

La lettre n°14

La transition vers IPv6 ne signe pas la fin d'IPv4

p.02

Ce qu'il faut retenir de la 2^{ème} édition du FFGNIA,
le Forum francophone de la gouvernance du
numérique et de l'intelligence artificielle

p.08

ENUM: pourquoi fermer ce qui fonctionne encore ?

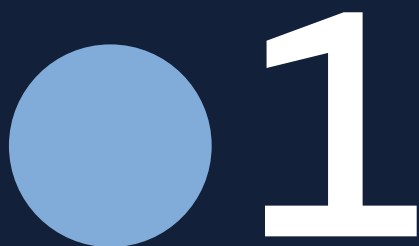
p.12

Brèves

p.16

L'Afnic y était

p.19



La transition vers IPv6 ne signe pas la fin d'IPv4

● Les adresses libres IPv4 sont devenues rares. Les blocs encore disponibles ne suffisent plus à répondre aux nouveaux besoins et les organisations qui en recherchent doivent désormais se tourner soit vers d'autres organisations acceptant de leur louer ou de leur transférer des adresses IP, soit vers un marché gris et très spéculatif où des ressources déjà attribuées mais non utilisées peuvent leur être transférées, contre des sommes parfois importantes. En parallèle, les politiques publiques encouragent, à raison, le déploiement d'IPv6, dont l'espace d'adressage extrêmement plus grand permet de répondre durablement à la croissance des usages.

À première vue, l'équation paraît simple : IPv6 est appelé à se généraliser, tandis que les adresses IPv4 ont acquis une vraie valeur marchande, du fait de leur rareté et de la nécessité pour de nombreux services, même nouveaux, de continuer à être accessibles par ce protocole, à côté d'IPv6. Les organisations qui en disposent auraient donc intérêt à les céder sans attendre. Ce raisonnement va pourtant un peu vite. Pour mieux comprendre pourquoi, il faut d'abord préciser ce que recouvre la « vente » d'adresses IPv4 et les règles qui l'encadrent, avant d'examiner si le déploiement d'IPv6 rend réellement ces ressources inutiles.

Peut-on « vendre » des adresses IPv4 ?

Pour comprendre le marché qui s'est développé autour des adresses IPv4, il faut d'abord revenir sur la façon dont les adresses IP sont attribuées et gérées à l'échelle mondiale. Il faut aussi comprendre les raisons de leur pénurie, qui a favorisé les transferts entre organisations sans pour autant en faire des biens ordinaires pouvant être vendus librement.

Qui attribue et gère les adresses IP ?

Dans les grandes lignes, une adresse IP publique indique aux réseaux vers quelle destination acheminer les données sur internet. La répartition de ces adresses doit donc être coordonnée : si deux organisations utilisaient indépendamment le même bloc, les réseaux ne sauraient plus de manière fiable vers laquelle diriger le trafic. C'est notamment pour prévenir ce type de conflit que les adresses IP sont administrées dans le cadre d'un système mondial de registres.

Au sommet de ce système, la fonction IANA (*Internet Assigned Numbers Authority*) permet d'administrer le registre mondial des adresses IP et attribue de grands blocs issus de cet espace d'adressage aux cinq registres internet régionaux, ou RIR : AFRINIC pour l'Afrique¹, APNIC pour l'Asie-Pacifique, ARIN pour l'Amérique du Nord et une partie des Caraïbes, LACNIC pour l'Amérique latine et l'autre partie des Caraïbes, et le RIPE NCC pour l'Europe, la Russie, le Moyen-Orient et une partie de l'Asie centrale.

Ces registres attribuent les ressources, enregistrent leurs titulaires et tiennent à jour les bases de données nécessaires à leur gestion. Ils appliquent des politiques élaborées par leurs communautés régionales. Il ne s'agit donc pas de règles fixées par une autorité publique mondiale, mais d'un système de gouvernance construit par la communauté technique de l'internet.

Pourquoi parle-t-on d'une pénurie des adresses IPv4 ?

IPv4 offre un espace d'adressage théorique d'environ 4,3 milliards d'adresses. Ce nombre, considérable au moment de la conception du protocole, est devenu insuffisant avec la diffusion mondiale d'internet, la multiplication des équipements connectés et l'extension des usages.

En 2011, l'IANA a distribué aux cinq RIR ses derniers grands blocs IPv4 disponibles. Les RIR ont ensuite atteint des situations de pénurie selon des calendriers et des règles propres à chaque région. Dans la région couverte par le RIPE NCC, le stock ordinaire d'adresses IPv4 est épuisé depuis novembre 2019. Seules de petites attributions issues de ressources récupérées restent accessibles à certaines organisations éligibles.

Les organisations qui cherchent des ressources IPv4 supplémentaires ont donc désormais le choix entre partager une même adresse publique entre plusieurs utilisateurs grâce

à un mécanisme appelé NAT (*Network Address Translation*), obtenir des adresses auprès de leur opérateur ou de leur hébergeur, solliciter une petite attribution lorsqu'elles y sont éligibles ou, enfin, se tourner vers le marché gris des adresses IPv4.

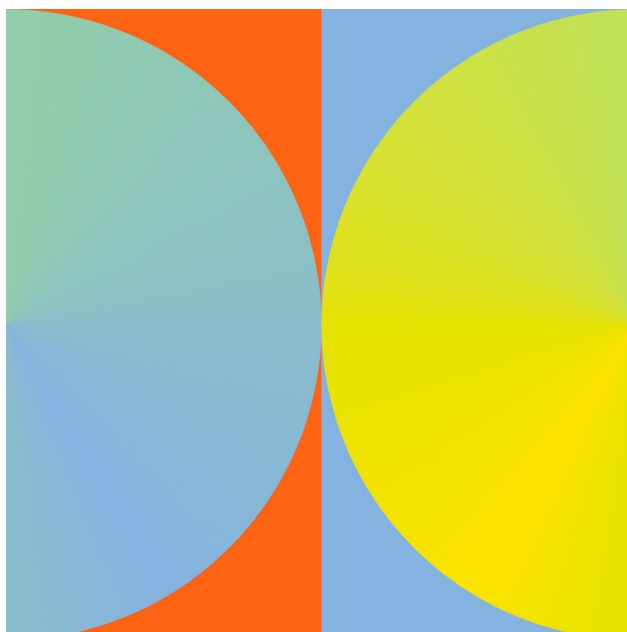
La « vente » d'adresses IPv4 est-elle une vente ordinaire ?

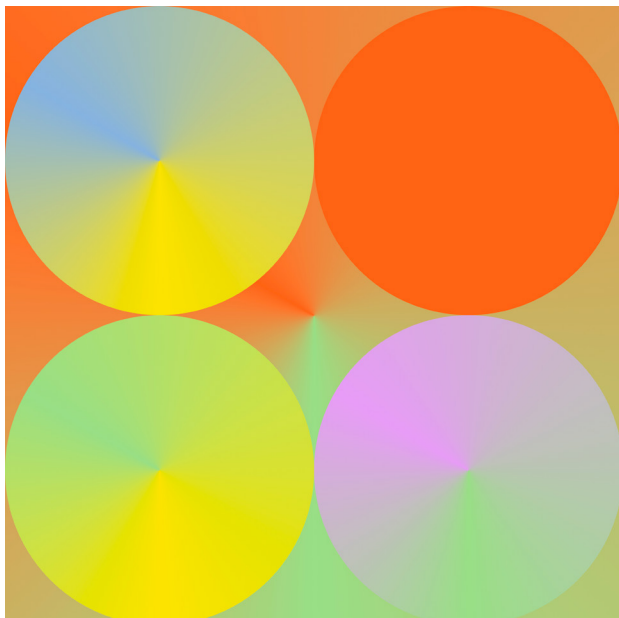
Le mot « vente » est commode, mais il peut induire en erreur. Dans le cadre contractuel du RIPE NCC, l'enregistrement d'un bloc d'adresses IP ne confère pas à son titulaire un droit de propriété sur les adresses elles-mêmes. Les textes parlent plutôt d'attribution, d'affectation et d'enregistrement.

Une organisation enregistrée comme titulaire d'un bloc IPv4 ne peut donc pas le vendre à proprement parler, mais peut néanmoins le transférer à une autre organisation, en contrepartie d'une somme convenue entre les parties. Le RIPE NCC ne fixe pas le prix et n'intervient pas dans leur accord commercial. L'opération s'apparente donc à une vente sur le plan économique, mais elle reste, dans les règles du registre, un transfert de ressources, nécessitant une information préalable du RIPE NCC².

Un accord commercial entre les parties ne suffit d'ailleurs pas à réaliser le transfert. Pour que celui-ci soit reconnu par le registre, il doit respecter les règles du RIR compétent et être inscrit dans sa base de données. Dans la région couverte par le RIPE NCC, les parties doivent notamment être correctement identifiées et présenter un accord signé par leurs représentants habilités. Le RIPE NCC vérifie que l'opération respecte ses règles, puis enregistre le changement de titulaire.

1. Pour une analyse de la crise de gouvernance traversée par AFRINIC et des tensions liées au marché des adresses IP, voir l'article « *Gestion des adresses IP : d'un enjeu purement technique à un objet de tensions géopolitiques* », La Lettre Afnic n°11 : <https://www.afnic.fr/wp-media/uploads/2025/12/La-Lettre-Afnic-N%C2%B011.pdf>
2. Voir l'Article 10 du RIPE NCC Standard Service Agreement : <https://www.ripe.net/publications/docs/ripe-812/>





en offre théoriquement 340 milliards de milliards de milliards de milliards, ce qui représente plus de 66 milliards de milliards d'adresses par cm^2 de la surface totale de la Terre. Cet écart gigantesque s'explique par le fait que chaque bit supplémentaire double le nombre de combinaisons possibles. IPv6 dispose donc d'un espace d'adressage sans commune mesure avec celui de son prédécesseur. C'est pourquoi son déploiement constitue la réponse la plus durable à la croissance d'internet.



IPv4 et IPv6 continueront de coexister

L'IETF (*Internet Engineering Task Force*) recommande depuis longtemps que les nouvelles implémentations prennent en charge IPv6. La RFC 6540³, publiée dès 2012, indique que les nouveaux systèmes IP doivent le supporter. Elle prévoit aussi explicitement qu'IPv4 et IPv6 continueront de coexister pendant de nombreuses années. À aucun moment elle ne déclare IPv4 obsolète et ne fixe une date pour sa disparition.

C'est parce qu'ici, il faut en réalité distinguer l'objectif à long terme et le chemin qui permet de l'atteindre. IPv6 permet certes de sortir durablement de la pénurie. Mais cela ne signifie pas que sa généralisation rend instantanément inutiles les réseaux et les services qui fonctionnent encore en IPv4.

L'IPv4 reste très largement utilisé

Tant que des réseaux, des services et des équipements restent accessibles uniquement en IPv4, les blocs déjà attribués conservent une utilité opérationnelle. En effet, IPv4 et IPv6 sont deux protocoles distincts qui ne sont pas nativement interoperables. Une organisation peut avoir entièrement modernisé son propre réseau en IPv6 ; mais si le service qu'elle cherche à joindre n'est disponible qu'en IPv4, elle doit encore disposer d'un moyen d'accéder à ce protocole. À défaut, la connexion ne peut pas être établie. Pour communiquer, le réseau de l'utilisateur et le service distant doivent en effet prendre en charge un protocole commun, à moins qu'un dispositif intermédiaire ne traduise ou ne transporte le trafic entre IPv6 et IPv4.

En France, où le déploiement d'IPv6 est pourtant particulièrement avancé, la transition ne progresse pas au même rythme chez les fournisseurs d'accès, les fournisseurs de contenus et les hébergeurs. Selon l'Arcep, le taux d'utilisation d'IPv6 en France atteignait 74,7 % à la fin

La situation est plus complexe lorsque les ressources passent d'un registre régional à un autre, car tous les RIR n'autorisent pas les transferts entre régions. Lorsqu'un tel transfert est possible, il doit être approuvé par les deux registres concernés et respecter les exigences applicables de part et d'autre. Selon les règles du RIR d'origine, l'organisation qui reçoit les adresses IP peut aussi devoir justifier ses besoins et expliquer l'usage qu'elle prévoit d'en faire.

Dans la région couverte par le RIPE NCC, les transferts peuvent par ailleurs être permanents ou temporaires. Dans le second cas, le bloc est enregistré au nom du bénéficiaire jusqu'à la date convenue, puis revient à son titulaire initial. Cette mise à disposition peut s'apparenter à une location. Une contrepartie financière peut être prévue dans l'accord conclu entre les parties, mais elle n'est pas imposée par les règles du RIPE NCC.

Il existe donc bien un marché des adresses IPv4, mais il s'agit d'un marché de transfert de ressources et non de la vente des adresses elles-mêmes. Alimenté par la pénurie et encadré par les règles des différents RIR, ce marché donne une valeur aux blocs déjà attribués. Cette valeur ne suffit toutefois pas à déterminer si une organisation a intérêt à les céder. Encore faut-il savoir quelle utilité ils conserveront à mesure qu'IPv6 se généralisera.

Passer à IPv6 signifie-t-il abandonner IPv4 ?

Le déploiement d'IPv6 apporte une réponse durable à la pénurie d'adresses IP, qui ne concerne en réalité qu'IPv4. Il ne fait toutefois pas disparaître les réseaux et les services qui utilisent encore IPv4. Pour mesurer l'utilité que conservent les blocs existants, il faut bien distinguer le passage à IPv6 de l'abandon d'IPv4.

IPv6 répond à la pénurie d'adresses IPv4

Si les adresses IPv4 sont codées sur 32 bits, les adresses IPv6 le sont sur 128 bits. Cela signifie que là où IPv4 permet de former environ 4,3 milliards d'adresses, IPv6

3. <https://datatracker.ietf.org/doc/html/rfc6540>

de 2025⁴, ce qui la plaçait au premier rang des cent pays comptant le plus d'internautes. Mais seuls 38 % des sites web et 25 % des serveurs de courrier électronique étaient accessibles en IPv6 à la même date.

Internet ne peut pas basculer d'un protocole à un autre sur la base d'une seule décision. Il est composé de très nombreux réseaux exploités par des opérateurs, des administrations, des entreprises, des universités et des fournisseurs de services indépendants. Aucune autorité mondiale ne peut imposer à l'ensemble de ces acteurs une date commune de migration. Les États et les organisations peuvent fixer des objectifs dans leur propre périmètre, mais ils ne peuvent décider seuls du basculement de l'internet mondial.

Le passage à IPv6 demande en outre davantage qu'une simple modification de configuration. Il faut vérifier la compatibilité des équipements et des logiciels, adapter les systèmes de sécurité et de supervision, former les équipes, tester les services et parfois remplacer du matériel. Pour les infrastructures anciennes ou complexes, cette transformation peut prendre plusieurs années et nécessiter des investissements importants.

IPv4 et IPv6 vont coexister encore longtemps

Les acteurs n'avancent donc ni au même rythme ni dans le même ordre. Certains réseaux utilisent déjà principalement IPv6, tandis que d'autres restent dépendants d'IPv4. Un service accessible aux uns doit pourtant continuer à l'être pour les autres. Il en résulte une longue période de coexistence. Celle-ci ne remet toutefois pas en cause la perspective, à long terme, d'un internet entièrement IPv6. Elle décrit simplement la situation dans laquelle les décisions doivent être prises d'aujourd'hui.

Cette période de coexistence est prise en compte de longue date par l'IETF. IPv4 et IPv6 n'étant pas directement compatibles, plusieurs mécanismes ont été normalisés afin que des réseaux ayant migré vers IPv6 puissent continuer à communiquer avec les services encore disponibles uniquement en IPv4.

Ainsi, le mécanisme NAT64, défini par la RFC 6146⁵, permet de traduire les échanges entre un appareil connecté en IPv6 et un service disponible uniquement en IPv4. L'architecture 464XLAT, décrite dans la RFC 6877⁶, permet à des applications conçues pour IPv4 de fonctionner sur un accès IPv6. D'autres mécanismes encore permettent de transporter des données IPv4 à travers le réseau IPv6 d'un opérateur. Ces solutions relèvent de ce que l'on appelle « *IPv4-as-a-Service* » (IPv4 en tant que service). Grâce à ces solutions, certaines parties d'une infrastructure peuvent fonctionner uniquement en IPv6 sans priver les utilisateurs de l'accès aux services encore disponibles en IPv4.

4. Rapport sur l'état de l'internet en France 2026, Arcep : <https://www.arcep.fr/actualites/actualites-et-communiqués/détail/n/rapport-annuel-tome3-160726.html>

5. <https://datatracker.ietf.org/doc/html/rfc6146>

6. <https://datatracker.ietf.org/doc/html/rfc6877>



Les invités de La Lettre - 3 questions à Hervé Clément et Patrick Ainard-Simonet

Hervé Clément est responsable du département Nommage, Adressage et Numérotation chez Orange. Il préside également le Conseil de l'adressage de l'ASO (Address Supporting Organization), l'organisme qui conseille l'ICANN sur les politiques relatives aux adresses IP, où il représente la région du RIPE NCC. Patrick Ainard-Simonet, quant à lui, est Chef de Projet IPv6 chez Orange. Ensemble, ils répondent aux questions de la Lettre Afnic, croisant leurs regards sur la gouvernance de l'adressage et sur les besoins d'un opérateur.

La Lettre Afnic : Bonjour Hervé Clément, bonjour Patrick Ainard-Simonet. Le déploiement d'IPv6 est bien avancé en France, même si tous les acteurs ne progressent pas au même rythme. Comment abordez-vous aujourd'hui cette transition ?

Hervé Clément : La manière de procéder dépend des caractéristiques et des contraintes de chaque réseau. Si le RIPE NCC encourage bien entendu la migration vers IPv6, il ne formule pas de recommandations particulières en faveur d'une technologie de transition. Mais, cela n'empêche pas d'avancer.

Patrick Ainard-Simonet : Chez Orange, la mise en œuvre est en effet déjà bien engagée. Sur le réseau mobile, par exemple, les terminaux sont configurés pour se connecter uniquement en IPv6 ; et notre objectif est d'« arrêter » IPv4 pour le marché grand public à l'horizon 2030.

LLA : Est-ce que cela signifie que vos clients ne pourront plus utiliser les services accessibles uniquement en IPv4 après cette date ?

PAS : Absolument pas. On parle ici du fonctionnement interne du réseau d'Orange : l'objectif est d'y acheminer les données de nos clients uniquement en IPv6. Mais ils pourront toujours accéder aux services en IPv4 grâce au mécanisme NAT64 qui assure et continuera d'assurer la traduction des échanges entre les deux protocoles.

LLA : Votre réseau fonctionnera donc entièrement en IPv6 à l'horizon 2030. Faut-il en déduire qu'Orange va céder toutes ses adresses IPv4 ?

HC : Si Orange participe déjà au marché secondaire des adresses IPv4, c'est avec parcimonie. Nos transferts de ressources vers l'extérieur sont d'ailleurs publics. Cette prudence s'explique par l'utilité que ces adresses conserveront même après le passage à IPv6 et la difficulté à évaluer nos besoins futurs. Avant de céder un bloc, nous devons donc considérer les usages auxquels il pourrait encore répondre.

Conserver ses adresses IPv4 ne freine pas la transition vers IPv6

On l'a vu plus haut, passer à IPv6 demande un travail spécifique de configuration, de mise à niveau et de vérification, plus ou moins important selon l'infrastructure. Cela demande du temps et des investissements, mais en aucun cas cela ne dépend du sort réservé aux ressources IPv4. Les conserver ne freine pas le déploiement d'IPv6, pas plus que les céder ne l'accélère.

Un lien indirect peut toutefois exister entre les deux. En cédant des adresses IPv4, l'organisation peut obtenir une recette qu'elle peut décider de réinvestir dans le passage à IPv6. Mais ce gain immédiat a une contrepartie : elle perd également l'usage du bloc IPv4 transféré et cesse d'en être le titulaire enregistré auprès du RIR. Si elle a de nouveau besoin d'adresses IPv4 quelques années plus tard, elle devra s'en procurer sur un marché dont elle ne maîtrise ni les prix ni la disponibilité.

Avant de céder définitivement un bloc IPv4, il convient donc non seulement de s'assurer qu'il n'est plus utilisé, mais aussi d'anticiper les besoins futurs. Pour un acteur public, la réflexion peut aller plus loin et intégrer les besoins de l'écosystème numérique français dans son ensemble. Si certains acteurs de cet écosystème avaient besoin d'adresses IPv4 à l'avenir, une mise à disposition temporaire, sous forme de location, pourrait alors être envisagée, sous réserve de garanties quant à leur utilisation. Il conviendrait notamment de s'assurer que les blocs concernés ne puissent être employés, directement ou indirectement, pour des activités relevant du marché gris et susceptibles de porter préjudice à l'écosystème numérique.

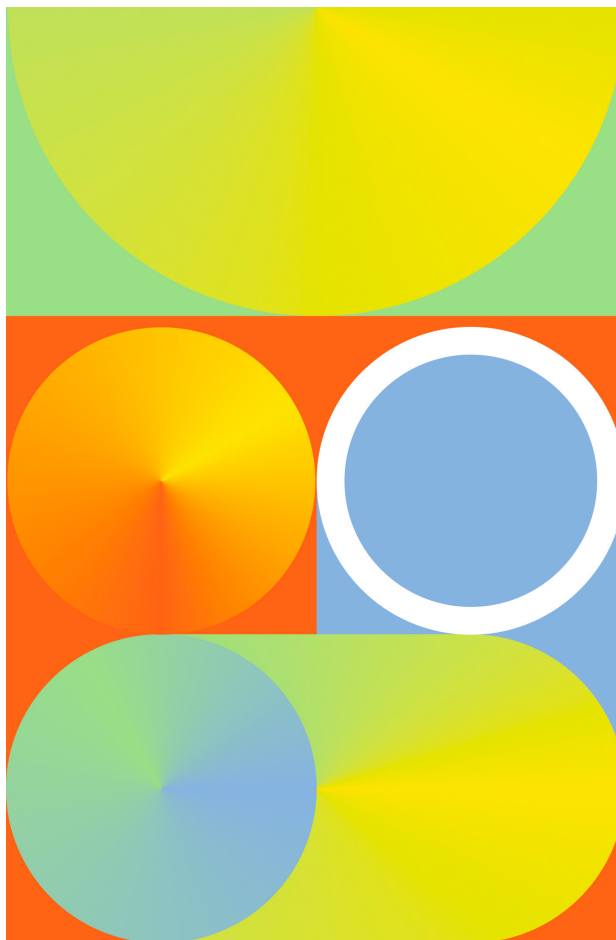
En cas de cession, il est également important de souligner que les transferts sont, comme indiqué plus haut, encadrés par des règles qui peuvent être différentes selon le statut des adresses concernées. Les adresses IP dites « Legacy », attribuées avant la création des RIR, sont soumises à des conditions moins strictes que celles dites « Allocated Space », distribuées par les RIR. Un examen minutieux de la situation s'impose donc, sauf à sortir des règles et à risquer de constater une non prise en compte du transfert par le RIR. Une telle situation pourrait avoir des conséquences en termes d'image, notamment en cas d'utilisation malveillante d'adresses IP vendues mais toujours considérées comme sous la responsabilité du vendeur ; ou même contractuelles si l'acheteur se retournait vers le vendeur au motif qu'il ne peut justement pas faire ce qu'il veut de « ses » adresses IP.

Au regard de ces enjeux, conserver les blocs IPv4 dont dispose encore l'État pourrait constituer un choix plus stratégique et plus utile au développement numérique du pays.

Une ressource à considérer dans la durée

À mesure qu'IPv6 se généralise, la question posée par les ressources IPv4 change de nature. Elle ne relève plus seulement du fonctionnement technique d'un réseau ni du prix auquel un bloc pourrait être cédé. Pour une organisation, et plus encore pour un acteur public, elle touche aussi à la continuité d'accès aux services, à la capacité de répondre à des besoins futurs et à la possibilité de mettre temporairement une ressource rare à la disposition d'autres acteurs.

Une cession peut certes procurer une recette susceptible de financer la modernisation du réseau. Mais elle ferme aussi une possibilité : celle de réutiliser, de réaffecter ou de mettre temporairement le bloc à disposition par la suite. Avant une opération définitive, la question n'est donc pas de prévoir la date à laquelle IPv4 disparaîtra, mais de déterminer si le gain immédiat justifie la perte durable de cette marge de manœuvre.





Ce qu'il faut retenir de la 2^{ème} édition du FFGNIA, le Forum francophone de la gouvernance du numérique et de l'intelligence artificielle

● Le FFGNIA2, la deuxième édition du Forum francophone de la gouvernance du numérique et de l'intelligence artificielle, s'est tenu le 3 juillet dernier à Genève. À l'initiative de l'Organisation internationale de la Francophonie, ce rendez-vous, dont l'Afnic était partenaire, précédait de quelques jours le Forum 2026 du sommet mondial sur la société de l'information et AI for Good, le sommet mondial consacré aux usages de l'intelligence artificielle au service du bien social. Ce choix de calendrier, particulièrement pertinent, a permis aux acteurs francophones de confronter leurs expériences avant ces deux grandes discussions internationales sur l'avenir du numérique et de l'IA.



Trois thèmes ont structuré la journée : l'équilibre entre réglementation et innovation, les effets de l'IA sur l'accès à la connaissance et les conditions nécessaires au développement d'infrastructures durables et souveraines. Ces questions sont étroitement liées. Réglementer suppose de comprendre les technologies et les infrastructures sur lesquelles elles reposent. Préserver l'accès à la connaissance exige de soutenir les personnes et les institutions qui produisent les contenus. Quant à la souveraineté, elle dépend autant de la maîtrise des infrastructures que des compétences nécessaires pour les exploiter.

Réguler sans brider l'innovation

La première plénière de la journée est partie d'une opposition récurrente. D'un côté, la réglementation chercherait à protéger les utilisateurs et à prévenir les dommages. De l'autre, l'innovation aurait besoin de liberté, de prévisibilité et de rapidité. Les échanges ont d'abord rappelé qu'une règle pouvait avoir des effets très différents selon les acteurs auxquels elle s'applique. Une grande plateforme dispose d'équipes juridiques et techniques capables d'absorber de nouvelles obligations. Une jeune entreprise ou encore une université moins bien dotée peut, au contraire, se retrouver freinée par des procédures trop longues ou trop imprévisibles. Une réglementation uniforme en apparence peut ainsi renforcer les acteurs qui occupent déjà une position dominante.

Cela ne signifie pas que l'absence de règles favoriserait nécessairement l'innovation. Dans des domaines comme l'éducation, la santé ou la finance, les entreprises ont besoin de savoir quelles données personnelles elles peuvent utiliser, dans quelles conditions et avec quelles garanties pour les personnes concernées. Un cadre clair peut donc devenir un facteur de confiance et faciliter à ce titre le déploiement d'un service auprès des utilisateurs.

Plusieurs principes ont ainsi été défendus au cours des ateliers qui ont suivi cette première plénière, ceux de la proportionnalité des obligations, de la neutralité technologique, de la transparence, de la prévisibilité et de l'ouverture à l'expérimentation. A notamment été évoquée la possibilité de tester un service à petite échelle, pendant une durée limitée, sous le contrôle du régulateur, sous la forme d'un bac à sable réglementaire. Ce type d'expérimentation permet d'observer les risques réels avant d'autoriser un déploiement plus large ou d'adapter les règles existantes.

Une régulation équilibrée suppose par ailleurs que régulateurs, entreprises, chercheurs, utilisateurs et communauté technique travaillent ensemble à la conception et à l'évaluation des règles. Chacun dispose en effet d'une partie des informations et leurs expertises se complètent. Les entreprises connaissent les contraintes de développement, les régulateurs les objectifs de protection, les chercheurs les limites techniques et les utilisateurs les effets concrets des services.

La question de l'échelle a également été abordée. Si réguler au niveau national permet de tenir compte des besoins d'un pays et au niveau régional de faciliter l'harmonisation et d'éviter la multiplication de cadres incompatibles, certaines règles doivent rester internationales, car internet repose sur des standards communs et sur l'interconnexion de réseaux situés dans des juridictions différentes. L'enjeu est donc ici de réussir à répartir les responsabilités entre ces différents niveaux.

L'IA facilite l'accès au savoir, mais fragilise sa production

La deuxième plénière portait sur la manière dont l'IA transforme l'accès à la connaissance. Certains progrès sont évidents, comme les outils de traduction et d'interprétation qui permettent de rendre accessibles des documents qui ne l'étaient pas jusqu'alors pour des raisons linguistiques. Dans le monde, mais aussi dans un espace francophone composé de langues et de cultures très diverses, l'IA peut ainsi favoriser la circulation des savoirs.

Mais l'IA modifie aussi le chemin qui mène à l'information. C'est ce qu'a notamment expliqué Xavier Merlin, membre du collège de l'Arcep, en présentant les conclusions du récent rapport « *IA générative : des défis pour l'avenir de l'internet ouvert* »⁷ de l'Arcep. Là où un moteur de recherche propose des liens à consulter et à comparer, un assistant IA sélectionne plusieurs contenus pour produire directement une réponse, au risque de rendre moins visibles les sources utilisées et de réduire la liberté de choix de l'internaute.

7. Voir le rapport « *IA générative : des défis pour l'avenir de l'internet ouvert* », Arcep : https://www.arcep.fr/uploads/tx_gspublication/rapport-ia-generative-defis-internet-ouvert-janvier2026.pdf

Ces nouveaux usages de l'IA affectent également les producteurs de contenus. Les systèmes d'IA ont besoin de textes, d'images, de données et de bases de connaissances produites par de vraies personnes. Or, si les utilisateurs obtiennent une réponse sans consulter les sites d'origine, sans avoir parfois connaissance des sources utilisées, ces sites peuvent perdre une partie de leur audience. Pour les médias, les éditeurs ou les créateurs, cela peut fragiliser leurs revenus et, donc, le financement de nouveaux contenus. Pour les projets collaboratifs, tels que Wikipedia par exemple, cela peut réduire les occasions de transformer un lecteur en contributeur.

Comme nous l'expliquions déjà dans La Lettre Afnic n°13⁸, cela pourrait même, à terme, affecter l'IA elle-même. Les modèles ont besoin de contenus humains, récents et diversifiés. Si la production de ces contenus diminue, ou si les modèles sont de plus en plus entraînés sur des textes générés par d'autres modèles, leur matière première s'appauvrit, un phénomène appelé « effondrement des modèles ».

Préserver la diversité des contenus en ligne ne consiste pas seulement à en produire de nouveaux. Il faut aussi rendre accessibles ceux qui existent déjà mais qui n'ont pas encore été numérisés, notamment dans les bibliothèques et les fonds d'archives, tout en respectant les droits qui leur sont attachés. La consultation d'un document, son analyse automatique et son utilisation pour entraîner un modèle constituent en effet des usages différents qui ne soulèvent pas les mêmes questions de propriété intellectuelle, d'attribution et de rémunération.

L'atelier consacré à la numérisation des contenus inexploités, auquel participaient la Bibliothèque royale de Belgique et l'Organisation mondiale de la propriété intellectuelle, a par ailleurs montré l'ampleur du travail à accomplir. Numériser un fonds ne consiste pas uniquement à photographier des livres ou des archives. Pour qu'un contenu puisse être recherché, compris et réutilisé, il faut également le décrire, le contextualiser et lui associer des métadonnées. Sans cet effort, une partie du patrimoine francophone risque de rester absente des ressources accessibles en ligne et, par conséquent, des données utilisables par les systèmes d'IA.

La souveraineté se mesure à la capacité de maintenir un service

La troisième séquence était consacrée aux infrastructures durables et souveraines. La plupart des services numériques donnent une impression d'immatérialité. Ils reposent pourtant sur des infrastructures bien réelles, telles que des centres de données, des serveurs, des câbles, des réseaux électriques, des satellites ou encore des équipements de télécommunication. Leur fonctionnement dépend aussi de logiciels et de services, du cloud aux systèmes de résolution des noms de domaine.

La souveraineté ne se résume pas à la localisation de ces infrastructures et services. Un centre de données installé sur un territoire peut dépendre d'un logiciel étranger ou d'un prestataire unique. À l'inverse, une infrastructure exploitée avec des partenaires étrangers peut offrir

une certaine autonomie si elle repose sur des standards ouverts et permet de changer facilement de fournisseur.

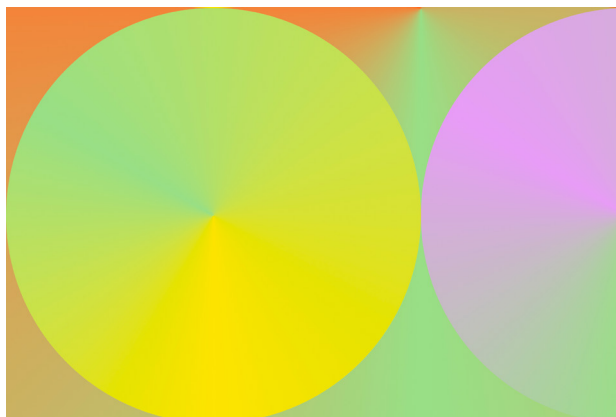
La véritable question, quand on parle de souveraineté, est celle de la continuité. Que se passe-t-il lorsqu'un câble est endommagé, lorsqu'un fournisseur interrompt un service ou lorsqu'une décision prise à l'étranger en limite soudainement l'accès ? Pour faire face, il faut pouvoir disposer de plusieurs routes, de solutions de remplacement et de personnes capables de maintenir ou de restaurer les services.

Les câbles sous-marins rendent cette dépendance particulièrement visible. Ils transportent la quasi-totalité des échanges intercontinentaux de données. Leur résilience dépend du nombre de routes disponibles, de la diversité des points d'atterrissage et de la rapidité des réparations. Ces mécanismes ont déjà été détaillés dans La Lettre Afnic n°9⁹, mais le FFGNIA les a replacés dans une réflexion plus large : un territoire ne peut agir que s'il dispose des compétences et des capacités techniques nécessaires pour assurer la continuité de ses communications.

Les échanges ont également porté sur la dépendance à l'égard de fournisseurs étrangers, illustrée par le cas des modèles d'IA Fable 5 et Mythos 5. En juin 2026, une décision américaine de contrôle des exportations a conduit Anthropic à suspendre l'accès à ses modèles pour l'ensemble de ses clients, partout dans le monde. L'interruption a été temporaire, les restrictions rapidement levées, mais cela a montré qu'un service utilisé dans plusieurs pays pouvait devenir indisponible pour tous à la suite d'une seule décision.

Rechercher davantage de souveraineté ne signifie néanmoins pas tout produire soi-même. Il s'agit plutôt de connaître et d'anticiper ses dépendances, de disposer de solutions de remplacement et de former les compétences nécessaires. Cette capacité doit aussi durer dans le temps. Une infrastructure que l'on ne peut pas alimenter, entretenir ou renouveler ne reste pas souveraine très longtemps. Durabilité et souveraineté se rejoignent ainsi autour d'une même question, celle de la viabilité des services essentiels.

8. Voir l'article « Intelligence artificielle : un nouvel enjeu de répartition des ressources et du capital dans l'économie numérique », Lettre Afnic n°13 : <https://www.afnic.fr/wp-media/uploads/2026/07/La-Lettre-Afnic-13.pdf>
9. Voir l'article « Internet face aux coupures de câbles sous-marins : pourquoi le réseau tient bon ? », Lettre Afnic n°9 : <https://www.afnic.fr/wp-media/uploads/2025/04/La-Lettre-Afnic-9.pdf>



Vers un agenda francophone du numérique

Le premier Forum francophone de la gouvernance du numérique et de l'intelligence artificielle en 2025 avait permis d'établir un espace de discussion et de dégager plusieurs priorités communes au sein de la communauté francophone¹⁰. Les participants avaient alors également exprimé le souhait de pérenniser cet espace de concertation. Un an plus tard, l'organisation d'une deuxième édition confirme cette volonté d'inscrire le FFGNIA dans la durée et de faire émerger un véritable agenda francophone de la gouvernance du numérique.

10. Voir l'article « *Un forum pour renforcer la voix des pays francophones dans les débats internationaux sur la gouvernance du numérique et de l'IA* », Lettre Afnic n°11 : <https://www.afnic.fr/wp-media/uploads/2025/12/La-Lettre-Afnic-N%C2%B011.pdf>





ENUM: pourquoi fermer ce qui fonctionne encore ?

● ENUM est un protocole assez méconnu de l'internet. Créé au début des années 2000, il permet d'utiliser le système des noms de domaine pour relier un numéro de téléphone à des services de communication en ligne. Son déploiement public est resté limité, mais différents pays conservent des délégations actives. Pourtant, une consultation lancée en 2026 par l'UIT-T, le Secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications (UIT), envisage la fermeture de ce dispositif. Au-delà du sort d'ENUM, une question se pose : qui peut décider du retrait d'une infrastructure, qui plus est dont la gouvernance est partagée entre des acteurs des télécommunications, des acteurs de l'internet et des États ?

ENUM: un pont entre le téléphone et l'internet

Les réseaux téléphoniques et l'internet se sont développés avec des systèmes d'adressage différents. Le téléphone utilise des numéros organisés selon un plan international tenu par l'UIT selon la recommandation UIT-T E.164 qui en définit la structure. Pour les numéros géographiques, E.164 associe ainsi un préfixe de pays (par exemple, 33 pour la France, généralement écrit +33) à un numéro national, l'ensemble étant limité à quinze chiffres. Sur internet, les communications s'appuient principalement sur des adresses IP et des noms de domaine. Les services sont ainsi accessibles au moyen d'adresses web, électroniques ou encore de téléphonie sur IP.

Au tournant des années 2000, alors que les communications commençaient à migrer vers l'internet, les acteurs des télécommunications ont cherché un moyen de faire le lien entre ces deux univers. C'est ainsi qu'est né le protocole ENUM, pour « *E.164 Number Mapping* ». Son principe consiste à transformer un numéro de téléphone en un nom de domaine qui peut être interrogé dans le DNS (*Domain Name System*). Avec ENUM, une recherche dans le DNS permet d'indiquer si un numéro de téléphone est associé à une adresse de téléphonie sur IP, à une adresse électronique ou à un autre service de communication. Le protocole est normalisé par l'IETF (*Internet Engineering Task Force*) dans la RFC 6116¹¹.

Deux grands types d'usage d'ENUM se sont ensuite développés. L'ENUM public utilise une branche particulière du DNS mondial, appelée e164.arpa. C'est celui-ci qui est concerné par une éventuelle fermeture. L'ENUM privé reprend le même principe dans les réseaux internes des opérateurs de télécommunications. Cette seconde forme n'est pas forcément visible depuis l'internet public, mais elle est utilisée pour orienter des appels ou faciliter l'interconnexion entre réseaux.

Le RIPE NCC à l'origine de la consultation sur ENUM

Le RIPE NCC est l'un des cinq registres régionaux de l'internet. Il est notamment chargé d'allouer et d'enregistrer les adresses IP en Europe, au Moyen-Orient et dans une partie de l'Asie centrale. Il tient également une base de données publique contenant des informations techniques sur ces ressources. Pour ENUM, il exerce une fonction différente: il est l'opérateur technique de la zone e164.arpa.

La controverse sur ENUM prend son origine dans les travaux du RIPE NCC sur les moyens d'interroger sa base de données. À côté de WHOIS, utilisé depuis plusieurs décennies pour interroger sa base de données, le RIPE NCC propose également un accès par RDAP, un protocole plus récent, plus structuré et mieux adapté aux usages actuels¹². C'est dans ce contexte que le cas d'ENUM a été soulevé. Si les données d'enregistrement ENUM sont actuellement

11. <https://datatracker.ietf.org/doc/html/rfc6116>

12. À ce sujet, voir l'article « *Mort* » du protocole WHOIS : comment son successeur RDAP modernise l'accès aux données d'enregistrement des noms de domaine » dans La Lettre Afnic n°9 : <https://www.afnic.fr/wp-media/uploads/2025/04/La-Lettre-Afnic-9.pdf>

accessibles via WHOIS, leur consultation via RDAP renvoie une erreur. La question était donc, au départ, assez circonscrite : fallait-il étendre la prise en charge d'ENUM au service RDAP du RIPE NCC ?

Dans une contribution datée du 22 janvier 2026¹³, le RIPE NCC a demandé la marche à suivre à la Commission d'études 2 de l'UIT-T, qui traite notamment des questions de numérotation internationale, dont le plan E.164. La contribution du RIPE NCC ne demandait pas explicitement la fermeture d'ENUM. Elle invitait toutefois la Commission à se prononcer sur des questions qui dépassaient largement la seule adaptation de RDAP : ENUM devait-il toujours être considéré comme actif ? Fallait-il continuer à en assurer le fonctionnement ? Un déclassement du protocole ou une réduction de sa prise en charge étaient-ils appropriés ?

La Commission d'études 2 a ainsi examiné le sujet lors de sa réunion de février 2026, examen qui a conduit à l'ouverture d'une consultation des États membres. Le 26 mars, le Bureau de la normalisation des télécommunications (TSB selon son acronyme anglais), qui assure le secrétariat de l'UIT-T et ses échanges officiels avec les administrations nationales, a ainsi diffusé la circulaire 123¹⁴, qui demande aux administrations des 194 États membres de l'UIT d'indiquer, avant le 15 août 2026, si elles approuvent ou rejettent la fermeture du système.

C'est ainsi qu'une question de compatibilité entre RDAP et ENUM a débouché sur une consultation des États concernant la fermeture du système ENUM public sous e164.arpa.

Un système dont les responsabilités sont partagées

Pour comprendre pourquoi la démarche a fait réagir, il faut revenir à la manière dont ENUM a été organisé. Le dispositif repose sur plusieurs institutions, dont les rôles se complètent :

- L'IETF a défini le protocole technique.
- En son sein, l'IAB (*Internet Architecture Board*) veille à la cohérence générale de l'architecture de l'internet. L'IAB est notamment responsable, en coopération avec l'ICANN, du domaine « .arpa », sous lequel se trouve la zone e164.arpa.
- Le RIPE NCC s'est vu confier l'exploitation technique de e164.arpa par l'IAB. Il publie la zone dans le DNS et met en œuvre les modifications validées selon les procédures établies.
- L'UIT-T intervient également, parce que les numéros de téléphone ne sont pas des ressources ordinaires de l'internet. Les indicatifs de pays relèvent du plan international E.164, tandis que les plans de numérotation nationaux sont administrés par les États. Au sein de l'UIT-T, c'est le TSB qui fait le lien avec les administrations nationales. Il vérifie notamment que toute demande de délégation de la branche correspondant à un indicatif de pays a bien reçu l'accord dudit pays.

- Enfin, lorsqu'un pays participe à ENUM, une sous-zone correspondant à son indicatif téléphonique lui est déléguée. Son nom est obtenu en inversant les chiffres de l'indicatif, puis en ajoutant « .e164.arpa » : le préfixe 33 de la France devient ainsi 3.3.e164.arpa. L'État reste l'autorité administrative de cette délégation et peut en confier l'exploitation technique à un organisme spécialisé.

Ce dispositif repose donc sur un équilibre : l'IETF définit le standard, l'IAB est responsable du domaine d'infrastructure, le RIPE NCC l'exploite, tandis que l'UIT et les administrations nationales garantissent la correspondance avec les indicatifs téléphoniques. Aucun de ces acteurs ne détient à lui seul toutes les compétences nécessaires pour retirer l'infrastructure publique e164.arpa.

L'IAB l'a d'ailleurs rappelé dans sa réponse du 22 juin à la circulaire 123¹⁵. La consultation des États peut fournir des informations utiles sur leurs besoins, mais elle ne peut pas, à elle seule, décider du sort de e164.arpa ou du protocole ENUM. Le passage éventuel de la RFC 6116 au statut « *Historic* », qui signifierait qu'elle n'est plus considérée comme une spécification actuelle, devrait suivre les procédures ouvertes et fondées sur le consensus de l'IETF. Le retrait de la zone publique nécessiterait dès lors une coordination entre l'IAB, l'UIT-T et le RIPE NCC.

Des délégations toujours actives

Il ne s'agit pas de présenter ENUM comme un succès. Le service destiné au grand public n'a jamais connu le développement imaginé au début des années 2000. La France conserve néanmoins plusieurs délégations actives, correspondant au +33 ainsi qu'à différents indicatifs ultra-marins. La Direction générale des entreprises représente l'État en tant qu'autorité administrative et c'est l'Afnic qui assure la maintenance technique des zones concernées.

La France n'est pas un cas isolé. D'autres pays maintiennent également leur délégation. Aux Pays-Bas, *Internet Society Nederland* a indiqué en mai 2026 que la zone associée au +31 était opérationnelle, protégée par DNSSEC, le mécanisme de sécurisation du DNS, et qu'aucune révocation n'était demandée. L'organisation dit même étudier de nouveaux usages de cette infrastructure¹⁶.

Chaque délégation correspondant à un indicatif de pays résulte de la décision d'un État de confier une responsabilité à une autorité ou à un opérateur identifié. Si les procédures existantes permettent déjà de retirer une délégation après consultation du pays concerné dès lors qu'elle est devenue inopérante, fermer l'ensemble d'e164.arpa aurait une tout autre portée. Cela supprimerait certes les délégations défaillantes, mais aussi celles qui fonctionnent encore et que les autorités concernées souhaitent conserver.

13. *Request for guidance from ITU-T SG2 on ENUM (e164.arpa) implementation in RDAP*, RIPE NCC : https://www.ripe.net/media/documents/ENUM_liaison_statement_ITU_T_SG2.pdf

14. Circulaire TSB 123, UIT-T : <https://datatracker.ietf.org/liaison/2150/>

15. <https://www.iab.org/announcements/iab-response-to-tsb-circular-123/>

16. Voir le message de Ruben Brave, président d'Internet Society Netherlands, publié le 2 mai 2026 sur la liste de diffusion du groupe de travail « Cooperation » de la communauté RIPE : <https://mailman.ripe.net/archives/list/cooperation-wg%4Oripe.net/thread/CTNLO6JUKXQA3MJV4VXRSQGLF4OA4JHB/>

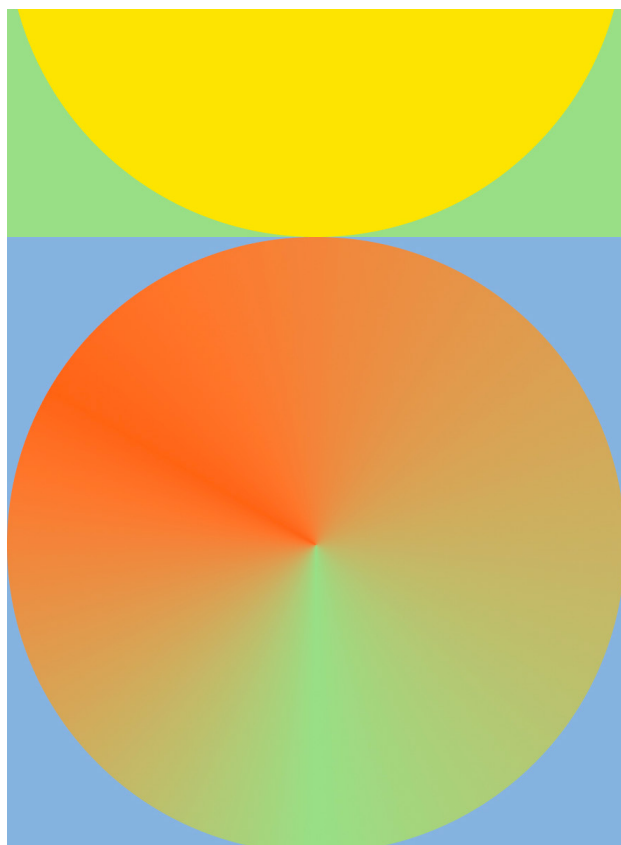
Une fermeture qui reste à justifier

Réexaminer une infrastructure ou un service ancien est légitime. Pour ENUM, la démarche pourrait conduire à corriger certaines configurations ou à retirer les délégations qui ne sont plus maintenues. Mais elle ne doit pas nécessairement mener à la fermeture de toute l'infrastructure.

La circulaire 123 mentionne le coût du maintien et de la modernisation d'ENUM, mais ne chiffre pas ces dépenses. Elle n'explique pas non plus pourquoi les difficultés constatées localement imposeraient une fermeture générale plutôt qu'un traitement ciblé des délégations concernées.

Les conséquences d'une fermeture restent également à évaluer. Des opérateurs de télécommunications et certains fournisseurs d'accès utilisent ENUM dans leurs réseaux internes. Ces systèmes reposent souvent sur des espaces DNS privés, indépendants de la zone e164.arpa. Certaines architectures techniques permettent toutefois aussi de réutiliser la zone publique ou certaines de ses délégations. Les informations disponibles ne permettent pas de savoir si de telles dépendances existent encore chez des opérateurs. Il n'est donc pas possible d'écarter d'éventuels effets collatéraux sans les interroger.

Avant toute décision, il faudrait ainsi préciser les économies attendues, recenser les systèmes susceptibles d'être touchés et prévoir les conditions d'une éventuelle transition. Le faible usage visible d'ENUM public ne suffit pas à établir que la fermeture d'e164.arpa serait sans conséquence, tout en posant des questions importantes en matière de gouvernance d'internet. En l'état des informations disponibles, une remise en ordre ciblée des délégations paraît plus appropriée qu'une fermeture.



04

Brèves

L'Afnic s'associe à l'École Polytechnique et l'UC Louvain pour lancer une thèse sur l'impact des agents IA sur internet

L'Afnic et l'École Polytechnique en cotutelle avec l'UC Louvain, viennent de lancer une thèse CIFRE intitulée « *How do AI agents reshape the Internet?* » (comment les agents IA remodelent-ils internet ?), consacrée aux effets concrets des agents d'intelligence artificielle sur l'architecture, le trafic et l'économie de l'internet.

Avec l'essor d'outils d'IA capables de rechercher, résumer ou restituer directement des informations, une partie des usages du web pourrait subir une nouvelle évolution. L'utilisateur ne consulte plus toujours un site directement, mais passe par un agent IA qui interroge le web à sa place ou s'appuie sur des informations déjà intégrées dans son modèle. Ces nouveaux usages entraînent de profonds changements : économiques, tout d'abord, car les sites risquent de perdre une partie de leurs revenus liés aux visites et à la publicité ; techniques, ensuite, car les flux ne circulent plus seulement entre les services web et les utilisateurs, mais passent aussi par les infrastructures des fournisseurs d'IA, ce qui modifie la topologie du trafic.

La thèse « *How do AI agents reshape the Internet?* » visera tout d'abord à mesurer quantitativement l'impact des agents IA sur le trafic internet : génèrent-ils une hausse du volume global de requêtes ou déplacent-ils simplement une partie du trafic existant ? Elle cherchera également à identifier et classer le trafic généré par ces agents, afin de le distinguer du trafic humain ou des bots classiques. Pour cela,

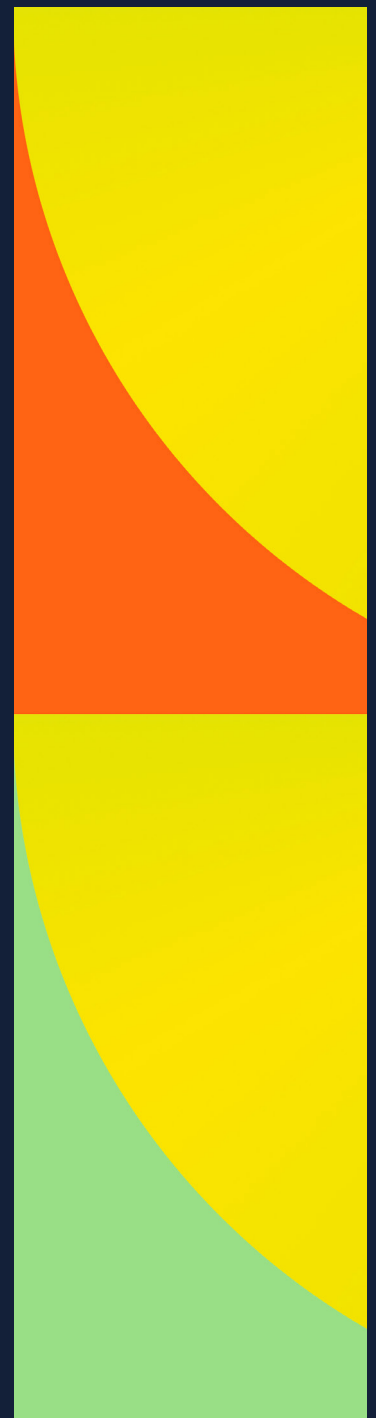
la recherche s'appuiera sur des données de trafic collectées à différents niveaux, notamment au niveau du DNS.

Un autre volet portera sur les possibles effets de centralisation. Le recours aux agents IA pourrait déplacer une partie du trafic vers un nombre restreint d'intermédiaires techniques, notamment les infrastructures des fournisseurs d'IA et les grands clouds. La recherche analysera ainsi la manière dont ces nouveaux usages peuvent modifier la circulation du trafic et s'intéressera aux adaptations possibles des protocoles réseau pour gérer ce nouveau type de flux.

Cette thèse, menée en collaboration entre l'École Polytechnique, l'UC Louvain et l'Afnic, s'inscrit dans une démarche de recherche appliquée, où l'expertise technique du DNS et de l'infrastructure internet joue un rôle central.

Reveal Day : la liste des candidatures à de nouvelles extensions internet bientôt dévoilée par l'ICANN

Le 12 août dernier, l'ICANN (*Internet Corporation for Assigned Names and Numbers*) a refermé la fenêtre de candidature au prochain cycle de création de nouvelles extensions internet personnalisées. Après plusieurs semaines consacrées aux vérifications administratives, l'ICANN devrait publier le 14 octobre 2026 la liste des projets déposés. Cette date, appelée « *Reveal Day* » ou « Jour du dévoilement », permettra de connaître les extensions demandées, qu'elles correspondent à une marque,





à un terme générique, à un territoire ou à une communauté, et les organisations qui les portent. On saura alors le nombre de projets déposés et les principaux secteurs concernés.

L'ICANN rendra également publiques certaines parties des dossiers et indiquera quelles candidatures portent sur une même extension. Dans cette hypothèse, les candidats qui avaient prévu une chaîne de remplacement dans leur dossier disposeront de quatorze jours pour éventuellement y recourir et substituer celle-ci à leur premier choix. Passé ce délai, l'ICANN publiera, lors du « *String Confirmation Day* » ou « Jour de la confirmation des chaînes » attendu en novembre, la liste confirmée des extensions demandées ainsi qu'une première liste des candidatures concurrentes.

Le *Reveal Day* et le *String confirmation Day* sont ainsi les deux prochaines étapes importantes du processus d'attribution des nouvelles extensions internet, mais surtout le point de départ d'une phase d'examen public appelée à se poursuivre pendant plusieurs mois. C'est en effet à leur suite que s'ouvriront les possibilités de commentaire et d'objection formelle, notamment en cas de risque de confusion avec une autre extension, d'atteinte à des droits, à l'intérêt public ou aux intérêts d'une communauté, avant la poursuite des évaluations qui pourraient conduire les premiers candidats retenus à signer un contrat avec l'ICANN à partir de la fin de l'année 2027.

Nouvel état d'alerte de sécurité nationale dans la Loi de programmation militaire : quels enjeux pour l'Afnic ?

L'article 21 du projet d'actualisation de la loi de programmation militaire 2024-2030¹⁷ prévoit la création d'un nouveau régime d'exception : l'état d'alerte de sécurité nationale. Déclenché par décret en conseil des ministres en cas de menace grave et actuelle pesant sur la sécurité nationale, ce dispositif viserait à donner à l'État des moyens d'action renforcés pour répondre rapidement à une situation de crise susceptible d'affecter la continuité des activités essentielles à la vie de la Nation ou de justifier le déploiement rapide de forces armées sur le territoire national.

Des mesures pourraient alors être prises pour renforcer la sécurité et la continuité d'activité d'opérateurs jugés essentiels, notamment les opérateurs d'importance vitale ou ceux dont la perturbation pourrait gravement affecter l'économie, la société, la défense ou la sécurité nationale.

Dans un tel contexte, le DNS pourrait avoir un rôle à jouer. L'accès à certaines données DNS peut en effet aider à reconstituer une infrastructure d'attaque, tandis que des injonctions sur des noms de domaine malveillants peuvent contribuer à en limiter ou neutraliser l'usage. Or, depuis la LPM de 2023, l'ANSSI peut déjà obtenir des données techniques anonymisées issues des caches DNS des résolveurs¹⁸ et demander, dans certaines hypothèses, des mesures portant sur un nom de domaine telles que son blocage ou sa suspension¹⁹.

Pour l'Afnic, l'enjeu de l'actualisation de la LPM 2024-2030 tient donc moins à la création de nouvelles mesures propres au DNS qu'à l'articulation entre ce nouveau régime d'alerte et les leviers déjà existants en matière de cybersécurité.

L'UNESCO et l'ICANN publient une note d'orientation sur l'acceptation universelle

L'UNESCO et l'ICANN ont lancé ce 3 juillet 2026, à l'occasion du deuxième Forum francophone sur la gouvernance du numérique et de l'IA, la version française de leur note d'orientation conjointe sur l'acceptation universelle, intitulée « *Promouvoir l'Acceptation universelle de tous les noms de domaine et adresses de courrier électronique en vue d'un internet multilingue* »²⁰.

Le principe d'acceptation universelle (*Universal Acceptance* en anglais) est simple : un nom de domaine ou une adresse électronique techniquement valides devraient fonctionner partout, quels que soient leur longueur, leur extension ou les caractères employés. Or, ce n'est pas toujours le cas. Les standards techniques permettant de créer des noms de domaine et des adresses électroniques dans différents alphabets existent déjà, mais leur prise en charge n'est pas systématique dans de nombreux services en ligne. Au-delà des dysfonctionnements techniques, l'enjeu est aussi linguistique. Il s'agit

de permettre à chacun d'utiliser internet dans sa langue et son système d'écriture.²¹

La promotion du multilinguisme et de la diversité linguistique dans l'espace numérique s'inscrit de longue date dans le mandat de l'UNESCO. Au travers de leur note d'orientation, l'UNESCO et l'ICANN appellent ainsi à agir au-delà de la seule dimension technique et proposent une approche structurée autour de quatre dimensions : la sensibilisation, l'appui aux politiques publiques, la mise en œuvre et le renforcement des capacités. Leur approche déplace donc le sujet de la disponibilité des standards à leur adoption effective par l'ensemble des acteurs. Elle s'inscrit dans la mise en œuvre du Pacte numérique mondial et des conclusions de la revue à 20 ans du SMSI, qui réaffirment l'objectif d'un internet accessible dans toutes les langues et tous les systèmes d'écriture.

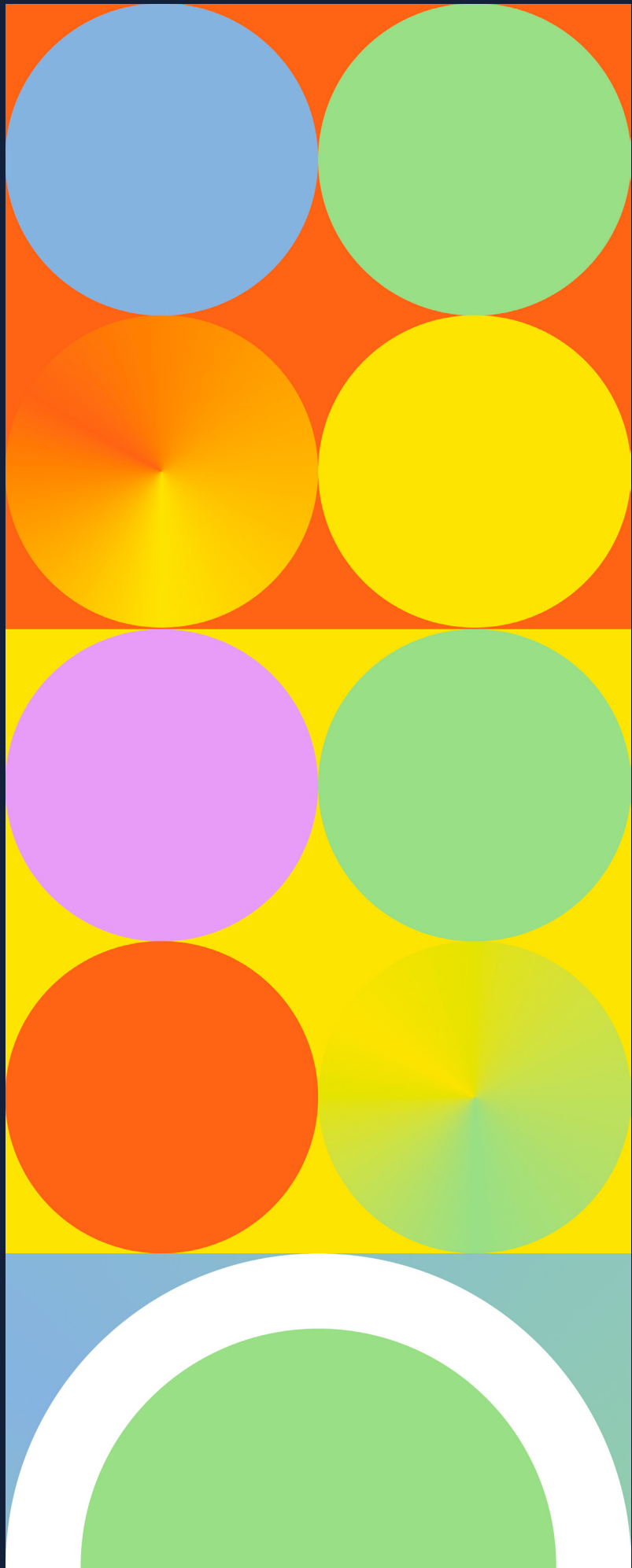
17. https://www.assemblee-nationale.fr/dyn/17/textes/I17b2695_texte-adopte-commission.pdf

18. Code de la défense, article L2321-3-1 : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047920558

19. Code de la défense, article L2321-2-3 : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047920539

20. Le document peut être consulté et téléchargé sur UNESDOC, la bibliothèque numérique de l'UNESCO : https://unesdoc.unesco.org/ark:/48223/pf0000398138_fre

21. Pour une présentation détaillée de l'Universal Acceptance et des obstacles techniques à sa mise en œuvre, consulter l'article « *Universal Acceptance : les défis d'un internet linguistiquement inclusif* » dans La Lettre Afnic n°4 : <https://www.afnic.fr/wp-media/uploads/2023/12/La-Lettre-Afnic-N%C2%B04.pdf>





L'Afnic y était

Forum 2026 du SMSI, du 6 au 10 juillet 2026, Genève, Suisse

L'Afnic était partenaire du Forum 2026 du Sommet mondial sur la société de l'information (SMSI), qui s'est tenu du 6 au 10 juillet à Genève, dans le cadre de la Semaine numérique de Genève. Celle-ci réunissait également le premier Dialogue mondial de l'ONU sur la gouvernance de l'IA (6 et 7 juillet), lors duquel Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique, est notamment intervenue, et le Sommet mondial sur l'intelligence artificielle au service du bien social, ou *AI for Good* (7 au 10 juillet). Cette séquence avait été précédée, le 3 juillet, du deuxième Forum francophone de la gouvernance du numérique et de l'intelligence artificielle (FFGNIA)²².

Outre les nombreuses rencontres bilatérales lors de ce Forum 2026 du SMSI, l'Afnic a participé à plusieurs sessions, notamment :

- La session de haut niveau « De l'accès à l'impact : un moteur pour le développement des infrastructures TIC », qui s'est intéressée à ce qui, au-delà du déploiement des réseaux et des infrastructures, permet aux populations d'accéder réellement aux services numériques. Une connexion ne suffit en effet pas si son coût reste trop élevé, si les compétences manquent ou si les utilisateurs ne disposent pas de contenus locaux et de services dans leur langue.
- La session « Post-quantique : préparer l'Internet à la cryptographie post-quantique », coordonnée par l'Afnic et la coalition dynamique de l'IGF sur les standards, la sécurité et la sûreté

sur Internet (IS3C), qui a porté sur les effets attendus de l'informatique quantique sur la sécurité de l'internet, notamment celle du DNS. Si la menace n'est pas immédiate, l'adaptation des standards, des équipements et des infrastructures prendra plusieurs années et doit donc être anticipée²³.

- La session « Façonner des sociétés intelligentes : le rôle des partenariats multi-parties prenantes », dont l'Afnic a assuré la modération, qui portait sur la place de ces partenariats dans la gouvernance du numérique. Les discussions ont mis en avant la complémentarité des pouvoirs publics, du secteur privé, de la société civile, de la communauté technique et du monde académique. Une approche confortée par le SMSI+20, la revue à vingt ans du SMSI, qui avait réaffirmé en décembre 2025 le modèle multi-acteurs de la gouvernance de l'internet²⁴.
- La session « Du dialogue à la pratique : les laboratoires multi-parties prenantes pilotés par les FGI régionaux et nationaux (NRI) pour la mise en œuvre des résultats du SMSI », qui a exploré le concept des laboratoires NRI, des espaces envisagés pour le partage d'expériences entre les initiatives nationales et régionales du Forum sur la gouvernance de l'Internet. L'objectif est de faire remonter les enseignements tirés au niveau local vers le FGI monde, puis vers le Forum du SMSI, afin de contribuer à la mise en œuvre des conclusions du SMSI+20 et du Pacte numérique mondial.

22. Voir l'article dédié dans ce même numéro.

23. À ce sujet, voir l'article « La transition vers la cryptographie post-quantique doit s'engager sans attendre », La Lettre Afnic n°12 : https://www.afnic.fr/wp-media/uploads/2026/03/La-Lettre-Afnic-12_170326.pdf

24. Voir l'article « Revue à 20 ans du SMSI : le texte final a été adopté par consensus à New York », La Lettre Afnic n°12 : https://www.afnic.fr/wp-media/uploads/2026/03/La-Lettre-Afnic-12_170326.pdf

5

L'Afnic y était

ICANN 86, du 8 au 11 juin 2026, Séville, Espagne

Lors du forum ICANN 86 organisé à Séville en juin dernier, l'Afnic a notamment suivi la session plénière consacrée aux effets actuels et à venir de l'intelligence artificielle sur les abus DNS. Devant une salle comble, les discussions ont examiné ce que l'IA change pour les attaquants, mais aussi pour les défenseurs.

Parmi les principaux points abordés lors de cette session :

- Une distinction importante a été rappelée entre automatisation et intelligence artificielle. Il est en effet possible d'automatiser l'enregistrement de noms de domaine à des fins abusives sans utiliser d'IA. Et si l'IA peut accroître l'ampleur et la qualité des attaques, les données présentées ne permettent pas encore d'en mesurer précisément l'impact, notamment parce qu'il est difficile de distinguer les campagnes assistées par IA de celles qui reposent sur une automatisation classique.
- Les discussions ont également porté sur l'évolution du rapport entre attaquants et défenseurs. Ces derniers disposent eux aussi de l'IA pour détecter les abus et y répondre. L'idée d'un écart nécessairement croissant entre les deux camps a ainsi été nuancée.
- Quant aux formes que pourraient prendre les attaques à l'avenir, la possibilité d'agents IA ciblant d'autres agents IA a été évoquée. La manière de répondre à ces attaques reste toutefois une question ouverte.
- L'identification des agents IA intervenant dans l'enregistrement de noms de domaine constitue enfin un autre point d'attention. Comment les identifier et assurer la traçabilité de leurs interventions lorsqu'ils agissent pour une personne ou pour un autre agent, tout en protégeant les données personnelles ?

L'IA ne change ainsi pas fondamentalement la nature des abus DNS, mais en transforme l'économie en rendant les outils d'attaque plus accessibles, en augmentant la vitesse et la qualité des campagnes et en compliquant certaines défenses. Dans ce contexte, la plénière s'est terminée sur un appel à la vigilance, à l'esprit critique et au partage d'expériences, tout en soulignant le décalage entre la rapidité des évolutions techniques et le temps nécessaire à l'élaboration des politiques et des standards.

Les prochains événements auxquels l'Afnic participe :

- 17 au 22 octobre 2026

ICANN 87

Bali, Indonésie

- 26 au 30 octobre 2026

RIPE 93

Sofia, Bulgarie

- 3 novembre 2026

Forum français sur la gouvernance d'Internet

Paris, France

- 9 et 10 novembre 2026

OARC 47

Vancouver, Canada

- 9 au 27 novembre 2026

Conférence de plénipotentiaires de l'UIT

Doha, Qatar

- 14 au 20 novembre 2026

IETF 127

San Francisco, USA

- 13 au 18 décembre 2026

Internet Governance Forum 2026

Nairobi, Kenya

- 18 au 29 janvier 2027

Réunions des groupes de travail du Conseil de l'IUT

Genève, Suisse

Votre contact

lalettre@afnic.fr

Directeur de publication: Pierre Bonis

Afnic | www.afnic.fr

7 avenue du 8 Mai 1845,
78280 Guyancourt