Internet
made in France

La lettre n°6

01 Brèves

L'Afnic s'associe à l'IRT SystemX pour évaluer et optimiser l'empreinte environnementale des protocoles DNS

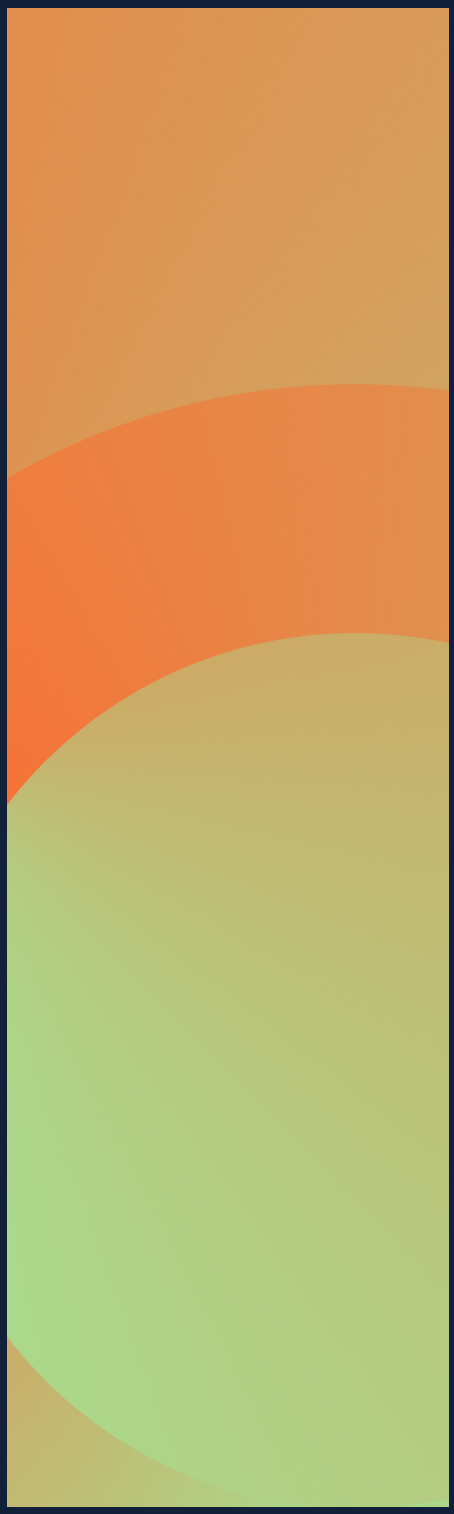
L'Afnic et l'IRT SystemX, institut de recherche français spécialisé dans la recherche appliquée aux systèmes complexes, viennent d'officialiser un accord de partenariat bilatéral visant à promouvoir l'Ingénierie Numérique des Systèmes du futur. Dans ce cadre, l'Afnic intègre le projet Impact Environnemental du Numérique (IEN) mené par l'IRT SystemX, visant à proposer une approche systémique pour évaluer, mieux comprendre et réduire les impacts directs et indirects des systèmes numériques sur l'environnement. L'Afnic apporte un nouveau cas d'usage en lien direct avec ses activités de Registre Internet et d'opérateur de services numériques, le DNS, aux côtés d'acteurs majeurs porteurs d'autres cas d'usages : Airbus Protect, Teclib', Total Energies et CentraleSupélec.

Cet accord marque une étape significative dans la collaboration entre les deux organisations, avec pour objectifs de lever les verrous scientifiques et technologiques associés aux protocoles et infrastructures internet, avec un focus tout particulier sur le DNS.

Les négociations pour le Pacte Numérique Mondial progressent

Le 2 mai dernier, se déroulait la deuxième lecture du projet de Pacte Numérique Mondial, présenté par les délégations de la Suède et de la Zambie, co-facilitatrices des discussions, afin de poursuivre des négociations. Une première version révisée du pacte a été diffusée le 15 mai, reflétant les contributions diverses recueillies lors des consultations préliminaires.
Les consultations se sont poursuivies en juin et en juillet sur une deuxième révision du texte, avec pour objectif d'atteindre un consensus avant le Forum politique de haut niveau se tenant du 8 au 18 juillet 2024. L'adoption finale du texte est prévue par vote en septembre 2024 lors du Sommet de l'Avenir des Nations Unies.

Le Pacte Numérique Mondial vise à établir des principes partagés pour un futur numérique inclusif, sûr et ouvert, aligné avec les objectifs de développement durable (ODD) des Nations Unies. Il donnera également le ton pour le SMSI+20, la revue à 20 ans du Sommet Mondial sur la Société de l'Information prévue en 2025, en posant les bases d'une coopération internationale plus efficiente et coordonnée face aux défis numériques émergents.



2

NETmundial+10 : réaffirmer les principes d'une gouvernance d'internet multi-acteurs

Les 29 et 30 avril derniers, dix ans après le premier sommet NETmundial, la communauté internationale s'est à nouveau réunie à São Paulo au Brésil pour discuter de l'avenir de la gouvernance d'internet. Organisé par la communauté multi-acteurs brésilienne, NETmundial+10 s'est déroulé dans un contexte de transformations numériques toujours plus rapides et de défis globaux toujours plus nombreux. L'Afnic était présente comme il y a dix ans, et s'est exprimée dans le cadre des acteurs de la communauté technique.

L'événement a visé à réaffirmer et à adapter les principes de gouvernance établis en 2014 lors de la première instance, tout en répondant aux nouvelles réalités numériques.
Au cœur des discussions : la transparence, l'inclusion et la collaboration multi-acteurs, des principes essentiels pour assurer un internet libre, ouvert et sécurisé pour tous.

Un contexte historique sur fond d'affaire Snowden

NETmundial est une initiative internationale née en 2014 de la communauté multi-acteurs brésilienne et convoquée à la suite de l'affaire Snowden (voir notre encadré) qui avait souligné la nécessité de recréer la confiance dans la transparence et la sécurité d'internet. Son objectif était donc de réunir un maximum de participants et de décideurs au niveau international pour réaffirmer les modalités de la gouvernance d'internet, venant ainsi compléter le Sommet Mondial sur la Société de l'Information (SMSI) qui s'était déroulé en deux phases, en 2003 à Genève et en 2005 à Tunis.

Répercussions de l'affaire Snowden sur la gouvernance d'internet

L'affaire Snowden, qui avait éclaté en juin 2013, fait référence aux révélations faites par Edward Snowden, un ancien employé de la CIA *(Central Intelligence Agency)* et sous-traitant de la NSA *(National Security Agency)*, respectivement l'agence de renseignement et l'agence de renseignement électronique des États-Unis. Il avait à l'époque divulgué des documents classifiés exposant l'ampleur et la nature intrusive des programmes de surveillance électronique mis en place par la NSA : des millions de personnes, y compris des citoyens, des entreprises et des administrations publiques, et pas uniquement aux États-Unis, étaient ainsi surveillées dans leurs activités en ligne, sans leur consentement.

Or, les grands organismes de la gouvernance d'internet – parmi lesquels l'ICANN *(Internet Corporation for Assigned Names and Numbers)*, l'IETF *(Internet Engineering Task Force)*, le W3C *(World Wide Web Consortium)*… – se situent sur le territoire américain. À ce titre, le gouvernement des États-Unis se veut le garant d'une gouvernance multi-acteurs et transparente de l'internet – une autorité morale américaine qui existe dans les faits, reconnue par tous. Que les États-Unis aient profité de ce statut pour espionner le monde entier a engendré une véritable crise de crédibilité du système de gouvernance d'internet. Si le sujet vous intéresse et que vous souhaitez l'approfondir, nous vous invitons à écouter le podcast Derrière le .fr de l'Afnic, et plus particulièrement l'épisode 2 « L'impact des grandes affaires sur la gouvernance » de la collection 4 « La gouvernance de l'internet ».

Après l'affaire Snowden, deux visions contradictoires de l'avenir de la gouvernance d'internet se sont élevées.
Certains affirmaient que, puisque le système existant n'avait pas réussi à garantir la transparence et le respect de la vie privée sur internet, il fallait le rejeter en faveur d'une gestion centralisée au niveau des Nations Unies. À l'inverse, d'autres pensaient que la proposition d'une gestion onusienne représentait une forme de régression, que le problème n'était pas lié au système mais à son application, et qu'il valait mieux s'assurer qu'aucun acteur ne puisse plus l'utiliser à mauvais escient.

NETmundial 2014 : une réussite multi-acteurs

Pour la première édition de NETmundial en 2014, et malgré le caractère informel de l'initiative, la communauté internet brésilienne avait réussi à mobiliser un grand nombre de participants – délégations gouvernementales, entreprises privées, ONG, organismes techniques…

Le texte qui avait été adopté, confirmant le système de gouvernance d'internet existant et écartant sa gestion par les Nations Unies, selon un consensus entre tous les acteurs de la communauté internet, se veut depuis un texte de référence, clair et concis. Il affirme ainsi que, pour qu'internet fonctionne, son système de gouvernance ne doit pas être interétatique mais multi-acteurs, et que tous – société civile, universitaires, organismes techniques et gouvernements – doivent pouvoir prendre la parole, discuter, apporter leur expertise, sans légitimité absolue. Surtout, ce texte a complété utilement l'affirmation du système multi-acteurs déjà présente au sein du Sommet Mondial sur la Société de l'Information (SMSI), en esquissant une définition du rôle de chacun des acteurs (dont la légitimité varie en fonction des sujets et thématiques abordés) et des modalités d'organisation de ce dialogue.

Pourquoi un NETmundial+10 en 2024 ?

NETmundial+10 ne vise pas à simplement célébrer les 10 ans de l'initiative. Cette année est concentrée en discussions internationales sur la gouvernance d'internet qui pourraient remettre en cause le système actuel et qui, pour le moins, l'interrogent.

La négociation d'un Pacte numérique mondial (ou *Global Digital Compact* en anglais) est ainsi prévue cette année, comme cela avait été proposé par le secrétaire général des Nations Unies dans le document « Notre programme commun » de 2021.
Ce pacte sera soumis au vote de l'assemblée générale des Nations Unies à l'occasion du Sommet de l'avenir qui se tiendra les 22 et 23 septembre prochains à New York.
Le Pacte numérique mondial vise à définir les principes d'un avenir numérique accessible, libre et sécurisé pour tous. Ouvert aux contributions et aux avis, il entend traiter de questions liées à internet telles que la confiance, la sécurité, la connectivité, l'utilisation des données personnelles et les droits humains en ligne, mais aussi de la régulation de l'intelligence artificielle. À ce titre, le Pacte numérique mondial pourrait déboucher sur la création de nouvelles structures de la gouvernance d'internet, notamment au sein du système des Nations-Unies.

2024 sera également l'année du bilan et de l'évaluation du SMSI, afin notamment de déterminer la pérennisation ou la disparition du Forum pour la Gouvernance d'Internet (FGI). La création du FGI avait été décidée lors de la 2ème phase du SMSI à Tunis en 2005, dans le but de poursuivre dans la durée les discussions et la recherche de consensus sur la gouvernance d'internet. Le FGI fait toutefois aujourd'hui l'objet de critiques quant à son efficacité et sa capacité à répondre aux défis actuels. Dans le même temps, beaucoup s'accordent à dire que cet instrument, qui peut être amélioré, est infiniment plus inclusif que toute organisation qui serait purement onusienne et représente ainsi un forum adéquat pour épouser l'évolution des défis et l'émergence de nouveaux acteurs. Le caractère parfois perçu comme confus de son organisation et de ses résultats est l'autre face de la médaille d'un FGI très plastique et agile, permettant d'embrasser l'évolution d'internet et du numérique.

Ces événements pourraient remettre en question le système actuel de gouvernance d'internet, comme après l'affaire Snowden. La communauté internet brésilienne a donc décidé d'un nouveau NETmundial pour réévaluer et réaffirmer les principes d'une gouvernance d'internet transparente et multi-acteurs, reposant sur un consensus de la communauté internet dans son ensemble.

Un processus participatif pour arriver au consensus

Comme en 2014, NETmundial+10 a été orchestré comme un événement véritablement multi-acteurs. Dès fin 2023, un secrétariat a envoyé des questionnaires à toutes les parties prenantes de la gouvernance d'internet et collecté les réponses. Sur cette base, il a rédigé le brouillon d'une déclaration visant à renforcer la gouvernance de l'internet et les processus de politique numérique *(« Strengthening Internet governance and digital policy processes »)*, qui a ensuite été présenté à l'ouverture de NETmundial+10 le 29 avril dernier à São Paulo, au Brésil.

Au cours de l'événement, le texte a été discuté paragraphe par paragraphe, offrant à chacun la possibilité de s'exprimer, et mis à jour quotidiennement. Le 30 avril, au terme des deux jours, la déclaration, reflétant un consensus général, a été votée par acclamation.

On notera à cette occasion que le système ouvert multi-acteurs, permettant aux gouvernements, à la société civile, à la communauté technique et à la communauté académique de travailler ensemble, peut être, quand il est bien conduit, d'une redoutable efficacité. L'adoption de cette déclaration, dans tout autre système, aurait pu prendre des mois, voire des années !

Que contient le texte voté ?

Le texte voté – *NETmundial+10 Multistakeholder Statement* (Déclaration multi-acteur NETmundial+10) – comporte quatre dimensions principales :

- **La déclaration réaffirme la nécessité d'une gouvernance multi-acteurs.** Elle insiste sur les notions d'ouverture, de transparence et de consensus. Elle s'oppose à une vision ultra-libérale, dominée par de grandes entreprises, ou purement gouvernementale ou intergouvernementale de la gouvernance d'internet.
- **La déclaration propose des instructions détaillées sur la manière de mettre en œuvre une gouvernance d'internet multi-acteurs.** En ce sens, la déclaration de 2024 va plus loin que celle de 2014. Elle indique avec précision comment les gouvernements, le secteur privé, la société civile, les universitaires, les organismes techniques et la communauté mondiale peuvent collaborer de manière transparente et inclusive pour élaborer des politiques et prendre des décisions concernant internet.
- **La déclaration s'élargit à des problématiques qui ne sont pas purement internet.** Les modèles des grands sujets structurants du numérique (au-delà de l'internet), tels que l'intelligence artificielle, la désinformation, la haine en ligne, le poids des grandes plateformes, etc., ont également été abordés lors de NETmundial+10. La déclaration les inclut ainsi, suggérant que les principes de gouvernance d'internet sont suffisamment solides pour inspirer la gouvernance de ces autres espaces numériques, tout en distinguant ces sujets de la pure gouvernance de l'internet.
- **La déclaration exprime sa position vis-à-vis des processus actuellement en cours aux Nations Unies concernant la gouvernance d'internet et le numérique.** Elle réaffirme, notamment dans le contexte du Pacte numérique mondial et de la réévaluation de la pertinence du FGI, la nécessité de renforcer et d'améliorer la dimension multi-acteurs de la gouvernance d'internet. Elle encourage à nouveau ici une collaboration efficace et inclusive entre les gouvernements, le secteur privé, la société civile, les universitaires, les organismes techniques et la communauté mondiale.

Analyse des enjeux communs à chaque catégorie de la communauté internet multi-acteurs

NETmundial+10 a offert à chaque partie prenante l'opportunité de s'exprimer. Une grande diversité de perspectives et d'enjeux a ainsi émergé, mettant parfois en lumière les points de vue, questionnements ou inquiétudes partagés par un même groupe.
Voici l'analyse que l'Afnic a pu en tirer.

La société civile a mis l'accent sur deux sujets principaux. Tout d'abord, la prise en compte des droits humains sur internet et la question de responsabilité qui en découle, notamment en termes de diversité linguistique et culturelle.

Elle a également exprimé des préoccupations quant à la « tokénisation », processus selon lequel les minorités sont certes représentées mais de manière symbolique et superficielle, ou toujours au travers des mêmes experts, sans chercher à diversifier les voix ou à inclure des points de vue différents qui pourraient être plus pertinents.

Les gouvernements présents ont majoritairement exprimé leur adhésion à une gouvernance d'internet multi-acteurs, rejetant la perspective d'une gestion par les Nations Unies.

Il est toutefois à noter que la représentation gouvernementale était en net recul en 2024 par rapport à la première édition, et ce, de deux manières.
Alors que NETmundial 2014 avait attiré des ministres et élus de haut niveau, l'édition 2024 a vu la participation de directeurs ou sous-directeurs d'administrations publiques, majoritairement. De plus, en 2014, presque tous les pays avaient répondu à l'appel, tandis qu'en 2024, les gouvernements représentés étaient principalement occidentaux.

La communauté technique a fait état de ses craintes, redoutant que la déclaration finale ne soit polluée par les tensions géopolitiques actuelles et ne prenne pas compte de la réalité technique d'internet. Elle a réaffirmé à ce titre que l'infrastructure actuelle fonctionne et qu'elle évolue régulièrement, selon les principes mêmes de la recherche du consensus et de l'étude d'impact par les acteurs techniques des changements.

Elle a également plaidé pour une distinction claire entre la gouvernance d'internet et celle des champs qui ne sont pas purement internet mais en dépendent – intelligence artificielle, désinformation, haine en ligne, etc. Le brouillon de la déclaration proposé au premier jour des débats avait en effet remplacé le terme "gouvernance d'internet" par "gouvernance numérique", ce que la communauté technique n'avait pas manqué de remarquer.

Le monde universitaire, quant à lui, est beaucoup trop vaste et diversifié pour qu'une ligne directrice spécifique ait pu se distinguer lors de NETmundial+10. Il reste tout de même que la nécessité d'intégrer au dialogue sur la gouvernance de l'internet les travaux scientifiques non techniques (sociologiques, économiques, géographiques et environnementaux, notamment) a fait consensus au sein de la communauté académique qui a porté cette demande de manière claire et répétée.

Le Brésil, enfin, s'est démarqué comme une puissance de la communauté internet multi-acteurs. Le pays n'a pas seulement organisé et accueilli NETmundial+10.
Il a réussi à prouver que son approche multi-acteurs, incarnée notamment par le CGI.br *(Comitê Gestor da Internet no Brasil)*, l'organisme brésilien chargé de coordonner les initiatives et les politiques liées à internet au Brésil, mais aussi les discussions sur NETmundial+10, était un exemple à suivre.

Grâce à une organisation efficace, le Brésil a réussi à diriger les débats de manière inclusive et transparente, mettant en évidence la pertinence et la faisabilité d'une gouvernance d'internet collaborative. Et ce, de manière efficace : entre la convocation de l'événement et la signature de la déclaration, seulement six mois se sont écoulés ; et entre la présentation du brouillon et le vote du texte final, seulement deux jours.

Et maintenant, quel avenir pour la gouvernance d'internet ?

Sur la base d'un consensus général des participants en présence et en ligne, la déclaration de NETMundial+10 réaffirme la nécessité d'un modèle de gouvernance multi-acteurs et propose des directives concrètes.
Dans ces conditions, le Forum sur la Gouvernance de l'Internet (FGI) – bien qu'il puisse nécessiter des réformes et des adaptations – demeure l'enceinte privilégiée pour poursuivre les discussions et garantir la participation de tous aux principes de gouvernance d'internet.
En effet, le FGI représente lui aussi un consensus – certes par défaut, car complexe et coûteux, aucune partie n'étant pleinement satisfaite de ses modalités – qu'il faut préserver pour que la gouvernance d'internet puisse continuer à s'inspirer des principes d'ouverture, de transparence et d'inclusivité qui y sont discutés.

03

La directive NIS2 va indéniablement renforcer la cybersécurité au sein de l'Union européenne, mais attention aux effets de bord

La directive NIS2 *(Network and Information Systems)* de l'Union européenne représente une étape majeure pour la cybersécurité au sein de l'UE. Elle étend en effet, par rapport à NIS1, les exigences de sécurité à un plus grand nombre de secteurs et d'acteurs, et renforce les obligations de gestion des risques et de notification des incidents. La directive, entrée en vigueur le 16 janvier 2023, doit être transposée en droit national par les États membres avant le 17 octobre 2024. Quelle analyse peut-on faire, à date, des avancées que NIS2 va apporter à la posture de cybersécurité de l'Union européenne, mais aussi des points à surveiller pour limiter les potentiels effets négatifs lors de sa mise en œuvre ?

La directive NIS2 apporte son lot d'avancées positives pour la cybersécurité européenne

La directive NIS2 marque une étape cruciale dans le renforcement de la cybersécurité au sein de l'Union européenne. En réponse à l'évolution rapide des menaces numériques et à la nécessité de protéger des infrastructures critiques de plus en plus interconnectées, cette directive présente des mesures ambitieuses.
En visant une harmonisation des pratiques de sécurité et une amélioration de la résilience des services numériques, NIS2 promet des avancées significatives pour assurer la sécurité et la continuité des services essentiels.

NIS2 va renforcer le socle commun de cybersécurité dans l'Union européenne. La directive vise à établir un minimum commun de cybersécurité à travers l'Union européenne, en harmonisant un socle de bonnes pratiques des acteurs du numérique ou des acteurs économiques critiques utilisant le numérique. Pour ce faire, elle élargit par rapport à NIS1 son champ d'application à de nouveaux secteurs qui, dans une société et une économie toujours plus connectées, sont une cible de plus en plus fréquente pour les acteurs hostiles privés ou étatiques. Parmi les secteurs d'activité nouvellement inclus dans NIS2 : les services postaux et d'expédition, la gestion des déchets ou encore les fournisseurs de services numériques.

900
entités étaient concernées par NIS1 en France ; avec NIS2, elles seront 15 000.

NIS2 prend en compte la chaîne d'approvisionnement *(supply chain).* Le nombre d'entités concernées par les obligations de bonnes pratiques, de transparence et de reporting vis-à-vis de la sécurité de leurs actifs numériques, n'augmente pas seulement par l'extension des secteurs d'activité concernés. La nouvelle directive introduit en effet également la notion de « chaîne d'approvisionnement ». La spécialisation, la technicité et la complexité de la gestion des services numériques amènent souvent les entreprises à sous-traiter certains de leurs aspects à des sociétés plus expertes. En prenant en compte les prestataires numériques qui accompagnent les services critiques, et pas uniquement les organisations qui les proposent, NIS2 adopte une approche holistique de la cybersécurité, contribuant ainsi à une meilleure résilience globale du secteur.

Plus de personnes seront sensibilisées à la cybersécurité. Avec l'élargissement des secteurs concernés et la prise en compte de la chaîne d'approvisionnement, un nombre croissant d'organisations seront impactées par NIS2. À titre de comparaison, environ 900 entités étaient concernées par NIS1 en France ; avec NIS2, elles seront 15 000 – et par extension, toutes les personnes qui les composent. Ce sont autant d'opportunités supplémentaires de sensibilisation à la cybersécurité. Le facteur humain joue souvent un rôle clé dans la réussite des cyberattaques. Avec plus de personnes formées à la cybersécurité, ce sont aussi les risques qui seront significativement réduits.

Entités essentielles et entités importantes sont distinguées. NIS2 fait preuve de plus de souplesse que NIS1 en différenciant les entités essentielles des entités importantes. Cette distinction reconnaît le niveau de criticité des missions et permet aux acteurs de proportionner leurs efforts de sécurité en fonction de l'importance des services qu'ils fournissent.
Par exemple, une entreprise régionale de production d'énergie renouvelable sera considérée comme une entité importante, là où un opérateur de réseau électrique national sera classé comme une entité essentielle, sujette à des obligations de cybersécurité plus strictes en raison du vaste impact potentiel qu'une cyberattaque pourrait avoir sur ses services.

Les pays bénéficieront de flexibilité dans la transposition nationale de la directive. Étant une directive et non une réglementation, NIS2 offre aux États membres de l'Union européenne une certaine latitude pour la transposer en droit national, leur permettant de tenir compte des spécificités locales. NIS2 sera ainsi au plus près de la réalité du terrain dans chacun des pays, tout en conservant une homogénéité grâce au socle commun. Ce n'est qu'ainsi que des boucles d'amélioration et des évolutions positives pourront être enclenchées – allant, selon les pays, d'obligations modestes pour faire progresser les pratiques les moins avancées, jusqu'à des obligations solides pour renforcer celles déjà bien en place.

La collaboration et la posture européennes seront renforcées. NIS2 va également inciter les 27 pays de l'Union européenne à collaborer à un projet commun. La directive, en tant que facteur de résilience économique, pourrait ainsi constituer un atout fondamental pour l'Europe, lui conférant un avantage compétitif significatif par rapport à d'autres régions. En effet, si la coopération est une réussite, elle représentera un acquis stratégique, renforçant la position économique et sécuritaire de l'Europe sur la scène internationale.

Mais NIS2 comporte également des points de vigilance

Bien que NIS2 constitue une avancée importante pour la cybersécurité au sein de l'Union européenne, il existe plusieurs aspects de la directive qui nécessitent une attention particulière. Sa mise en œuvre, bien qu'ambitieuse, comporte des défis et des nuances qui pourraient poser des problèmes pratiques et opérationnels. Ces points de vigilance doivent être examinés afin de garantir que les objectifs de sécurité et de résilience soient atteints sans imposer de contraintes disproportionnées ou injustifiées aux différents acteurs impliqués.

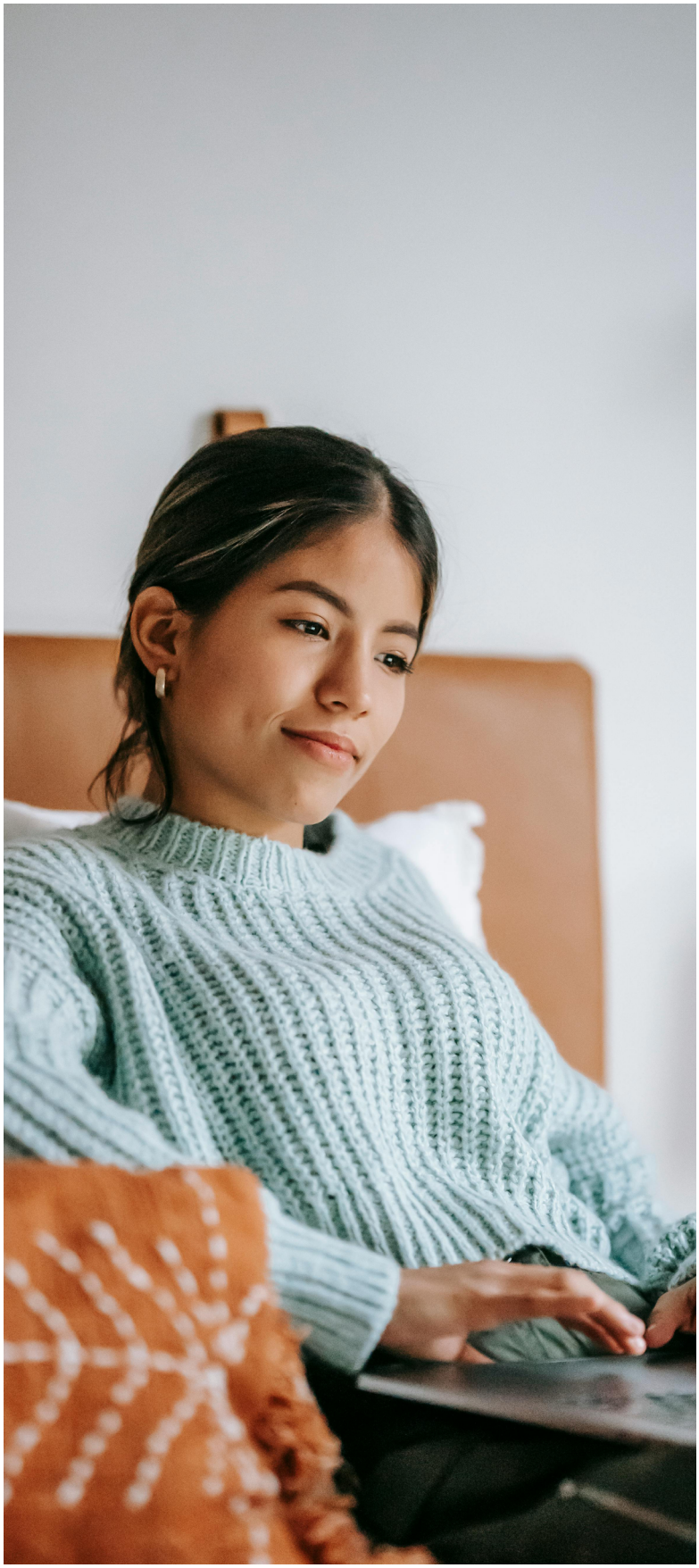
NIS2 considère tous les acteurs du DNS comme essentiels (et ce n'est pas justifié). Si NIS2 a la vertu de proposer un dispositif proportionnel et proportionné faisant la différence entre entité importante et entité essentielle, il est dommage que cette distinction n'ait pas été opérée pour les acteurs du DNS. Tous, quelle que soit leur taille, y sont considérés comme essentiels. Les offices d'enregistrement, en charge d'extensions de premier niveau, méritent bien entendu leur statut d'entités essentielles – comme l'Afnic dans sa gestion du .fr. Mais tous les acteurs économiques qui distribuent des noms de domaine et hébergent des serveurs DNS ne sont pas pareillement critiques pour l'économie ou les pays concernés. Si les obligations de cybersécurité sont transposées dans les mêmes conditions et avec les mêmes exigences aux bureaux d'enregistrement qu'aux offices d'enregistrement, et ce, quelle que soit leur taille, cela pourrait engendrer :

- Une forte consolidation du marché et la disparition d'acteurs qui n'auraient peut-être pas les moyens ou la volonté de mettre en œuvre ces exigences. Économiquement, cela signifie une réduction de la concurrence, une augmentation des coûts pour les consommateurs, et potentiellement une innovation ralentie dans le secteur en raison du manque de diversité et de dynamisme parmi les acteurs du marché.
- Au-delà d'un problème économique, cela représente également un risque de SPOF *(Single Point Of Failure ou point de défaillance unique)*. En effet, la concentration excessive du marché entre les mains de quelques acteurs augmenterait la vulnérabilité du système global. Si l'un de ces acteurs venait à défaillir, les conséquences seraient bien plus graves, car il n'y aurait plus suffisamment de diversité et de redondance pour absorber le choc et maintenir la continuité des services essentiels.
- Enfin, les bureaux d'enregistrement pourraient également être tentés d'externaliser l'hébergement DNS de leurs clients vers d'autres acteurs, potentiellement en dehors de l'Union européenne, pour éviter d'être considérés comme entité essentielle. Des noms de domaine européens, avec des titulaires européens et des services européens, seraient alors supervisés par des entreprises non situées dans l'Union européenne.

Une approche plus nuancée, prenant en compte la nature et la criticité des activités de chaque acteur, aurait été plus appropriée.

Les sanctions ne sont pas toujours proportionnelles à la criticité des missions. En cas de non-respect des obligations, NIS2 prévoit des sanctions calculées sur la base du chiffre d'affaires global de l'entreprise, ce qui pénalise les acteurs économiques dont seule une petite partie relève de la gestion de services numériques critiques. Chez les acteurs du DNS, par exemple, pour qui la vente de noms de domaine, régie par NIS2, est une activité bien souvent minoritaire, des pénalités basées sur l'ensemble de leur chiffre d'affaires seraient disproportionnées et excessivement sévères.
Une mesure plus juste aurait été de les baser sur le chiffre d'affaires généré uniquement par l'activité essentielle.

Ici encore, ces entreprises pourraient être découragées de conserver leurs activités critiques minoritaires car le risque est disproportionné par rapport aux avantages, avec le même impact qu'au point précédent (concentration du marché, SPOF, externalisation des services en dehors de l'UE).



NIS2 manque de clarté quant aux responsabilités des différents acteurs de la chaîne d'enregistrement des noms de domaine. On parle ici plus précisément de l'Article 28 de la directive NIS2. Celui-ci impose *« aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de collecter les données d'enregistrement de noms de domaine et de les maintenir exactes et complètes au sein d'une base de données spécialisée »*, sans pour autant préciser le rôle et les responsabilités de chacun – office d'enregistrement, bureau d'enregistrement, revendeur ou proxy – dans cette mission.

Cela pose un problème quant à la qualité de la base de données des titulaires. NIS2 ne précisant pas à qui exactement revient la charge de renseigner et maintenir cette base de données, le risque de redondance est majeur.
Les États membres de l'Union européenne doivent se saisir de cette marge d'interprétation que leur offre la directive NIS2 et préciser les responsabilités de chacun dans leur transposition nationale, pour que le respect des obligations puisse être attribué et vérifié.

L'application de NIS2 aux acteurs non européens est précisée, mais peu probable. Si la directive NIS2 vise à améliorer la cybersécurité au sein de l'Union européenne, elle risque de se heurter à d'importants freins à l'heure d'appliquer ses exigences aux acteurs non européens opérant au sein de l'UE. L'Article 21 de la directive stipule en effet que les prestataires de services numériques non établis dans l'UE mais qui y offrent des services doivent désigner un représentant sur le territoire et se conformer aux mêmes exigences de cybersécurité que les entités européennes. Mais en pratique, il est peu probable que l'UE puisse imposer ces exigences à des entités étrangères (tout comme c'était déjà le cas dans NIS1, mais jamais mis en œuvre).

Cette situation crée une inégalité de traitement et risque de compromettre l'efficacité des mesures de cybersécurité en Europe, car les acteurs non européens pourraient ne pas respecter les mêmes standards de sécurité.
En la matière, NIS2 est souvent comparée au RGPD (Règlement général sur la protection des données). Mais cette référence n'est pas vraiment pertinente, car le non-respect du RGPD peut être qualifié et prouvé sans avoir à auditer les processus internes (par la dénonciation des utilisateurs, par exemple). C'est beaucoup plus complexe avec NIS2. C'est pourquoi les menaces de lourdes amendes n'auront peut-être aucun effet, car l'application des sanctions nécessite l'intervention de l'Union européenne au travers d'une vérification et d'un audit des processus internes qui peuvent être refusés par les acteurs non européens.

D'ailleurs, un point particulier de la directive renforce cette perspective : NIS2 stipule ne pas s'appliquer aux serveurs racines du DNS. Il existe 13 serveurs racines dans le monde. NIS2 a bien intégré le fait qu'il serait compliqué pour l'ENISA *(Agence de l'Union européenne pour la cybersécurité)* de toquer à la porte de chacun d'entre eux, notamment les 10 serveurs racines situés sur le territoire américain, pour en auditer les processus internes. Les serveurs racines ont donc été exclus des obligations de NIS2. Il faut dire aussi qu'il existe des milliers de copies des serveurs racines dans le monde, ce qui assure la résilience même si l'un des 13 « originaux » est compromis.

NIS2
représente une avancée significative pour la cybersécurité en Europe.

Si la directive NIS2 représente une avancée significative pour la cybersécurité en Europe, en étendant les obligations de sécurité à un plus grand nombre d'acteurs et en intégrant des mesures pour renforcer la résilience des chaînes d'approvisionnement, des précautions doivent donc être prises pour assurer une mise en œuvre cohérente et proportionnée afin de minimiser les effets négatifs potentiels et de maximiser les bénéfices pour la cybersécurité au sein de l'Union européenne.

Les prochains événements auxquels l'Afnic participe :

20 au 26 juillet 2024
IEFT 120

Vancouver, Canada

29 juillet au 2 août 2024
Groupe consultatif de la normalisation des télécommunications de l'UIT.

Genève, Suisse

30 septembre au 11 octobre 2024
Réunion des groupes de travail du Conseil et des groupes d'experts de l'UIT.

Genève, Suisse

3 octobre 2024
Forum sur la Gouvernance de l'Internet (FGI) France.

Paris, France

4 octobre 2024
Journée du Conseil scientifique de l'Afnic (JCSA24).

La Défense, France

15 au 24 octobre 2024
WTSA-24 (Assemblée mondiale de normalisation des télécommunications).

New Delhi, Inde

26 et 27 octobre 2024
OARC 43.

Prague, République tchèque

28 octobre au 1er novembre 2024
RIPE 89.

Prague, République tchèque

2 au 8 novembre 2024
IETF 121.

Dublin, Irlande

9 au 14 novembre 2024
ICANN 81.

Istanbul, Turquie

afnic
Internet made in France

Votre contact

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
7 avenue du 8 Mai 1945,
78280 Guyancourt