Internet
made in France

La lettre n°9

1

« Mort » du protocole WHOIS : comment son successeur RDAP modernise l'accès aux données d'enregistrement des noms de domaine

Depuis plus de 40 ans, le protocole WHOIS permet d'accéder aux informations d'enregistrement des noms de domaine, comprenant notamment les nom et prénom du titulaire, ses coordonnées, la date de création et d'expiration de son domaine, ou encore des informations techniques s'y rapportant, notamment le bureau d'enregistrement auquel le nom de domaine est rattaché. Initialement conçu pour offrir un moyen de contacter le gestionnaire d'un nom de domaine en cas de problème technique, le WHOIS est aujourd'hui progressivement abandonné au profit d'un autre protocole : RDAP.

L'origine du protocole WHOIS et ses limites actuelles

Le protocole WHOIS a vu le jour dans les années 1980, à une époque où internet était encore un réseau essentiellement académique et militaire. Son objectif était simple : fournir un moyen d'interroger des bases de données contenant des informations d'enregistrement des noms de domaine et des adresses IP. Basé sur une requête envoyée en texte brut via le port 43, il permet d'accéder à ces données stockées par les registres et les bureaux d'enregistrement.

Si cette approche a longtemps semblé suffisante, les utilisateurs l'ont utilisé pour des buts qui n'étaient pas initialement les siens, à savoir « vérifier » les données des titulaires et non simplement les « contacter ». Si on ajoute le fait que ces données sont masquées pour des raisons légitimes de protection des données personnelles[1] , l'utilisation du protocole a commencé à poser problème et à nécessiter une autre approche. Le WHOIS ne prévoit en effet aucun mécanisme de contrôle d'accès : une requête retourne systématiquement à tous les mêmes informations d'enregistrement, selon la politique du registre concerné. À l'époque de sa création, la logique était celle de la transparence : un nom de domaine étant une ressource technique, son titulaire devait pouvoir être contacté facilement.

Cette transparence a fini par poser problème sur plusieurs plans :

- **La sécurité et la confidentialité.** Les informations personnelles des titulaires de noms de domaine étaient accessibles à tous, sans distinction entre personnes physiques et morales, du moins pour la majorité des extensions de premier niveau génériques comme le .com. Cette exposition a, par le passé, donné lieu à de nombreux abus, du spam ciblé aux tentatives d'usurpation d'identité.

  Plus récemment, des chercheurs ont également démontré que les informations accessibles via WHOIS pouvaient être exploitées pour contourner certaines vérifications de propriété de domaine et obtenir frauduleusement des certificats TLS, un risque souligné par Google qui recommande d'abandonner l'usage du WHOIS dans ces procédures.

- **L'absence de standardisation des réponses.** Chaque registre structurant ses bases de données différemment, l'exploitation automatisée des données est compliquée. Le protocole ne permettant pas de normaliser la manière dont les informations sont fournies, cela pose de nombreux problèmes d'interopérabilité.

  De plus, certains registres fonctionnent sur un modèle dit « *thin WHOIS* », où seules les informations techniques sont centralisées par le registre, tandis que les bureaux d'enregistrement gèrent toutes les données des titulaires ; et d'autres adoptent un modèle « *thick WHOIS* », où toutes les informations d'enregistrement sont stockées directement par le registre (voir notre encadré). Cette diversité complexifie l'accès aux informations et leur régulation.

- **Les évolutions réglementaires,** et notamment l'entrée en vigueur du RGPD, ont rendu difficile la compatibilité du WHOIS avec les nouvelles exigences en matière de protection des données.

Conçu pour un internet ouvert et collaboratif, le protocole WHOIS s'est ainsi retrouvé dépassé par la complexité croissante de l'écosystème des noms de domaine et les évolutions réglementaires. Ce qui a précipité la nécessité d'un protocole plus moderne et structuré.

« *Thin WHOIS* » vs. « *Thick WHOIS* » : deux modèles de gestion des données d'enregistrement

Tous les registres de noms de domaine ne stockent pas les mêmes informations dans leurs bases de données. On distingue deux modèles : le « *thin WHOIS* » et le « *thick WHOIS* » :

- **Dans un modèle « *thin WHOIS* »**, le registre ne conserve que des données techniques sur le nom de domaine (comme les serveurs DNS) et délègue la gestion des informations du titulaire aux bureaux d'enregistrement. C'est le modèle utilisé pour des extensions comme .com ou .net, où les données des titulaires sont stockées et gérées directement par le bureau d'enregistrement choisi par l'utilisateur.

- **À l'inverse, un modèle « *thick WHOIS* »** centralise toutes les informations d'enregistrement directement dans la base de données du registre. Cela signifie que les informations des titulaires, y compris leurs coordonnées, sont stockées et accessibles via une seule source, simplifiant ainsi la gestion des accès et le contrôle des données. Ce modèle est utilisé par certains gTLD comme .info et par des ccTLD comme .fr.

Le modèle « *thick WHOIS* » présente plusieurs avantages par rapport au « *thin WHOIS* ». En centralisant toutes les données au niveau du registre, il permet une gestion plus homogène de l'accès aux informations, réduit la dépendance aux bureaux d'enregistrement et facilite la mise en œuvre de contrôles réglementaires, notamment en matière de conformité au RGPD. De plus, en cas de litige ou d'enquête, il est plus simple d'accéder aux informations d'un titulaire sans avoir à naviguer entre plusieurs bureaux d'enregistrement aux pratiques potentiellement différentes.

1. L'Afnic a été un registre pionnier au niveau mondial, en masquant les données personnelles dès 2006, tout en mettant en place un mécanisme de levée d'anonymat simple et rapide pour les autorités et les ayant droit.
   Voir https://www.afnic.fr/noms-de-domaine/resoudre-un-litige/demande-divulgation-donnees/

Le RGPD et l'anonymisation massive des données d'enregistrement : une erreur d'interprétation fatale ?

En mai 2018, l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) a marqué un tournant pour la gestion des données d'enregistrement des noms de domaine. Conçu pour encadrer le traitement des informations personnelles en Europe, le RGPD imposait de nouvelles obligations aux acteurs de l'écosystème des noms de domaine, notamment en ce qui concerne la collecte et la divulgation des données des titulaires.

Jusqu'alors, le WHOIS permettait d'accéder librement aux informations des titulaires, qu'ils soient des personnes physiques ou morales. Le RGPD, lui, visait uniquement la protection des données personnelles des individus — les entreprises et autres organisations n'étaient donc pas concernées par ces restrictions. Pourtant, au lieu d'adopter une approche mesurée et proportionnée, l'ICANN a pris la décision radicale de masquer toutes les informations nominatives, y compris celles des personnes morales, rendant le WHOIS globalement inutile.

Cette décision ne s'est appliquée qu'aux extensions sous la régulation de l'ICANN, notamment les gTLD (les domaines de premier niveau génériques, comme .com, .org ou .net). Les ccTLD (les domaines de premier niveau nationaux, comme le .fr pour la France ou le .de pour l'Allemagne), quant à eux, relevant de l'autorité de leur registre national, ont eu la liberté de définir leurs propres règles. Certains ont suivi la même approche que l'ICANN, tandis que d'autres ont maintenu un certain niveau d'accès aux données d'enregistrement, comme le .fr qui continue à publier les données des personnes morales.

Dans ce contexte, les bureaux d'enregistrement et registres opérant sous l'autorité de l'ICANN ont appliqué une politique de « *restricted for privacy* » sur l'ensemble des données non techniques des titulaires, ne laissant accessibles que les informations strictement liées au fonctionnement du domaine, comme les serveurs DNS. Cette anonymisation massive a eu des effets immédiats et problématiques : les ayants droit, qui se reposaient sur le WHOIS pour lutter contre le cybersquatting et la contrefaçon, se sont retrouvés dans l'incapacité d'identifier facilement les responsables de certains sites frauduleux. Les autorités de certification, qui utilisaient le WHOIS et ces données pour valider l'authenticité des certificats SSL, ont dû revoir leurs procédures. Même les forces de l'ordre ont rencontré des obstacles dans leurs enquêtes sur des activités illicites en ligne.

C'est ainsi que la mort du WHOIS a été précipitée. Un protocole dont l'utilité reposait sur l'accès à des informations d'enregistrement devenait, par définition, obsolète dès lors que ces données disparaissaient. En vidant le WHOIS de sa substance, l'ICANN a accéléré la transition vers un nouveau modèle de gestion des accès aux informations d'enregistrement : le RDAP.

NIS2 : un autre cadre réglementaire qui impacte la gestion des données d'enregistrement

Adoptée par l'Union européenne, la directive NIS2 *(Network and Information Security 2)* vise à renforcer la cybersécurité des infrastructures critiques, y compris celles liées aux noms de domaine. L'article 28 de cette directive, notamment, impose aux registres et bureaux d'enregistrement de nouvelles obligations en matière de collecte, de vérification et d'accès aux données d'enregistrement des noms de domaine. Ils doivent désormais :

- **Collecter et maintenir des données d'enregistrement précises et complètes** dans une base de données dédiée.
- **Vérifier ces données,** afin de garantir qu'elles soient exactes et à jour.
- **Permettre un accès rapide aux « demandeurs légitimes »** (autorités judiciaires, forces de l'ordre, etc.), avec une obligation de réponse dans les 72 heures.
- **Rendre publiques les données** qui ne sont pas considérées comme des données personnelles.

Si cette approche vise à lutter contre les abus en ligne et à harmoniser les pratiques en matière de transparence des données d'enregistrement, elle entretient également une ambiguïté quant au rôle réel de ces informations dans le fonctionnement du DNS. L'article 28 justifie en effet ces obligations en affirmant qu'elles contribuent à « *la sécurité, la stabilité et la résilience du DNS* ». Cette formulation laisse entendre que les données d'enregistrement des noms de domaine sont techniquement nécessaires au bon fonctionnement du DNS, ce qui n'est pas le cas. À tel point que, même si le WHOIS était définitivement coupé et n'était pas remplacé par RDAP, cela n'empêcherait pas le DNS de fonctionner.

Pour une analyse plus approfondie de l'impact de NIS2 sur l'écosystème des noms de domaine, consultez l'article « *La directive NIS2 va indéniablement renforcer la cybersécurité au sein de l'Union européenne, mais attention aux effets de bord* » paru dans La Lettre Afnic #6.

RDAP : un protocole pensé pour dépasser les limites du WHOIS

Face à l'impasse créée par l'anonymisation excessive des données d'enregistrement, la nécessité d'un protocole plus adapté est devenue évidente. En réalité, l'IETF *(Internet Engineering Task Force)* avait dès 2015 anticipé les problématiques soulevées par le WHOIS, et conçu le RDAP pour le remplacer. Ce protocole apporte deux évolutions majeures qui redéfinissent l'accès aux données d'enregistrement :

- **Une infrastructure plus moderne.** La première grande différence entre les deux protocoles réside dans leur architecture technique. WHOIS est un protocole certes fonctionnel mais vieillissant, limité par l'absence de standardisation : chaque registre peut en effet structurer ses bases différemment, ce qui complique l'interopérabilité et l'exploitation automatisée des données. RDAP, en revanche, repose sur des API et un format de réponse structuré en JSON (pour *JavaScript Object Notation*, un format de données textuelles structuré), ce qui permet aux machines d'interpréter plus facilement les résultats et d'intégrer les données dans des systèmes tiers sans besoin d'intervention manuelle.
- **Une gestion différenciée des accès.** Le plus grand changement apporté par RDAP est la gestion des droits d'accès. Contrairement à WHOIS, où tout le monde voit exactement les mêmes informations sans distinction, RDAP permet d'attribuer des niveaux d'accès différenciés en fonction de l'utilisateur. Un internaute lambda pourra consulter certaines données publiques, tandis qu'un ayant droit, une autorité de régulation ou une entité gouvernementale pourra obtenir des informations plus détaillées après authentification. Ce modèle répond directement aux problématiques soulevées par le RGPD : les données sensibles des particuliers ne sont plus accessibles à tous, mais restent consultables par les acteurs ayant un intérêt et un besoin légitimes d'y accéder.

C'est cette capacité à équilibrer protection des données et accès contrôlé qui a poussé l'ICANN à rendre RDAP obligatoire pour tous les gTLD et bureaux d'enregistrement accrédités. Si le WHOIS reste encore techniquement fonctionnel, son utilisation est désormais limitée, et l'ICANN a acté sa disparition avec un programme de « *sunset* » officiel, c'est-à-dire un retrait planifié et progressif du protocole.

« Launching RDAP ; Sunsetting WHOIS »

Le passage de WHOIS à RDAP ne s'est pas fait du jour au lendemain. Comme pour toute transition impliquant des infrastructures techniques majeures, le déploiement de RDAP a été progressif et encadré. Dès 2019, l'ICANN a imposé aux bureaux d'enregistrement et aux registres des gTLD de mettre en place ce nouveau protocole, sans pour autant immédiatement couper le WHOIS. Cette cohabitation des deux systèmes a permis d'assurer une continuité de service tout en laissant aux acteurs du marché le temps d'adapter leurs infrastructures.

Depuis le 28 janvier 2025, toutefois, RDAP est devenu le seul protocole officiellement reconnu par l'ICANN pour la remontée des informations d'enregistrement. Cela signifie que, pour les gTLD et les bureaux d'enregistrement accrédités par l'ICANN, le WHOIS est en phase de « *sunset* », progressivement déprécié et remplacé par RDAP.

Mais cela ne signifie pas que le WHOIS disparaît totalement. Certains registres, notamment parmi ceux gérant des ccTLD indépendants de l'ICANN, n'ont pas encore mis en place RDAP et continuent d'utiliser exclusivement WHOIS. D'autres ont adopté RDAP tout en conservant WHOIS en parallèle. C'est notamment le cas de l'Afnic, qui a anticipé la transition vers RDAP dès 2021, malgré l'absence d'une obligation imposée par l'ICANN.

> **Cela lui a permis de définir des niveaux d'accès différenciés aux données d'enregistrement, en fonction du profil et des besoins des demandeurs.**

Ainsi, certaines autorités publiques françaises, comme la CNIL, le FISC ou les forces de l'ordre, bénéficient d'un accès facilité, sur simple authentification, à l'ensemble des données d'enregistrement des noms de domaine en .fr, tandis que les autres utilisateurs doivent justifier d'un besoin légitime.

Des adaptations nécessaires pour les acteurs de l'écosystème des noms de domaine

Pour les bureaux d'enregistrement soumis aux règles de l'ICANN, cette transition a nécessité des adaptations techniques importantes. WHOIS fonctionne sur un modèle simple et universel, tandis que RDAP repose sur une gestion différenciée des accès. Cela implique non seulement la mise en place d'API conformes aux standards RDAP, mais aussi l'intégration de systèmes d'authentification et d'autorisation permettant de définir qui peut voir quelles informations. Le passage à RDAP a ainsi nécessité des investissements techniques pour adapter les infrastructures, mais aussi pour former les équipes à la gestion des nouveaux mécanismes d'authentification et d'autorisation.

Les bureaux d'enregistrement et les registres ont en effet dû s'adapter à une nouvelle dynamique centrée sur la gestion des données personnelles. Avec le WHOIS, l'accès était binaire : soit une information était visible, soit elle ne l'était pas. Avec RDAP, la granularité des accès implique une relation plus fine entre les différents acteurs de l'écosystème, notamment pour déterminer qui est légitime à consulter quelles données.

Une réponse aux limites du WHOIS, mais pas une solution absolue

La disparition progressive du WHOIS n'est pas réellement le résultat d'un besoin de modernisation, mais avant tout d'une série d'évolutions réglementaires et de choix s'y rapportant. Le protocole a longtemps rempli sa fonction, offrant un accès simple et direct aux informations des titulaires de noms de domaine. Mais avec le renforcement des exigences en matière de protection des données, notamment dans le cadre du RGPD, son fonctionnement est devenu de plus en plus difficile à concilier avec ces nouvelles contraintes.

C'est surtout l'interprétation excessive du RGPD par l'ICANN qui est en cause. Le WHOIS est alors devenu largement inutilisable dans de nombreux cas, précipitant la nécessité d'un nouveau modèle. RDAP s'inscrit dans cette continuité, avec une approche plus fine et adaptable, permettant de différencier les accès en fonction des besoins et des profils des utilisateurs.

Toutefois, cette transition ne règle pas tous les débats. Rappelons que WHOIS et RDAP ne sont que des protocoles d'accès, pas les bases de données en elles-mêmes. Leur évolution ne modifie donc pas la nature des données conservées, ni la façon dont elles sont stockées, mais redéfinit uniquement la manière dont on y accède. Et la question de l'accès ne dépend pas uniquement du protocole utilisé : elle est aussi conditionnée par les politiques des registres et bureaux d'enregistrement, qui définissent quelles données sont publiques ou restreintes. En d'autres termes, même avec un protocole plus avancé comme RDAP, l'accès aux données reste toujours déterminé par les règles établies par les instances de régulation et de gestion des noms de domaine, selon les réglementations en vigueur et leurs interprétations possibles.

2

SMSI+20 : la gouvernance d'internet à l'heure du grand bilan

Vingt ans après le Sommet Mondial sur la Société de l'Information (SMSI, ou WSIS en anglais pour *World Summit on the Information Society*), qui avait posé les bases de la gouvernance d'internet, beaucoup de choses ont changé. De nouvelles préoccupations ont émergé, venant nuancer la perception initiale d'un internet uniquement synonyme de progrès et d'innovation. Il est désormais également devenu un espace de tensions et d'affrontements géopolitiques, et un terrain propice aux activités criminelles. C'est dans ce contexte que la gouvernance d'internet telle qu'on la connaît aujourd'hui va faire l'objet cette année d'un bilan.

En 2025, le SMSI+20 doit en effet faire le bilan de ces 20 dernières années, dans le prolongement de la revue à 10 ans de 2015, et répondre à une question clé : le modèle actuel de gouvernance — basé sur une approche multipartite impliquant États, communauté technique, entreprises, société civile et organisations internationales — est-il encore pertinent ?

Genève vs New York : deux salles, deux ambiances

Depuis 2005, les discussions sur la gouvernance d'internet se déroulent principalement à Genève, où se réunissent les institutions spécialisées. Là-bas, les débats sont techniques, concrets et portés par des experts.

Mais cette année, le centre de gravité se déplace vers New York, à proximité de l'Assemblée Générale de l'ONU. Un changement qui n'est pas anodin : quand une discussion bascule de Genève à New York, c'est qu'elle devient hautement politique. Cette dynamique s'inscrit d'ailleurs dans une tendance amorcée depuis plusieurs mois, une série de précédents ayant déjà renforcé le rôle de New York dans les discussions sur le numérique :

- **L'adoption du Pacte Numérique Mondial** en septembre 2024 par l'Assemblée générale des Nations unies avait déjà amorcé un déplacement des discussions vers New York. Ce Pacte ne se limite pas à la gouvernance d'internet mais englobe toutes les technologies numériques et émergentes — un signe que l'ONU cherche à adopter une approche plus large, privilégiant un cadre intergouvernemental à New York, plutôt qu'un dialogue plus technique et plus multipartite tel qu'il peut exister à Genève.
- **La création de l'*Office for Digital and Emerging Technologies* (ODET) à New York**, sous l'autorité du Secrétaire général de l'ONU, s'inscrit dans cette même dynamique en centralisant la coordination des politiques numériques au sein du système onusien. Présenté comme un levier pour structurer l'action des Nations unies sur ces questions, ce bureau renforce le rôle de New York. Le rôle exact de l'ODET dans la revue à 20 ans du SMSI reste à préciser, ainsi que le fonctionnement concret de ce nouveau bureau et son rôle dans les discussions numériques.
- **L'accélération des tensions géopolitiques** autour du contrôle des infrastructures numériques, de la régulation des plateformes et des modèles d'intelligence artificielle a également contribué à recentrer les discussions à New York. Ces enjeux, qui touchent directement aux rapports de force entre États, trouvent une place naturelle au sein des négociations intergouvernementales. Mais cette centralisation n'est pas sans soulever des interrogations sur l'avenir des forums ouverts et multipartites qui ont structuré la gouvernance d'internet jusqu'ici.

Trois dossiers brûlants au menu du SMSI+20

Pour mieux appréhender le poids des discussions à venir dans le cadre de la revue à 20 ans du SMSI, il est essentiel de comprendre les grandes tensions qui traversent la gouvernance d'internet aujourd'hui.

Le modèle multipartite survivra-t-il ?

Le SMSI de 2005 avait posé un principe fort : les États ne sont pas les seuls à avoir voix au chapitre dans la gouvernance d'internet. Entreprises, communauté technique, société civile, chercheurs et organisations internationales ont aussi leur rôle à jouer.

Aujourd'hui, ce modèle multipartite est de plus en plus contesté. Certains États, comme la Chine et la Russie, préfèreraient un contrôle plus direct par les gouvernements et contestent l'idée d'un internet gouverné par des mécanismes ouverts et collaboratifs, estimant que le modèle multipartite ne joue pas en leur faveur et les prive d'une influence qu'ils jugent légitime sur les décisions stratégiques.

Le risque dans le contexte du SMSI+20, c'est que les discussions servent à justifier un basculement vers un modèle plus étatisé, au détriment des instances existantes.

Que faire du Forum sur la Gouvernance de l'Internet (FGI) ?

Le FGI, créé par le SMSI en 2005, reste l'un des espaces privilégiés de dialogue multi-parties prenantes, où tous peuvent venir discuter des défis liés à internet. Son mandat arrivant à échéance, le SMSI+20 doit décider de son renouvellement.

Bonne nouvelle : le Pacte Numérique Mondial le mentionne explicitement, ce qui laisse penser qu'il sera prolongé. Mais se trouvera-t-il marginalisé ou au contraire renforcé ?

La gouvernance d'internet doit-elle être mise à jour à l'ère de l'IA et de la multiplication des régulations ?

En 2005, on parlait surtout de fracture numérique et de connectivité. En 2025, les sujets portent plus sur l'intelligence artificielle, la cybersécurité, la régulation des plateformes et les grandes réglementations numériques comme le RGPD (Règlement général sur la protection des données), le règlement sur les services numériques (parfois connu sous l'acronyme DSA pour *Digital Services Act*) ou celui sur les marchés numériques.

Les fameuses lignes d'actions du SMSI, qui définissent les axes stratégiques de développement et les organisations en charge, doivent être mises à jour pour mieux refléter ces nouveaux enjeux. Par exemple, la C5 (Cybersécurité) et la C7 (E-learning, E-health) pourraient intégrer des questions liées à l'intelligence artificielle. Un travail d'alignement avec le Pacte Numérique Mondial et les objectifs de développement durable est par ailleurs déjà en cours.

Un calendrier dense

Le processus du SMSI+20 sera jalonné de plusieurs grandes étapes en 2025.

Définition des modalités de la revue

En janvier 2025, le Président de l'Assemblée générale des Nations unies a nommé les représentants permanents du Kenya et de la Lituanie comme co-facilitateurs pour piloter les consultations intergouvernementales visant à finaliser les modalités de la revue à 20 ans du SMSI. Cette première phase vient de se terminer avec une reprise à l'identique des modalités de la revue à 10 ans, ce qui doit maintenant être adopté par l'Assemblée générale de l'ONU.

La revue : consultations et bilans des avancées

Une fois les modalités validées, deux co-facilitateurs seront désignés pour superviser la revue du SMSI+20. Il est attendu que le Kenya et la Lituanie, déjà en charge des consultations intergouvernementales sur les modalités, soient reconduits sur le fond. Cette étape visera à recueillir les contributions des États et des parties prenantes.

Parallèlement, la Commission de la science et de la technologie au service du développement (CSTD) des Nations unies, organe subsidiaire du Conseil économique et social (ECOSOC) des Nations unies, fera le bilan sur les avancées et formulera des recommandations dans un rapport attendu pour juin 2025 pour ajuster les priorités du SMSI à l'ère actuelle.

La revue finale en décembre 2025

Le processus culminera avec une réunion de haut niveau de l'Assemblée générale de l'ONU, prévue les 16 et 17 décembre 2025 à New York. Ce sommet devra valider les conclusions des consultations intergouvernementales, qui comprendront une phase de consultation des parties prenantes et les négociations intergouvernementales.

Le SMSI+20 ne sera pas un simple exercice de bilan : il posera les bases du SMSI pour les 10 prochaines années tout en assurant une cohérence avec le Pacte Numérique Mondial et les objectifs de développement durable de l'Agenda 2030. Rappelons que la force d'internet repose sur sa gouvernance ouverte, où les parties prenantes, États, entreprises, société civile, communautés techniques et académiques collaborent à son évolution. La revue à venir doit être l'occasion de renforcer ce modèle, et non de l'affaiblir au profit d'une vision plus centralisée et intergouvernementale.

03

Internet face aux coupures de câbles sous-marins : pourquoi le réseau tient bon ?

Ces derniers mois, plusieurs incidents ont remis sur le devant de la scène la question des câbles sous-marins de télécommunications : coupures inexpliquées en mer Baltique, endommagements au large de Taïwan, sans parler des tensions géopolitiques qui ravivent les inquiétudes autour de la sécurité des infrastructures numériques. Pourtant, ces coupures ne sont ni nouvelles ni particulièrement plus fréquentes qu'avant.
Elles rappellent simplement une réalité souvent méconnue : internet repose sur un maillage complexe de câbles déployés au fond des océans, qui assurent l'essentiel des communications mondiales.

Dans la majorité des cas, ce type d'incident passe totalement inaperçu pour les utilisateurs finaux. Pourquoi ces coupures, volontaires ou accidentelles, ne paralysent-elles pas immédiatement internet ? Pourquoi certaines régions continuent de fonctionner normalement, tandis que d'autres se retrouvent isolées ? La réponse tient en un mot : la résilience — un savant équilibre entre redondance des infrastructures, mécanismes de routage et stratégies d'acteurs privés et publics.

L'importance des câbles sous-marins dans les communications mondiales

Invisibles aux yeux du grand public, les câbles sous-marins de télécommunications assurent pourtant l'essentiel du trafic internet. Aujourd'hui, près de 99% des échanges mondiaux de données transitent en effet par ces infrastructures, permettant le bon fonctionnement de la navigation sur internet, des réseaux sociaux au e-commerce, en passant par les transactions financières et les services cloud.

Un réseau de câbles construit sur près de deux siècles

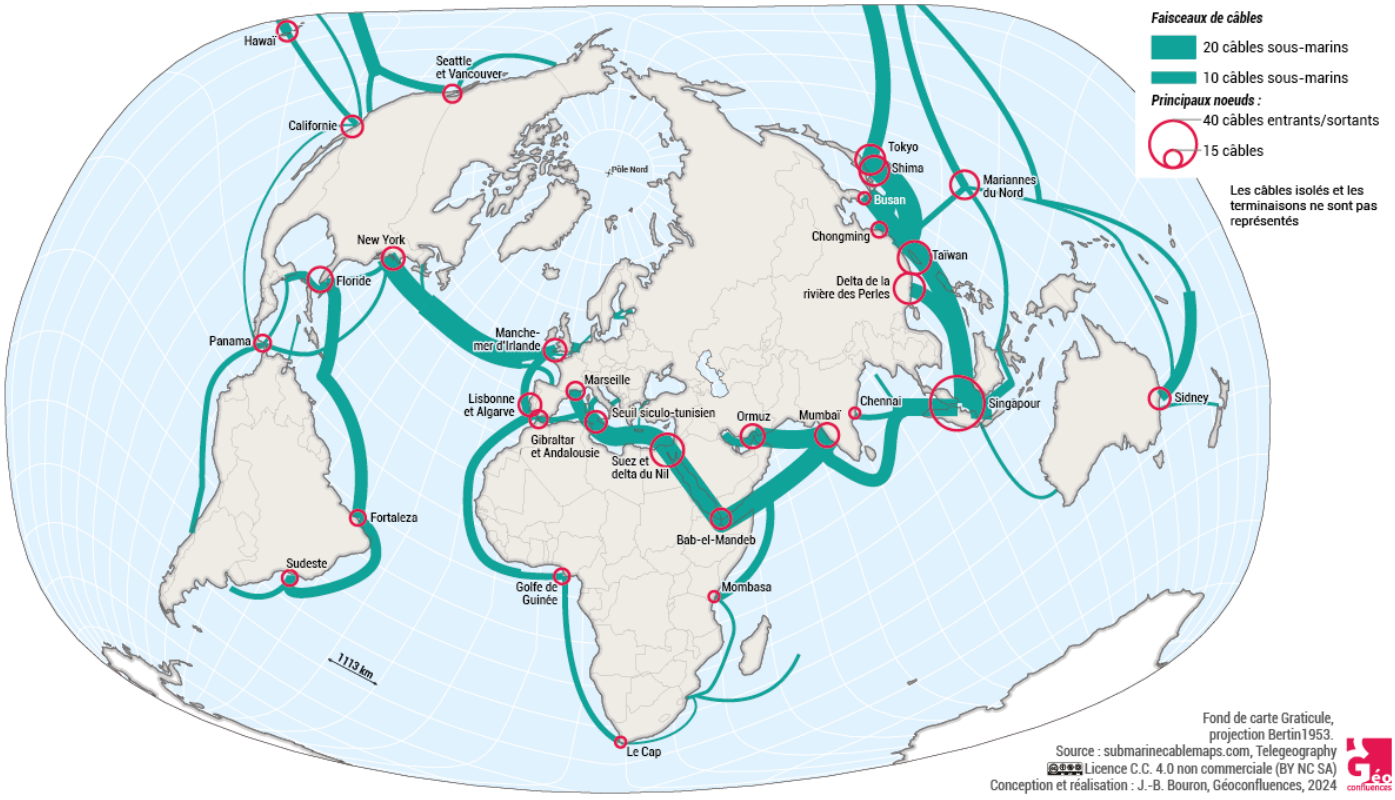
L'histoire des câbles sous-marins ne date pas d'hier. Le premier câble, déployé entre Calais et Douvres à des fins de transmissions télégraphiques, a été inauguré en 1851 à l'occasion de la toute première exposition universelle de Londres — marquant le début d'un réseau mondial de communication sous-marine.

Les câbles ont ensuite accompagné les évolutions technologiques : après les messages en morse, ils ont transporté la voix avec le téléphone, puis la donnée avec l'essor d'internet. Aujourd'hui, 570 systèmes de câbles sous-marins sont en service à travers le monde, et plus de 80 sont en projet. Ils maillent ainsi les océans, totalisant des milliers de kilomètres de fibre optique et reliant continents, pays et grandes métropoles.

L'implication croissante des GAFAM dans les infrastructures sous-marines

Historiquement, les câbles sous-marins étaient principalement financés et exploités par des consortiums d'opérateurs télécoms et d'États. Aujourd'hui, 90% à 95% des nouveaux câbles sont financés, en partie ou en totalité, par les GAFAM. Et les projets se multiplient. Meta vient, par exemple, d'annoncer en février dernier son « Projet Waterworth », le déploiement d'un gigantesque câble sous-marin de plus de 50 000 km, visant à relier l'Amérique du Nord, l'Amérique du Sud, l'Europe, l'Afrique et l'Asie.

Cette montée en puissance des géants du numérique soulève plusieurs enjeux stratégiques. Contrairement aux consortiums historiques qui mutualisaient l'accès aux câbles, les GAFAM en deviennent propriétaires et maîtrisent ainsi l'ensemble de la chaîne de transmission des données. Ce contrôle leur offre un avantage considérable sur la qualité de service et les coûts, mais renforce aussi leur emprise sur l'infrastructure mondiale d'internet.



Carte de Jean-Benoît Bouron, extraite de Catherine Biaggi et Laurent Carroué, « Les grands détroits et canaux internationaux dans la géopolitique des mers et océans, un système très hiérarchisé sous tensions multiformes », *Géoconfluences*, juin 2024

Les causes des coupures de câbles sous-marins

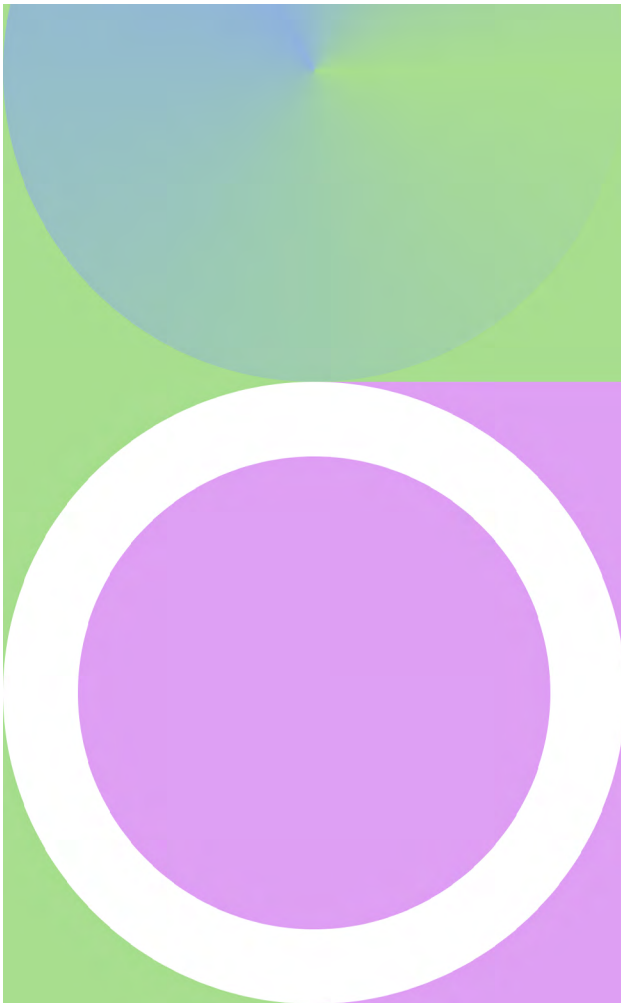
Les câbles sous-marins sont relativement fragiles et donc exposés aux incidents. Si la majorité des ruptures sont accidentelles, certaines peuvent aussi résulter d'actions délibérées, notamment dans des contextes géopolitiques tendus.

Activités humaines et dommages involontaires : la cause la plus répandue

Près de 70% des dommages aux câbles sous-marins sont dus aux activités humaines, en particulier la pêche commerciale et le mouillage des navires. Les chaluts traînés sur le fond marin ou les ancres larguées par erreur peuvent en effet accrocher un câble et l'endommager, voire le sectionner.

Catastrophes naturelles : quand les forces de la nature s'en mêlent

Les mouvements géologiques et les catastrophes naturelles figurent également parmi les principales causes de ruptures de câbles. Un séisme sous-marin, un glissement de terrain ou une éruption volcanique peuvent provoquer un déplacement brutal du fond océanique et endommager ces infrastructures. L'exemple le plus marquant reste l'éruption volcanique aux Tonga en 2022, qui a coupé le seul câble reliant l'archipel au reste du monde, plongeant le pays dans un isolement quasi total pendant plusieurs semaines.



Actes malveillants : un risque en hausse dans un contexte géopolitique tendu

Si les ruptures intentionnelles restent rares, elles sont de plus en plus évoquées dans un contexte de tensions internationales. Couper un câble sous-marin peut être une stratégie pour perturber les communications d'un pays ou d'une région. En mer Baltique, plusieurs incidents depuis 2024 ont alimenté les soupçons de sabotage, notamment après la rupture inexpliquée de deux câbles reliant l'Europe du Nord. Ces événements ont renforcé les efforts de surveillance de la zone, notamment par l'OTAN.

La résilience du réseau internet face aux coupures de câbles sous-marins

Si les câbles sous-marins sont essentiels aux communications et aux échanges de données dans le monde, leur fragilité pose la question de la résilience du réseau internet. Pourtant, dans la majorité des cas, même en cas de rupture, les utilisateurs ne perçoivent aucune interruption de service. Cela est rendu possible grâce à des mécanismes techniques et à la redondance des infrastructures.

La multiplication des routes

Dans les régions bien connectées, le trafic peut être redirigé automatiquement en cas de coupure de câble. Internet repose sur un principe de multiplicité des routes, permettant aux données de prendre un chemin alternatif lorsqu'un lien ne peut plus être fait. C'est ce maillage qui garantit une connectivité quasi ininterrompue dans les grandes zones économiques interconnectées comme l'Europe ou l'Amérique du Nord.

En revanche, dans les zones isolées où les options de connexion sont limitées, une coupure peut avoir des conséquences bien plus graves. Lors de l'éruption volcanique aux Tonga en 2022, l'unique câble sous-marin reliant l'archipel au reste du monde a été sectionné, plongeant le pays dans un isolement numérique quasi total. Durant les 38 jours nécessaires à la réparation du câble, des solutions alternatives ont été mises en place pour rétablir partiellement les communications. Des liaisons satellites avaient alors été utilisées, mais leur débit bien plus faible et leur latence élevée n'ont permis de rétablir qu'une fraction des services habituels, principalement pour les communications essentielles et les services d'urgence[2]. Cet événement souligne la vulnérabilité des infrastructures de communication dans les régions dépendant d'un seul câble et l'importance de diversifier les moyens de connexion pour assurer une résilience optimale.

2. Il est cependant à noter que l'efficacité et l'interopérabilité des communications satellites est en nette et rapide progression. Voir par exemple la Release 17 du 3GPP, supportant désormais officiellement dans la 5G la composante spatiale. Cf. le numéro « La Terre vue d'en haut » de la revue « Enjeux Numériques » https://annales-des-mines.org/wp-content/uploads/2024/09/EN-2024-03-Numero-complet-version-internet.pdf

Le rôle central du protocole BGP

Lorsqu'un câble sous-marin est endommagé, ce n'est pas seulement une question d'infrastructure : c'est aussi une question de routage. C'est ici qu'intervient le protocole BGP *(Border Gateway Protocol)*, essentiel au fonctionnement continu d'internet.

BGP est en effet le protocole qui permet aux réseaux autonomes (*Autonomous Systems* ou AS), c'est-à-dire les différentes infrastructures de chaque fournisseur d'accès à internet (FAI) et opérateur réseau, de s'échanger des informations sur les routes disponibles pour transmettre les données en ligne. Si une liaison est rompue, le protocole ajuste automatiquement les itinéraires pour acheminer le trafic via un autre chemin disponible. C'est ce mécanisme qui fait que les utilisateurs ne perçoivent généralement pas les coupures de câbles.

Comment fonctionne BGP en cas de coupure de câble sous-marin :

- **Annonce des routes et recalcul des itinéraires.** Chaque AS utilise BGP pour annoncer les routes par lesquelles il est capable de faire transiter les données. Si un câble est coupé, les annonces concernées disparaissent, indiquant ainsi aux autres réseaux qu'ils doivent choisir un nouvel itinéraire.
- **Propagation des changements dans l'ensemble du réseau.** Lorsqu'une rupture est détectée, BGP diffuse rapidement la mise à jour aux autres réseaux, leur signalant que la route précédente n'est plus disponible. Les opérateurs ajustent alors leurs politiques de routage pour privilégier des chemins alternatifs.

Quels leviers pour renforcer la sécurité et la résilience des câbles sous-marins ?

Si internet continue de fonctionner malgré les coupures de câbles sous-marins, c'est donc grâce à des mécanismes de redondance et de routage. Toutefois, l'augmentation des risques liés aux tensions géopolitiques et aux actes malveillants impose de renforcer la protection de ces infrastructures critiques.

Sécuriser les points d'atterrissement

Les points d'atterrissement, c'est-à-dire l'endroit où les câbles sous-marins émergent sur terre, sont particulièrement sensibles. Dans de nombreux pays, ces infrastructures sont situées dans des zones stratégiques et placées sous surveillance renforcée. En France, par exemple, certains points d'atterrissement sont sous protection militaire. Ces sites sont aussi équipés de dispositifs de sécurité renforcée pour prévenir toute tentative d'intrusion ou de sabotage.

Surveiller les infrastructures sous-marines en mer

Assurer une surveillance directe des câbles sur l'ensemble de leur parcours sous-marin est pratiquement impossible en raison de leur longueur et de leur emplacement à grande profondeur. Toutefois, la surveillance peut être renforcée dans les zones sensibles, notamment autour des détroits et des points de passage stratégiques où ces câbles sont plus accessibles.

En janvier 2025, l'OTAN a ainsi intensifié sa vigilance sur les infrastructures sous-marines en mer Baltique à travers l'opération « Baltic Sentry », qui mobilise des frégates, des avions de patrouille maritime et des drones navals. L'objectif est de détecter d'éventuelles activités suspectes autour des points sensibles et de prévenir tout sabotage, même si une surveillance continue sous l'eau reste techniquement très limitée.

Renforcer la diversité des routes de connexion

Pour limiter l'impact d'une coupure, la solution la plus efficace reste la multiplication des points d'atterrissement et des routes alternatives. Les GAFAM, déjà très présents dans le secteur, poursuivent leurs investissements massifs pour contrôler directement le transport des données entre leurs infrastructures. En parallèle, des initiatives portées par des entités publiques ou des partenariats public-privé continuent également d'émerger. Tous ces projets visent à assurer un maillage plus fin encore du réseau mondial de communication et à renforcer ainsi sa résilience.

Préserver une diversité d'acteurs

Une grande partie des câbles sous-marins sont aujourd'hui la propriété d'acteurs privés, notamment les GAFAM. Or, une trop forte domination du marché par un petit nombre d'acteurs peut fragiliser la résilience du réseau, en réduisant la diversité des routes de connexion et les alternatives. C'est pourquoi il est important de maintenir un équilibre entre financements privés et initiatives publiques afin d'éviter qu'internet ne passe entièrement sous le contrôle des grandes plateformes technologiques.

Conscients de ces enjeux stratégiques, certains pays cherchent à reprendre la main sur ces infrastructures et préserver leur souveraineté numérique. La France, par exemple, a renationalisé en 2024 Alcatel Submarine Networks (ASN), un acteur clé de la fabrication et de la pose de câbles sous-marins, en acquérant 80% de son capital. Si cette initiative ne remet pas en cause le contrôle exercé par les GAFAM sur l'exploitation des infrastructures, elle permet néanmoins de préserver une expertise clé dans un secteur stratégique.

Coopérer à l'international

La résilience des câbles passe également par une meilleure collaboration internationale. En novembre 2024, l'UIT (Union Internationale des Télécommunications) a ainsi lancé son Organe consultatif international pour la résilience des câbles sous-marins, composé de 40 experts du monde entier, issus des secteurs public et privé. Cet organe vise à garantir que les câbles soient conçus, déployés et entretenus avec une résilience renforcée.

Pour approfondir cette démarche, l'UIT, en partenariat avec le Comité international de protection des câbles (ICPC), a également organisé en février dernier le Sommet international sur la résilience des câbles sous-marins, à Abuja au Nigeria. Cet événement a réuni gouvernements, opérateurs télécoms et experts en cybersécurité pour discuter des vulnérabilités actuelles et des stratégies pour y répondre.

Conclusion

Malgré les coupures accidentelles ou intentionnelles, internet continue de fonctionner grâce à une architecture pensée pour la résilience. La redondance des câbles sous-marins et la capacité des réseaux à recalculer en temps réel les routes de connexion grâce au protocole de routage BGP permettent d'absorber la majorité des incidents sans impact pour les utilisateurs finaux.

Si certaines zones restent vulnérables en raison d'une moindre densité de câbles, les initiatives visant à multiplier les points d'atterrissement et à renforcer les infrastructures locales contribuent à améliorer cette robustesse. Toutefois, la résilience du réseau ne repose pas uniquement sur des solutions techniques : elle dépend aussi de la diversité des acteurs impliqués dans leur financement et leur gestion. Or, la montée en puissance des GAFAM dans ce domaine tend à réduire la pluralité des consortiums, au risque de concentrer le contrôle des communications mondiales entre les mains de quelques acteurs privés.

Dans un contexte géopolitique sous tension, cette tendance pourrait raviver des préoccupations autour de la souveraineté numérique et de l'indépendance des infrastructures critiques. L'enjeu est donc aussi désormais de garantir un équilibre entre initiatives publiques et investissements privés pour préserver un internet à la fois ouvert, sécurisé et résilient sur le long terme.

4

Intelligence artificielle et gestion du réseau : quelles promesses pour quelles réalités ?

Entre streaming, cloud gaming, objets connectés ou encore télétravail, les usages d'internet sont toujours plus variés et sollicitent de plus en plus l'infrastructure réseau. Les exigences augmentent et les réseaux doivent s'adapter en permanence. Pour garantir une qualité de service optimale, il ne suffit plus d'ajouter des câbles et des antennes : il faut aussi gérer plus intelligemment les infrastructures existantes.

Dans ce contexte d'expansion, il devient difficile d'assurer la gestion des réseaux de manière entièrement manuelle. C'est là que l'intelligence artificielle (IA) entre en scène, en apportant des capacités d'analyse et d'adaptation en temps réel. Déjà présente dans de nombreux domaines, elle pourrait transformer la gestion des réseaux en rendant les ajustements plus rapides, plus fins et plus intelligents.

Mais cette intégration de l'IA dans la gestion du réseau pose également des questions. Comment l'adapter à des infrastructures aussi variées que celles d'internet ? Peut-elle vraiment prendre des décisions autonomes sans risquer de perturber le fonctionnement du réseau ? Et comment s'assurer que ses choix restent explicables pour ceux qui en ont la responsabilité ?

L'IA, prochaine étape de l'évolution des réseaux ?

L'intégration de l'intelligence artificielle dans la gestion des réseaux s'inscrit dans une transformation plus large et plus ancienne des infrastructures réseau, qui sont passées d'un modèle entièrement matériel à un fonctionnement de plus en plus virtualisé.

Des infrastructures matérielles aux réseaux programmables

Pendant longtemps, les réseaux étaient en effet essentiellement constitués d'équipements matériels. Chaque fonction reposait sur un élément physique défini : les routeurs guidaient le trafic, les commutateurs reliaient les machines, les antennes assuraient la transmission. Modifier un réseau nécessitait souvent une intervention humaine, que ce soit pour configurer un appareil, ajouter de la capacité ou résoudre une panne.

Aujourd'hui, de plus en plus de fonctions réseau sont assurées par des logiciels, grâce à des technologies comme la virtualisation des fonctions réseau (NFV) ou les réseaux définis par logiciel (SDN). Concrètement, cela signifie que le comportement du réseau peut être programmé et modifié à distance, sans avoir à toucher physiquement aux équipements.

Dans la 5G, ce principe va même encore plus loin avec le *network slicing*, qui permet de découper un réseau en plusieurs sous-réseaux virtuels. Chacun peut être optimisé pour un usage spécifique : un canal ultra-réactif pour les voitures autonomes, un autre à forte capacité pour le streaming vidéo, et ainsi de suite.

Ces évolutions rendent le réseau plus flexible, mais aussi plus complexe à gérer. Les capacités des outils traditionnels sont dépassées, nécessitant des approches plus dynamiques. C'est ici que l'IA peut apporter une réponse.

Ce que l'IA peut (et ne peut pas) faire

L'intelligence artificielle ne remplace pas le réseau, mais elle peut aider à mieux l'exploiter. Son principal atout est d'analyser en temps réel une quantité massive de données et d'anticiper les évolutions avant qu'un problème ne survienne.

Elle peut, par exemple, surveiller et analyser le trafic pour détecter les anomalies, la congestion ou les tentatives d'attaque ; optimiser les ressources en ajustant automatiquement la bande passante, en activant ou désactivant certaines capacités réseau en fonction de la demande ; prédire les incidents avant qu'ils ne provoquent une panne, et dans certains cas, proposer des corrections.

Mais l'IA ne peut pas tout faire. Elle ne remplace pas la supervision humaine et ne prend pas toujours les meilleures décisions, notamment lorsqu'elle est confrontée à des situations inédites ou mal comprises. Elle ne peut pas non plus modifier l'infrastructure physique d'un réseau : elle peut gérer les ressources disponibles, mais si un câble est endommagé ou qu'une antenne tombe en panne, une intervention humaine reste nécessaire.

L'IA dans la gestion des réseaux est donc un outil puissant, mais ni omniscient, ni omnipotent. C'est pourquoi elle ne peut se substituer ni à la supervision humaine, ni aux infrastructures physiques qu'elle gère.

L'IA est-elle prête à gérer nos réseaux ?

Si le potentiel de l'IA dans la gestion des réseaux est indéniable, son intégration à grande échelle soulève de nombreuses questions techniques et opérationnelles. Un draft d'un groupe de travail à l'IETF — *« Research Challenges in Coupling Artificial Intelligence and Network Management »* — liste ainsi plusieurs de ces défis à relever avant qu'une automatisation intelligente puisse être déployée à grande échelle.

Hétérogénéité des infrastructures

Les réseaux ne sont pas construits de manière uniforme. Certains opérateurs s'appuient encore principalement sur des équipements physiques traditionnels, tandis que d'autres ont largement intégré des infrastructures virtualisées avec NFV et SDN. De plus, chaque réseau repose sur des protocoles, des architectures et des fournisseurs différents.

Cela pose un problème majeur pour l'IA : comment créer un système qui puisse s'adapter à cette diversité ? Une IA entraînée sur un réseau très virtualisé pourra-t-elle fonctionner sur un réseau plus classique, où les interventions matérielles sont encore nécessaires ? Peut-on définir un cadre standard pour que toutes ces IA interagissent entre elles, quelle que soit l'architecture sous-jacente ?

Aujourd'hui, il n'existe pas encore de réponse claire. Les solutions actuelles sont souvent adaptées à des environnements spécifiques, ce qui complique leur déploiement à grande échelle.

Explicabilité et confiance

Une IA qui gère un réseau prend des décisions qui peuvent avoir un impact direct sur la qualité de service, la consommation énergétique ou même la sécurité. Pour que ces décisions soient acceptées, elles doivent être compréhensibles, ou explicables.

Or, les modèles d'IA actuels manquent souvent de transparence : ils analysent d'énormes quantités de données et produisent des résultats sans toujours pouvoir expliquer leur raisonnement. Si une IA décide de rediriger un flux de données par un itinéraire différent, sur quelle base prend-elle cette décision ? Comment un opérateur réseau peut-il vérifier qu'elle ne privilégie pas certains services au détriment d'autres ? Que se passe-t-il si deux IA appliquent des stratégies contradictoires sur un même réseau ?

Le risque est que les ingénieurs et les gestionnaires de réseau hésitent à utiliser ces systèmes, par peur de perdre le contrôle. C'est pourquoi l'explicabilité est importante : chaque décision d'une IA doit être justifiable et traçable, afin que les équipes puissent comprendre et, si nécessaire, corriger son fonctionnement.

Sécurité et impact sur la performance

L'ajout d'IA dans la gestion des réseaux ouvre aussi la porte à de nouvelles vulnérabilités. En premier lieu, les IA peuvent être attaquées. Si une IA repose sur des données réseau pour apprendre et prendre des décisions, un attaquant pourrait en effet manipuler ces données pour fausser son comportement. On parle alors d'empoisonnement des données. Par exemple, si une IA apprend qu'un pic de trafic signifie une congestion qui nécessite d'activer plus de ressources, un attaquant peut générer artificiellement un faux pic de trafic, incitant l'IA à mobiliser des ressources inutilement et à créer une surcharge du réseau.

L'IA représente également un risque pour la qualité de service. Elle repose en effet sur des algorithmes complexes et parfois gourmands en calculs. Et cela soulève une nouvelle question : cela peut-il ralentir le réseau au lieu de l'optimiser ? Si une IA met plusieurs secondes à prendre une décision, son action peut arriver trop tard pour être utile. Si trop d'IA fonctionnent en parallèle, elles peuvent générer une surcharge de données et perturber le fonctionnement du réseau. Pour être réellement efficace, une IA doit donc être rapide, légère et bien calibrée pour ne pas devenir un frein à la performance globale du réseau.

Le cadre AINEMA : structurer l'IA dans la gestion des réseaux

Un autre groupe de travail à l'IETF tente d'apporter des réponses aux questions de l'IA dans la gestion du réseau avec le cadre AINEMA *(AI Network Management Framework)*. Présenté dans le draft *Artificial Intelligence Framework for Network Management*, AINEMA propose une approche modulaire et interopérable pour intégrer l'IA dans la gestion des réseaux. Il ne s'impose pas comme une solution toute faite, mais comme un ensemble de bonnes pratiques tenant compte des contraintes techniques et opérationnelles.

Une architecture pensée pour intégrer l'IA

AINEMA part du principe qu'une IA appliquée à la gestion d'un réseau ne peut pas fonctionner seule, en prenant des décisions isolées et sans coordination avec le reste du système. Elle doit s'inscrire dans une architecture cohérente, où les données sont centralisées, les analyses croisées et les décisions intégrées à une gestion globale du réseau. L'approche d'AINEMA repose ainsi sur trois principales composantes :

- **Une architecture des données.** L'IA a besoin de données fiables et bien structurées pour fonctionner. L'architecture des données définit comment récupérer, organiser et stocker ces informations. Cela inclut les métriques du réseau (trafic, qualité de service, état des équipements), les événements critiques (incidents, pannes, attaques détectées) et les décisions prises par l'IA, afin d'assurer une traçabilité. Sans un modèle de données robuste, l'IA risque de produire des analyses biaisées ou inexploitables.
- **Des modules d'IA spécialisés.** AINEMA ne repose pas sur une seule IA globale, mais sur plusieurs modules d'IA spécialisés, chacun ayant un rôle précis. Par exemple, un module peut analyser la congestion et proposer un meilleur routage, un autre peut ajuster l'attribution des fréquences pour améliorer la qualité des connexions, un troisième peut détecter des anomalies qui signalent une tentative de cyberattaque. L'idée est que chaque module fasse une tâche spécifique et que tous puissent fonctionner ensemble.
- **Un orchestrateur central, l'IA Hub.** Si chaque module d'IA prend des décisions isolées, il y a un risque de conflits : l'un peut vouloir activer plus de capacité pendant qu'un autre tente d'économiser de l'énergie. Pour éviter cela, AINEMA prévoit un « IA Hub », une sorte de chef d'orchestre qui coordonne les différents modules IA pour éviter des décisions contradictoires ; supervise leur fonctionnement et peut désactiver un module s'il produit des erreurs ; s'assure que l'IA reste alignée avec les règles de gestion du réseau définies par les opérateurs. Cet IA Hub agit comme un centre de supervision, garantissant que l'intelligence artificielle améliore le réseau sans en perdre le contrôle.

L'interopérabilité, une condition sine qua non

Comme le soulignait le draft *Research Challenges in Coupling Artificial Intelligence and Network Management*, un réseau est un système hétérogène, qui combine des équipements, des logiciels et des protocoles venant de différents fournisseurs. Pour éviter que l'IA ne soit un frein à cette diversité, le cadre AINEMA met l'accent sur l'interopérabilité à plusieurs niveaux :

- **Interopérabilité avec les infrastructures existantes.** L'IA doit pouvoir fonctionner avec les réseaux physiques et virtuels, sans nécessiter un remplacement complet des équipements.
- **Interopérabilité entre différentes IA.** Les opérateurs utilisent déjà des outils d'optimisation et d'automatisation. Il faut que les nouvelles IA puissent communiquer avec celles qui existent déjà.

- **Interopérabilité des modèles de données.** Pour éviter que chaque fournisseur de matériel ou d'IA développe son propre format de données, des standards comme YANG (*Yet Another Next Generation*, un langage de modélisation utilisé pour décrire la configuration et la gestion des équipements réseau) sont envisagés pour assurer une compatibilité entre systèmes.

L'objectif est d'éviter que chaque acteur développe son IA de son côté, créant des silos technologiques incompatibles entre eux. L'IA ne doit pas fragmenter davantage l'écosystème réseau, mais au contraire permettre une gestion plus fluide et adaptable.

Normes et régulations : un cadre encore flou

L'IA dans la gestion des réseaux est encore en phase d'exploration. Les premiers déploiements existent, mais ils restent limités à des cas d'usage spécifiques. Pour aller plus loin, il ne suffira pas d'améliorer la technologie : il faudra aussi structurer un cadre commun et clarifier les règles qui encadreront son utilisation.

Car, même si les régulateurs commencent à s'intéresser au sujet, il n'existe à ce jour pas encore de réglementation ou de norme universelle encadrant l'usage de l'IA dans la gestion des réseaux. Celle-ci soulève pourtant de nombreuses questions de régulation en matière de transparence et de responsabilité, concernant notamment :

- **La neutralité du net.** Si une IA décide dynamiquement d'allouer plus de ressources à certains services (par exemple, la vidéo en streaming), peut-on garantir qu'elle ne favorise pas certains acteurs au détriment d'autres ?
- **La responsabilité en cas de panne.** Si une décision prise par une IA entraîne une interruption de service, qui est responsable ? L'opérateur ? Le fournisseur de l'algorithme ?
- **Le respect des réglementations locales.** Certains pays imposent des exigences strictes sur la gestion des données réseau. Comment assurer que l'IA respecte également ces contraintes locales ?

L'IA est-elle l'avenir de la gestion des réseaux ?

L'IA appliquée à la gestion des réseaux n'est plus une hypothèse de laboratoire : les premières implémentations existent déjà et les acteurs du secteur en expérimentent activement les technologies. Mais cette avancée s'accompagne d'une question de fond :

> **Jusqu'où veut-on automatiser la gestion des réseaux ?**

L'enjeu n'est pas seulement technique, il est également stratégique. Une IA qui optimise la gestion des flux et anticipe les pannes peut améliorer la qualité de service. Mais une IA qui prend des décisions mal calibrées, mal comprises ou difficilement contrôlables peut aussi introduire des risques nouveaux.

Un autre point à prendre en considération est la diversité des réseaux et des usages. Les besoins en IA pour gérer des réseaux opérés à des fins spécifiques — comme un réseau industriel ou dédié à des services critiques — ne sont pas forcément les mêmes que ceux des réseaux internet qui doivent, par nature, être plus neutres et tolérants. Une IA performante sur un réseau dédié pourrait-elle ainsi s'adapter aux exigences de l'internet global ?

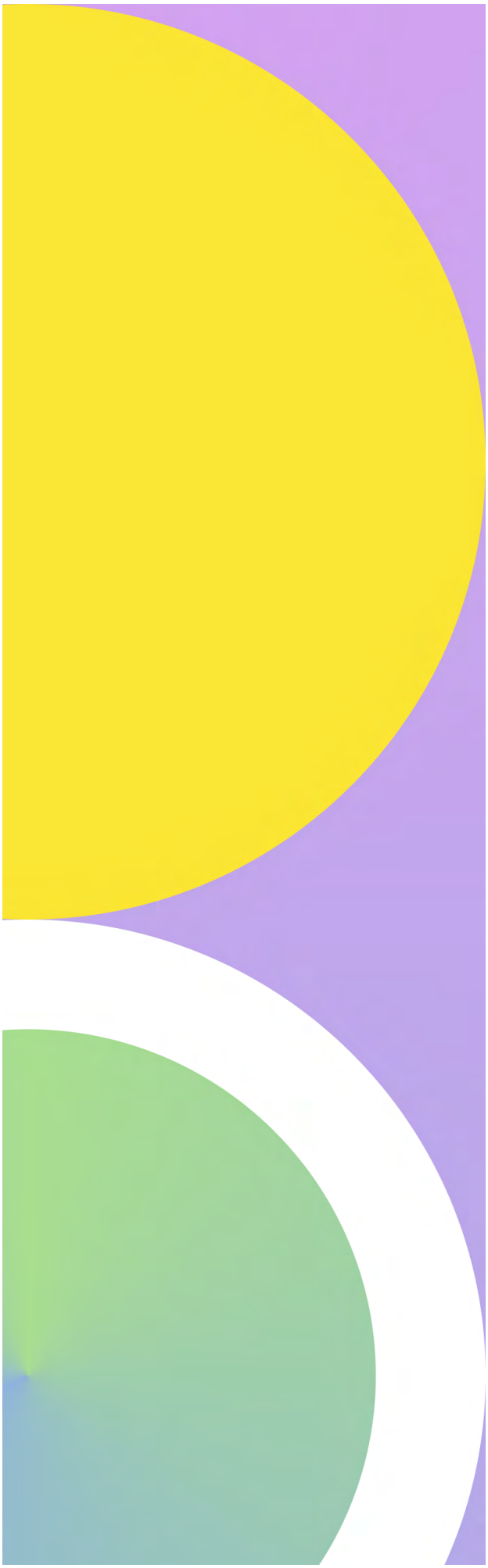
On peut s'interroger sur la pertinence, ici, du principe de robustesse de Postel : « *Be conservative in what you do, be liberal in what you accept from others* ». Si ce principe a façonné l'architecture d'internet, une IA dédiée à la gestion des réseaux peut-elle, elle aussi, en suivre la logique ? Peut-elle être conservatrice dans ses décisions pour éviter les incohérences et les failles de sécurité, tout en restant assez flexible pour gérer des flux et des usages variés et évolutifs ?

En l'absence de cadre réglementaire clair et d'un consensus sur son rôle, l'IA restera, pour l'instant, un outil complémentaire et non un élément central de la gestion des réseaux. Ce sont maintenant les choix des opérateurs, des industriels et des régulateurs qui détermineront si, à l'avenir, l'IA deviendra un levier d'efficacité ou une contrainte de plus à gérer.

05

Quel est l'impact de l'Intelligence Artificielle sur l'écosystème des noms de domaine ?

Chaque (r)évolution technologique s'accompagne de son lot de prédictions radicales. Depuis des années, on annonce ainsi régulièrement la fin des sites internet : il y a dix ans, les applications mobiles étaient censées les rendre obsolètes ; plus récemment, le Métavers devait redéfinir notre manière de naviguer en ligne. Aujourd'hui, c'est l'Intelligence Artificielle (IA) qui menacerait l'écosystème des noms de domaine.
Si une révolution est effectivement en marche avec l'IA, reste à savoir si elle va simplement redessiner les règles du jeu, ou changer la nature même du terrain.



La fin des sites internet : plus proche du mythe que de la réalité

Ce n'est pas la première fois que la disparition prochaine des sites internet, et donc de l'écosystème des noms de domaine, est annoncée. Pourtant, l'Histoire a montré qu'ils ont systématiquement su évoluer et s'adapter aux nouvelles tendances numériques.

Quand les applications mobiles devaient remplacer l'internet

Il y a une dizaine d'années, avec l'explosion des applications mobiles, on entendait déjà que les sites internet deviendraient obsolètes. Pourquoi ouvrir un navigateur quand une application pouvait offrir une expérience plus fluide, plus optimisée et plus immersive ? Certains experts annonçaient même la disparition progressive du web au profit d'un internet entièrement « *app-driven* », où chaque service aurait son application dédiée.

Ce qu'il s'est réellement passé ? Plutôt qu'un remplacement, c'est une complémentarité qui s'est installée. Les applications ont pris une place centrale dans nos usages, mais elles n'ont pas supplanté les sites web. Pourquoi ? Parce que l'ouverture et l'accessibilité d'internet restent inégalées : une page web s'affiche sur n'importe quel appareil, sans avoir à télécharger une application, et offre une souplesse que les apps ne peuvent pas toujours garantir. Aujourd'hui encore, même les géants du numérique comme Instagram, Airbnb ou Amazon continuent de miser sur leurs sites web en parallèle de leurs applications.

Ce que le Métavers n'a pas réussi à faire

Plus récemment, c'est le Métavers qui était censé tout chambouler. Avec la montée en puissance des univers immersifs et de la réalité virtuelle, certains imaginaient un web entièrement en 3D où les sites traditionnels deviendraient obsolètes. Fini les pages web : nous devions entrer dans des boutiques virtuelles, explorer des espaces interactifs et interagir avec des avatars en temps réel.

Le bilan aujourd'hui : l'engouement initial s'est largement essoufflé. Le Métavers existe toujours, mais il reste un marché de niche, utilisé principalement pour des expériences spécifiques de jeux vidéo, de formation ou encore de collaboration à distance. Il n'a pas réussi à s'imposer comme une alternative viable à l'internet traditionnel, en partie à cause des contraintes techniques et de l'adoption limitée par le grand public.

Et l'Intelligence Artificielle, dans tout ça ?

Depuis l'essor des IA génératives comme Mistral, ChatGPT, Gemini ou Copilot, la manière dont nous accédons à l'information est en train d'évoluer. Au lieu de saisir une recherche sur Google et de parcourir une liste de résultats, nous avons désormais la possibilité d'obtenir une réponse instantanée et synthétisée.

Et si l'IA peut fournir directement des réponses précises, quel rôle jouent encore les sites internet ? Va-t-on assister à une chute de leur trafic, voire à leur disparition progressive ? La réponse n'est pas aussi tranchée.

Certes, l'IA change la façon dont nous effectuons des recherches en ligne : là où les moteurs traditionnels sont des outils de classement qui redirigent vers des sites web, les IA s'imposent comme des moteurs de réponses, synthétisant le contenu pour l'utilisateur.

Il ne faut toutefois pas oublier qu'un site internet ne sert pas seulement à répondre à une question, il sert surtout à passer à l'action. Acheter un produit, réserver une place, s'inscrire à un événement, consulter une offre… Ces actions nécessitent un site internet. L'IA ne remplace pas ces interactions, elle les oriente différemment. Un site internet est aussi un espace de confiance et d'indépendance. Contrairement aux plateformes tierces, il permet aux marques et aux entreprises de maîtriser leur image, leur message et leur relation avec leurs utilisateurs.

Loin de rendre les sites obsolètes, l'IA semble plutôt redéfinir la façon dont on y accède. Elle devient une nouvelle porte d'entrée, un nouveau filtre entre l'utilisateur et l'information. Et dans cet écosystème, la visibilité en ligne ne disparaît pas, elle se joue autrement.

Recherche d'information sur internet : un changement profond des usages

Pendant longtemps, les moteurs de recherche — au premier rang desquels, Google — ont été le passage obligé pour trouver une information sur internet. La visibilité en ligne n'était quasiment dictée que par leurs algorithmes, qui déterminaient quels sites bénéficiaient du trafic. Mais aujourd'hui, cette domination est remise en question.

Si Google détient encore une très large majorité du marché de la recherche, cumulant près de 91 % de parts de marché dans le monde, son hégémonie jusqu'alors incontestée se fissure. De plus en plus d'utilisateurs, notamment parmi les moins de 40 ans, se tournent vers d'autres plateformes pour leurs recherches. Parmi les alternatives émergentes, deux acteurs se distinguent particulièrement : TikTok, devenu une référence chez les jeunes générations, et les IA génératives, qui offrent des réponses synthétiques instantanées.

TikTok, le « moteur de recherche » des jeunes générations

Si TikTok a d'abord été perçu comme une simple plateforme de divertissement, son rôle a largement évolué. Aujourd'hui, près de 45% des utilisateurs de la génération Z préfèrent utiliser TikTok pour leurs recherches en ligne plutôt que Google. Qu'il s'agisse de découvrir des produits, de chercher des recommandations de voyage ou d'obtenir des conseils sur un sujet précis, les jeunes générations ont un penchant pour les résultats vidéo courts et immersifs, plutôt que les liens traditionnels.

Contrairement aux moteurs de recherche classiques, qui affichent une liste de résultats classés par algorithme, TikTok fonctionne sur un principe de découverte algorithmique ultra-personnalisée. L'utilisateur n'a pas besoin de formuler sa requête avec précision : l'application affine ses suggestions en fonction de ses intérêts et de son comportement de navigation.

L'IA, un « moteur de réponses » qui transforme la recherche

L'essor des IA génératives marque un tournant dans l'accès à l'information. Contrairement aux moteurs de recherche traditionnels qui classent des liens, ces IA synthétisent directement une réponse structurée en s'appuyant sur plusieurs sources. C'est une révolution dans la manière dont les internautes consomment l'information : au lieu de naviguer entre plusieurs sites, ils obtiennent une réponse immédiate, sans avoir à quitter l'interface de l'IA.

Ce modèle séduit un nombre croissant d'utilisateurs. Une étude récente montre que 39% des Français utilisent activement l'IA générative, avec une adoption qui varie toutefois selon les générations : plus marquée chez les plus jeunes (74% des 18-24 ans, 55% des 25-34 ans) que chez les plus âgés (35% des 45-59 ans, 17% des 60-75 ans). Cette disparité reflète des attentes différentes vis-à-vis de la recherche en ligne : tandis que les plus jeunes privilégient des réponses instantanées et directes, les générations plus âgées semblent plus attachées à une navigation traditionnelle, basée sur la consultation de plusieurs sources.

La manière dont nous accédons à l'information est en pleine mutation. La recherche ne repose plus uniquement sur un classement de pages web, mais aussi sur des modèles de recommandation et de synthèse qui redéfinissent la visibilité en ligne. Dans ce nouvel environnement, la question n'est plus seulement d'être bien positionné sur Google, mais aussi d'exister au sein de ces nouveaux écosystèmes. Et pour cela, il faut comprendre les logiques du SEO (*Search Engine Optimization*, ou référencement naturel) et du GEO (*Generative Engine Optimization*, ou optimisation pour les moteurs génératifs).

SEO et GEO : deux stratégies pour une même finalité

Comment assurer la visibilité des sites web dans un environnement où l'IA joue un rôle croissant ? Si le SEO a longtemps été la clé du référencement sur Google, l'émergence des moteurs génératifs a fait apparaître un nouveau levier : le GEO. Ces deux approches ne sont finalement pas si différentes et répondent au même besoin fondamental : permettre aux utilisateurs d'accéder aux contenus qu'ils recherchent.

Le SEO, ou l'art de se positionner sur Google et les moteurs traditionnels

Le SEO, ou référencement naturel, est une discipline bien connue des professionnels du web. Il vise à optimiser la visibilité d'un site dans les résultats des moteurs de recherche traditionnels comme Google, Bing ou Qwant, et capter ainsi du trafic qualifié et durable. Le SEO repose sur :

- **Un contenu pertinent et structuré**, pour répondre à l'intention de recherche des internautes, avec des articles bien rédigés et informatifs. Un contenu de qualité est essentiel, car les moteurs de recherche favorisent les pages qui apportent des réponses claires et précises aux utilisateurs, tout en garantissant une bonne expérience de lecture.
- **Une autorité et une popularité bien établies** avec des *backlinks* valorisants, c'est-à-dire des liens entrants provenant d'autres sites web réputés, qui recommandent ou citent un contenu. Plus un site est mentionné par des sources fiables, plus il gagne en crédibilité aux yeux des moteurs de recherche.
- **Une expérience utilisateur optimisée** en termes de vitesse de chargement, d'ergonomie mobile et de design. Un site rapide et facile à parcourir améliore en effet non seulement la satisfaction des visiteurs, mais c'est aussi un critère clé dans les algorithmes des moteurs de recherche.

Le GEO, ou comment exister dans les réponses des IA génératives

Là où le SEO optimise la visibilité sur les moteurs de recherche traditionnels, le GEO vise à faire apparaître un contenu dans les réponses des IA génératives. Celles-ci synthétisant l'information à partir de sources qu'elles considèrent comme fiables, l'objectif du GEO est donc d'optimiser le contenu pour être reconnu comme une référence par ces IA.
Cela passe par :

- **Une structuration claire et accessible du contenu**, avec des informations hiérarchisées et des données bien contextualisées. Tout comme le SEO, les IA génératives privilégient les contenus bien organisés et faciles à analyser. Un texte structuré avec des titres explicites, des paragraphes cohérents et une information bien segmentée facilite la compréhension par les modèles d'IA.
- **La notoriété et la crédibilité du site.** Les IA génératives ne se contentent pas d'explorer le web, elles sélectionnent les sources qu'elles considèrent comme fiables. Plus un site est mentionné sur des plateformes d'autorité (médias, publications académiques, sites institutionnels, blogs influents), plus il a de chances d'être pris en compte. Cette reconnaissance passe aussi par l'expertise perçue du site, qui peut être renforcée par une bonne stratégie de contenu et des *backlinks* de qualité.
- **L'optimisation des métadonnées et le balisage sémantique**, en utilisant des données structurées de type « schema.org » (un format permettant d'indiquer la nature précise d'un contenu : article, produit, événement, recette, etc.) pour faciliter la compréhension par les IA. Les moteurs génératifs exploitent en effet les données structurées pour mieux interpréter les contenus. L'ajout de balises schema.org, de méta-descriptions explicites et de formats enrichis leur permet de mieux comprendre le contexte et la nature d'un contenu.

En réalité, le GEO n'est pas une révolution, mais une extension du SEO. De fait, si un site est bien optimisé pour Google, il a déjà une longueur d'avance pour être pris en compte par les IA génératives.

Les sites internet restent indispensables pour passer à l'action

On pourrait penser que ces nouvelles logiques de référencement remettent en cause l'intérêt même des sites internet. Après tout, si les IA peuvent fournir des réponses immédiates, pourquoi cliquer sur un lien ? Mais cette vision est incomplète : répondre à une question n'est pas suffisant. À un moment donné, l'utilisateur doit passer à l'action.

Le site internet, un espace d'indépendance et de conversion

Accéder rapidement à une information est une chose, mais pour réserver, acheter ou s'inscrire, il faut un espace où l'intérêt peut être converti en engagement réel. C'est précisément le rôle que joue le site internet.

Un site internet, c'est aussi un espace de liberté et de contrôle. Contrairement aux plateformes tierces (Google, TikTok, ChatGPT…), un site appartient à son propriétaire, qui décide de son contenu, de son design et de sa monétisation.

De plus, Amazon, Facebook, TikTok, Google et consorts sont des modèles fermés. Lorsqu'un commerçant vend exclusivement sur Amazon ou lorsqu'une marque dépend uniquement des réseaux sociaux, elle est soumise aux règles et algorithmes de ces plateformes. Un changement d'algorithme, et tout peut s'effondrer. Les IA génératives fonctionnent selon une logique similaire : elles sélectionnent les sources qu'elles jugent pertinentes, et il n'existe aucune garantie qu'un site soit toujours cité. À l'inverse, un site web est un point d'ancrage durable sur le web.

Loin de disparaître, les noms de domaine continuent de croître

Si l'IA représentait une menace réelle pour les sites internet, on s'attendrait à une chute du nombre de noms de domaine enregistrés. Or, les chiffres disent tout le contraire : il ne cesse en effet d'augmenter. À fin 2024, on comptait 364,3 millions de noms de domaine enregistrés dans le monde, soit 4,4 millions de plus ou une hausse de +1,2% par rapport à l'année précédente.

Non seulement l'IA ne freine pas le marché des noms de domaine, mais elle contribue même à dynamiser certaines extensions. Le .ai, par exemple, explose ces dernières années. Il s'agit en réalité d'un domaine de premier niveau national (*ccTLD*) appartenant officiellement à Anguilla, un territoire britannique situé dans les Caraïbes. Mais, identique à l'acronyme d'intelligence artificielle en anglais, il est désormais bien souvent adopté par les entreprises et startups spécialisées dans le domaine. L'extension comptait ainsi 572 000 enregistrements fin 2024, en hausse de +400% sur les 5 dernières années.

> **Ces chiffres montrent une chose : les sites internet sont toujours bien au cœur de l'écosystème digital.**

Peu importe l'évolution des modalités de recherche, les entreprises, les marques et les créateurs de contenu continuent de miser sur leur propre espace numérique.

L'IA facilite aussi la création et la gestion des sites web

L'IA ne fait pas que changer la manière dont nous accédons aux sites internet, elle modifie aussi la façon dont ils sont conçus et gérés. Aujourd'hui, de nombreux outils exploitent l'intelligence artificielle pour accélérer et simplifier la création et l'alimentation de sites internet, les rendant plus accessibles que jamais.

De nombreuses plateformes permettent en effet désormais de générer un site en quelques minutes, simplement en décrivant son activité ou ses besoins via un prompt (c'est-à-dire une instruction textuelle). La rédaction de contenu, la mise en page, l'optimisation SEO, voire la génération d'images et de vidéos peuvent être automatisées. Ce qui nécessitait auparavant des compétences techniques et du temps est désormais réalisable rapidement, avec peu d'expertise.

Cela ne signifie pas pour autant que l'humain devient obsolète. Un site performant ne repose pas uniquement sur l'automatisation, mais aussi sur une stratégie, une identité et une personnalisation que seule une approche réfléchie peut apporter. L'IA est un levier puissant pour gagner du temps, mais elle ne remplace pas l'intelligence et la sensibilité humaines : la créativité, l'originalité, le sens du détail, la vision stratégique…

L'IA ne va pas remplacer le web, elle le redéfinit

L'IA générative transforme indéniablement nos usages en ligne, mais elle ne signe pas pour autant la fin des sites internet et de l'écosystème des noms de domaine. Elle redistribue le trafic, elle change la manière dont on trouve une information, mais elle ne remplace pas le besoin pour une marque ou une entreprise de disposer d'un espace en ligne qui lui est propre.

Les sites internet restent en effet le seul endroit où l'on est réellement chez soi, où l'on contrôle son message, son audience et sa monétisation. Le véritable enjeu aujourd'hui n'est pas de choisir entre moteurs de recherche et IA, entre SEO et GEO, mais d'adapter sa visibilité aux nouvelles réalités du web. Car une chose est sûre : tant qu'il y aura des actions à réaliser, il y aura des sites internet pour les concrétiser.

Les prochains événements auxquels l'Afnic participe :

- **5 au 7 mai 2025**
  CEPT, réunions COM-ITU
  Stockholm, Suède

- **12 au 14 mai 2025**
  EuroDIG 2025
  Strasbourg, France

- **12 au 16 mai 2025**
  RIPE 90
  Lisbonne, Portugal

- **21 au 23 mai 2025**
  CENTR Jamboree 2025
  Lyon, France

- **9 au 12 juin 2025**
  ICANN 83, Forum de politiques
  Prague, Tchéquie

- **17 au 27 juin 2025**
  Conseil de l'UIT
  Genève, Suisse

- **23 au 27 juin 2025**
  Forum sur la gouvernance de l'Internet
  Lillestrøm, Norvège

- **5 et 6 juillet 2025**
  Forum francophone sur la gouvernance du numérique et de l'IA
  Genève, Suisse

- **7 au 11 juillet 2025**
  SMSI+20, Événement de haut niveau
  Genève, Suisse

- **9 au 25 juillet 2025**
  IETF 123
  Madrid, Espagne

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