Internet
made in France

La lettre n°7

1

DNS et systèmes de noms alternatifs : la nécessité d'une interopérabilité

Avec l'émergence aujourd'hui de systèmes de noms alternatifs, souvent basés sur des technologies comme la blockchain, internet connaît un nouveau tournant dans son évolution. Ces systèmes, s'affranchissant du DNS traditionnel pour enregistrer et résoudre des noms de domaine, entendent offrir plus de flexibilité. Mais ce faisant, ils sont également la source de nouvelles préoccupations en matière de sécurité et de confusion pour les utilisateurs, remettant plus globalement en cause la stabilité d'internet.

Brève histoire du DNS

Le DNS *(Domain Name System)* constitue un pilier essentiel de l'internet. Il a été mis en place au début des années 1980 pour simplifier l'accès aux ressources en ligne en remplaçant, pour les utilisateurs, les adresses IP – des combinaisons de chiffres – par des noms de domaine faciles à mémoriser (par exemple, *51.178.83.21* versus *www.afnic.fr*).

Grâce à une gouvernance multi-parties organisée et structurée, à une infrastructure fiable et à un mécanisme de résolution des noms de domaine bien rôdé (voir notre encadré), le DNS fonctionne ainsi depuis des décennies de manière sûre, desservant des milliards d'utilisateurs à travers le monde. Il a non seulement soutenu l'expansion fulgurante du web, mais a su s'adapter au fil du temps aux défis technologiques.

Aujourd'hui, de nouvelles technologies, telles que la blockchain, proposent des systèmes de noms de domaine alternatifs. Ces nouveaux systèmes soulèvent des questions importantes en termes de gouvernance et de sécurité, mais aussi de compatibilité technique avec le DNS.

Comment fonctionne la résolution de noms de domaine dans le DNS ?

Le mécanisme de résolution des noms de domaine repose sur une structure hiérarchique. Lorsque qu'un utilisateur saisit le nom de domaine afnic.fr, par exemple, une requête est envoyée à un résolveur DNS, qui va rechercher l'adresse IP correspondante. Si cette information n'est pas déjà dans sa mémoire cache, il va interroger, dans cet ordre :

- **Les serveurs racines,** qui vont lui fournir des informations sur les serveurs de noms faisant autorité pour le TLD, ou domaine de premier niveau, du nom de domaine recherché (dans notre cas le .fr).
- **Les serveurs TLD,** qui vont le diriger vers les serveurs faisant autorité pour le nom de domaine spécifique (ici, afnic.fr).
- **Les serveurs hébergeant le nom de domaine,** qui fourniront en retour l'adresse IP correspondante.

Ce mécanisme de résolution permet de convertir efficacement les noms de domaine en adresses IP, opérant en arrière-plan de manière totalement autonome. Tous les jours, rien que sur le .fr, ce sont ainsi des milliards de requêtes qui sont réalisées et de noms de domaine qui sont résolus, avec une expérience fluide et transparente pour les utilisateurs.

Un système de noms alternatif, qu'est-ce que c'est ?

Les systèmes de noms alternatifs sont des solutions qui visent à remplacer ou compléter le DNS traditionnel en offrant des méthodes différentes pour résoudre des noms de domaine. Ces systèmes peuvent être classés en deux principales catégories.

Les systèmes alternatifs reposant sur le protocole DNS conservent des mécanismes proches du DNS mais sur des infrastructures qui ne dépendent pas de l'ICANN *(Internet Corporation for Assigned Names and Numbers)*. Par exemple, des projets comme OpenNIC offrent des domaines et une résolution de noms en dehors du système de noms de domaine conventionnel. S'ils promettent une plus grande liberté d'expression et moins de censure, ces systèmes soulèvent néanmoins des défis concernant la gestion des racines alternatives et la nécessité d'une interopérabilité avec le DNS pour assurer une résolution de noms fluide et sécurisée.

Les systèmes alternatifs basés sur la blockchain utilisent la technologie blockchain pour créer et résoudre des enregistrements de « noms de domaine »[1]. L'Ethereum Name Service (ENS), par exemple, permet à ses utilisateurs d'enregistrer des « noms de domaine » en .eth et de les utiliser pour accéder à diverses ressources en ligne. L'Ethereum étant à la fois une plateforme de blockchain et une cryptomonnaie, l'ENS avait initialement été conçu pour simplifier les transactions liées aux portefeuilles de cryptomonnaie. Les utilisateurs peuvent ainsi transmettre des « noms de domaine » conviviaux au lieu d'adresses longues et compliquées (généralement une suite de 42 caractères hexadécimaux, par exemple *0x5A2eB3D1F5f39A3d2aF8F9D8c1eC78A2CAbB0B87*) pour recevoir des fonds. Aujourd'hui, l'ENS permet d'associer des identités numériques non seulement à des adresses de portefeuille Ethereum, mais également à d'autres ressources en ligne.

1. Si nous utilisons les guillemets pour « nom de domaine » concernant l'approche de la blockchain, c'est qu'il ne s'agit pas véritablement de noms de domaine, mais d'identifiants qui en ont l'apparence. Et pour cause, les noms de domaine sont des identifiants qui sont liés au « système des noms de domaine ».

Des systèmes de noms alternatifs qui manquent cruellement de gouvernance

Les systèmes de noms alternatifs, bien qu'innovants et prometteurs, ont un grand défaut : aucune gouvernance n'a été clairement définie pour mettre en place les principes, normes, règles et procédures nécessaires à leur bon fonctionnement, à leur évolution pérenne et à la protection des utilisateurs.

> **Sans réelle gouvernance, les systèmes de noms alternatifs affectent la sécurité d'internet et la confiance des utilisateurs.**

A l'inverse, la gouvernance du DNS repose sur un écosystème complexe d'organisations multi-parties, impliquant un panel d'acteurs provenant de secteurs publics et privés, ainsi que de la société civile. Elles incluent notamment l'ICANN, qui coordonne la gestion des noms de domaine et des adresses IP à l'échelle mondiale, ou encore l'IETF *(Internet Engineering Task Force)* et le W3C *(World Wide Web Consortium)*, qui élaborent des standards techniques et des protocoles qui garantissent l'interopérabilité des services internet. Elles sont en grande partie décentralisées dans leur gouvernance opérationnelle, comme le montre le rôle des registres internet de ccTLDs tels que l'Afnic, ou celui des registres internet régionnaux tels que RIPE-NCC.

Cette approche multi-parties assure que différentes perspectives et expertises sont prises en compte dans le processus de décision, ce qui est essentiel pour répondre aux défis de sécurité et de fiabilité de l'internet. De plus, des forums de discussion et des groupes de travail réunissent des représentants de divers pays et secteurs pour échanger des idées et collaborer sur les bonnes pratiques en matière de gouvernance de l'internet. Cette diversité d'organisations et de parties prenantes contribue à la légitimité et à la résilience du DNS, tout en favorisant une évolution d'internet basée sur une régulation et une innovation équilibrées.

Sans réelle gouvernance, les systèmes de noms alternatifs ont un impact significatif sur la stabilité et la sécurité d'internet, comme le soulignent différents rapports du SSAC, le comité consultatif sur la sécurité et la stabilité de l'ICANN, et du Bureau du directeur technique de l'ICANN. On y retrouve notamment ces inquiétudes :

- **Collisions de noms.** La coexistence de plusieurs systèmes de noms entraîne une situation où un même nom peut être résolu différemment selon le contexte, ce qui est une source d'ambiguïté.

  Dans son rapport « Report on the Evolution of Internet Name Resolution », le SSAC souligne que ces noms qui coexistent dans le DNS et dans des systèmes alternatifs peuvent causer des collisions, entraînant des résultats imprévisibles pour les utilisateurs et entamant ainsi leur confiance dans les identifiants internet. C'est d'autant plus vrai qu'aucune régulation uniforme n'encadre ces systèmes alternatifs en termes de préemption, ce qui laisse place à des incertitudes sur la propriété et complique la résolution des litiges.

- **Effets sur l'accessibilité.** L'absence de coordination entre les systèmes de noms alternatifs complique leur utilisation par le grand public. Le rapport « Challenges with Alternative Name Systems » du Bureau du directeur technique de l'ICANN indique que la plupart des utilisateurs d'internet ne connaissent pas l'existence de ces systèmes et ne disposent pas des compétences techniques nécessaires pour y accéder. Par conséquent, un utilisateur peut cliquer sur un lien pointant vers un nom alternatif sans les outils ou configurations adéquats, ce qui entraîne des erreurs d'accès et une expérience utilisateur dégradée.

- **Fragmentation de l'internet.** Le manque de gouvernance pourrait également conduire à une fragmentation de l'internet. Le rapport du SSAC précédemment cité met en garde contre la création d'écosystèmes distincts pour chaque système de noms alternatif, ce qui va à l'encontre de l'idéal d'un internet unifié. L'absence de mécanismes de coordination pourrait créer des silos, rendant la communication et l'interopérabilité entre les systèmes de noms de plus en plus difficiles.

- **Risques de sécurité.** Tout cela accroît également les risques de sécurité. Le rapport « Advice on Name Collision Analysis » du SSAC fait référence aux menaces pesant sur la sécurité et la vie privée des utilisateurs, notant que les technologies comme les codes QR et les URL raccourcies peuvent masquer des noms non fiables ou en dehors du DNS traditionnel, ouvrant ainsi la porte à des actes malveillants. Cela donne aux cybercriminels davantage d'opportunités pour tromper les utilisateurs et compromettre la sécurité des transactions en ligne.

L'approche d'une interopérabilité avec le DNS

Ces problématiques de gouvernance ne sont pas les seules préoccupations liées aux systèmes de noms alternatifs. D'autres considérations plus techniques se font également sentir, appelant à la nécessité d'une meilleure interopérabilité avec le DNS. En effet, la coexistence de ces systèmes de noms alternatifs sans la bonne coordination avec le DNS peut aggraver les difficultés déjà présentes et entraîner des complications supplémentaires, affectant non seulement la stabilité de l'internet mais aussi la capacité des utilisateurs à naviguer de manière fluide et transparente dans l'écosystème numérique.

Cette problématique est d'autant plus pregnante que les systèmes de noms alternatifs utilisant la blockchain « imitent » les noms de domaine. Sans que l'on sache totalement quels problèmes ils règlent, ces nouveaux identifiants se présentent comme des « noms de domaine », ce qui rend leur développement d'autant plus problématique. Mais dès lors qu'ils existent, outre la nécessité impérieuse de développer un cadre de gouvernance multi-acteurs transparent pour leur gestion, la question de pose de leur intéropabilité avec le DNS.

Pour garantir que les systèmes de noms alternatifs puissent fonctionner efficacement tout en préservant la sécurité et la fiabilité d'internet, une approche pourrait consister à développer des normes et bonnes pratiques qui favorisent leur interopérabilité avec le DNS. Des travaux en cours à l'IETF vont justement dans ce sens. Dans l'internet-draft « Integration of DNS Domain Names into Application Environments: Motivations and Considerations » publié en août 2024, le groupe de travail de l'IETF porté par Verisign donne ses recommandations qui incluent, entre autres, la création d'un cadre pour la résolution des noms de domaine qui permette aux utilisateurs de naviguer facilement entre les systèmes de noms alternatifs et le DNS, sans rencontrer de barrières techniques ou de problèmes de compatibilité.

> **Il est impératif de développer des normes et bonnes pratiques qui favorisent l'interopérabilité des systèmes de noms alternatifs avec le DNS.**

En facilitant l'intégration, ces efforts visent à garantir que la transition vers des systèmes de noms alternatifs se fasse de manière fluide et sécurisée, tout en maintenant la stabilité et la sécurité de l'internet. Le draft souligne ainsi l'importance d'un cadre générique qui permettrait à diverses applications, y compris celles basées sur la blockchain, de se conformer à un ensemble d'exigences relatives à la gestion des noms de domaine.

L'internet-draft de l'IETF cite notamment les sept « Qualités d'une intégration DNS », listant les bonnes pratiques à suivre pour garantir une intégration efficace et sécurisée des noms de domaine dans les environnements d'application :

- **1. Prendre en compte le cycle de vie des noms de domaine.** Toute application utilisant le DNS doit prendre en compte les différentes étapes du cycle de vie des noms de domaine, telles que leur expiration ou la modification de leurs clés de sécurité DNSSEC, et évoluer avec leur état dans le DNS.
- **2. Valider le contrôle des domaines.** Pour qu'une intégration DNS soit sécurisée, il est essentiel que seul le titulaire légitime d'un nom de domaine ou une personne autorisée puisse initier cette intégration. Cela signifie qu'il doit y avoir des processus de vérification en place pour s'assurer que toute demande d'intégration provienne d'une source légitime.
- **3. Garantir la complétude des noms de domaine.** L'intégration doit permettre l'utilisation de tout nom de domaine à partir du moment où il respecte les critères techniques. Cela permettrait d'éviter ainsi d'éventuelles exclusions pour des raisons non techniques.
- **4. Anticiper l'évolution du protocole DNS.** Les normes et protocoles DNS ne sont pas figés et évoluent avec le temps. Les intégrations DNS doivent être en mesure de s'adapter à ces évolutions, garantissant ainsi une continuité et une sécurité à long terme.
- **5. Reconnaître que l'attribution des identifiants peut changer.** L'intégration ne doit pas supposer qu'un nom de domaine reste toujours associé à un même titulaire. Des changements (suppression, réenregistrement, transfert…) peuvent en effet survenir qui, s'ils ne sont pas pris en compte, peuvent entraîner une confusion, notamment en attribuant à tort un ancien contenu à un titulaire actuel.
- **6. Considérer la diversité des interfaces de gestion DNS.** L'intégration doit tenir compte des différentes interfaces de gestion DNS disponibles pour les utilisateurs, car elles peuvent varier considérablement. Cela peut compliquer les processus d'activation et de configuration des actions nécessaires à l'intégration DNS, qui doit donc s'assurer d'être la plus intuitive et accessible possible, quelle que soit l'interface utilisée.
- **7. Supporter différents types d'enregistrements DNS.** Les types d'enregistrement des systèmes de noms alternatifs ne sont pas encore largement adoptés, ce qui peut entraîner des problèmes de compatibilité avec les fournisseurs DNS et mener à des échecs de résolution.

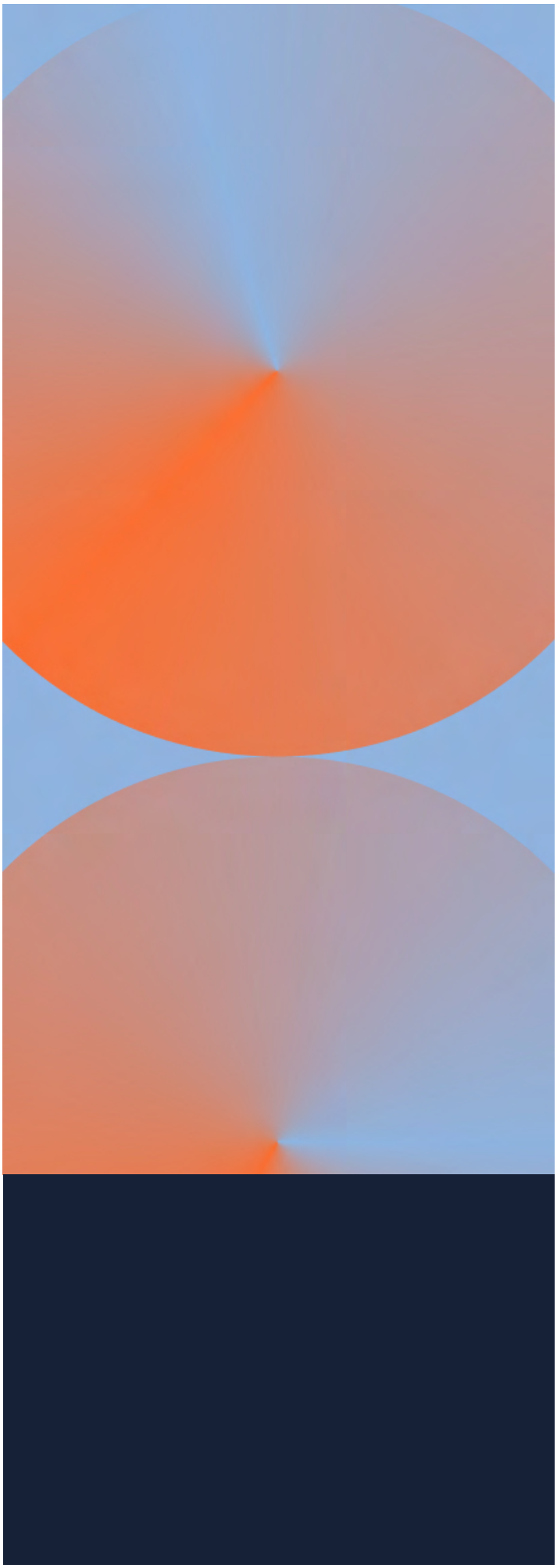
Les intégrations DNS doivent être conçues pour gérer ces échecs, en prévoyant de pouvoir passer par un autre résolveur ou en intégrant des solutions de résolution directement dans l'intégration.

Ces travaux à l'IETF mettent en lumière l'engagement de la communauté technique à explorer des solutions qui favorisent non seulement l'innovation, mais aussi la sécurité et la stabilité de l'internet.

L'arrivée de systèmes de noms alternatifs représente une étape importante dans les discussions sur l'évolution d'internet et des systèmes. Ces nouvelles solutions peinent à expliciter quels problèmes réels du DNS elles entendent surmonter, alors que les questions de sécurité et de gouvernance qu'elles soulèvent sont préoccupantes. Si des initiatives techniques mondiales telles que celles menées à l'IETF sont essentielles pour garantir l'interopérabilité entre le DNS et les systèmes de noms alternatifs, il est tout aussi important que des discussions soient également lancées au niveau national et européen.

La participation active d'acteurs français tels que l'Afnic aux travaux internationaux montre que la France est prête à prendre sa part dans le débat. Ces discussions permettraient non seulement de prendre en compte les spécificités locales, mais aussi de renforcer notre contribution à l'élaboration de solutions pérennes pour l'avenir de l'internet.

Il nous faut aujourd'hui collectivement réfléchir à la manière dont nous pourrions intégrer les systèmes de noms alternatifs tout en garantissant la confiance des utilisateurs et la stabilité du réseau. Car ces systèmes ne peuvent fonctionner en vase clos, ils dépendent indiscutablement d'une interconnexion efficace entre eux et avec le DNS existant. Cela implique de surmonter des défis techniques et de gouvernance, mais aussi de favoriser des échanges constructifs entre toutes les parties prenantes pour construire un avenir numérique toujours plus sûr et inclusif.



02

Publication de la RFC 9620 : intégrer les droits humains dans la conception des protocoles internet

La RFC 9620, publiée en septembre de cette année par l'IRTF *(Internet Research Task Force)*, traite de l'importance d'intégrer les droits humains dans la conception des protocoles internet. Elle propose aux développeurs des recommandations pour s'assurer que leurs technologies prennent en compte ces principes tels que la liberté d'expression, la vie privée et la non-discrimination. Bien que ces recommandations ne soient pas contraignantes, le fait qu'elles aient été formalisées et publiées dans un document officiel témoigne d'une volonté d'une partie croissante de la communauté technique de placer la RSE au cœur des décisions techniques.

S'ils ne sont pas intrinsèquement bienveillants ou malveillants, les protocoles internet, en fonction de l'usage qu'on en fait, peuvent avoir un impact positif ou négatif sur le respect des droits et libertés fondamentaux. Mal conçus ou détournés de leur usage initial, ils peuvent faciliter la surveillance de masse, permettre la censure ou exposer les données personnelles à des abus.

C'est précisément pour répondre à ces risques que la RFC 9620, intitulée *« Guidelines for Human Rights Protocol and Architecture Considerations »*, a été publiée. Son principal objectif est de sensibiliser les concepteurs de protocoles internet au fait que leurs choix techniques peuvent avoir des répercussions directes ou indirectes sur les droits humains. Pour ce faire, la RFC 9620 leur fournit des recommandations concrètes pour intégrer ces considérations dès la phase de conception de leurs protocoles et ainsi réduire le risque que leurs technologies ne deviennent des outils de surveillance, de censure ou de discrimination.

Des recommandations alignées sur les principes des droits de l'Homme

La RFC 9620 s'appuie sur des textes internationaux pour définir les droits humains. Elle fait notamment référence à la Déclaration universelle des droits de l'homme (DUDH) adoptée par les Nations unies en 1948, qui établit les droits et libertés fondamentaux de chaque individu. Elle se base également sur le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels. Adoptés en 1966, ces deux textes détaillent et complètent les dispositions de la DUDH en précisant les obligations des États pour garantir ces droits.

En s'appuyant sur ces textes, la RFC 9620 s'assure que les recommandations fournies aux développeurs de protocoles s'inscrivent dans un cadre reconnu à l'échelle mondiale.

Un héritage éthique et technique des RFC 8280 et 6973

La RFC 9620 complète et met partiellement à jour la RFC 8280 *« Research into Human Rights Protocol Considerations »*, un document explorant comment les protocoles internet peuvent affecter les droits fondamentaux au travers d'études de cas et d'exemples concrets, en reprenant notamment la section qui traitait des considérations liées aux droits humains dans la conception des protocoles internet. Elle s'inspire également, dans son approche « dès la conception », de la RFC 6973 *« Privacy Considerations for Internet Protocols »*, qui se concentre spécifiquement sur les impacts des protocoles sur la vie privée et la protection des données personnelles, et introduit le concept de *« Privacy by Design »*.

L'apport de la RFC 9620 réside dans sa capacité à unifier et élargir ces précédents travaux : elle étend les réflexions amorcées par la RFC 8280 et s'inspire de la méthodologie « dès la conception » de la RFC 6973 pour l'appliquer à la considération des droits humains dès la conception des protocoles internet. C'est au fond une approche très « RSE » de l'IRTF, même si cette dernière peut avoir des limites, dans la mesure où elle pourrait affaiblir l'approche de neutralité technologique en faisant faire de la « politique » aux protocoles, même pour les meilleures raisons.

21 recommandations pour des protocoles internet plus éthiques

Dans son contenu, la RFC 9620 propose ainsi un ensemble de 21 recommandations *(guidelines)* pour les concepteurs de protocoles internet. Ces recommandations invitent les développeurs à se poser les « bonnes questions » lors de la conception ou de l'amélioration de leurs protocoles afin d'anticiper les éventuels impacts sur des droits humains.

On y retrouve des réflexions sur les intermédiaires, par exemple, qui peuvent intercepter ou altérer les communications, ce qui pose des risques pour la vie privée, la protection des données ou la liberté d'expression. Les concepteurs sont ainsi invités à se demander si leur protocole nécessite des nœuds intermédiaires et dans quelle mesure les utilisateurs peuvent les contrôler, avec des questions guides comme : *« Le protocole impose-t-il ou encourage-t-il l'intervention d'intermédiaires ? »*, *« Ces intermédiaires peuvent-ils affecter la confidentialité ou la sécurité des communications ? »*.

Ici, nous avons une illustration des limites potentielles de cette approche. Elle semble induire que tout intermédiaire présente un risque, ce qui est vrai, mais déduit en creux que le mieux serait peut-être de s'en passer, ce qui est contestable. Tout n'est pas dans le protocole lui-même, la couche de transparence et de gouvernance multi-acteurs nécessaire au déploiement d'internet est un outil puissant de contrôle par les internautes de ces intermédiaires, qui ont un rôle dans l'efficacité des protocoles.

La décentralisation est un autre sujet, afin de s'assurer que les protocoles ne dépendent pas d'un seul point de contrôle et réduire ainsi les risques de censure et de contrôle monopolistique des communications. Dans ce contexte, la RFC 9620 invite les développeurs à se poser les questions :

« Le protocole favorise-t-il la décentralisation ? » ou « Peut-il fonctionner sans points de contrôle centralisés ? ».

Ici encore, si ces questions semblent relever du truisme, elles peuvent devenir pernicieuses puisqu'elles induisent que tout point de centralisation représente un danger, ce qui est vrai, mais méconnaît une fois de plus l'intérêt d'une gouvernance de ces points de contrôle, en incitant simplement à leur contournement dès la conception.

L'anonymat et le pseudonymat sont également abordés dans la RFC 9620, avec des questions qui portent cette fois-ci sur la protection de l'identité des utilisateurs : *« Le protocole permet-il aux utilisateurs de rester anonymes ou d'utiliser des pseudonymes ? », « Minimise-t-il l'utilisation d'identifiants persistants pouvant être liés à une personne spécifique ? »*. Ces questions visent la prise en compte de la protection des utilisateurs contre la surveillance indésirable et la protection de leur vie privée, notamment dans les régions où l'expression d'opinions libres peut entraîner des persécutions.

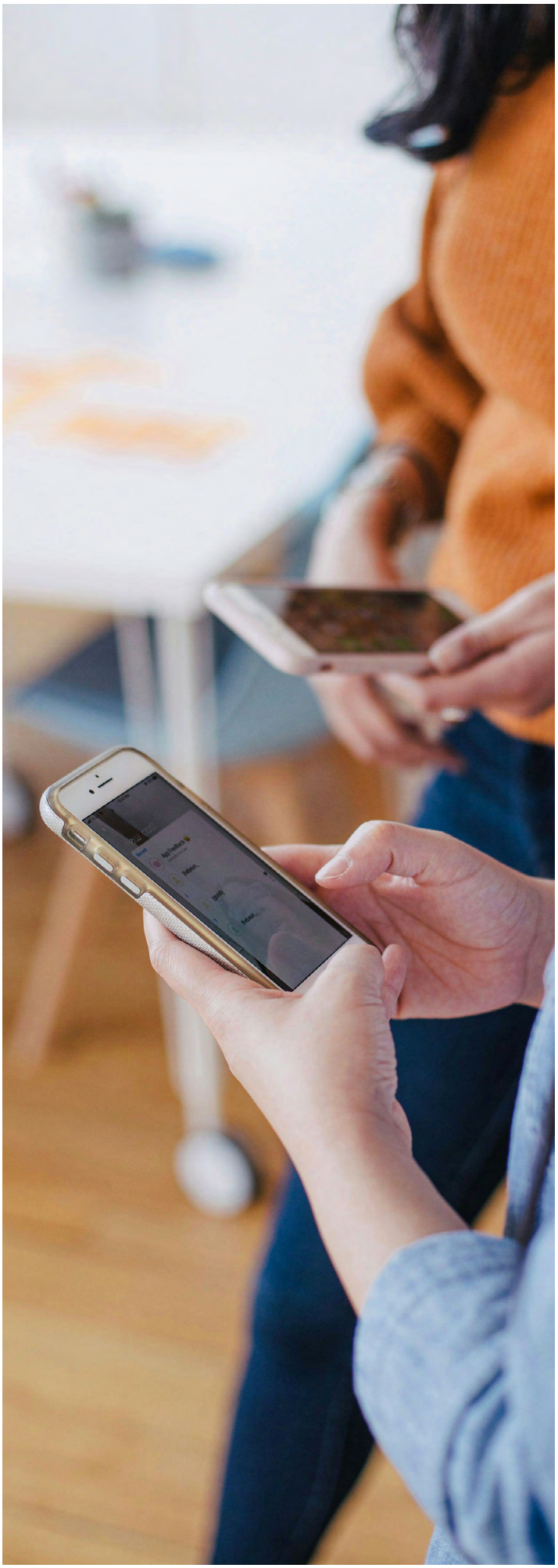
Pour autant, il est discutable d'indiquer que les protocoles doivent, *« by design »*, rendre toute identification des utilisateurs impossible. Il s'agit d'un choix politique qui n'est pas toujours aussi binaire de celui de la protection des utilisateurs contre des pouvoirs autocratiques. La recherche par un système judiciaire indépendant de personnes suspectées de graves violations des mêmes droits de l'homme pourrait elle-même être entravée si tous les protocoles internet rendaient véritablement impossible l'identification des utilisateurs, quel que soit le contexte.

Ici encore, si les intentions sont louables, une grande vigilance doit être de mise pour garantir la neutralité des protocoles. En faire des outils d'anonymisation systématique et absolue, comme une certaine interprétation pourrait y conduire, n'est pas neutre.

Une initiative bienvenue, mais qui nécessite une approche prudente

L'approche RSE contient, entre autres, le respect des droits humains. Il est donc pertinent que les organisations de standardisation d'internet s'approprient ces questions. On aurait pu d'ailleurs imaginer une RFC déclinant des recommandations pour chacun des piliers des objectifs de développement durable, mais ce travail, probablement utile, serait extrêmement long. Il aurait cependant l'intérêt de mettre en balance diverses exigences telles que celle, d'une part, de la décentralisation totale et celle, d'autre part, de l'impact environnemental d'une telle décentralisation, et d'évaluer les conséquences de ces choix.

Cependant, l'approche consistant à vouloir « empêcher » toute violation des droits humains par les protocoles établis n'est pas la même chose que de vouloir empêcher que les protocoles violent les droits humains. La deuxième approche est légitime et nécessaire, la première est sujette à caution. Elle porte le risque d'une vision technocentrée des droits humains qui règlerait comme techniquement la question de leur effectivité. Si nous n'en sommes pas là, et si ces travaux sont très intéressants, gardons à l'esprit, malgré tout, cet adage qui nous rappelle que l'enfer est pavé de bonnes intentions.



Quelles sont les étapes menant à la publication d'une RFC ?

Une RFC *(Request for Comments)* est un document officiel publié pour proposer des solutions techniques, des bonnes pratiques ou des recherches expérimentales visant à assurer le bon fonctionnement d'internet. Les RFC proviennent principalement de l'IETF *(Internet Engineering Task Force)*, mais aussi de l'IRTF *(Internet Research Task Force)* et, dans une moindre mesure, de l'IAB *(Internet Architecture Board)* ou de soumissions indépendantes.

Les RFC sont classées en quatre catégories principales : les *Standards Track*, destinées à devenir des normes ; les *Informational RFC*, dont le but est de fournir des informations techniques ou pratiques à la communauté internet ; les *Experimental RFC*, pour les propositions de technologies, protocoles ou méthodes à tester dans des environnements réels ; et les *Best Current Practice (BCP)*, qui décrivent les bonnes pratiques reconnues dans le secteur.

La publication d'une RFC suit un processus collaboratif rigoureux, garantissant que les propositions sont minutieusement examinées avant de devenir des normes ou des recommandations. En voici les différentes étapes :

- **1. Lancement d'une idée.** Le processus débute lorsqu'une nouvelle idée (de norme, de protocole, de bonnes pratiques, etc.) est proposée. Cette idée peut être discutée de manière informelle lors de sessions BoF *(Birds of a Feather)* à l'IETF ou dans un groupe de recherche de l'IRTF, afin d'en vérifier l'intérêt et la faisabilité.
- **2. Publication d'un internet-draft.** Une fois qu'un sujet a été validé, un groupe de travail à l'IETF ou de recherche à l'IRTF est créé. Ce groupe est responsable de la discussion initiale et de l'élaboration d'un internet-draft, c'est-à-dire d'une première ébauche de la RFC.
- **3. Discussions dans les groupes de travail.** L'internet-draft soumis, le groupe de travail est chargé de perfectionner le document à travers des réunions et des discussions. Le draft est soumis à une série de révisions avant de devenir suffisamment mature pour être examiné plus largement.
- **4. Approbation par les superviseurs.** Le draft finalisé est alors transmis aux directeurs de domaine *(Area Directors)* à l'IETF ou au président du groupe de recherche concerné à l'IRTF, pour une évaluation approfondie. Ces derniers s'assurent que le document respecte les standards attendus.
- **5. Appel à commentaires.** À l'IETF, l'internet-draft entre ensuite dans une phase de *Last Call* ou appel à commentaires, visant à obtenir des retours plus large de la communauté. Pour les soumissions de l'IRTF, un processus similaire de revue communautaire peut être mis en place.
- **6. Révision et approbation finale.** Après l'appel à commentaires, l'IESG *(Internet Engineering Steering Group)*, le comité de direction de l'IETF, évalue les retours. Si des modifications sont nécessaires, elles sont intégrées, puis l'IESG donne son approbation finale pour la publication. À l'IRTF, cette étape est assurée par l'IRSG (*Internet Research Steering Group*).
- **7. Publication par l'éditeur des RFC.** Le document est ensuite transmis à l'éditeur des RFC *(RFC Editor)* pour un travail d'édition, de formatage et de vérification de la qualité. Après cette étape, il est publié officiellement en tant que RFC avec un numéro unique et classé selon sa catégorie en *Standards Track, Informational, Experimental* ou *BCP*.

Il est enfin à noter que les RFC ne sont pas figées dans le temps : elles peuvent être amendées, mises à jour ou remplacées par de nouvelles RFC à mesure que les technologies évoluent et que les besoins de la communauté changent. Certaines RFC peuvent également être déclarées obsolètes lorsque leur contenu n'est plus d'actualité.

03

Le Pacte Numérique Mondial a été adopté

Le Pacte Numérique Mondial a été adopté lors du Sommet de l'avenir des Nations Unies en septembre 2024. Affichant des objectifs clairs et des engagements concrets, ce pacte ambitionne de créer un cadre où le numérique est un vecteur de progrès pour tous. En s'attaquant aux inégalités, il cherche en effet à ce que toutes les personnes dans le monde, peu importe leur situation géographique ou socio-économique, puissent accéder et profiter en toute sécurité des technologies et de l'internet. À ce sujet, il réitère la nécessité d'une gouvernance d'internet inclusive et multi-parties, une condition indispensable pour garantir qu'internet demeure un outil au service de tous.

Il aura fallu plus de trois ans pour que le Pacte Numérique Mondial voit le jour. L'initiative prend en effet sa source en 2020, lors du 75ème anniversaire de l'Organisation des Nations Unies, en pleine pandémie de Covid-19 et dans un contexte de crises mondiales interconnectées qui menacent la santé, l'économie et l'environnement. À cette occasion, les États Membres s'étaient engagés à renforcer la gouvernance mondiale au bénéfice des générations actuelles et futures.

Après une longue phase de négociations auxquelles l'Afnic a activement participé à la fois directement, par exemple en s'impliquant dans le processus NETmundial, et indirectement en suivant aux côtés des pouvoirs publics l'avancée des négociations et en analysant les aspects techniques, le Pacte Numérique Mondial a finalement été adopté par consensus en septembre dernier lors du Sommet de l'avenir organisé par les Nations Unies. Il vise à créer un cadre d'action mondial qui réponde aux défis liés à la transformation numérique, à la réduction des fractures numériques et à la définition de principes pour un avenir numérique ouvert et sécurisé, tout en promouvant des solutions inclusives et équitables à l'échelle mondiale, et en renforçant la coopération internationale.

Un contexte de volonté de réforme de la gouvernance d'internet

Le Pacte Numérique Mondial est adopté dans un contexte particulier, puisque les années 2024 et 2025 sont particulièrement riches en discussions difficiles sur la gouvernance d'internet et sur la pertinence d'en réviser les structures actuelles. Cet écosystème, où chaque événement informe et enrichit les autres, vise à contribuer à une gouvernance d'internet plus concertée et adaptée au monde d'aujourd'hui.

Le Pacte Numérique Mondial fait notamment écho à NETmundial+10, qui s'est déroulé en avril dernier au Brésil (pour plus de détails, voir l'article *« NETmundial+10: réaffirmer les principes d'une gouvernance d'internet multi-acteurs »*, paru dans La Lettre Afnic n°6 de juillet 2024). L'événement a réaffirmé les principes établis lors de la première conférence NETmundial de 2014, tout en les adaptant aux nouvelles réalités numériques. La communauté internet y a clairement exprimé sa volonté de poursuivre une gouvernance multi-parties prenantes d'internet : une dynamique qui a certainement eu un impact sur l'adoption du Pacte Numérique Mondial plus tard dans l'année, celui-ci prenant en compte ces principes de collaboration et d'inclusivité.

La communauté internationale se prépare par ailleurs au SMSI+20, la revue à 20 ans du Sommet Mondial sur la Société de l'Information qui se déroulera en 2025 et vise à évaluer et à revitaliser les engagements pris à Genève et à Tunis en 2003 et 2005. Cette revue est très attendue car elle va permettre d'examiner les avancées réalisées depuis le SMSI et d'en adapter les engagements aux défis d'aujourd'hui, notamment quant au Forum sur la Gouvernance de l'Internet (FGI).
Il ne fait aucun doute que le texte voté lors de NETmundial+10 et l'adoption du Pacte Numérique Mondial s'inviteront dans ces discussions à venir.

Un autre élément de contexte est l'Agenda 2030 des Nations Unies, dont l'échéance approche à grands pas. Cet agenda, qui comprend les 17 objectifs de développement durable (ODD), met en avant — entre autres — l'importance de l'inclusion numérique et de l'accès équitable aux technologies de l'information. Les pays du Sud, en particulier, attendent avec impatience que les promesses faites lors de l'adoption de l'Agenda 2030 soient tenues, notamment en ce qui concerne l'amélioration de l'accès à internet et des infrastructures numériques. La convergence des discussions, du Pacte de l'Avenir (auquel le Pacte Numérique Mondial est annexé) et, prochainement, du SMSI+20 reflète cette attente et souligne la nécessité d'une gouvernance d'internet inclusive, équitable et durable.

Le rôle du numérique pour un avenir meilleur

Le Pacte Numérique Mondial s'intègre en annexe du Pacte pour l'avenir, qui établit un plan global pour la gouvernance mondiale et la coopération internationale, et appelle à un multilatéralisme renouvelé afin de mieux répondre aux besoins des populations et de la planète. Le Pacte pour l'avenir établit ainsi des priorités claires pour la coopération internationale, notamment en termes de lutte contre les inégalités, de promotion de la paix et de protection de l'environnement.

Le Pacte pour l'avenir reconnaît notamment que, malgré les difficultés actuelles dans le monde, les progrès scientifiques et technologiques peuvent contribuer à l'éradication de la pauvreté, à la sécurité alimentaire, à la santé et à la protection de l'environnement, c'est-à-dire à l'atteinte des objectifs de développement durable des Nations Unies. Il insiste également sur la nécessité de fonder ces avancées scientifiques et technologiques sur des valeurs humaines communes, y compris les technologies émergentes telles que l'intelligence artificielle, afin qu'elles profitent à tous ; et d'en gérer les risques de manière responsable, afin d'éviter de perpétuer des inégalités. Il engage enfin à favoriser un environnement équitable pour le développement scientifique, à encourager la circulation des talents et à soutenir les capacités des pays en développement.

Pacte Numérique Mondial : 5 objectifs pour un numérique équitable et durable

Dans ce contexte, le Pacte Numérique Mondial énonce cinq objectifs, visant à garantir que les technologies numériques ne creusent pas les inégalités existantes mais, au contraire, contribuent à un avenir numérique inclusif et durable.

Objectif n°1 : « Réduire toutes les fractures numériques et avancer plus rapidement dans la mise en œuvre des objectifs de développement durable »

Le premier objectif du Pacte Numérique Mondial est de garantir une connectivité universelle, c'est-à-dire permettre à tous les êtres humains de disposer d'une connexion à internet à un coût abordable et en toute sécurité, de développer les compétences numériques qui leur sont utiles et de pouvoir accéder à des contenus adaptés à leurs besoins sociaux, culturels et linguistiques. Cela permettrait de réduire les inégalités numériques qui persistent entre et à l'intérieur des pays, et de permettre à un plus grand nombre de personnes, notamment dans les zones rurales et défavorisées, d'accéder aux avantages des technologies numériques.

Dans cet objectif du Pacte Numérique Mondial, les Nations Unies s'engagent ainsi, d'ici 2030, à établir des indicateurs de connectivité, à investir dans les infrastructures et à tenir compte des besoins des populations vulnérables et des questions de genre, tout en promouvant des solutions durables.

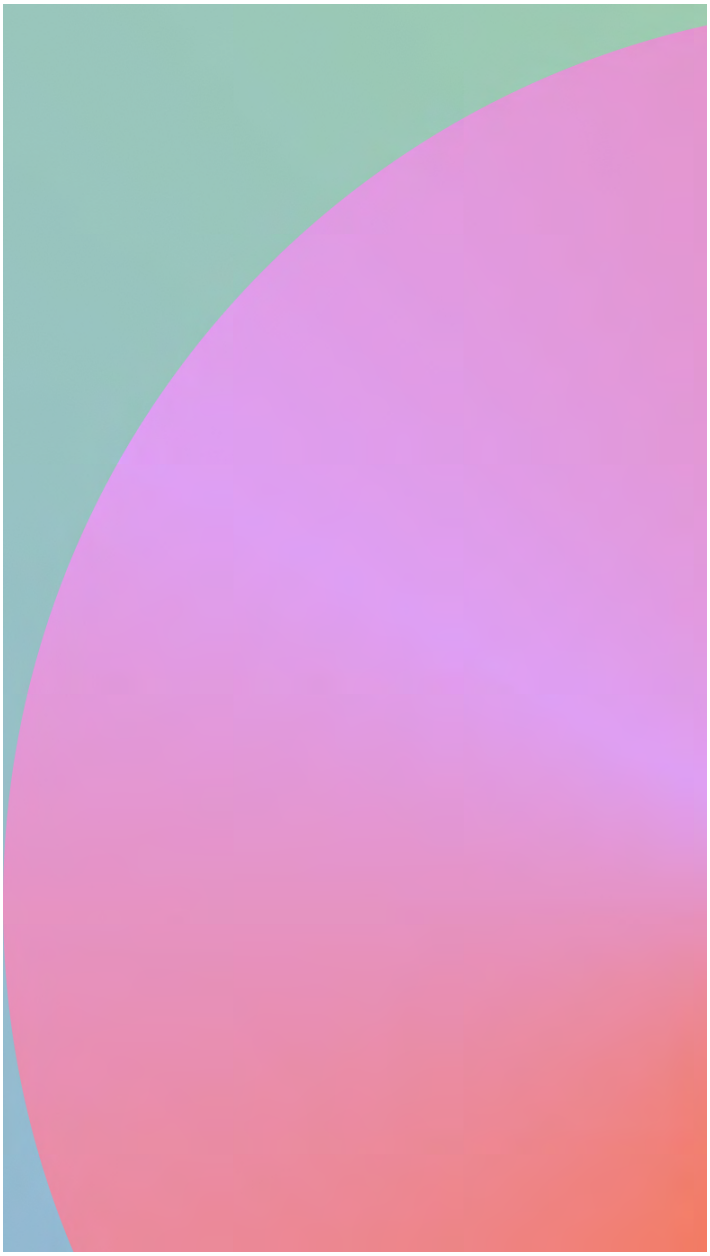
Il est à noter que le Pacte Numérique Mondial cite explicitement dans cet objectif les biens publics numériques, tels que les logiciels libres et les données ouvertes, et les infrastructures publiques numériques comme des *« moteurs essentiels de la transformation et de l'innovation numérique inclusive »*. Les Nations Unies s'engagent à les promouvoir, les renforcer et les développer.

> **Nous estimons que ces biens publics numériques et ces infrastructures publiques numériques sont des moteurs essentiels de la transformation et de l'innovation numériques inclusives.**
>
> **Objectif 1 – Point 16**

Objectif n°2 : « Rendre l'économie numérique plus inclusive et faire profiter toutes et tous de ses avantages »

Le Pacte Numérique Mondial vise par ailleurs à garantir un accès équitable aux technologies numériques, incluant la possibilité d'acquérir et de développer des compétences et des moyens de recherche. Cet objectif vise à garantir que tous puissent disposer des outils nécessaires pour favoriser le développement économique et renforcer la compétitivité, mais aussi créer un environnement propice à la recherche et au développement, et permettre l'innovation.

À ce titre, les engagements du Pacte Numérique Mondial incluent notamment la promotion d'un environnement numérique équitable et inclusif pour les petites et moyennes entreprises, l'assistance technique aux pays en développement, ainsi que l'encouragement à l'innovation et à la coopération internationale pour renforcer les capacités numériques et faciliter l'accès aux technologies.



Objectif n°3 : « Favoriser un espace numérique inclusif, ouvert, sûr et sécurisé qui respecte, protège et promeut les droits humains »

Cet objectif du Pacte Numérique Mondial vise à assurer le respect, la protection et la promotion des droits humains dans l'espace numérique, en garantissant que toutes les technologies numériques soient conformes aux normes internationales et que tous les utilisateurs aient la possibilité d'accéder à l'information et de s'exprimer sans crainte de discrimination ni de répression. Il traite également de la nécessité de lutter contre les violences en ligne et de créer un environnement numérique sûr, en mettant en place des normes de sécurité et des politiques adaptées, en particulier pour la protection des enfants. Il fait aussi état de l'importance d'un accès à une information fiable et précise, appelant à des programmes d'éducation aux médias pour lutter contre la désinformation et promouvoir la transparence des plateformes numériques.

> **Nous considérons que la gouvernance d'internet doit conserver son caractère mondial et multipartite et associer pleinement les États, le secteur privé, la société civile, les organisations internationales, les milieux technologiques et universitaires et toutes les autres parties concernées, chacune selon son rôle et ses missions.**
>
> **Objectif 3 – Point 27**

Il reconnaît notamment la nécessité d'une gestion mondiale et multi-parties d'internet pour y parvenir et souligne qu'internet est une ressource essentielle pour une transformation numérique équitable, nécessitant un environnement ouvert, stable et sécurisé pour tous. Le Pacte appelle à la coopération entre États, secteur privé et société civile pour garantir un accès équitable.

Il reconnaît également le rôle central du Forum sur la Gouvernance d'Internet (FGI) et engage à soutenir les efforts des pays en développement pour participer à cette gouvernance.

On pourra cependant regretter, une fois de plus, que cette approche, même quand elle soutient l'implication de tous les acteurs et non uniquement celle des gouvernements, soit décidée par les gouvernements seuls dans le cadre onusien. L'effacement du rôle de la communauté technique, souvent garante de la pérenité et de l'ouverture des protocoles à la base du fonctionnement d'internet, est un signal à prendre en compte et qui peut inquiéter, laissant potentiellement le champ libre au lancement d'une bataille de normes et de standards poussés par différents États qui pourraient avoir des agendas divergents des objectifs de cette déclaration.

> **Nous sommes conscients de l'importance que revêt le Forum sur la gouvernance d'internet, qui est la principale instance multipartite d'échanges sur ces questions.**
>
> **Objectif 3 – Point 28**

Objectif n°4 : « Promouvoir des modèles de gouvernance des données qui soient responsables, équitables et interopérables »

Le Pacte Numérique Mondial vise à établir des modèles de gouvernance des données qui soient à la fois responsables, équitables et interopérables — abordant la nécessité de garantir la confidentialité et la sécurité des données, d'encourager le partage et l'interopérabilité des données, ainsi que de s'assurer que les données servent les objectifs de développement durable. La coopération internationale est ici essentielle pour renforcer les capacités des pays, en particulier ceux en développement, afin de mieux gérer leurs systèmes de données.

Dans ses engagements, le Pacte Numérique Mondial avance la création de cadres de gouvernance des données efficaces, le renforcement des capacités de collecte et de traitement des données, la mise en place de normes pour prévenir la discrimination et la promotion des flux de données transfrontières sécurisés. De plus, il est prévu de mobiliser des ressources pour améliorer l'accès et la qualité des données dans le but d'atteindre les ODD.

Objectif n°5 : « Renforcer la gouvernance internationale de l'intelligence artificielle pour le bien de l'humanité. »

Le dernier objectif du Pacte Numérique Mondial appelle enfin à une gouvernance équilibrée et inclusive de l'intelligence artificielle (IA), impliquant tous les pays, notamment ceux en développement.

Les engagements pris incluent notamment l'évaluation des impacts de l'IA sur le développement durable, la promotion de systèmes d'IA transparents et responsables, et le renforcement des capacités, notamment par des partenariats internationaux. L'ONU est ici désignée pour jouer un rôle clé dans l'établissement de normes et la facilitation d'une coopération mondiale sur l'IA.

Que les engagements se traduisent en actions

Par ses considérations et ses engagements, le Pacte Numérique Mondial est une nouvelle étape vers une gouvernance numérique plus inclusive et équitable.
En reconnaissant l'importance du Forum sur la Gouvernance d'Internet (FGI), le Pacte Numérique Mondial s'inscrit dans la lignée des consultations menées pendant deux ans et affiche une volonté de dialogue inclusif pour une gouvernance multi-parties d'internet. Mais devant les inégalités actuelles, des limites peuvent être soulevées, notamment sur la manière dont toutes les parties prenantes pourront effectivement être représentées.

Traduire les grands principes posés par le Pacte Numérique Mondial en actions nécessitera une articulation avec le SMSI et l'Agenda 2030 et une attention particulière sur l'implémentation et la mise en œuvre concrète des engagements par les parties prenantes. Enfin, en étendant drastiquement le champ de ce que l'on nomme la gouvernance de l'internet, à des sujets qui ne relèvent pas stricto sensu de la gouvernance technique d'internet, le pacte prend le risque de mettre en scène son impuissance. En effet si l'ensemble des acteurs techniques du fonctionnement d'internet sont en général présents dans les enceintes de standardisation et d'élaboration de politiques (IETF, ICANN, Registres internet régionaux), il n'en va pas de même, loin s'en faut, des acteurs privés dominants de sujets tels que l'intelligence artificielle, le big data et même les réseaux sociaux. Ainsi, et même si ces sujets nécessitent indubitablement un regard et une implication des gouvernements, en faire des sujets à part entière de la gouvernance d'internet porte le risque d'une discussion in fine confisquée par les États, en l'absence des principaux acteurs qui se déroberaient à l'exercice.

04

En bref : les meilleurs moments du Forum sur la Gouvernance de l'Internet France 2024

Le 3 octobre dernier se déroulait l'édition 2024 du Forum sur la Gouvernance de l'Internet France. Cet événement constitue un point de rencontre important pour les acteurs du numérique locaux, offrant un espace pour échanger des idées et réfléchir aux défis contemporains, facilitant ainsi le dialogue sur les questions de gouvernance et d'accès équitable aux ressources numériques.

Gouvernance d'internet et enjeux multi-parties

Le Forum sur la Gouvernance de l'Internet France 2024 s'est inscrit dans la lignée des discussions qui animent actuellement la communauté internet. Dans un contexte où le principe d'une gouvernance d'internet multi-parties été réaffirmé lors de NETmundial+10 plus tôt cette année, et dans le Pacte Numérique Mondial adopté en septembre dernier, il sera à nouveau questionné à l'occasion du 20ème anniversaire du Sommet Mondial sur la Société de l'Information en 2025, avec en tête l'Agenda 2030 des Nations Unies qui s'approche également à grands pas.

Lors de la plénière d'ouverture, Cédric Wachholz, Chef de la section pour les politiques numériques et la transformation numérique de l'UNESCO, a exprimé sa satisfaction quant à l'adoption du Pacte Numérique Mondial. *« Ce qui est important pour nous, c'est d'avoir une approche holistique et inclusive »*, a-t-il déclaré, avant de mettre également l'accent sur le développement des capacités, en particulier dans les pays en développement, afin de garantir un accès équitable aux technologies. Dans ce cadre, l'UNESCO organise d'ailleurs un Forum mondial sur l'IA et la transformation numérique dans le secteur public, qui se tiendra en février 2025 et s'intéressera au renforcement des capacités des administrations publiques pour exploiter efficacement l'IA (intelligence artificielle) et les technologies numériques.

Cette notion de *« capacity building »* est également portée par Chris Mondini, Directeur général Europe de l'ICANN. Pour son initiative Coalition pour une Afrique digitale, l'ICANN s'est entouré de partenaires, au premier rang desquels l'Afnic, pour renforcer l'infrastructure internet et soutenir ainsi le développement de l'économie numérique en Afrique. L'initiative inclut notamment *« des formations sur l'utilisation du DNS et l'installation de DNSSEC, […] mais aussi de la formation institutionnelle, c'est-à-dire, pour les organisations, comment traduire cet accès aux ressources et technologies dans leurs efforts sociaux, en fournissant des services publics, dans l'économie, pour l'innovation »*, a-t-il expliqué.

Dans ce contexte, a également été annoncé un partenariat entre l'UNESCO et l'ICANN à l'occasion de la Journée de l'Acceptance Universelle, prévue pour mars 2025. L'acceptance universelle (ou *universal acceptance*) vise à garantir que tous les noms de domaines, quelle que soit leur langue ou leur alphabet, soient acceptés et fonctionnent de manière cohérente sur toutes les plateformes internet — un autre moyen de créer un environnement numérique inclusif, permettant à tous les utilisateurs d'accéder pleinement aux ressources en ligne et de participer à l'écosystème numérique mondial.

Olivier Crépin-Leblond, président de l'Internet Society au Royaume-Uni, a quant à lui souhaité clarifier les différentes dimensions de la gouvernance d'internet et faire la distinction entre la gouvernance opérationnelle, axée sur les aspects techniques de l'infrastructure, et la gouvernance stratégique, davantage tournée vers les politiques de contenu et les enjeux sociétaux — cette dernière se retrouvant trop souvent au centre des discussions à son goût, au détriment de la première. Il a également souligné que l'avenir de la gouvernance d'internet ne réside pas dans une opposition entre le multilatéralisme et un système multi-parties prenantes, mais dans leur complémentarité, selon les sujet traités. En nuançant toutefois : *« Bien sûr, dès qu'il y a des sujets qui sont des sujets de société, il faut absolument un système multi-parties prenantes, puisque c'est l'utilisateur final qui fait de l'internet ce qu'est l'internet. Sans utilisateur, l'internet n'existe pas. »*

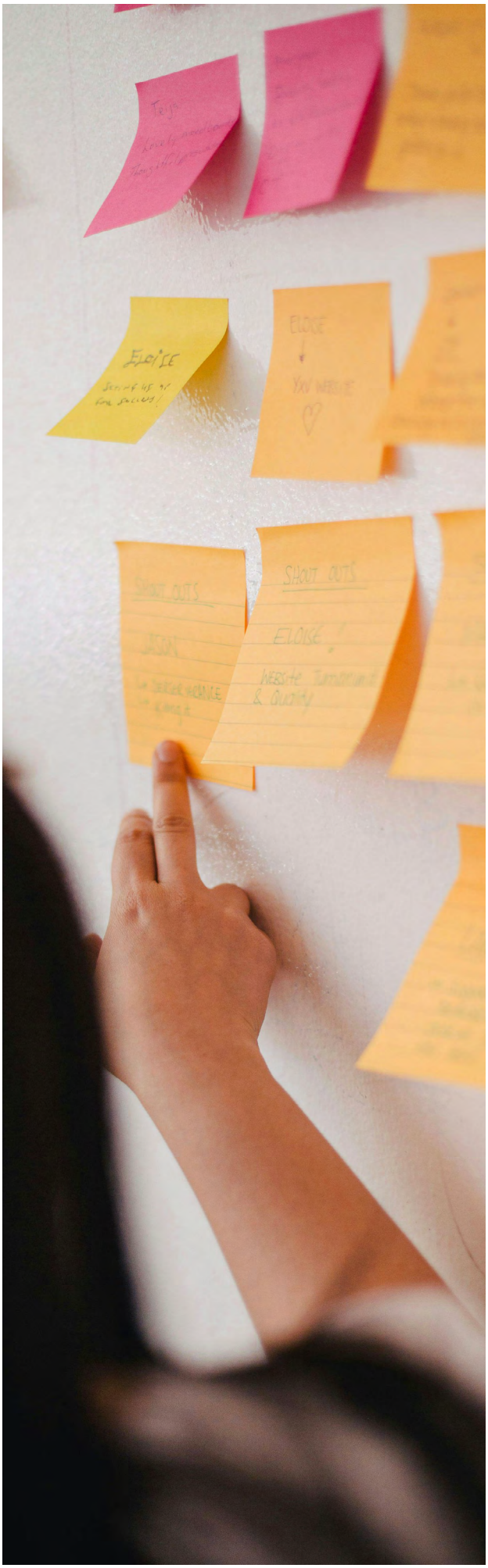
Lorsque la géopolitique s'invite dans les questions de gouvernance d'internet

Lors de sa keynote, Henri Verdier, Ambassadeur pour le numérique, Ministère de l'Europe et des affaires étrangères, a également souligné l'importance d'une gouvernance d'internet qui reflète la diversité des acteurs et doit, à ce titre, rester ouverte et inclusive face aux nouvelles réalités géopolitiques. Il a mis en garde contre les forces qui pourraient vouloir centraliser cette gouvernance au détriment d'une approche plus démocratique, rappelant qu'*« aujourd'hui, le bloc des démocraties fait front »*, mais qu'il est crucial d'éviter un dialogue international qui se limite à des questions de pouvoir. Il a ainsi encouragé une réflexion collective sur la gouvernance d'internet, affirmant que *« nous aurons besoin de tout le monde, de vigilance, d'information et de solidarité »* pour préserver cet espace numérique en tant que bien commun, accessible à tous.

Ces enjeux politiques et de pouvoir ont également été détaillés lors de l'atelier *« Cyber-résilience et géopolitique »* comme des défis liés à l'accès à internet :

- **Enjeux de pouvoir.** Le contrôle exercé par certains États sur les infrastructures internet peut mener à des pratiques de censure. Par exemple, en Russie, l'État peut bloquer l'accès à certains contenus et couper internet durant des manifestations, illustrant ainsi les implications d'un autoritarisme numérique.
- **Enjeux politiques.** Les tensions entre pays peuvent entraver les solutions d'interconnectivité. Par exemple, les problèmes géographiques au Pakistan poussent le pays à chercher des solutions auprès de ses voisins, mais les tensions politiques, comme celles avec l'Inde, limitent ces possibilités de coopération.

La cyber-résilience se définissant comme la capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, tout en maintenant un niveau satisfaisant de fonctionnement et de sécurité, les discussions lors de cet atelier ont mis en lumière d'autres types d'enjeux. Ainsi, certains défis géographiques, tels que les inondations et les tremblements de terre au Pakistan, compliquent le déploiement et l'entretien des infrastructures de fibre optique. Les défis techniques, tels que le coût de l'infrastructure et la rareté des compétences locales, ont également été abordés. Ces facteurs peuvent ralentir l'installation et la réparation des réseaux, rendant certains territoires vulnérables et exposés à des périodes d'immobilisation prolongées.



Des pratiques numériques plus responsables

Le RGESN (référentiel général d'écoconception des services numériques) a été présenté, lors d'une keynote dédiée présentée par Xavier Merlin, Membre du collège de l'ARCEP, comme un cadre élaboré par l'ARCEP pour aider les développeurs à intégrer les préoccupations environnementales dans la conception et le développement de services numériques, afin de réduire leur impact écologique. Christophe Gotteland, Coach RSE chez TGS France, a d'ailleurs reconnu, lors de la plénière de clôture, que *« dans les entreprises du secteur tertiaire, et en particulier du numérique, les sujets d'écoconception prennent tout leur sens, avec le poids de plus en plus important du numérique à la fois dans les pratiques managériales et dans l'impact environnemental global »*.

Lors d'un atelier animé par l'ARCEP, quatre axes ont été identifiés pour mieux comprendre et réduire l'empreinte environnementale du numérique : premièrement, prolonger la durée de vie des terminaux pour limiter la production de nouveaux équipements. Cela a été confirmé plus tard par Sandrine Elmi Hersi, Cheffe de l'unité Internet ouvert à l'ARCEP, lors de la plénière de clôture : *« Si vous souhaitez construire une démarche numérique responsable au niveau d'une organisation, le premier levier, c'est de stabiliser le parc de terminaux. »*

Les axes suivants incluent de réduire les pratiques incitatives qui poussent les utilisateurs à passer plus de temps sur leurs appareils et à en acquérir de nouveaux ; de diminuer les ressources matérielles et énergétiques utilisées tout au long du cycle de vie des équipements ; et enfin, de renforcer la transparence des entreprises sur leurs pratiques environnementales afin de permettre aux utilisateurs de faire des choix éclairés.

C'est un sujet qui a également été longuement abordé lors de la plénière de clôture. Selon Céline Lanfranchi-Signol, Directrice Stratégie, Innovation et ESR de la Communauté d'agglomération de Saint-Quentin-en-Yvelines, la RSE s'impose désormais comme un argument de vente, prenant l'exemple d'entreprises *« qui sont passées d'une stratégie de coût à une stratégie de valeur ajoutée »* parce qu'elles sont, derrière, capables de vendre un engagement. Mathieu Delemme, Président de CTRL-A, a quant à lui tenu à préciser que l'écoconception ne doit pas être considérée comme une contrainte dans les entreprises, mais une initiative vertueuse, puisque *« faire de l'écoconception, au final, c'est améliorer aussi l'expérience utilisateur »*.

Dans un esprit similaire, l'atelier *« QSE-IP – gouvernance et management intégré des activités numériques »* a marqué le lancement officiel d'une task force dédiée aux risques liés au numérique dans les entreprises et à la façon dont ils peuvent être anticipés, gérés et transformés en opportunités d'amélioration continue. Un constat préoccupant a émergé : si les industries traditionnelles ont déjà intégré des systèmes de pilotage pour la qualité, la sécurité et l'environnement (QSE), de telles fonctions sont encore quasiment absentes dans le secteur numérique. Cet atelier a ainsi permis de poser des bases pour une meilleure prise en compte des enjeux

QSE-IP (Qualité, Sécurité, Environnement, Inclusion, vie Privée) et a invité à réfléchir à des recommandations concrètes pour améliorer la gouvernance des activités numériques.

Le FGI France 2024 a également fait la part belle à l'intelligence artificielle (IA)

Le Forum a également été marqué par l'organisation d'un hackathon et d'un idéathon proposant d'explorer les façons dont l'intelligence artificielle peut transformer les systèmes de santé, en challengeant la créativité des participants autour d'un projet de système d'optimisation par l'IA du filtrage des urgences dans les hôpitaux, et répondre à des enjeux sociétaux.

« L'objectif, autant du hackathon que de l'idéathon, était vraiment de mettre en relation des personnes de divers milieux, de les faire discuter, puis de leur montrer que l'IA est à la fois accessible, mais beaucoup aussi une question d'éthique », a déclaré Louis-Philippe Markus Gaulin, Gestionnaire de programme — Création de jeux vidéo, chez Fusion Jeunesse, qui a coorganisé les deux événements.

Le sujet a également été abordé lors d'un atelier intitulé *« Quelle place pour les citoyens dans la gouvernance de l'IA ? Qui ? Quoi ? Quand ? Comment ? »*, qui a mis en lumière l'importance d'impliquer les citoyens dans les discussions entourant l'IA. Les participants ont souligné que la gouvernance de l'IA doit s'accompagner de processus clairs, intégrant tous les acteurs concernés pour garantir une représentation équitable. Les associations telles que l'Association Interconnectée et l'Association Mission Publique ont présenté leurs démarches pour favoriser la participation citoyenne, notamment par le biais de concertations territoriales et de dialogues internationaux.

Les enjeux discutés lors de cet atelier incluent la nécessité de garantir que les voix des citoyens soient entendues et considérées dans le processus décisionnel. Si les politiques publiques ignorent ces voix, cela peut renforcer la méfiance entre les citoyens et les institutions. L'inclusion de toutes les populations, notamment les travailleurs de l'IA dans les pays défavorisés, a été soulignée comme essentielle pour assurer une gouvernance équitable et représentative.

En conclusion, le Forum sur la Gouvernance de l'Internet France 2024 a mis en lumière des enjeux majeurs pour l'avenir du numérique. L'événement a permis des échanges constructifs autour de la gouvernance multi-parties prenantes d'internet, en lien avec des questions clés comme l'inclusion, la cyber-résilience et l'écoconception. Les discussions ont montré la nécessité de renforcer les capacités numériques, particulièrement dans les pays en développement, tout en favorisant une gouvernance plus inclusive et démocratique face aux défis géopolitiques et techniques.

L'accent mis sur les pratiques numériques responsables, à travers des initiatives comme le RGESN et l'adoption de démarches plus écoresponsables, souligne l'engagement croissant des acteurs du numérique envers un avenir durable. En parallèle, l'importance d'inclure les citoyens dans la gouvernance de l'intelligence artificielle a été fortement soulignée, tout comme le besoin de transparence et de dialogue pour garantir que les systèmes numériques servent le bien commun.

Le Forum sur la Gouvernance de l'Internet est plus que jamais un lieu de convergences pour échanger sur les aspects éthiques, d'inclusivité, de géopolitique et de responsabilité sociale et environnementale au cœur du numérique. Pour autant, de par la nature même de ces enjeux, ces derniers doivent continuer à être abordés séparément des aspects de gouvernance technique d'internet, qui trouvent leur expression dans les organismes spécialisés. Dans le contexte de l'adoption récente du Pacte Numérique Mondial, cette distinction entre gouvernance technique de l'internet, et enjeux politiques et sociétaux plus larges, prend une fois de plus tout son sens.

Les prochains événements auxquels l'Afnic participe :

- **26 et 27 octobre 2024**
OARC 43

Prague, République tchèque

- **28 octobre au 1er novembre 2024**
RIPE 89

Prague, République tchèque

- **2 au 8 novembre 2024**
IETF 121

Dublin, Irlande

- **9 au 14 novembre 2024**
ICANN 81

Istanbul, Turquie

afnic

Internet made in France

Votre contact

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
7 avenue du 8 Mai 1845,
78280 Guyancourt