Internet
made in France

La lettre n°13

Intelligence artificielle : un nouvel enjeu de répartition des ressources et du capital dans l'économie numérique p.02

La neutralité du net à l'épreuve des nouvelles portes d'entrée vers l'internet p.05

RGESN : vers une nouvelle version du référentiel d'écoconception des services numériques p.08

Protocole ECH : un pas de plus vers la protection de la vie privée sur internet p.12

Brèves p.15

L'Afnic y était p.18

1

Intelligence artificielle : un nouvel enjeu de répartition des ressources et du capital dans l'économie numérique

Le débat public sur l'intelligence artificielle se concentre généralement sur deux de ses dimensions : ses effets sur le travail et les organisations, d'une part, et son empreinte énergétique et environnementale, d'autre part. Ces deux angles sont évidemment importants, mais ils ne couvrent pas toutes les transformations en cours. Un troisième sujet mérite aujourd'hui d'être davantage examiné : celui de la concentration des investissements, et par effet domino des capacités de calcul et des infrastructures, autour d'un nombre limité d'acteurs de l'IA.

La question n'est pas de savoir s'il faudrait freiner l'intelligence artificielle. L'IA est déjà un levier de productivité, d'expérimentation et de transformation pour de nombreux secteurs. Mais plutôt de savoir si son développement, par son intensité capitalistique inédite, risque de modifier durablement les équilibres de financement au sein de l'économie numérique. Autrement dit, dans un contexte où l'IA attire une part croissante du capital disponible – selon l'OCDE[1], les entreprises d'IA ont capté 61 % du capital-risque mondial en 2025 –, quelles capacités reste-t-il pour financer le reste de l'écosystème numérique : contenus, logiciels, infrastructures, cybersécurité, réseaux ou encore services d'intérêt général ?

Une innovation portée par des acteurs déjà dominants

Les grandes ruptures numériques ont souvent été associées à l'émergence de nouveaux entrants capables de remettre en cause les positions établies. Microsoft et HP ont, par exemple, accompagné le passage d'une informatique dominée par les grands systèmes d'IBM à une informatique plus distribuée, centrée sur le logiciel, le poste individuel et des équipements plus accessibles. Google, de son côté, a rompu avec la logique des portails comme Yahoo en imposant un accès à l'information via la recherche algorithmique.

Dans le cas de l'IA, le paysage apparaît plus ambivalent. Certaines entreprises récentes jouent bien un rôle moteur : OpenAI, Anthropic, Mistral AI ou xAI ont contribué à accélérer l'innovation et à populariser les grands modèles. Mais cette dynamique ne se déploie pas en dehors de l'économie numérique dominante. Les principaux systèmes d'IA sont soit développés directement par les grandes plateformes, soit fortement adossés à leurs capacités de financement, de cloud, de calcul ou de distribution. Gemini est porté par Google, Llama par Meta. OpenAI s'est développé avec l'appui structurant de Microsoft, Anthropic avec ceux d'Amazon et de Google. xAI s'inscrit dans l'écosystème d'Elon Musk et de X.

C'est la différence avec les ruptures technologiques précédentes. L'IA ne menace pas ces grands acteurs du numérique, elle leur donne plutôt un nouveau terrain d'expansion. Pour développer les modèles les plus puissants, il faut du calcul, des puces, du cloud, des données, des réseaux, des capacités de distribution et beaucoup de capital. Ces ressources sont déjà largement entre les mains des mêmes groupes. L'IA risque donc moins de redistribuer les cartes que de renforcer ceux qui les tiennent déjà.

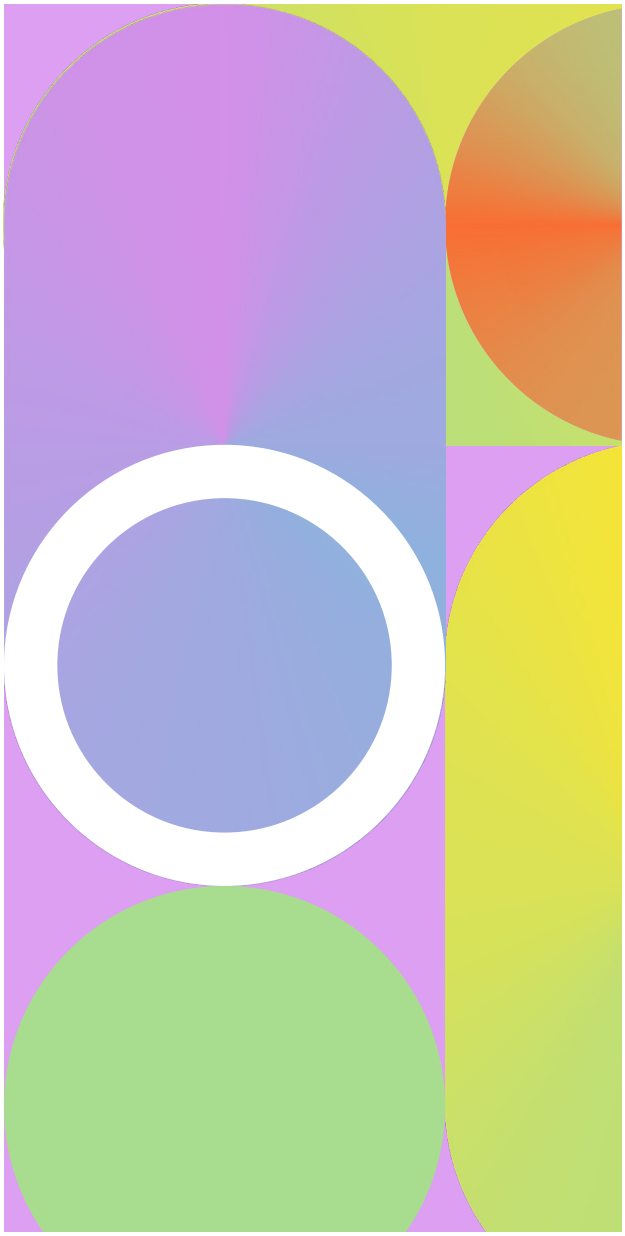
Le paradoxe d'un effet d'éviction

Quand l'IA concentre les capacités de financement, elle déplace les arbitrages des investisseurs, des banques, des marchés et des grands groupes au détriment d'autres acteurs du numérique. Le risque n'est pas seulement que l'IA remplace certains métiers ou certains services. Il est qu'elle rende plus difficile le financement de ceux qui produisent les contenus, les données, les logiciels et les infrastructures dont elle dépend pourtant.

Les médias et producteurs de contenus en offrent un premier exemple. La question n'est pas seulement de savoir si l'IA remplacera une partie du travail journalistique ou éditorial. Elle est aussi de savoir si les acteurs qui créent des contenus originaux pourront continuer à en financer la production. Ces acteurs évoluent déjà dans un environnement fragile : revenus publicitaires de plus en plus incertains, abonnés difficiles à convertir et à fidéliser, accès aux audiences encore largement dépendant des plateformes. Si l'attention des investisseurs et des grands partenaires économiques se déplace encore davantage vers l'IA, produire des contenus originaux risque de devenir toujours plus difficile à soutenir.

C'est un paradoxe, car les systèmes d'IA, et en particulier l'IA générative, ont besoin de contenus humains, structurés, diversifiés et récents. Ils dépendent d'acteurs capables de produire de l'information, de la documentation, de l'analyse, des œuvres, des bases de connaissances, des données métiers. Mais si ces acteurs perdent en capacité de financement, la ressource dont l'IA se nourrit s'appauvrit elle aussi. Car des travaux ont montré que l'entraînement répété de modèles sur des données produites par d'autres modèles pouvait conduire à une dégradation progressive de leurs performances, phénomène connu sous le nom de « model collapse » ou effondrement des modèles[2].

Le même raisonnement vaut pour les autres acteurs de l'économie numérique. Les éditeurs de logiciels, les entreprises de cybersécurité, les hébergeurs, les réseaux de diffusion de contenu (CDN), les opérateurs d'interconnexion, les registres ou les bureaux d'enregistrement ne sont pas en marge du sujet. Ils fournissent les logiciels, les réseaux, les services de confiance, la sécurité, l'adressage, la résolution de noms, l'hébergement et l'interconnexion sans lesquels l'IA ne peut pas tenir ses promesses.



1. OECD : https://www.oecd.org/fr/about/news/announcements/2026/02/ai-firms-capture-61-percent-of-global-venture-capital-in-2025.html
2. Sur la notion de « model collapse », voir Inria, 20 février 2025 : https://www.inria.fr/fr/risque-effondrement-collapse-ia-generatives

Des infrastructures de plus en plus sollicitées

La question du capital mais surtout, pour ces acteurs, de l'accès à une ressource physique accessible qualitativement et quantitativement ne peut pas être séparée de celle des infrastructures. L'IA repose sur des ressources matérielles considérables : puces spécialisées, serveurs, centres de données, capacités de stockage, réseaux, câbles sous-marins, foncier, refroidissement, raccordements électriques, interconnexion… Autant de ressources qui ne sont pas infinies.

Lorsque les grands acteurs de l'IA sécurisent des capacités de calcul, réservent des GPU, financent des centres de données ou développent leurs propres réseaux, ils ne renforcent pas seulement leur position. Ils modifient aussi les conditions d'accès à ces ressources pour les autres acteurs du numérique, pour qui une moindre disponibilité, des délais plus longs et des coûts plus élevés peuvent se traduire par des arbitrages à faire : maintenir l'existant plutôt qu'investir, retarder certains projets, réduire les marges consacrées à la sécurité ou à la résilience…

En résumé, si l'IA mobilise une part croissante des ressources critiques du numérique, les autres acteurs disposent alors de moins de moyens pour maintenir et renouveler leurs contenus, données, logiciels et infrastructures. Or, nous l'avons déjà vu, ce sont précisément ces contenus, données, logiciels et infrastructures qui permettent à l'IA de fonctionner. À terme, l'IA risque donc d'affaiblir le socle qui conditionne sa propre qualité.

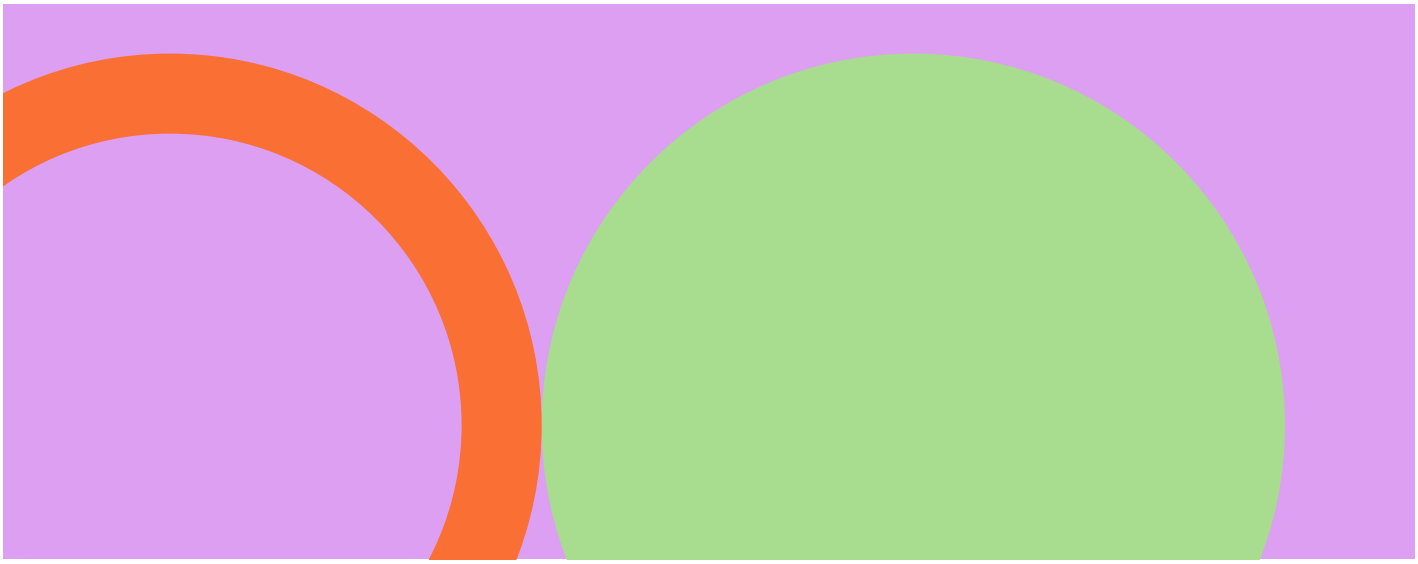
Réguler l'offre ne suffit peut-être plus

Cette tendance à préempter les ressources pose une question de régulation économique. Les politiques en matière de concurrence, qu'elles soient nationales ou européennes, savent traiter certains problèmes bien identifiés : abus de position dominante, ententes, pratiques de verrouillage, acquisitions susceptibles de réduire la concurrence…
Ces outils restent bien entendu indispensables, mais l'IA déplace une partie du problème en amont : avant même la concurrence entre services, se pose la question de l'accès aux ressources qui permettent de les développer.

> **L'IA donne parfois l'impression de pouvoir se suffire à elle-même.**

Le problème ne se limite pas à l'existence de quelques grands fournisseurs de modèles, de cloud ou de puces. Il vient aussi du fait que quelques acteurs peuvent mobiliser, très vite et à très grande échelle, les ressources dont tout le numérique a besoin. C'est ce qui rend le sujet délicat pour les politiques publiques. Faut-il mieux encadrer l'accès à ces ressources critiques ? Faut-il rendre plus visible leur répartition entre acteurs ? Faut-il prévoir des formes de mutualisation, notamment pour les plus petites structures, la recherche ou les infrastructures d'intérêt général ? Derrière ces questions, il y en a une plus générale : comment éviter que la course à l'IA ne transforme le capital, le calcul et les infrastructures en ressources réservées aux seuls acteurs capables de les capter ?

L'IA donne parfois l'impression de pouvoir se suffire à elle-même. C'est une illusion. Elle dépend d'un internet ouvert, de contenus produits par des humains, de réseaux interopérables, d'infrastructures résilientes, d'acteurs spécialisés, de standards, de registres, de politiques de cybersécurité et d'un tissu économique capable de financer autre chose que l'IA elle-même.



2

SÉRIE INTERNET OUVERT

La neutralité du net à l'épreuve des nouvelles portes d'entrée vers l'internet

Adopté en 2015 et applicable depuis le 30 avril 2016, le règlement (UE) 2015/2120 du Parlement européen et du Conseil établissant des mesures relatives à l'accès à un internet ouvert a consacré une idée simple mais essentielle pour la neutralité du net : l'accès à internet ne doit pas dépendre des choix techniques ou commerciaux des fournisseurs d'accès. Les utilisateurs doivent pouvoir choisir librement les contenus auxquels ils accèdent ou qu'ils diffusent, les applications et services qu'ils utilisent ou proposent, ainsi que les terminaux avec lesquels ils se connectent. Les fournisseurs d'accès, eux, doivent traiter le trafic de manière égale, sans discrimination, restriction ou interférence injustifiée.

Cette règle a été novatrice parce qu'elle traduisait juridiquement une caractéristique historique d'internet : la séparation entre les infrastructures d'accès et les contenus qui y circulent. En Europe, le règlement a ainsi donné un socle commun à une intuition technique, économique et démocratique : internet doit rester un espace où l'intermédiaire technique ne devient pas le gardien des usages.

> Les conditions d'accès à internet ont profondément changé.

Dix ans plus tard, le constat est double. D'un côté, le règlement a joué son rôle. L'Arcep estime qu'il s'est révélé « *efficace et résilient* »[3] pour prévenir les discriminations entre contenus et préserver la liberté de choix des internautes. De l'autre, les conditions d'accès à internet ont profondément changé. Les fournisseurs d'accès ne sont plus les seules portes d'entrée vers les contenus et les services en ligne. Les moteurs de recherche, les systèmes d'exploitation, les magasins d'applications, les navigateurs, les réseaux sociaux et, désormais, les assistants d'IA générative structurent à leur tour l'expérience d'internet. L'enjeu, aujourd'hui, est donc de s'assurer, à chaque nouvelle couche d'intermédiation, que l'ambition d'un internet ouvert demeure effective.

Un texte court, mais un cadre vivant

Le règlement internet ouvert repose sur quelques piliers : la liberté de choix des utilisateurs, le traitement égal du trafic, la transparence des offres. Les mesures de gestion de trafic restent possibles, mais elles doivent être transparentes, non discriminatoires, proportionnées et fondées sur des différences objectives de qualité de service, non sur des considérations commerciales.

L'application du règlement a nécessité un travail d'interprétation au fil des ans, porté au niveau européen par le groupe des régulateurs européens, le BEREC (selon son acronyme anglais)[4]. Dès 2016, les premières lignes directrices ont permis d'harmoniser la lecture par les autorités nationales de régulation. Elles ont ensuite été révisées en 2020, puis en 2022, notamment pour intégrer la jurisprudence de la Cour de justice de l'Union européenne. L'objectif : réduire le risque d'interprétations divergentes.

L'interprétation du règlement s'est notamment précisée autour du « tarif nul », qui désigne les offres permettant à un utilisateur d'accéder à certains services sans que les données consommées soient décomptées de son forfait.

Présentées comme avantageuses pour l'utilisateur, elles peuvent néanmoins aller à l'encontre de la neutralité du net : si un service de streaming vidéo, une plateforme musicale ou un réseau social ne « consomme » pas le forfait, alors cela peut orienter le choix de l'utilisateur. La Cour de justice de l'Union européenne a clarifié la question dans un arrêt de principe *Telenor* de 2020[5], puis dans plusieurs affaires *Vodafone* et *Telekom Deutschland* en 2021[6]. Elle a jugé que certaines offres de « tarif nul » méconnaissaient l'obligation de traitement égal du trafic, car même sans blocage ni bridage, le fait de rendre certains services plus avantageux à utiliser peut favoriser certains contenus ou applications au détriment des autres.

La neutralité se joue aussi dans la capacité à contrôler

La neutralité du net pose par ailleurs un véritable défi de mise en application : comment détecter une priorisation, un bridage ou une dégradation discriminatoire, dans des réseaux complexes, dynamiques, parfois gérés automatiquement ? En France, ce règlement est complété par la loi pour une République numérique du 7 octobre 2016 qui fait de l'ARCEP la gardienne de cette neutralité du net en lui donnant des pouvoirs d'enquête et de sanction pouvant atteindre 3 % du chiffre d'affaires des opérateurs. L'Autorité a également développé une approche par les outils : l'application Wehe[7] permet aux utilisateurs de tester d'éventuels bridages ou priorisations, tandis que la plateforme « J'alerte l'Arcep »[8] leur permet de signaler des anomalies.

La surveillance reste néanmoins difficile. Les pratiques problématiques ne prennent pas toujours la forme d'un blocage frontal. Elles peuvent relever de la congestion, de l'interconnexion, d'une politique de qualité de service, de l'architecture d'une offre mobile ou, demain, de formes plus fines de discrimination permises par l'évolution des réseaux. La 5G, par exemple, rend possible le « *network slicing* », qui consiste à découper virtuellement un même réseau en plusieurs « tranches » offrant des niveaux de qualité de service différents. Le *network slicing* n'est pas incompatible en soi avec la neutralité du net, dès lors qu'il répond à des besoins techniques objectifs. Mais il appelle une vigilance particulière s'il conduit à réserver de meilleures conditions d'accès à certains services commerciaux au détriment de l'accès internet général.

La même vigilance s'impose pour les « services spécialisés ». Le règlement internet ouvert permet en effet aux opérateurs de proposer, à côté de l'accès internet classique, certains services optimisés nécessitant un niveau de qualité garanti, par exemple pour des usages médicaux, industriels ou de sécurité. Ces services ne sont pas incompatibles avec la neutralité du net, car ils ne relèvent pas exactement du même service que l'accès général à internet. Mais ils doivent rester strictement encadrés. Ils ne peuvent ni se substituer à l'accès internet, ni en dégrader la qualité. C'est précisément ce qui en fait un sujet de contrôle pour le régulateur : vérifier qu'un besoin technique réel justifie l'optimisation et qu'elle ne devient pas une forme déguisée de priorisation commerciale.

3. « L'Arcep publie le troisième volet de son rapport annuel sur l'état de l'internet en France », 4 juillet 2025 : https://www.arcep.fr/actualites/actualites-et-communiques/detail/n/numerique-040725.html
4. Introduction to open internet : https://www.berec.europa.eu/en/all-topics/introduction-to-open-internet
5. Cour de justice de l'Union européenne, « COMMUNIQUE DE PRESSE n° 106/20 » : https://curia.europa.eu/site/upload/docs/application/pdf/2020-09/cp200106fr.pdf
6. Cour de justice de l'Union européenne, « COMMUNIQUE DE PRESSE n° 145/21 » : https://curia.europa.eu/site/upload/docs/application/pdf/2021-09/cp210145fr.pdf
7. La boite à outils de l'Arcep : https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/la-neutralite-de-linternet/la-boite-a-outils-de-larcep.html
8. J'alerte Arcep : https://jalerte.arcep.fr

De la neutralité des réseaux à l'ouverture des points d'accès

Très tôt, le débat français de la neutralité du net a dépassé la seule couche réseau. L'Arcep a porté la question des terminaux comme un maillon faible de l'internet ouvert[9]. Garantir des tuyaux neutres ne suffit pas si, à l'autre bout de la chaîne, le système d'exploitation, le magasin d'applications, le navigateur ou les applications préinstallées limitent les choix de l'utilisateur.

Le débat n'a pas immédiatement abouti à un principe général de neutralité des terminaux. Mais il a anticipé une évolution majeure du droit européen. Le règlement sur les marchés numériques (connu sous l'acronyme DMA de l'anglais *Digital Markets Act*)[10] impose désormais des obligations à certaines grandes plateformes, qualifiées de contrôleurs d'accès (« *gatekeepers*[11] »), lorsqu'elles maîtrisent des points d'entrée sur internet tels que les systèmes d'exploitation, les magasins d'applications ou les navigateurs. L'enjeu est ici d'éviter qu'un utilisateur soit orienté, par défaut, vers les services de l'acteur qui contrôle son terminal, par exemple lorsqu'un téléphone privilégie son propre navigateur internet, son magasin d'applications ou d'autres applications préinstallées.

Ce déplacement du débat est important. La neutralité du net, telle qu'elle est encadrée par le règlement de 2015, vise d'abord les fournisseurs d'accès à internet et le traitement du trafic. L'internet ouvert, lui, relève d'une ambition plus large. Il suppose que les utilisateurs conservent une capacité réelle à choisir leurs contenus, leurs services et leurs outils, même lorsque l'accès passe par des interfaces qui hiérarchisent, recommandent, préinstallent ou résument.

L'IA générative : nouveau test pour l'internet ouvert

L'IA générative ne remet pas en cause la neutralité du net au sens classique. Elle ne bloque pas un paquet IP, ne ralentit pas une application, ne priorise pas un flux réseau. Mais elle peut devenir une nouvelle porte d'entrée vers internet. En cela, elle prolonge le débat ouvert avec les moteurs de recherche, les assistants vocaux et les magasins d'applications, tout en le radicalisant.

Les services d'IA générative peuvent en effet concentrer l'interaction de l'utilisateur dans une interface unique, qui sélectionne, reformule, structure l'information, accède à certains services tiers et propose une réponse en langage naturel. Le risque n'est pas seulement que l'utilisateur clique moins, c'est aussi qu'il explore moins.

Trois questions émergent ici[12]. La première concerne la découvrabilité : lorsqu'une IA générative résume une réponse, elle peut réduire la visibilité des sources et le trafic vers les sites d'origine. La deuxième concerne la délégation du choix : lorsqu'un assistant recommande un service, réserve un billet ou sélectionne un contenu, l'utilisateur doit pouvoir comprendre selon quels critères, avec quels partenariats éventuels et avec quelle marge de choix. La troisième concerne l'architecture ouverte de l'écosystème : si quelques assistants deviennent des interfaces privilégiées d'accès à internet, la visibilité, l'interconnexion et la valorisation des contenus pourraient dépendre d'un nombre réduit d'acteurs.

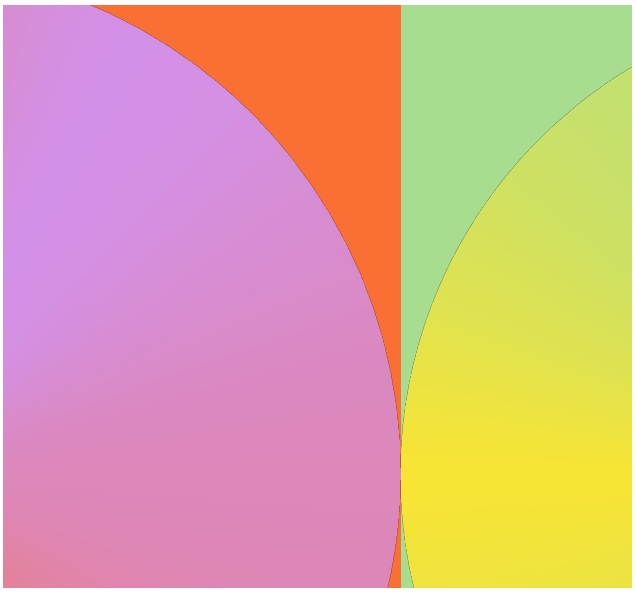
Ces enjeux ne relèvent pas directement de la neutralité du net au sens du règlement de 2015, mais ils prolongent la même interrogation : comment préserver un accès ouvert et transparent à internet lorsque de nouveaux intermédiaires s'interposent entre l'utilisateur et les contenus ? Ils confirment également que l'ouverture d'internet ne peut plus être pensée uniquement depuis l'accès réseau. Elle doit être interrogée à chaque couche où se joue la liberté effective de choisir, de publier, d'être trouvé et d'innover.

La neutralité du net, première brique de l'internet ouvert

La force du règlement sur l'internet ouvert est d'avoir posé une règle claire dans un environnement mouvant. Dix ans après, cette règle est toujours pertinente. Elle protège l'utilisateur contre les discriminations de trafic et rappelle que l'accès à internet est aussi une condition d'accès à l'information, à la liberté d'expression, à l'activité économique et à la participation démocratique.

Le règlement de 2015 vise d'abord les fournisseurs d'accès, mais l'accès à internet ne dépend plus seulement d'eux. Il passe aussi par des terminaux, des navigateurs, des moteurs de recherche, des magasins d'applications et, de plus en plus, par des assistants d'IA générative. C'est pourquoi la neutralité du net doit être pensée comme une première brique de l'internet ouvert : indispensable pour garantir un accès non discriminatoire au réseau, mais à replacer dans un contexte où d'autres intermédiaires peuvent aussi orienter l'accès aux contenus et services en ligne.

Cette réflexion inaugure une série d'articles consacrée à l'internet ouvert. Après ce premier volet dédié à la neutralité du net, les prochains numéros prolongeront l'analyse autour des nouvelles conditions d'accès aux contenus, aux services et aux infrastructures numériques, notamment à l'heure de l'IA générative et des standards ouverts.



9. L'influence des terminaux et plateformes sur l'ouverture d'internet : https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/linfluence-des-terminaux-et-plateformes-sur-louverture-dinternet.html
10. The Digital Markets Act : https://digital-markets-act.ec.europa.eu/index_en
11. Gatekeepers Portal : https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en
12. Ces questions feront l'objet d'un examen plus approfondi dans un prochain article de cette série consacrée à l'internet ouvert.

03

RGESN : vers une nouvelle version du référentiel d'écoconception des services numériques

Publié en 2024, le Référentiel général d'écoconception des services numériques, ou RGESN, est d'ores et déjà devenu plus qu'un simple document de référence. À mesure que les organisations s'en saisissent, il devient un objet de travail : on l'interprète, on le teste, on l'applique à des services très différents, on en mesure les apports, mais aussi les zones qui restent à préciser. Cette appropriation est le signe d'un référentiel vivant, désormais confronté à des pratiques réelles. C'est une bonne chose car l'écoconception numérique ne peut rester un simple principe. Pour produire des effets, elle doit se traduire en critères compréhensibles, en méthodes d'évaluation, en preuves, en arbitrages et en feuilles de route.

C'est précisément l'ambition du RGESN : aider les organisations à passer d'une intention, celle de concevoir des services numériques plus sobres, à une démarche structurée, mesurable et améliorable dans le temps. Les premiers retours de terrain montrent toutefois que, pour y parvenir pleinement, des ajustements sont encore nécessaires : clarifier certains critères, harmoniser les pratiques d'audit, mieux documenter les cas de non-applicabilité, rendre les déclarations d'écoconception plus comparables… C'est ainsi un nouveau chantier qui s'ouvre désormais pour le RGESN : celui de son évolution.

Un référentiel pour structurer les démarches d'écoconception des services numériques

Le RGESN[13] s'inscrit directement dans la dynamique de la loi REEN[14], qui vise à réduire l'empreinte environnementale du numérique en France. Élaboré par l'Arcep et l'Arcom avec l'appui de l'ADEME, il traduit cette ambition en critères concrets à respecter pour concevoir, évaluer et améliorer les services numériques au regard de leur impact environnemental.

Une grille d'évaluation simplifiée pour faciliter l'appropriation

Le RGESN n'est pas parti de rien. Il prolonge un ensemble de référentiels et de travaux déjà existants, notamment le GR491[15], guide de référence de conception responsable des services numériques. Ce dernier constitue un corpus très complet, avec plus de 500 critères. Cette richesse en fait un outil précieux pour les experts, mais aussi un objet difficile à prendre en main pour une organisation qui cherche à structurer une première démarche d'évaluation.

Le RGESN répond à ce besoin d'opérationnalisation. Il propose 78 critères, répartis en neuf thématiques : stratégie, spécifications, architecture, expérience et interface utilisateur, contenus, frontend, backend, hébergement et algorithmie. Ce format plus resserré permet d'entrer plus vite dans la démarche, sans pour autant renoncer à une vision globale du service numérique et de l'ensemble de son cycle de vie.

Un outil de diagnostic plus qu'un label

La logique du RGESN n'est pas celle d'un label figé, mais celle d'un progrès mesurable. Il offre une grille mobilisable pour lancer un diagnostic, documenter les pratiques existantes et prioriser les actions. Le score obtenu n'est donc pas une fin en soi. Il sert surtout à établir une situation de départ (quels critères sont déjà couverts, lesquels ne le sont pas, quels points relèvent réellement d'une non-applicabilité, quelles pratiques existent déjà sans être suffisamment formalisées, etc.) et un suivi dans le temps. L'exercice montre vite que l'écoconception est autant une question de méthode que de technique. Il ne suffit pas d'identifier de bonnes pratiques, encore faut-il pouvoir les documenter, les justifier et les inscrire dans les processus de conception, de développement et d'exploitation.

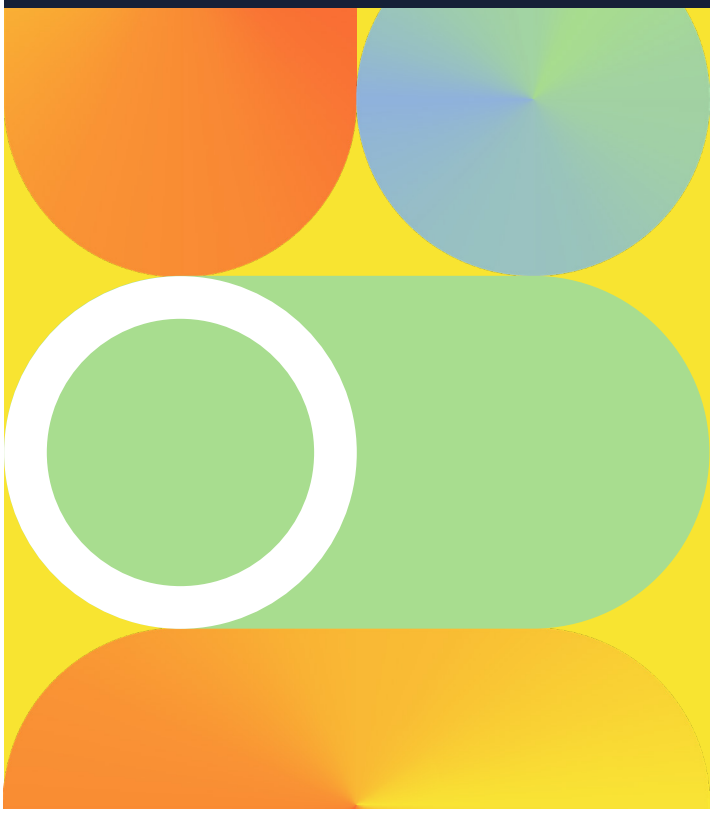
C'est l'un des apports du RGESN. Il aide à distinguer ce qui est fait, ce qui peut être prouvé, ce qui reste informel et ce qui doit être amélioré. Dans beaucoup d'organisations, des pratiques utiles existent déjà, mais elles reposent sur des habitudes, des choix historiques ou des personnes identifiées. Tant qu'elles ne sont pas formalisées, elles restent fragiles.

Le RGESN dans la démarche numérique responsable de l'Afnic

À l'Afnic, l'appropriation du RGESN s'est construite à partir d'une première action très concrète : la formation des équipes techniques à l'écoconception numérique. Cette formation a rapidement fait émerger une attente plus globale : disposer d'un diagnostic plus précis des pratiques existantes et des leviers d'amélioration possibles.

En 2025, l'Afnic a donc engagé une première autoévaluation à partir de la grille RGESN publiée en ligne, aboutissant à un niveau de conformité de 47 %. L'association a ensuite été accompagnée par Ctrl-a, groupement d'agences spécialisé dans le numérique responsable, afin de bénéficier d'un regard externe et d'établir une feuille de route opérationnelle. Une nouvelle évaluation a confirmé un niveau de conformité de 50 % et permis de distinguer deux familles d'actions : des améliorations rapides, portant notamment sur la documentation, la traçabilité ou l'intégration de réflexes d'écoconception dans les cycles de développement ; et des chantiers plus structurels, liés par exemple à l'architecture ou à l'outillage.

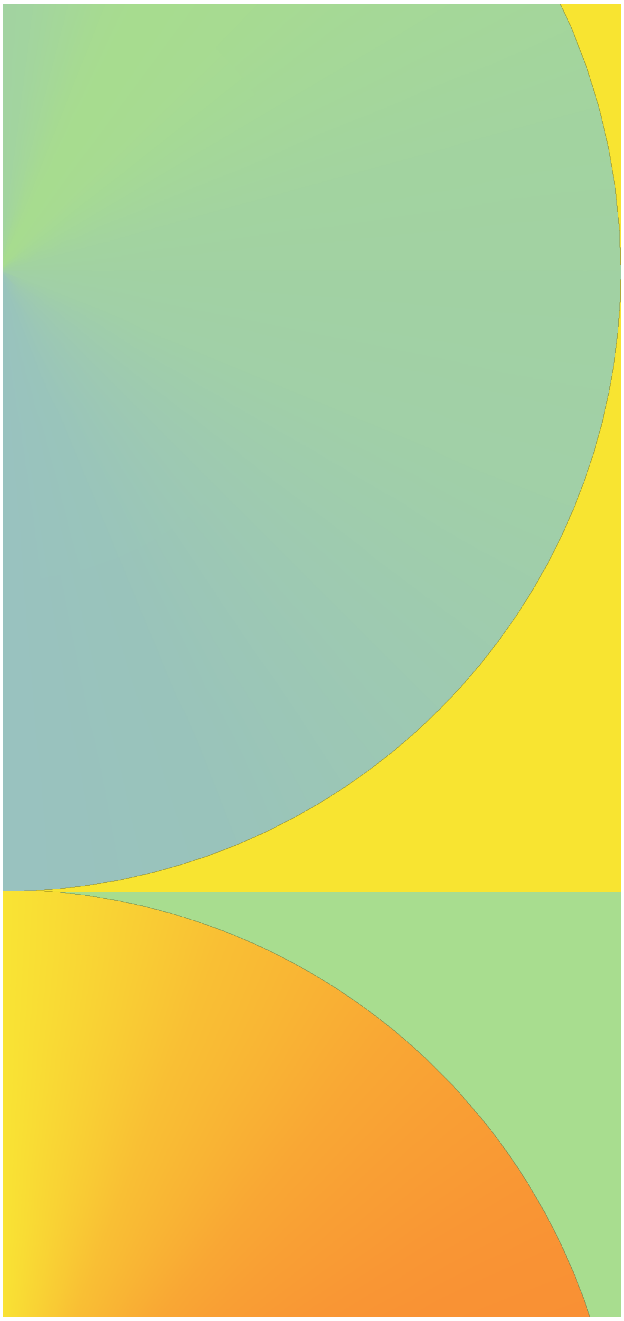
Les premières actions issues de la feuille de route seront engagées dès 2026, avec une priorité donnée aux gains les plus accessibles et les plus utiles pour préparer les évolutions de fond. La trajectoire complète permettra d'atteindre un niveau de conformité sensiblement plus élevé, évalué à 73 %.



13. Référentiel général d'écoconception de services numériques (RGESN) – 2024 : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/
14. LOI n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France ⓘ : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272
15. GR491 : https://gr491.isit-europe.org

Le référentiel permet ainsi de transformer des intentions parfois dispersées en trajectoire de progrès. Il donne un cadre commun pour faire dialoguer les métiers concernés – produit, design, développement, exploitation, achats, conformité, communication, etc. – autour de critères partagés.

À noter également : l'Organisation internationale de normalisation vient à son tour de publier en mars 2026 la norme ISO/IEC TS 20125-1:2026[16], intitulée *Digital services ecodesign*, le fruit de trois années de contributions collectives. La norme établit un cadre international structuré pour intégrer les principes d'écoconception à chaque étape du cycle de vie d'un service numérique de sa conception à sa mise hors service en couvrant les dimensions techniques, organisationnelles et fonctionnelles qui conditionnent l'impact environnemental d'un produit digital. L'application de cette nouvelle norme reste volontaire mais confirme le potentiel réel de contribution de l'écoconception à la réduction de l'impact environnemental du numérique, notamment dans un contexte où l'essor de l'intelligence artificielle génère une consommation énergétique et matérielle croissante.



Des difficultés d'application identifiées

Dès lors qu'il est utilisé comme outil de diagnostic, le RGESN fait émerger des questions très concrètes. Il n'est pas toujours évident d'appliquer une série de critères génériques à des services numériques préexistants au RGESN et aussi variés que des sites web, des API, des logiciels SaaS, des plateformes vidéo, des outils reposant sur un système d'intelligence artificielle, etc. Il faut en préciser le sens, déterminer comment les vérifier concrètement et tenir compte des contraintes techniques et organisationnelles.

La première difficulté tient à l'interprétation des critères. Certains peuvent donner lieu à des lectures différentes selon le service audité, les preuves disponibles ou la méthode retenue par l'auditeur. Or, si deux évaluations proches aboutissent à des résultats trop différents, le référentiel perd une partie de sa valeur comme cadre commun. La prochaine étape consistera donc à mieux préciser les attendus, les moyens de test et les cas dans lesquels un critère peut être considéré comme applicable, non applicable ou partiellement couvert.

La deuxième difficulté concerne la preuve. Le RGESN suppose de documenter les choix de conception, les arbitrages réalisés et les éléments permettant de vérifier qu'une pratique est bien en place. Mais tout ne relève pas du même niveau de communication. Certaines informations sont utiles pour l'audit ou le pilotage interne, d'autres ont vocation à figurer dans la déclaration publique d'écoconception. Clarifier cette distinction est important pour éviter que la déclaration ne devienne un document trop technique, difficile à produire et peu lisible pour ses destinataires.

Enfin, plusieurs retours soulignent la nécessité de mieux adapter certains critères à la diversité des services numériques. Le RGESN s'applique à des objets très différents, dont les contraintes ne sont pas toujours comparables. Une plateforme, une application métier, un service fortement dépendant de briques tierces ou un système intégrant de l'algorithmie ne soulèvent pas les mêmes questions qu'un site web classique. Certains critères doivent donc être clarifiés pour éviter une application trop mécanique, voire des arbitrages contre-productifs.

Ces points appellent un travail de stabilisation du référentiel. Non pour en modifier l'esprit, mais pour en faciliter l'application dans des contextes variés.

Des travaux engagés pour faire évoluer le référentiel

Les difficultés identifiées dans les premières applications du RGESN alimentent désormais plusieurs travaux de mise à jour. L'Arcep et l'Arcom ont notamment lancé, avec la participation de l'ADEME, le Forum des parties prenantes de l'écoconception numérique, dont la première édition s'est tenue le 19 mai 2025. Cette instance de dialogue réunit des experts et des praticiens de l'écoconception numérique afin de suivre la mise en œuvre du référentiel et de recueillir les retours d'expérience de l'écosystème.

16. ISO/IEC TS 20125-1:2026 : https://www.iso.org/standard/86105.html

En parallèle, le Consortium RGESN s'est structuré en janvier 2025 autour d'expertes et d'experts du numérique responsable, avec le soutien financier de l'ADEME et de l'Afnic. Sa note de synthèse[17], publiée en janvier 2026, rassemble les propositions issues d'un travail bénévole mené pendant l'année 2025, à partir d'expériences d'audit, d'accompagnement et de mise en œuvre du référentiel. Le Consortium indique avoir réuni près de 70 personnes, dont 45 membres actifs signataires de la charte, au sein de 9 groupes de travail.

Ces travaux donnent une idée assez précise des évolutions attendues. Sur les 78 critères du RGESN, 42 ont fait l'objet de propositions ayant atteint un consensus : 19 correctifs minimes, 15 modifications importantes, 6 suppressions et 2 nouveaux critères proposés. Les sujets remontés rejoignent les difficultés observées sur le terrain : clarifier les termes, réduire les marges d'interprétation, préciser les contextes d'application, alléger certains moyens de test trop lourds, supprimer ou fusionner des critères lorsque leur lien avec l'écoconception est insuffisamment établi, ou encore couvrir certains angles morts du référentiel.

La déclaration d'écoconception fait aussi partie des points à retravailler. Le Consortium relève l'absence d'un modèle déclaratif réellement homogène, la lourdeur du modèle textuel proposé et la diversité des déclarations publiées, qui rend difficile la comparaison d'un service à l'autre. Il propose notamment un modèle simplifié de déclaration et un modèle de rapport d'audit, afin de rendre les évaluations plus lisibles et plus homogènes.

L'évolution du RGESN pourrait donc prendre plusieurs formes. Certaines corrections relèvent de la clarification ou de la précision, sans modifier les scores obtenus lors des audits déjà réalisés. D'autres supposeraient une révision plus profonde de certains critères et pourraient relever d'une version plus structurante. Si les premiers travaux du Consortium distinguaient des propositions assimilables à une « version 1.1 » et d'autres relevant plutôt d'une « version 2 », les échanges récents semblent désormais privilégier une évolution directe du RGESN vers une « version 2 ».

> **Le référentiel est généraliste, mais certains critères restent très marqués par les usages web.**

À plus long terme, deux pistes se dégagent également : introduire davantage de granularité dans les moyens de test pour rendre l'évaluation plus guidée et envisager des déclinaisons du RGESN par type de service numérique. Cette seconde piste répond à une difficulté récurrente : le référentiel est généraliste, mais certains critères restent très marqués par les usages web, alors que les services numériques concernés peuvent être

des applications métier, des services SaaS, des systèmes embarqués, des services intégrant de l'IA ou des plateformes complexes.

L'objectif n'est donc pas de repartir de zéro. Il s'agit plutôt de consolider un socle désormais utilisé. Conserver une grille commune, tout en la rendant plus claire, plus homogène et plus facile à appliquer.

Un cadre pour inscrire l'écoconception dans la durée

Le RGESN ne prétend pas répondre à lui seul à la question de l'empreinte environnementale du numérique. Il ne se substitue pas à une stratégie environnementale complète, mais l'outille sur le périmètre des services numériques. Il aide à poser les bonnes questions, à documenter les réponses, à rendre les arbitrages visibles et à organiser une progression dans le temps.

Pour l'Afnic, cette démarche rejoint une conviction déjà ancienne : la performance technique, la sécurité, la protection des données et la responsabilité environnementale ne doivent pas être traitées comme des sujets séparés. Un service numérique de qualité doit être fiable, sécurisé, maintenable, accessible et conçu avec une attention réelle aux ressources qu'il mobilise.

C'est aussi ce que peut permettre l'évolution du RGESN : faire de l'écoconception non plus une démarche ponctuelle, mais une composante durable de la qualité et de la confiance numérique.

17. Le Consortium RGESN a publié la synthèse de ses travaux 2025 : https://www.temesis.com/blog/le-consortium-rgesn-a-publie-la-synthese-de-ses-travaux-2025/

4

Protocole ECH : un pas de plus vers la protection de la vie privée sur internet

L'évolution des protocoles de sécurité sur internet tend à réduire la quantité d'informations exposées en clair lors des communications. Après le chiffrement du contenu des échanges avec TLS (*Transport Layer Security*), puis celui des requêtes DNS via DoH (*DNS over HTTPS*) ou DoT (*DNS over TLS*), une nouvelle étape consiste à ne plus exposer en clair le nom de domaine demandé lors de l'établissement d'une connexion. C'est l'objet du protocole ECH (*Encrypted Client Hello*), défini par la RFC 9849 publiée en mars 2026.

Une information longtemps restée visible

Lorsqu'un utilisateur souhaite accéder à un site web, la connexion sécurisée TLS débute par un message appelé *ClientHello*. Celui-ci contient notamment une extension, le SNI (*Server Name Indication*), qui indique au serveur le nom de domaine souhaité. Historiquement, ce SNI est transmis en clair.

Pour mieux comprendre pourquoi, il faut regarder ce qu'il se passe concrètement, dans la plupart des cas, lorsqu'un internaute souhaite se connecter à un site :

- Résolution DNS : lorsqu'il tape l'adresse du site dans son navigateur, celui-ci va interroger un résolveur pour obtenir l'adresse IP correspondant au nom de domaine. Cette requête et sa réponse peuvent être chiffrées via DoH ou DoT.
- Ouverture de la connexion TCP : une fois l'adresse IP obtenue, le client va ouvrir une connexion TCP (*Transmission Control Protocol*) vers cette adresse, c'est-à-dire un canal de communication fiable sur lequel les échanges vont ensuite avoir lieu.
- Démarrage de TLS – message *ClientHello* : sur cette connexion TCP, le client va initier le protocole TLS (*Transport Layer Security*), qui permet de sécuriser les échanges en assurant leur chiffrement et leur intégrité. Cette étape débute par l'envoi d'un message *ClientHello*, qui inclut notamment le SNI, c'est-à-dire le nom de domaine visé.
- Établissement de la session TLS : le serveur répond au *ClientHello*, les paramètres cryptographiques sont négociés, puis les deux parties établissent une clé de session. C'est à partir de ce moment que les échanges commencent à être chiffrés par TLS.

Autrement dit, le *ClientHello* reste en clair parce qu'il intervient avant que la session TLS ne soit établie. À ce stade, le serveur a encore besoin de connaître le nom de domaine demandé, notamment pour présenter le bon certificat lorsqu'une même adresse IP héberge plusieurs sites. Or, aucune clé de session n'a encore été négociée entre le client et le serveur pour chiffrer cet échange.

Pourquoi le *ClientHello* en clair pose problème

Le fait que le *ClientHello* reste en clair pose d'abord un problème de respect de la vie privée. Même lorsque le contenu des échanges qui suivront est chiffré, le fait de connaître le nom de domaine demandé en dit déjà beaucoup sur l'usage d'internet par un utilisateur. Ces informations peuvent être exploitées pour observer le trafic, identifier des sites consultés et même, dans certains contextes, alimenter des activités de renseignement, voire d'espionnage. La RFC 9849[18] définissant ECH rappelle d'ailleurs que le SNI en clair reste l'une des informations les plus sensibles encore exposées dans TLS 1.3.

Ces informations peuvent également être exploitées à des fins de censure, pour empêcher l'accès à certains sites en particulier. C'est d'autant plus simple à mettre en œuvre que le *ClientHello* est un message standardisé, dans lequel l'information recherchée se trouve à un emplacement prévisible. Cet usage est d'ailleurs bien documenté. En Russie[19], notamment, plusieurs travaux de recherche ont montré que des dispositifs de censure inspectent le SNI afin de repérer des noms de domaine de sites figurant sur des listes de blocage, puis d'interrompre la connexion, notamment en injectant de faux paquets TCP RST qui simulent une déconnexion du serveur.

Le fonctionnement d'ECH et le rôle du DNS

Pour résoudre ce problème, il faudrait pouvoir chiffrer le SNI et, plus largement, l'ensemble des informations sensibles contenues dans le message *ClientHello*. Mais comment chiffrer ce message alors même qu'il intervient avant l'établissement de la connexion TLS, c'est-à-dire avant que le client et le serveur ne disposent d'une clé commune ?

Cela suppose que le client ait pu récupérer en amont les éléments nécessaires à ce chiffrement. La RFC 9849 décrit précisément le mécanisme qui permet d'y parvenir. Elle n'impose toutefois pas une méthode unique pour publier la configuration nécessaire : en théorie, celle-ci peut être fournie par différents moyens, par exemple via une configuration manuelle et statique côté client. En pratique, la solution la plus naturelle, et sans doute celle qui sera la plus utilisée, consiste à publier cette configuration ECH dans le DNS, d'où elle est récupérée lors de la résolution du nom de domaine. Cet amorçage via le DNS, au moyen des enregistrements SVCB/HTTPS et du paramètre ech, est quant à lui décrit dans la RFC 9848[20].

Le client peut ensuite utiliser la configuration ECH pour protéger les informations sensibles du *ClientHello* : un message interne (*ClientHelloInner*) chiffré, contenant notamment le SNI, est encapsulé dans un message externe (*ClientHelloOuter*), visible et compatible avec l'infrastructure existante. Le serveur, disposant de la clé privée correspondante, est capable de déchiffrer ce *ClientHelloInner* et d'identifier le nom de domaine demandé sans l'exposer sur le réseau.

Une protection particulièrement efficace pour les environnements mutualisés

Si ECH permet de renforcer la confidentialité des échanges, il ne rend pas pour autant une communication totalement anonyme. L'adresse IP de destination reste en effet visible, car elle est nécessaire à l'acheminement des paquets sur le réseau. C'est pourquoi l'intérêt d'ECH varie, en réalité, selon les architectures d'hébergement. Pour un site reposant sur un serveur dédié, où une adresse IP correspond en pratique à un

18. RFC 9849 : https://www.rfc-editor.org/rfc/rfc9849.pdf
19. Sur la censure et la surveillance des infrastructures internet en Russie, voir notamment Françoise Daucé, Benjamin Loveluck et Francesca Musiani (dir.), « Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012-2022 », Presses des Mines, 2023 : https://cis.cnrs.fr/genese-d-un-autoritarisme-numerique/
20. RFC 9848 : https://www.rfc-editor.org/rfc/rfc9848.pdf

seul nom de domaine, le gain en confidentialité reste limité. En revanche, dans les environnements mutualisés, tels que les plateformes d'hébergement ou les réseaux de diffusion de contenu (CDN), une même adresse IP peut servir de nombreux sites. ECH empêche alors de déterminer précisément le nom de domaine effectivement consulté.

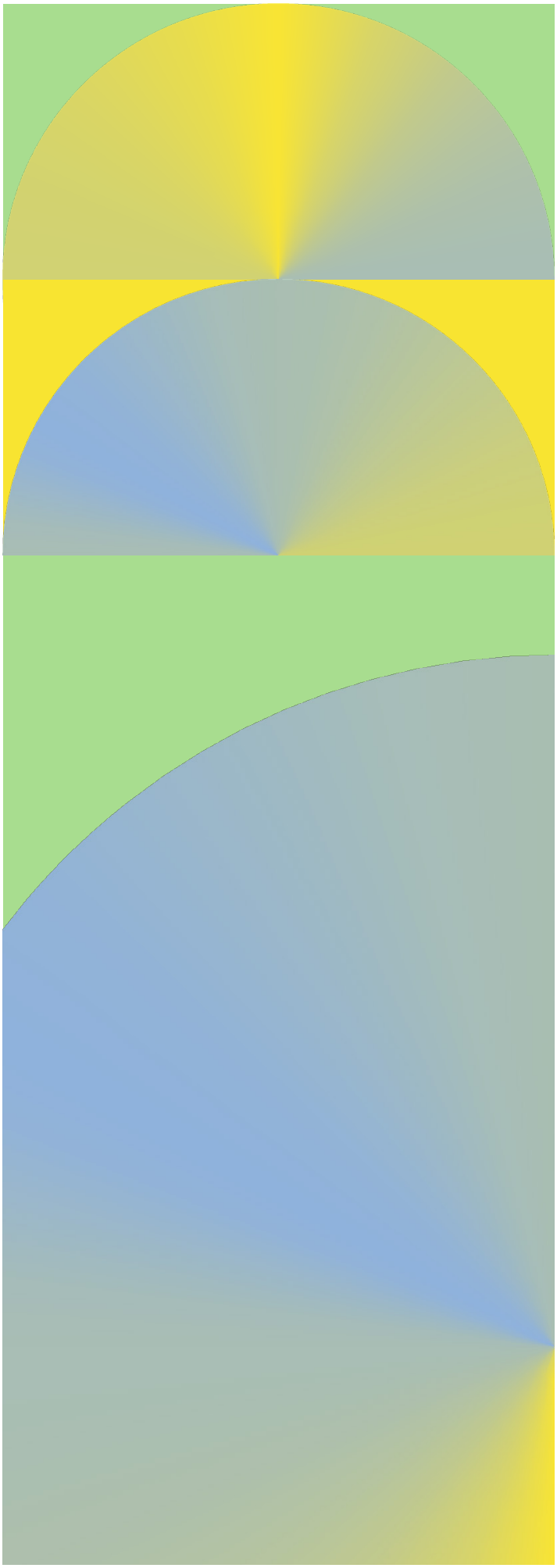
ECH n'a donc pas vocation à s'imposer partout, ni d'ailleurs au même rythme. Si certains navigateurs ont déjà commencé à l'intégrer côté client, sa mise en œuvre côté serveur demeure plus lourde, car elle suppose à la fois une prise en charge du mécanisme dans TLS et la publication dans le DNS des informations nécessaires au chiffrement du *ClientHello*. L'intégration d'ECH dans OpenSSL 4.0[21], annoncée en avril 2026, constitue à ce titre une étape importante. Elle facilite l'adoption du mécanisme par les logiciels serveurs qui s'appuient sur cette bibliothèque, même si le déploiement opérationnel dépendra encore des choix d'architecture et du support effectif dans les différents composants de l'écosystème.

Le déploiement d'ECH ne sera par ailleurs pas neutre pour les autorités publiques. Lorsqu'il s'agit de reconstituer un historique de navigation sur internet à des fins d'enquête, le SNI transmis en clair est un indice directement exploitable pour identifier un nom de domaine visé. En chiffrant cette information, ECH est donc susceptible de rendre moins efficaces les méthodes qui reposent sur l'observation passive du *ClientHello*. Il ne faut pas en déduire pour autant que toute capacité d'identification disparaît.
L'adresse IP de destination reste visible, de même que certaines métadonnées de connexion telles que l'heure, la durée ou les volumes échangés. D'autres sources peuvent également être disponibles, comme les données DNS lorsqu'elles ne sont pas chiffrées. Toutes ces données peuvent encore nourrir des recoupements. Pour les forces de l'ordre, l'enjeu sera avant tout d'anticiper cette perte de visibilité sur le SNI en clair et d'adapter certaines de leurs méthodes d'enquête.

En conclusion

En permettant de chiffrer des informations sensibles qui restaient jusqu'ici exposées en clair au moment de l'établissement d'une connexion, ECH marque une nouvelle étape dans l'évolution des protocoles de sécurité sur internet. Il contribue à mieux protéger le nom de domaine demandé et constitue à ce titre un pas de plus vers un meilleur respect de la vie privée en ligne.

Le déploiement d'ECH montre aussi que le DNS ne se limite plus à sa fonction traditionnelle de résolution des noms de domaine. En servant à publier les informations nécessaires à la mise en œuvre du protocole, il devient un maillon direct de la sécurité des communications. Cela renforce, en retour, l'importance des mécanismes destinés à sécuriser le DNS lui-même. L'intégrité des informations publiées, tout comme la confidentialité des requêtes permettant de les obtenir, prennent une importance croissante à mesure que le DNS participe plus étroitement à la protection des échanges.



21. OpenSSL 4.0 Released With Encrypted Client Hello, RFC 8998 Support : https://www.phoronix.com/news/OpenSSL-4.0-Released

05 Brèves

Nouvelle obligation de signalement des vulnérabilités exploitées du CRA : un défi pour l'open source

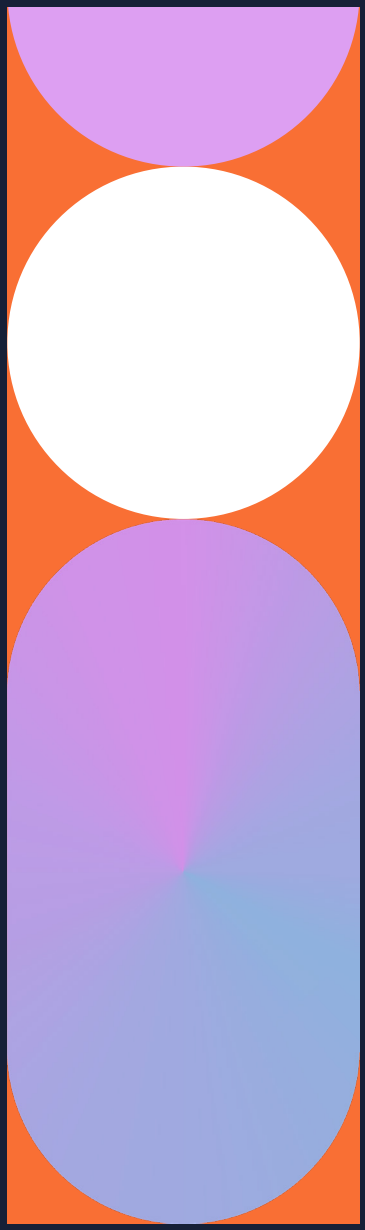
À partir du 11 septembre 2026, une première brique opérationnelle du *Cyber Resilience Act* (CRA) entrera en application. Les fabricants de produits mis sur le marché intérieur de l'Union européenne seront tenus de signaler les vulnérabilités activement exploitées et les incidents graves ayant une incidence sur la sécurité des produits comportant des éléments numériques[22].

Ces signalements devront passer par la « *Single Reporting Platform* », une plateforme opérée par l'ENISA[23], l'agence de l'Union européenne pour la cybersécurité. Une première alerte devra être transmise dans les 24 heures après la prise de connaissance de l'événement, suivie d'éléments complémentaires sous 72 heures, puis d'un rapport final, dans un délai de 14 jours pour les vulnérabilités et d'environ un mois pour les incidents. Le non-respect de ces obligations pourra donner lieu à des sanctions pouvant aller jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial.

Cette nouvelle obligation interpelle particulièrement la communauté open source. Le logiciel libre occupe une place importante dans l'écosystème numérique européen et mondial, mais il repose souvent sur des modèles très différents de ceux des éditeurs logiciels : communautés de développeurs, mainteneurs bénévoles, fondations ou structures aux moyens limités. En principe, le CRA ne vise pas les logiciels libres dès lors qu'ils sont mis à disposition hors de toute activité commerciale. Leurs développeurs ou mainteneurs ne devraient donc pas, dans ce cas, être concernés par la future obligation de signalement des vulnérabilités exploitées.

Mais la situation se complexifie lorsqu'un logiciel open source est intégré, distribué ou exploité dans le cadre d'une offre ou d'un service mis sur le marché. Dans certains modèles open source, la frontière entre mise à disposition non commerciale et utilisation dans un contexte économique peut être difficile à tracer. Le CRA a d'ailleurs créé le nouveau rôle d'« intendant de logiciel open source » pour certaines structures qui soutiennent durablement des projets libres destinés à être utilisés commercialement, sans pour autant être qualifiées de fabricants. La question est de savoir où se situe la responsabilité : du côté des mainteneurs du projet open source, de l'éventuel intendant qui le soutient ou de l'acteur qui l'intègre dans son propre produit ou service ? En pratique, cette incertitude pourrait aussi engendrer des pressions d'éditeurs ou d'intégrateurs sur les mainteneurs open source, malgré la distinction opérée par le CRA entre les différents rôles de l'écosystème.

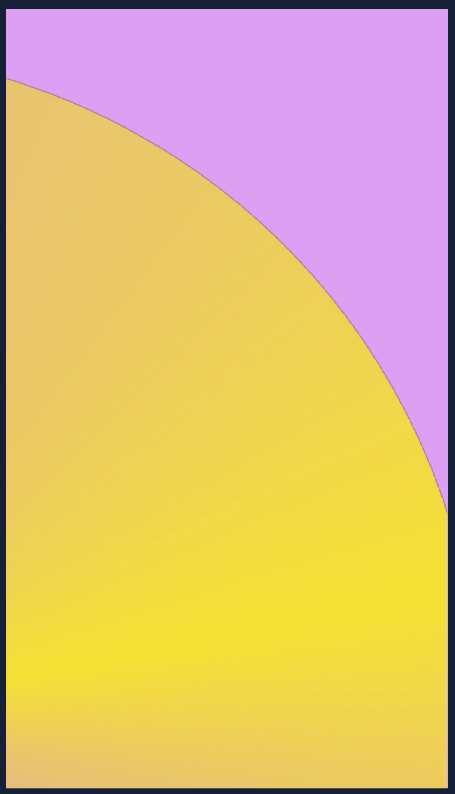
Autre point d'attention : les entreprises qui réutilisent des briques open source dans leurs propres produits ou services seront amenées, notamment via le SBOM (*Software Bill of Materials*), l'obligation de nomenclature logicielle imposée par le CRA, à demander davantage d'informations, de garanties ou de documentation sur leur sécurité. Le risque est alors de déplacer une partie de la charge de conformité vers les communautés du logiciel libre qui ne disposent pas toujours des moyens juridiques, organisationnels ou financiers nécessaires•••



22. CRA Reporting : https://digital-strategy.ec.europa.eu/en/policies/cra-reporting
23. Single Reporting Platform SRP : https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp

••• Enfin, se pose aussi la question du suivi des vulnérabilités dans la durée. Une faille peut être corrigée rapidement dans le projet open source d'origine, tout en restant présente dans des produits ou services qui n'ont pas encore intégré la mise à jour. Le CRA pourrait donc contribuer à responsabiliser davantage les acteurs en aval, mais aussi raviver une crainte : que certains préfèrent éviter des composants ouverts jugés plus complexes à documenter ou à suivre, au profit de solutions fermées.

L'application du *Cyber Resilience Act* soulève donc encore des questions importantes pour l'open source, et tout particulièrement pour les nombreuses briques logicielles libres au cœur des services de nommage, de routage, de résolution, de supervision ou de sécurisation des réseaux, essentielles au fonctionnement de l'internet. Des ambiguïtés sur les rôles, les responsabilités et les charges attendues pourraient en effet fragiliser les communautés techniques très actives, parfois bénévoles, dont dépend une partie de la résilience de l'internet. Au niveau européen, les lignes directrices de la Commission devront donc aider à préciser l'application du règlement à ces situations hybrides. Il sera également important de prévoir, en complément du CRA, des dispositifs incitatifs ou de soutien à l'open source et d'en mesurer l'efficacité pour éviter le désinvestissement des communautés techniques.



Post-quantique : les calendriers commencent à se resserrer

En déclarant avancer son calendrier de migration post-quantique à 2029, dans un billet publié sur son blog technique le 25 mars dernier[24], Google ajoute un signal à une tendance déjà bien engagée : l'échéance post-quantique se rapproche. L'entreprise explique avoir ajusté son modèle de menace, notamment pour les services d'authentification et les signatures numériques, et recommande aux autres équipes d'ingénierie de faire de même.

Cette annonce intervient alors que plusieurs feuilles de route publiques restent plutôt calées sur un horizon 2030-2035. Le calendrier du NIST, l'agence américaine notamment en charge des standards et des recommandations technologiques, auquel Google fait lui-même référence dans son article, évoque une dépréciation progressive des systèmes vulnérables après 2030 et leur abandon après 2035. En France, comme nous le rappelions dans La Lettre Afnic n°12[25], l'ANSSI considère qu'à l'horizon 2030 il ne sera plus raisonnable d'acquérir des solutions ne prenant pas en compte la cryptographie post-quantique.

Google justifie le resserrement de son calendrier par les progrès observés sur le matériel quantique, la correction d'erreurs et les estimations de ressources nécessaires pour casser les cryptosystèmes actuels. En mai 2025, des chercheurs de Google estimaient ainsi qu'une clé RSA-2048 pourrait, en théorie, être factorisée par un ordinateur quantique disposant d'un million de qubits bruités pendant une semaine[26]. Ce chiffre reste très au-dessus des capacités actuelles – les machines pertinentes étant encore de l'ordre de quelques centaines à quelques milliers de qubits –, mais il représente une baisse d'un facteur 20 par rapport à une estimation Google de 2019. D'autres travaux récents[27] vont encore plus loin, avançant que la factorisation de RSA-2048 pourrait être réalisée avec moins de 100 000 qubits physiques, sous certaines hypothèses d'architecture et de correction d'erreurs•••

24. Quantum frontiers may be closer than they appear : https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/
25. « La transition vers la cryptographie post-quantique doit s'engager sans attendre », Lettre Afnic n°12 : https://www.afnic.fr/wp-media/uploads/2026/03/La-Lettre-Afnic-12_170326.pdf
26. Tracking the Cost of Quantum Factoring : https://blog.google/security/tracking-cost-of-quantum-factori/
27. « The Pinnacle Architecture: Reducing the Cost of Factoring 2048-bit RSA by an Order of Magnitude », arXiv, février 2026 : https://arxiv.org/pdf/2602.11457

••• Il faut toutefois lire ces annonces avec deux précautions. D'une part, elles relèvent aussi d'une compétition industrielle où les acteurs du quantique ont intérêt à démontrer l'urgence, notamment pour attirer financements et attention. D'autre part, plus le sujet deviendra sensible, moins les informations détaillées sur les méthodes, les seuils techniques et les marges d'erreur seront nécessairement publiques.

Reste que le signal converge : l'échéance post-quantique tend à se rapprocher dans les discours des grands acteurs. Pour une entreprise comme Google, dont l'activité repose structurellement sur la donnée et la confiance numérique de milliards d'utilisateurs, avancer le calendrier n'est pas anodin. Même si l'ordinateur quantique cryptographiquement pertinent n'est pas encore là, la migration doit être anticipée, car l'inventaire des usages cryptographiques, les changements de protocoles, les tests d'interopérabilité et la gestion des signatures prendront plusieurs années. Le risque n'est donc pas seulement de voir arriver trop tôt une machine capable de casser les algorithmes actuels, il est surtout de commencer à s'y préparer trop tard.

Pour sa part, l'Afnic et ses équipes ont engagé des travaux en interne, mais également avec d'autres acteurs de la communauté technique, pour évaluer les impacts sur le DNS et son extension de sécurité DNSSEC pour la communauté et en tant que Registre internet. Elle est par exemple investie dans la coalition dynamique du Forum sur la gouvernance de l'Internet IS3C[28], coorganisant plusieurs webinaires et réunions (forum EuroDig 2026), à la fois de sensibilisation générale et plus spécifiques sur les grands enjeux de la transition vers la cryptographie post-quantique au niveau des services d'infrastructures internet comme le DNS et le routage. De plus, les équipes techniques de l'Afnic testent actuellement des matériels français de chiffrement (HSM) pour valider leur compatibilité avec les prérequis de la cryptographie post-quantique et leur intégration au sein de nos systèmes de registre.

28. IGF Dynamic Coalition on Internet Standards, Security and Safety (IS3C) : https://www.intgovforum.org/en/filedepot_download/273/30786

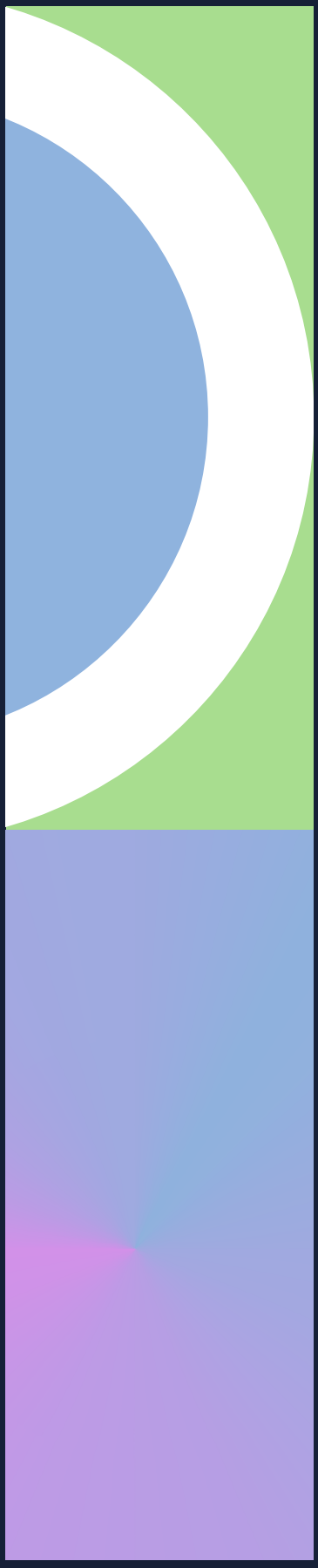
Un leader du « Web3 » et des systèmes de noms alternatifs se recentre sur le DNS

Le signal est venu d'Unstoppable Domains, société américaine qui s'était fait connaître en commercialisant des « noms de domaine » de systèmes alternatifs basés sur la blockchain. Dans un message publié sur X[29], Matthew Gould, son fondateur et CEO, a récemment reconnu que les noms exclusivement Web3 relevaient largement de la vague crypto de 2021 et n'avaient pas réussi à s'imposer sur le marché grand public. Selon lui, les noms de domaine relevant du DNS représentent désormais plus de 90 % de l'activité d'Unstoppable Domains et pourraient dépasser 99 % dans les deux à trois ans à venir.

L'annonce ne signifie pas nécessairement la disparition des usages blockchain liés aux noms. Ils conservent une utilité de niche, notamment pour associer un identifiant lisible à une adresse de portefeuille crypto. Mais elle marque un tournant, la fin du discours de rupture et « d'émancipation » qui présentait les systèmes de noms alternatifs comme une possible relève du DNS.

Ce repositionnement est d'autant plus notable qu'Unstoppable Domains a longtemps été l'un des plus fervents promoteurs des « noms de domaine » Web3 : .crypto, .nft, .wallet, .blockchain, mais aussi, depuis 2023, la distribution de noms en .eth. Force est toutefois de constater qu'en dehors de l'écosystème crypto, ces identifiants restent difficiles à utiliser comme de véritables noms de domaine : ils nécessitent souvent des outils spécifiques, ne sont pas pris en charge partout et peuvent entraîner des erreurs d'accès ou des problèmes de résolution[30]. Dès 2024, Unstoppable Domains obtenait d'ailleurs une accréditation ICANN comme bureau d'enregistrement, signe d'un recentrage déjà engagé vers les noms relevant du DNS.

Cette annonce d'Unstoppable Domains rappelle ainsi que, pour le grand public, un nom de domaine n'a de valeur que s'il peut être facilement utilisé et résolu. C'est précisément ce que permet le DNS à l'échelle mondiale.



29. Post de Matthew Gould sur X : https://x.com/mattgould/status/2033684862964519041
30. Pour plus de détails, voir « DNS et systèmes de noms alternatifs : la nécessité d'une interopérabilité », La Lettre Afnic n°7, novembre 2024 : https://www.afnic.fr/wp-media/uploads/2024/11/Lettre-afnic-V2-2-1-2.pdf

6 L'Afnic y était

FOSDEM, les 31 janvier et 1er février 2026, Bruxelles, Belgique

L'Afnic a participé au FOSDEM (*Free and Open Source Software Developers' European Meeting*), grand rendez-vous européen du logiciel libre organisé sur le campus de l'Université libre de Bruxelles. Très ancré dans les communautés techniques, cet événement gratuit et sans inscription réunit chaque année plus de 8 000 participants. L'essentiel du programme est organisé autour de « devrooms », accueillant des interventions, des ateliers et des discussions ouvertes consacrés au logiciel libre et à ses différents domaines d'application. L'Afnic y a suivi en particulier la devroom DNS, qui a notamment accueilli une présentation de Cascade, un nouvel outil de signature DNSSEC développé en logiciel libre par NLnet Labs. Au-delà des présentations, le FOSDEM est aussi un lieu d'échanges directs entre communautés, propice au partage d'expérience et à la coopération.

Les prochains événements auxquels l'Afnic participe :

- **3 juillet 2026**
  Forum francophone de la gouvernance du numérique et de l'IA
  Genève, Suisse

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

- **18 au 24 juillet 2026**
  IETF 126
  Vienne, Autriche

- **10 et 11 septembre 2026**
  CENTR CSR workshop
  Paris, France

- **17 au 22 octobre 2026**
  ICANN 87
  Bali, Indonésie

- **26 au 30 octobre 2026**
  RIPE 93
  Sofia, Bulgarie

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