d'émissions de CO_2. À titre de comparaison, les émissions annuelles de l'hébergement d'un nom de domaine sont de 153 g, une valeur qui inclut non seulement les émissions liées aux serveurs, mais aussi celles des employés et de l'infrastructure immobilière nécessaires.

Nous avons également vu que les systèmes de nommage basés sur la blockchain reposent sur un principe de décentralisation et de distribution des données. Ils stockent donc généralement l'intégralité de la chaîne de blocs sur chaque nœud du réseau. Cela signifie que chaque nœud de la blockchain doit stocker et maintenir une copie complète de toutes les transactions et enregistrements. En comparaison, le DNS traditionnel utilise un système de hiérarchie où les enregistrements DNS sont répartis sur quelques serveurs, permettant une utilisation plus efficace des ressources de stockage.

Discussion : Le système de nommage basé sur la blockchain suscite un débat passionné quant à sa pertinence pour remplacer le DNS traditionnel. Bien que la décentralisation de la blockchain puisse offrir des avantages en termes de résilience aux pannes et de résistance aux cyberattaques, elle ne garantit pas l'élimination totale de la centralisation. Les systèmes de nommage basés sur la blockchain présentent également des préoccupations en matière d'efficacité énergétique, avec une grosse consommation due aux calculs complexes nécessaires au mécanisme de consensus.

D'un autre côté, le DNS traditionnel a fait face à des problèmes de sécurité, mais des extensions telles que DNSSEC montrent un potentiel pour renforcer la sécurité du système existant. De plus, le DNS bénéficie d'une infrastructure établie et d'une utilisation plus efficace des ressources.

En fin de compte, la décision de remplacer le DNS par la blockchain dépendra des compromis que la communauté internet est prête à faire en termes de centralisation, de cybersécurité et d'efficacité énergétique.

3

Mésusages des protocoles et risques de fragmentation

Tout l'intérêt de l'internet réside dans son universalité : je peux, depuis chez moi ou depuis mon bureau, écrire un courrier électronique à une Bolivienne ou un Taïwanais, consulter un site Web chinois ou ukrainien, bavarder sur un réseau social avec des gens de tous les pays. Le contraire de cette unité, de cette universalité, serait la fragmentation de l'internet, sa séparation en divers ilots qui ne peuvent plus communiquer entre eux. Mais la question est complexe ; qu'est-ce que c'est, exactement, la fragmentation ? Quel rôle jouent les protocoles de l'infrastructure de l'internet dans cette éventuelle fragmentation ?

L'unité de l'internet

C'est la particularité la plus étonnante de l'internet : alors qu'il est composé de réseaux très divers, relevant d'organisations variées, parfois d'entreprises en concurrence directe, et qu'il couvre presque tous les pays, même quand ces pays ont de mauvaises relations, voire sont en conflit ouvert, malgré cela, l'internet reste une entité unique. L'époque où l'on devait choisir d'être sur tel ou tel réseau privé, parce qu'ils ne communiquaient pas entre eux, est bien oubliée.

Cette particularité prend sa source dans deux points :

1. La normalisation technique, c'est-à-dire le fait que certaines techniques doivent être mises en œuvre par tout le monde afin de créer cette unicité. C'est le cas d'IP *(Internet Protocol)*, BGP *(Border Gateway Protocol)* et du DNS *(Domain Name System)*.

2. Le choix par tous les participants de l'unicité : même si l'on n'aime pas ses concurrents et ses ennemis, tout le monde, à part de rares exceptions[1], estime que les avantages de la connectivité l'emportent sur ses inconvénients.

C'est ainsi qu'émerge l'internet : il est composé de dizaines de milliers d'opérateurs différents[2], qui se connectent à un certain nombre d'autres opérateurs et, de proche en proche, tout le monde est connecté. L'utilisation généralisée d'IP pour formater les données transférées sur le réseau, et de BGP pour échanger les informations de routage, c'est-à-dire les informations permettant à chaque opérateur de savoir où il doit envoyer les données, sont parmi les rares technologies qui doivent être mises en œuvre par tout le monde.

En pratique, le DNS, le système qui permet d'obtenir des informations essentielles à partir d'un nom de domaine (comme *fr.wikipedia.org* ou *www.service-public.fr*), est également obligatoire, pour la presque totalité des usages. Sans lui, on aurait certes un internet unifié, mais très peu utilisable.

Le risque de fragmentation

Aujourd'hui, l'internet n'est pas fragmenté[3]. Mais les problèmes sont fréquents et l'unicité de l'internet n'est pas parfaite en permanence. Des forces importantes poussent en effet à la fragmentation. Elles peuvent avoir leur source dans une volonté de privatisation lucrative de parties de l'internet, ou dans la volonté d'acteurs étatiques d'utiliser les protocoles pour « forcer » techniquement des décisions politiques. Pour le premier cas, on peut citer comme exemple les cas où un opérateur refuse de s'appairer (de se connecter et d'échanger des informations de routage) avec un autre,

1. La Corée du Nord, où il n'y a pratiquement pas d'accès internet pour la très grande majorité de la population, est un exemple d'une telle exception.
2. On utilise souvent le sigle AS, pour Autonomous System. En gros, un AS égale un opérateur.
3. On parle bien de l'internet, le réseau, et pas de tel ou tel service qui tourne dessus. Si TikTok est censuré dans un pays, cela ne signifie pas que l'internet dans son ensemble soit fragmenté.

comme le long conflit entre les opérateurs Cogent et Hurricane Electric au sujet de leur appairage en IPv6.

Mais la source principale de fragmentation est plutôt dans la politique. Par exemple, le 1er juin 2023, le gouvernement mauritanien a coupé tous les accès à l'internet depuis un réseau mobile. Dans cet exemple, la coupure est totale. Mais on peut voir des coupures partielles. Un exemple classique est la censure exercée, par divers moyens techniques, par des États. La question ici n'est pas de porter un jugement sur la légitimité ou la légalité de telles interventions, mais sur leurs effets sur l'unicité de l'internet, et sur les moyens existants de repérer ces opérations. Comme ces actions empêchent l'accès à certains services depuis certains pays, on peut les classer dans la rubrique « fragmentation ».

Un point important est l'observation de cette fragmentation : s'il y a fragmentation, comment le savoir et le vérifier ? Heureusement, l'internet dispose d'un grand nombre de mécanismes d'observation et de vérification, gérés par des organisations différentes. On peut citer notamment les sondes Atlas du RIPE[4], le service RIS, le projet NetBlocks et les sondes OONI. Ces données et d'autres sont d'ores et déjà largement étudiées par des chercheurs, par exemple, en France, l'équipe GEODE à l'université Paris 8.

Le cas de BGP

BGP *(Border Gateway Protocol)* est le mécanisme normalisé par lequel les opérateurs internet échangent les informations de routage. Par exemple, un routeur de l'Afnic va utiliser BGP pour annoncer à tous ses pairs, tous les opérateurs auquel il est connecté : « Pour joindre les adresses IP 2001:678:c::/48, tu peux passer par moi ». Transmise de proche en proche, cette information finira par être connue de tout l'internet, qui pourra alors joindre ces adresses.

BGP est parfois qualifié de « protocole politique » car l'émetteur des annonces a un contrôle complet sur ce qu'il annonce, et à qui. BGP permet donc de mettre en œuvre sa politique, chaque opérateur ayant évidemment toute latitude pour décider de l'interconnexion de son réseau. Un opérateur peut donc choisir de se couper de l'internet[5] en arrêtant ses sessions BGP avec ses pairs.

Dans le cas le plus extrême, un opérateur peut complètement couper une liaison. C'est ce qu'ont fait Cogent et Lumen en décidant de « débrancher » tous leurs clients russes en 2022[6]. Nul besoin de BGP pour cela, l'opérateur arrête simplement la ou les interfaces réseau concernées. Notez qu'il peut s'agir d'une décision locale à l'opérateur, ou bien d'une politique décidée par l'État et appliquée par les opérateurs.

On peut aussi citer le cas du risque de fragmentation accidentelle suite à un bogue dans les logiciels, comme cela s'était produit le 2 juin 2023, avec toutefois des conséquences limitées.

Le cas de DNS

DNS *(Domain Name System)* est le mécanisme normalisé par lequel les logiciels obtiennent les informations techniques dont ils ont besoin, pour un nom de domaine donné. Ainsi, si je veux écrire à *CNAF-BP-Noms-de-domaine@cnaf.fr*, le DNS permettra au logiciel de messagerie de savoir que le serveur à contacter est *mel1.cnaf.fr*. Si, en théorie, on peut se passer du DNS pour certains usages, en pratique, pour la quasi-totalité des utilisateurs, sans DNS, il n'y a pas d'internet.

Les noms de domaine sont organisés en un arbre dont le point de départ, la racine, fait régulièrement l'objet de discussions politiques. L'administrateur d'un réseau local peut toujours configurer son réseau de manière à utiliser une autre racine que celle qui est utilisée par presque tout le monde. C'est permis, c'est techniquement facile, mais personne ne le fait[7] car cela serait une forme de fragmentation de l'internet, ce que tout le monde veut éviter. En effet, même si l'internet lui-même restait unifié, une fragmentation du DNS reviendrait, pour presque tous les usages, à une fragmentation de l'internet.

Un autre risque de fragmentation se pose du côté des machines qui interrogent le DNS (on les nomme les résolveurs). Ces machines peuvent être configurées pour mentir sur certains noms, rendant impossible, ou très difficile, l'accès aux services utilisant ce nom. Cette technique est utilisée pour des raisons diverses (blocage des publicités, mise en œuvre de décisions de justice ou d'autorités administratives…). Elle contribue à une fragmentation partielle de l'espace des noms de domaine, et donc de l'internet.

Les conséquences de la fragmentation

L'effet immédiat de la fragmentation est évident : l'impossibilité de contacter telle ou telle personne, ou de visiter tel ou tel service. Mais il y a aussi des effets moins évidents, aussi bien sur le plan technique que sur celui des usages.

4. L'Afnic utilise par exemple ces sondes pour vérifier que le .fr est accessible de tout l'internet, et avec de bonnes performances.
5. Cela peut être choisi de façon temporaire, par exemple en cas de problème de sécurité immédiat.
6. Sur la question de l'application à l'internet de sanctions contre tel ou tel pays, voir le rapport du RIPE *Sanctions and the Internet*.
7. Cela n'interdit évidemment pas des expérimentations comme le projet Yeti.

Sur le plan technique, on note que certaines activités de fragmentation vont ajouter un risque pour la robustesse de l'internet. Par exemple, mettre en place un mécanisme permettant de bloquer l'accès à tel ou tel nom de domaine crée un risque qu'une défaillance de ce mécanisme ne bloque d'autres noms[8], et donc affaiblisse l'internet. Voir à ce sujet le rapport du conseil scientifique de l'Afnic : *Conséquences du filtrage internet par le DNS*.

De même, comme un très grand nombre de services internet dépendent à leur tour d'autres services internet, une fragmentation a souvent des effets plus étendus que ce qui pourrait être prédit. Si l'ensemble des liaisons internet avec les États-Unis était coupé, non seulement on ne pourrait évidemment plus joindre de correspondant aux États-Unis mais, en outre, un grand nombre de services nationaux serait en panne, en raison d'une dépendance[9] à un service aux États-Unis. Ainsi, un domaine enregistré en France mais dont tous les serveurs de noms faisant autorité sur ce domaine sont situés à l'étranger serait hors d'état de fonctionner en cas de fragmentation.

Sur le plan des usages, la fragmentation contribue à dérouter les utilisateurs, à rendre l'utilisation de l'internet plus complexe, et donc à abaisser le niveau de confiance et de sécurité. Par exemple, l'internet repose largement sur la notion d'identificateur unique. Noms de domaine et adresses IP sont censés être uniques au niveau mondial[10]. Cette unicité découle du caractère arborescent de leur allocation (une racine qui délègue à des acteurs qui délèguent à leur tour et ainsi de suite). Si des « racines alternatives » étaient largement utilisées, les utilisateurs ne sauraient jamais, en voyant une adresse Web, si elle fonctionne sur la racine qu'ils utilisent. C'est pour avertir contre ce risque qu'a été écrit le *RFC 2826: IAB Technical Comment on the Unique DNS Root*.

Le concept de racines alternatives, très ancien et qui n'a jamais connu de succès, réapparaît de nos jours sous l'étiquette « Web 3 ». Le terme n'a pas de définition rigoureuse mais, en général, il inclut un enregistrement des noms sur une chaîne de blocs. En soi, c'est une innovation tout à fait légitime mais elle peut mener à une certaine fragmentation. Pour l'instant, il n'y a aucune coordination entre ces différentes racines (une telle coordination serait évidemment politiquement très complexe). Même si les différentes racines sont assez raisonnables pour ne pas utiliser un domaine de premier niveau déjà créé par une autre, il reste qu'un nom en *.quelquechose* pourrait donc ne fonctionner que si l'utilisateur se trouve utiliser une certaine racine. On ne saurait donc jamais, en transmettant une adresse Web à quelqu'un, si elle fonctionnera.

Les couches supérieures

Nous avons vu jusqu'ici l'infrastructure de l'internet, le socle indispensable à toute communication. Mais les utilisateurs n'interagissent pas directement avec l'infrastructure, ils passent par des services. L'internet permet à chacun de créer ses services, et cette décentralisation est importante. Toutefois, il faut constater (et regretter) que beaucoup d'utilisateurs se concentrent sur un petit nombre de services, en général, dans le cas de la France, de nationalité états-unienne. Un blocage appliqué sur tout ou partie de ces services, sans être à proprement parler une fragmentation de l'internet, va, en pratique, couper beaucoup d'utilisateurs de certaines activités.

On notera que ces services sont souvent spécifiques à un pays : c'est bien avant l'invasion de l'Ukraine que les Russes utilisaient bien plus souvent Vkontakte que Facebook, le choix d'un service de communication pouvant dépendre de considérations nationales. Chacun étant libre de choisir ses services de communication, on ne peut pas parler ici de fragmentation[11].

On notera que la diversité des services ne signifie pas fragmentation. Il est intéressant ici d'opposer le monde des messageries instantanées[12] à celui du fédivers. Ce dernier, réseau social décentralisé, repose sur de nombreux services divers, mais qui communiquent tous ensemble, par le biais du protocole normalisé ActivityPub[13]. Le monde des messageries instantanées est au contraire très fragmenté[14].

Enfin, on ne doit pas parler de fragmentation dès qu'il existe des obstacles à la communication, autrement tout serait fragmenté. Le plus évident de ces obstacles est la langue : on ne va pas dire qu'il y a fragmentation du Web parce que je suis incapable de lire une page Web en japonais. De même, contrairement à ce qu'avait prétendu un certain discours, le RGPD (Règlement Général sur la Protection des Données) ne fragmente pas l'internet parce qu'il limite les transferts de données ou alors il faudrait considérer que toute régulation fragmente.

En conclusion

Aujourd'hui, l'internet n'est pas fragmenté, du moins son cœur, son infrastructure. La machine d'Alice peut toujours envoyer un paquet IP à la machine de Bob, si tous les deux le désirent. Mais la situation future est moins claire, des forces puissantes souhaiteraient davantage de contrôle et de fermeture, et on ne peut donc pas garantir que l'internet gardera son unité, qui nécessite une action quotidienne.

8. Un exemple récent est le blocage accidentel de Telegram en mai 2023.
9. Et pas toujours bien connue, ni bien maitrisée.
10. Les experts pointus noteront qu'il y a des exceptions comme les adresses IP privées, mais qui ne changent pas la question fondamentale.
11. Du moins tant qu'il n'y a pas de censure des autres services.
12. Signal, Telegram, WhatsApp, etc.
13. Sur l'interopérabilité des services, on consultera avec profit l'excellent rapport du Conseil National du Numérique.
14. Des protocoles normalisés comme XMPP ou, plus récemment, Matrix, existent mais sont peu utilisés.

Les prochains événements auxquels l'Afnic participe

5 juillet 2023
JCSA23 : Journée du Conseil scientifique de l'Afnic
La Défense, France

6 juillet 2023
Forum sur la gouvernance de l'internet France
Paris, France

11 au 21 juillet 2023
Conseil 2023 de l'UIT
Genève, Suisse

22 au 28 juillet 2023
IETF 117
San Francisco, États-Unis

6 et 7 septembre 2023
OARC 41
Da Nang, Vietnam

18 au 29 septembre 2023
Réunion des groupes de travail du Conseil et des groupes d'experts de l'UIT
Genève, Suisse

8 au 12 octobre 2023
Forum sur la gouvernance de l'internet 2023
Kyoto, Japon

21 au 26 octobre 2023
ICANN 78
Hambourg, Allemagne

afnic
Internet made in France

VOTRE CONTACT

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
Immeuble Stephenson,
1 rue Stephenson,
78180 Montigny-le-Bretonneux