COMMISSION
EUROPÉENNE

Bruxelles, le 10.11.2025
COM(2025) 673 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Analyse de la nécessité et de la faisabilité d'un système d'information et d'alerte sur les noms de domaine pour les indications géographiques conformément à l'article 35, paragraphe 3, du règlement (UE) 2024/1143

GLOSSAIRE DES PRINCIPAUX TERMES TECHNIQUES

ccTLD (Country-Code Top-Level Domain, domaine de premier niveau national):

Domaine de premier niveau attribué à un pays ou territoire spécifique, composé de deux lettres (par exemple, «.fr», «.de») et géré par un registre national.

Cybersquattage:

L'enregistrement ou l'utilisation de mauvaise foi d'un nom de domaine identique ou semblable au point de prêter à confusion à une dénomination protégée, telle qu'une marque ou une indication géographique, dans l'intention de tirer indûment profit de sa réputation, d'induire les consommateurs en erreur ou de revendre le domaine à des fins lucratives.

DNS (Domain Name System, système de noms de domaines):

Le système de dénomination hiérarchique qui traduit les noms de domaine lisibles par l'homme (comme «example.eu») en adresses IP numériques utilisées par les ordinateurs pour se localiser sur internet.

DAS (Domain Availability Service, service de disponibilité des noms de domaines):

Un service utilisé pour vérifier si un nom de domaine spécifique est disponible pour l'enregistrement ou s'il a déjà été pris, généralement au moyen de requêtes automatisées dans les registres de domaines.

NS (Name Server, serveur de noms):

Serveur au sein du DNS qui stocke et gère les enregistrements reliant les noms de domaine à des adresses IP, permettant aux utilisateurs d'accéder à des sites internet en utilisant des noms plutôt que des adresses numériques.

RDAP (Registration Data Access Protocol, protocole d'accès aux données d'enregistrement):

Un protocole internet standard qui offre un accès structuré et lisible par machine aux données d'enregistrement de domaines, remplaçant progressivement l'ancien système WHOIS. Le RDAP offre des fonctionnalités améliorées en matière de sécurité, de normalisation et de protection des données.

WHOIS (Who Is):

Un service internet qui fournit des informations de base sur un nom de domaine enregistré, telles que son statut, son bureau d'enregistrement et ses dates d'enregistrement.

1. INTRODUCTION

Les indications géographiques (IG) sont une pierre angulaire de la politique de qualité de l'Union européenne. Elles protègent les dénominations de produits spécifiques dont les qualités ou la réputation sont liées à leur origine géographique et au savoir-faire traditionnel des producteurs. Le marketing numérique et la présence en ligne étant devenus essentiels à la commercialisation de ces produits, la protection des IG dans le système de noms de domaine (DNS) est devenue de plus en plus importante.

Afin de renforcer la protection des IG dans ce domaine, l'article 35 du règlement (UE) 2024/1143[1] impose à la Commission d'analyser, au plus tard le 14 novembre 2025, la nécessité et la faisabilité d'un système d'information et d'alerte sur les noms de domaine au niveau de l'UE pour les indications géographiques et de présenter un rapport contenant ses principales conclusions. Ce rapport peut être accompagné, s'il y a lieu, d'une proposition législative.

Un système d'information et d'alerte sur les noms de domaine permettrait aux demandeurs d'une IG de vérifier si une IG est déjà enregistrée en tant que nom de domaine et, s'ils le souhaitent, de recevoir des alertes lorsqu'un nom de domaine identique à une IG est enregistré.

Le présent rapport résume les résultats de cette analyse et examine comment une fourniture volontaire d'informations par les registres ccTLD établis dans l'UE pourrait fonctionner dans la pratique. Il remplit l'obligation énoncée à l'article 35, paragraphe 3, du règlement (UE) 2024/1143 et présente les conclusions de la Commission.

2. CONTEXTE JURIDIQUE ET POLITIQUE

Base juridique

Le règlement (UE) 2024/1143 du Parlement européen et du Conseil concernant les indications géographiques relatives au vin, aux boissons spiritueuses et aux produits agricoles reconnaît l'importance croissante de la protection des IG dans le DNS, étant donné que ces droits sont de plus en plus vulnérables face aux enregistrements abusifs de noms de domaine et fréquemment ciblés par de tels enregistrements, souvent appelés «cybersquattage». Afin de renforcer la protection des IG dans ce domaine, le règlement (UE) 2024/1143 introduit la possibilité de mettre en place un système d'information et d'alerte sur les noms de domaine.

En vertu de l'article 35, paragraphe 2, du règlement, la Commission peut confier à l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) la mise en place et la gestion d'un tel système. La même disposition prévoit que les registres ccTLD établis dans l'UE participent sur une base volontaire en fournissant des informations et des données pertinentes à l'EUIPO.

L'article 35, paragraphe 3, du règlement impose à la Commission d'analyser s'il serait nécessaire et faisable de mettre en place un tel système, en tenant compte de la manière

[1] Règlement (UE) 2024/1143 du Parlement européen et du Conseil du 11 avril 2024 concernant les indications géographiques relatives au vin, aux boissons spiritueuses et aux produits agricoles, ainsi que les spécialités traditionnelles garanties et les mentions de qualité facultatives pour les produits agricoles (JO L, 2024/1143, 23.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1143/oj).

dont la fourniture volontaire d'informations et de données par les registres pourrait fonctionner en pratique. La Commission doit soumettre les résultats de l'analyse au Parlement européen et au Conseil d'ici le 14 novembre 2025.

Nécessité d'une action coordonnée entre les secteurs des IG

L'analyse des IG agricoles au titre du règlement (UE) 2024/1143 s'effectue parallèlement à l'obligation énoncée à l'article 72, paragraphe 2, du règlement (UE) 2023/2411[2] relatif aux IG artisanales et industrielles. Cette disposition impose à la Commission d'analyser, au plus tard le 2 juin 2026, la faisabilité de la mise en place d'un système d'information et d'alerte pour prévenir l'utilisation abusive des IG artisanales et industrielles dans le DNS.

Ces dispositions s'inscrivent dans le cadre plus large de la politique de l'UE visant à renforcer la protection des droits de propriété intellectuelle en ligne, comme en témoignent le plan d'action de l'UE en faveur de la propriété intellectuelle[3] et l'élaboration de la recommandation de la Commission relative à des mesures visant à lutter contre la contrefaçon[4]. Ces dispositions répondent également aux préoccupations exprimées par les parties prenantes quant aux limites des mécanismes existants pour prévenir ou combattre l'utilisation abusive des IG en ligne.

Les IG de l'agriculture, de l'artisanat et de l'industrie reposent sur des fondements juridiques, des objectifs stratégiques et une architecture systémique potentielle similaires. Il est essentiel de garantir la cohérence des politiques et d'éviter les doubles emplois. Le présent rapport, sur lequel se fondera le futur rapport du 2 juin 2026, constitue un premier examen visant à déterminer s'il serait possible de mettre en place un système unique d'information et d'alerte sur les noms de domaine au niveau de l'UE, couvrant à la fois les IG agricoles et les IG pour les produits artisanaux et industriels, plutôt que deux systèmes distincts, chacun relevant de son propre cadre juridique. Cela contribuerait à garantir la cohérence et à favoriser une approche unifiée de l'UE en matière de protection des IG dans le DNS.

Le 4 décembre 2024, la Commission et l'EUIPO ont signé un accord administratif visant à renforcer la coopération dans des domaines tels que la protection et l'application des IG. L'accord fait spécifiquement état de la volonté des parties de coopérer en vue de l'élaboration d'un système d'information et d'alerte sur les noms de domaine et d'examiner si le système existant de l'EUIPO (actuellement utilisé pour les marques de l'UE dans le domaine de premier niveau .eu) pourrait être étendu aux IG, au moyen d'actes délégués, comme le prévoit l'article 35, paragraphe 2, du règlement (UE) 2024/1143.

---

2 Règlement (UE) 2023/2411 du Parlement européen et du Conseil du 18 octobre 2023 relatif à la protection des indications géographiques pour les produits artisanaux et industriels (JO L, 2023/2411, 27.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2411/oj).

3 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — Exploiter au mieux le potentiel d'innovation de l'Union européenne Un plan d'action en faveur de la propriété intellectuelle afin de soutenir la reprise et la résilience dans l'Union européenne, COM(2020) 760 final du 25 novembre 2020, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52020DC0760.

4 Recommandation de la Commission relative à des mesures visant à lutter contre la contrefaçon et à renforcer le respect des droits de propriété intellectuelle, C(2024) 1739, 19 mars 2024, JO L, 2024/915, https://single-market-economy.ec.europa.eu/publications/commission-recommendation-measures-combat-counterfeiting-and-enhance-enforcement-intellectual_en.

La Commission a également coopéré étroitement avec EURid, le registre du domaine de premier niveau .eu. À cet égard, la coopération s'est concentrée sur l'analyse des limites techniques et juridiques et sur la contribution à trouver une solution proportionnée et efficace.

3. MÉTHODOLOGIE ET SOURCES

Cette analyse s'appuie sur un certain nombre de sources d'éléments de preuve complémentaires.

- **Étude complète commandée par la Commission européenne**[5] (ci-après l'«étude»). Cette étude a recueilli des éléments de preuve sur les enregistrements abusifs de noms de domaine impliquant des IG et a examiné la faisabilité technique, juridique et organisationnelle d'un système d'information et d'alerte sur les noms de domaine axé sur les IG. Elle a également analysé les dispositions communes des cadres juridiques applicables aux indications géographiques agricoles, artisanales et industrielles et a conclu qu'une approche coordonnée de l'UE à l'égard de tout futur système serait techniquement réalisable et souhaitable sur le plan politique.
- **Document de prise de position du CENTR**[6]. Ce document officiel de prise de position a été rédigé par CENTR, l'association représentant les registres nationaux de noms de domaine en Europe. Ce document présente les points de vue et les préoccupations des membres concernant tout système d'information et d'alerte au niveau de l'UE.
- **Consultation ciblée des registres ccTLD de l'UE**. D'août à septembre 2025, la Commission a invité tous les registres ccTLD établis dans l'UE, EURid et CENTR à formuler des observations sur le modèle technique proposé et sur d'éventuelles formes de coopération volontaire. Leur retour d'information est pris en compte dans le présent rapport.
- **Réunions interservices bilatérales et échanges techniques**. Ces réunions ont rassemblé des services de la Commission, EURid (en ce qui concerne le fonctionnement du système d'alerte existant en matière de marques de l'UE pour le domaine .eu) et l'expert en propriété intellectuelle qui a contribué à l'étude.

4. ANALYSE DU BESOIN

Il devient de plus en plus important de protéger les indications géographiques dans le système des noms de domaine, étant donné que la commercialisation en ligne et le commerce électronique jouent un rôle croissant pour les producteurs d'IG. Bien que les cas documentés d'utilisation abusive des IG dans les noms de domaine semblent limités, cela reflète souvent des facteurs structurels plutôt qu'une absence de risque.

De nombreux groupements de producteurs d'IG sont des petites ou moyennes entreprises ou des associations qui ne disposent pas des ressources nécessaires pour surveiller systématiquement les enregistrements de noms de domaine. Ils s'appuient généralement

[5] Étude sur le système d'information et d'alerte sur les noms de domaine de propriété intellectuelle, commandée par la Commission européenne, préparée par Wavestone en collaboration avec Ivett Paulovics, rapport final - décembre 2023.

[6] Conseil des registres européens de noms de domaine de premier niveau nationaux, *Observations du CENTR sur la réforme des indications géographiques dans l'UE*, Bruxelles, 15 septembre 2022, disponible à l'adresse suivante: https://www.centr.org/news/news/comment-gi-reform.html.

sur des contrôles occasionnels ou n'agissent qu'une fois que des abus sont visibles sur le marché. Même lorsqu'une utilisation abusive est détectée, les producteurs décident souvent de ne pas agir parce que les procédures existantes sont coûteuses et complexes. Si certains services privés de surveillance existent, ils sont payants et conçus principalement pour les marques, ce qui les rend moins accessibles et pas totalement adaptés à la protection des IG.

La législation de l'Union, à savoir l'article 35, paragraphe 1, du règlement (UE) 2024/1143, impose désormais à tous les registres ccTLD de l'Union de reconnaître les IG comme des droits antérieurs valides dans le cadre de leurs mécanismes de règlement extrajudiciaire des litiges (REL). Il n'en a pas toujours été ainsi. Avant l'entrée en vigueur du règlement en mai 2024, la seule voie de recours disponible était souvent une action en justice devant les juridictions nationales. Étant donné que l'action en justice peut être longue, coûteuse et incertaine, de nombreux producteurs d'IG décidaient de ne pas recourir à cette option.

Au niveau international, les IG ne sont pas reconnues comme des droits pouvant bénéficier d'une protection en vertu des principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine (UDRP), la principale procédure de règlement des litiges pour les domaines génériques de premier niveau (gTLD) gérée par l'Organisation mondiale de la propriété intellectuelle. Cela signifie que la procédure n'est pas accessible aux producteurs d'IG.

Par conséquent, le nombre relativement faible de cas signalés d'utilisation abusive des IG dans les noms de domaine n'est pas nécessairement un indicateur fiable du niveau de risque réel: la capacité de surveillance limitée et la complexité des mécanismes d'application masquent l'ampleur réelle du problème. En outre, les mécanismes actuels de résolution des litiges relatifs aux noms de domaine sont intrinsèquement réactifs et ne remplissent pas de fonction préventive.

Un système d'information et d'alerte proactif au niveau de l'UE permettrait donc:

- d'aider les demandeurs d'une IG à détecter rapidement les enregistrements potentiellement abusifs et à agir avant qu'une atteinte à leur réputation ne se produise,

- de fournir un point d'accès unique pour vérifier si une IG a été enregistrée en tant que nom de domaine dans le paysage ccTLD par ailleurs fragmenté, ce qui améliorerait la transparence en matière d'enregistrement des noms de domaine sans divulguer de données à caractère personnel supplémentaires, et

- de renforcer le cadre global d'application pour les IG en ligne.

L'analyse de la Commission indique que, bien que les cas de cybersquattage portant sur des IG ne soient pas encore répandus, ils se produisent et peuvent avoir des conséquences graves sur le plan économique et de la réputation. Compte tenu de la visibilité croissante en ligne des produits couverts par une IG, un système préventif au niveau de l'UE peut donc être jugé nécessaire.

5. ANALYSE DE FAISABILITÉ

5.1. Modèles de systèmes alternatifs

Un système d'information et d'alerte sur les noms de domaine pour les IG fournirait deux services essentiels:

- **une fonction d'information**, qui permettrait aux demandeurs d'une IG de vérifier si un nom de domaine identique à une IG est déjà enregistré,

- **une fonction d'alerte**, qui enverrait des notifications facultatives lorsqu'un tel nom de domaine est nouvellement enregistré.

Ces fonctions reflètent le système d'alerte déjà en place pour les marques de l'UE (MUE) dans le domaine .eu, qui est géré conjointement par l'EUIPO et l'EURid. Ce système repose sur des recherches par correspondance exacte de noms de domaine et informe automatiquement les titulaires de marques de l'Union européenne (MUE) si un nom de domaine .eu identique est enregistré, sans aucun échange de données à caractère personnel des déclarants.

La Commission a tout d'abord examiné si le système existant pour les MUE dans le domaine .eu pouvait être étendu aux IG et aux ccTLD établis dans l'UE. Un certain nombre d'alternatives architecturales, qui diffèrent quant à la question de savoir qui effectuerait la mise en correspondance et comment les données seraient échangées, ont été analysées:

- **Mise en correspondance décentralisée.** Chaque registre ccTLD effectuerait des contrôles de disponibilité et enverrait les résultats à l'EUIPO.

- **Mise en correspondance centralisée.** L'EUIPO collecterait les données d'enregistrement auprès des registres et effectuerait lui-même les vérifications, de la même manière que pour le système existant pour les MUE dans le domaine .eu.

- **Modèle tiers.** Un intermédiaire collecterait ou mettrait en correspondance les données avant de transmettre les résultats à l'EUIPO.

Toutes ces approches sont techniquement réalisables en principe. Toutefois, chacune d'entre elles imposerait aux registres de mettre en œuvre des modifications importantes, notamment de développer des interfaces de programmation d'applications (API), qui sont des interfaces techniques standards permettant une communication automatisée entre les systèmes informatiques, de créer des outils de mise en correspondance ou d'exporter régulièrement des données d'enregistrement de noms de domaine. Ces modifications entraîneraient des coûts et des changements d'infrastructure pour les registres. D'un point de vue juridique, ces modèles nécessiteraient également des accords contractuels avec chaque registre pour régir le partage des données et éviter les risques liés à la confidentialité ou à la protection des données. La complexité et la charge de tels accords ont été considérées comme un obstacle majeur.

Les registres consultés dans le cadre de l'étude se sont largement opposés à ces solutions alternatives et, plus généralement, ont mis en doute la nécessité d'un système d'alerte spécifique aux IG. Ils ont indiqué que les modifications requises entraîneraient des coûts et des charges opérationnelles importants et ont fait part de leurs préoccupations quant à la protection et à la confidentialité des données. Ils ont estimé qu'un tel système n'était pas nécessaire et ont exprimé leur réticence à investir dans des changements d'infrastructure.

Dans son document de prise de position, le CENTR a également souligné que tout système de l'UE devrait rester volontaire et éviter les obligations inutiles. Le CENTR a souligné le faible nombre de litiges liés aux IG en ce qui concerne les noms de domaine, l'existence de mécanismes de REL et la nécessité d'éviter des charges supplémentaires pour les registres.

Compte tenu de ces limitations, une alternative supplémentaire a été examinée, qui ne nécessiterait pas d'étendre le système existant pour les MUE dans le domaine .eu aux IG et aux ccTLD établis dans l'UE. Il s'agirait plutôt de créer **un système d'IG spécifique géré par l'EUIPO et reposant principalement sur des outils DNS accessibles au public**. Il proposerait les mêmes fonctions d'information et d'alerte que le système actuel pour le domaine .eu, sur la base de correspondances exactes avec les IG enregistrées, mais il ne serait pas nécessaire que les registres exportent ou partagent des bases de données d'enregistrement. D'un point de vue technique, le système s'appuierait par défaut sur des **recherches sur des serveurs de noms (NS)**, une requête DNS standard qui vérifie simplement l'existence d'un nom de domaine. Lorsqu'une recherche sur des NS ne donne aucun résultat (par exemple, lorsqu'un nom est enregistré mais n'a pas encore été délégué[7]), elle pourrait être complétée par des requêtes automatisées au moyen:

- du **protocole WHOIS** ou son successeur sécurisé, le **protocole d'accès aux données d'enregistrement (RDAP)**, et/ou

- d'un **service de disponibilité des noms de domaine (DAS)**, lorsqu'un registre propose un tel service.

Ce modèle présente des avantages évidents. Il n'entraînerait aucun coût de développement ou de fonctionnement pour les registres ccTLD, ni aucune modification de leur infrastructure. Il s'appuierait également sur l'expérience acquise par l'EUIPO avec le système d'alerte déjà en place pour les MUE, créant ainsi des synergies. Le codage nécessaire serait développé au niveau central par l'EUIPO afin de permettre les recherches sur les NS et les requêtes WHOIS/RDAP. Ces méthodes utilisent uniquement des données DNS accessibles au public et n'exigent pas des registres qu'ils partagent les listes complètes des noms enregistrés (appelés «fichiers de zone») ou des données à caractère personnel. Un système fondé uniquement sur les recherches sur les NS pourrait fonctionner même sans la coopération des registres.

Toutefois, pour améliorer la précision et la couverture, la **coopération volontaire des registres pourrait prendre les formes suivantes**:

- **mettre sur liste blanche** l'adresse IP de l'EUIPO pour permettre les requêtes WHOIS ou RDAP automatisées, et/ou

- **accorder l'accès** à un DAS, lorsqu'un tel service existe.

Cela garantirait que le système couvre également les noms de domaine qui sont enregistrés mais qui ne sont pas encore délégués. Cette coopération resterait strictement volontaire et ne créerait aucune obligation juridique pour les registres.

---

[7] Un nom de domaine est «enregistré mais pas encore délégué» lorsqu'il est enregistré dans la base de données du registre et donc indisponible pour d'autres personnes souhaitant l'enregistrer, mais que le déclarant ne l'a pas encore relié à des serveurs de noms, de sorte qu'il ne conduit à aucun site internet ou service de courrier électronique.

5.2. Conclusion sur les modèles de systèmes alternatifs

D'après l'analyse, un système d'information et d'alerte sur les noms de domaine au niveau de l'UE géré par l'EUIPO et fondé sur des outils DNS standards et accessibles au public serait **le modèle le plus proportionné et le plus viable sur le plan technique**.

Des modèles architecturaux ambitieux sont techniquement possibles. Toutefois, ils devraient être exclus parce qu'ils entraîneraient des coûts disproportionnés, créeraient une complexité juridique et seraient confrontés à une forte opposition de la part des registres. En revanche, un modèle léger géré par l'EUIPO fondé sur des outils DNS standards et accessibles au public est réalisable sur les plans technique et juridique, pourrait être conçu de manière à être conforme aux exigences de l'UE en matière de protection des données et de cybersécurité, et réduirait au minimum les coûts et les charges opérationnelles. Il répond à bon nombre des préoccupations exprimées par les registres, à condition que la participation reste volontaire et que des garanties et des accords contractuels appropriés soient mis en place.

Ce modèle offre une solution techniquement réalisable et à faible impact, telle que décrite ci-dessus, qui:

- n'exige pas d'adaptations techniques ou de coûts de développement pour les registres,
- n'implique pas le partage de fichiers de zone, de données à caractère personnel ou d'autres données d'enregistrement, et
- s'appuierait sur des garanties juridiques claires, garantissant que toute donnée ou requête est utilisée uniquement pour le fonctionnement du système.

Toute coopération des registres ccTLD resterait strictement volontaire et ne créerait aucune obligation juridique pour eux.

Ce modèle proposé donnerait aux groupements de producteurs d'IG un outil préventif au niveau de l'UE contre le cybersquattage et l'utilisation abusive des IG dans les enregistrements de noms de domaine, tout en répondant aux principales préoccupations des exploitants de registres quant à la charge opérationnelle, à la protection des données et à la faisabilité technique.

6. CONSULTATION DES REGISTRES DE NOMS DE DOMAINE DE PREMIER NIVEAU NATIONAUX

6.1. Description de la consultation

Afin d'analyser la faisabilité de ce modèle et le souhait des registres de coopérer sur une base volontaire, la Commission a mené une consultation ciblée d'août à septembre 2025. Cette consultation s'adressait à l'ensemble des 27 registres ccTLD de l'UE, à EURid et au CENTR.

Au cours de la consultation, la Commission a présenté le modèle technique proposé et a demandé si les registres seraient, en principe, disposés à:

- mettre sur liste blanche l'adresse IP de l'EUIPO pour permettre les requêtes WHOIS automatisées,
  et/ou
- accorder l'accès à un DAS, lorsqu'un tel service est disponible.

Les contributions des registres sont prises en compte dans le présent rapport. Elles ont fourni une indication du niveau de participation volontaire qui pourrait être attendu pour un futur système d'information et d'alerte sur les noms de domaine au niveau de l'UE pour les IG.

6.2. Résultats de la consultation

Outre CENTR et EURid, 22 registres ccTLD de l'UE ont répondu.

Soutien au modèle proposé, sous réserve de garanties

La plupart des répondants ont indiqué qu'ils seraient, en principe, disposés à participer au modèle proposé au moyen d'au moins une des deux formes de coopération volontaire, à savoir:

- octroi d'un accès automatisé aux informations relatives à l'enregistrement des noms de domaine (via le protocole WHOIS ou le RDAP), ou

- octroi d'un accès à un DAS.

Les registres favorables à la coopération ont souligné de manière constante un certain nombre de garanties qui devraient être mises en place et des conditions pratiques qui devraient être remplies pour que la coopération soit acceptable.

- **Limitation de la finalité**. Toute donnée doit être utilisée strictement pour le fonctionnement du système d'information et d'alerte sur les noms de domaine au niveau de l'UE et uniquement pour vérifier la disponibilité des dénominations d'IG.

- **Protection des données**. La coopération doit respecter les exigences de l'UE en matière de protection des données et aucune donnée à caractère personnel ne devrait être partagée.

- **Cybersécurité et conformité à la directive SRI 2**. La coopération doit être conforme à la directive SRI 2 de l'UE[8], qui établit des règles communes de l'UE visant à garantir la sécurité des réseaux et des systèmes d'information et classe les registres de noms de domaine comme des «entités essentielles» soumises à des mesures strictes en matière de sécurité et de gestion des risques.

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

- **Des paramètres opérationnels clairs**. Le nombre et la fréquence attendus des requêtes automatisées (recherches sur les DNS) doivent être fixés et maintenus dans des limites raisonnables.

- **Exclusion des fichiers de zone**. Le partage des fichiers de zone doit rester exclu.

- **Préférence technologique**. Dans la mesure du possible, les requêtes devraient utiliser RDAP, le successeur moderne et plus sûr de WHOIS.

- **Concurrence équitable**. Tout accès privilégié de l'EUIPO aux données DNS ne doit pas fausser la concurrence sur le marché des services de protection des marques ni conférer à l'EUIPO un avantage préférentiel. Toute donnée obtenue aux fins de la protection des IG doit donc être utilisée strictement à cette fin.

Les registres ont en outre souligné que toute coopération avec l'EUIPO ne pouvait être envisagée que dans le cadre d'un **accord formel**. Un tel accord devrait définir clairement le champ d'application de la coopération, inclure des clauses de sécurité appropriées et répondre aux préoccupations plus larges soulevées au cours de la consultation.

Plusieurs registres ont également suggéré des améliorations pratiques, comme des projets pilotes. Par exemple: i) un modèle «push», dans le cadre duquel le registre informe lui-même l'EUIPO d'une correspondance entre les enregistrements plutôt que l'émission répétée de requêtes de la part de l'EUIPO (recherches dans le DNS), et ii) l'utilisation d'ensembles de données ouverts (listes quotidiennes ou données ouvertes mensuelles) afin de réduire la nécessité d'un accès spécial.

Réserves

Certains registres qui étaient par ailleurs ouverts à la coopération ont néanmoins remis en question l'ampleur de l'utilisation abusive des IG en ce qui concerne les domaines dans l'UE. Ils ont estimé que l'octroi d'un accès préférentiel, par exemple en mettant WHOIS sur une liste blanche ou en utilisant un DAS, était disproportionné dans ce contexte. Ils ont plutôt proposé de commencer par ce qui est déjà accessible au public, à savoir les recherches sur les NS, qui se bornent à vérifier l'existence d'un nom de domaine, tout en laissant ouverte pour plus tard la question de l'accès préférentiel pour l'EUIPO.

Une minorité de répondants ont indiqué qu'ils ne pouvaient pas soutenir le développement d'un tel système, invoquant la faible incidence des abus en matière d'IG et l'existence de risques pour la sécurité et de contraintes juridiques ou techniques.

Conséquences pour le modèle proposé

Les résultats de la consultation confirment que le modèle proposé, fondé principalement sur des recherches publiques sur les NS et, le cas échéant, complété par des requêtes WHOIS/RDAP ou un DAS, est réalisable sur le plan technique. Ils montrent également que la coopération volontaire est réaliste, à condition que la Commission et l'EUIPO mettent en place des garanties juridiques claires, maintiennent la charge opérationnelle à un niveau minimal et garantissent un accès normalisé et sécurisé (de préférence via RDAP), avec des limites raisonnables en ce qui concerne le nombre et la fréquence des requêtes.

Une approche progressive refléterait au mieux la diversité de la configuration des registres et les préoccupations exprimées. Une telle approche commencerait par ce qui peut déjà

être réalisé grâce à des recherches publiques sur les DNS, avant d'inclure progressivement les registres qui souhaitent fournir un accès volontaire supplémentaire. Des projets pilotes, comme le modèle «push» ou la publication d'ensembles de données ouverts, pourraient encore améliorer l'efficacité.

7. CONSTATATIONS ET CONCLUSIONS

L'analyse confirme que l'utilisation abusive des indications géographiques dans les noms de domaine, bien que sous-déclarée et donc difficile à quantifier, représente un risque réel et croissant pour la valeur économique et la réputation des produits couverts par une IG. Le faible nombre de cas signalés reflète plus probablement la capacité de surveillance limitée de nombreux groupements de producteurs et le caractère réactif des mécanismes existants de résolution des litiges plutôt que l'absence de risque.

Les outils d'application actuels pour les domaines de premier niveau nationaux de l'UE sont largement réactifs. Le règlement extrajudiciaire des litiges au niveau national ne prévoit de recours qu'en réponse à un litige, une fois qu'un nom de domaine a déjà été enregistré. Les procédures judiciaires sont souvent longues, coûteuses et imprévisibles, et les services de surveillance privés sont coûteux et principalement conçus pour les marques plutôt que pour les IG.

Un système préventif d'information et d'alerte sur les noms de domaine au niveau de l'UE contribuerait à combler cette lacune. En permettant aux demandeurs d'une IG de vérifier si un nom qu'ils entendent protéger en tant qu'IG a déjà été enregistré comme nom de domaine et de recevoir des alertes lorsque des noms identiques sont enregistrés, un tel système permettrait aux groupements de producteurs d'agir avant que ne se produisent des dommages sur le plan économique et de la réputation.

L'analyse confirme que la mise en place d'un système d'information et d'alerte sur les noms de domaine au niveau de l'UE pour les IG est à la fois nécessaire et réalisable sur le plan technique. Un tel système fournirait aux producteurs d'IG un outil de prévention contre le cybersquattage et contribuerait à protéger la réputation et la valeur économique des produits couverts par une IG dans l'environnement en ligne.

Le modèle le plus approprié est un système géré par l'EUIPO fondé sur des outils DNS standard accessibles au public et sur la coopération volontaire des registres ccTLD. Cette approche évite d'imposer aux registres d'adapter leur infrastructure ou de partager des données à caractère personnel.

L'analyse montre qu'un système fondé principalement sur des outils DNS publics pourrait être mis en œuvre sans exiger des registres qu'ils partagent des données à caractère personnel ou réalisent des modifications techniques. Un tel système reposerait en particulier sur des recherches sur des serveurs de noms. Le cas échéant, ces recherches seraient complétées par des requêtes WHOIS ou RDAP, ou par un service de disponibilité de domaine.

La consultation ciblée des registres ccTLD établis dans l'UE, du CENTR et d'EURid indique que la coopération volontaire est réaliste. La plupart des répondants ont exprimé

leur volonté de principe de permettre les requêtes WHOIS ou RDAP automatisées ou d'accorder un accès à un DAS, à condition que:

- la finalité du système soit strictement limitée à la protection des IG,
- la coopération soit conforme aux règles de l'UE en matière de cybersécurité, en particulier à la directive SRI 2 [directive (UE) 2022/2555], qui établit des règles communes de l'UE visant à garantir la sécurité des réseaux et des systèmes d'information, et
- les accords formels définissent clairement le champ d'application de la coopération et les garanties de sécurité nécessaires.

Les préoccupations soulevées par les registres, comme la nécessité de la proportionnalité, de solides garanties en matière de protection des données et d'une charge opérationnelle minimale, pourraient être résolues par une conception légère et une participation strictement volontaire.

Le présent rapport fournit la base factuelle et politique requise par l'article 35, paragraphe 3, du règlement (UE) 2024/1143 et satisfait à l'obligation d'analyser la nécessité et la faisabilité d'un tel système. Sur la base de cette analyse, la Commission n'a pas l'intention, à ce stade, de présenter une proposition législative.

8. PROCHAINES ÉTAPES

La Commission poursuivra la coordination interne et le dialogue avec les parties prenantes afin de déterminer le cadre le plus approprié pour un éventuel système d'information et d'alerte sur les noms de domaine au niveau de l'UE pour les indications géographiques.

Toute étape vers une proposition législative sera examinée conjointement avec:

- les conclusions de l'analyse séparée de la Commission sur les IG artisanales et industrielles au titre de l'article 72, paragraphe 2, du règlement (UE) 2023/2411, qui (comme indiqué dans le présent document) est attendue pour le 2 juin 2026, et
- d'autres consultations techniques et projets pilotes menés avec l'EUIPO, EURid et les registres ccTLD établis dans l'UE afin de tester les modalités pratiques et de veiller à ce que tout futur système soit proportionné et viable.