ICANN | GNSO

Generic Names Supporting Organization

Rapport final de l'étape 2 A du processus accéléré d'élaboration de politiques sur la spécification temporaire relative aux données d'enregistrement des gTLD

3 septembre 2021

Statut du présent document

Ce document constitue le rapport final des recommandations de l'équipe de la GNSO responsable de l'étape 2A du processus accéléré d'élaboration de politiques (EPDP) sur la spécification temporaire relative aux données d'enregistrement des gTLD, préparé à l'intention du conseil de la GNSO.

Avant-propos

L'objectif du présent rapport final est de documenter les éléments suivants du travail de l'équipe responsable de l'EPDP : (i) les délibérations sur les questions de la charte (ii) les contributions reçues sur le rapport initial de l'étape 2A de l'EPDP et leur analyse subséquente par l'équipe responsable de l'EPDP (iii) les recommandations de politiques ainsi que les niveaux de consensus y associés, et (iv) les directives de mise en œuvre, pour examen par le conseil de la GNSO.

Table des matières

Ce document a été traduit dans plusieurs langues dans un but purement informatif. Le texte original faisant foi (en anglais) peut être consulté sur : https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2a-updated-final-report-03sep21-en.pdf

1 Résumé analytique

1.1 Contexte

Le 17 mai 2018, le Conseil d'administration de l'ICANN a approuvé la spécification temporaire pour les données d'enregistrement des domaines génériques de premier niveau (gTLD) afin de permettre aux parties contractantes de se conformer aux exigences contractuelles existantes de l'ICANN tout en se conformant également au Règlement général sur la protection des données (RGPD) de l'Union européenne. Cette action du Conseil a déclenché le lancement du PDP par le conseil de la GNSO le 19 juillet 2018. Le PDP est mené en deux étapes : L'étape 1 a eu pour tâche de confirmer ou non la spécification temporaire avant le 25 mai 2019 ; l'étape 2 a été chargée de discuter, entre autres éléments, d'un modèle normalisé d'accès aux données d'enregistrement non publiques (SSAD).

Le conseil de la GNSO a adopté le rapport final de l'étape 2 lors de sa réunion du 24 septembre 2020 ; toutefois, en réponse à une demande de certains membres de l'équipe responsable de l'EPDP, le conseil de la GNSO a demandé à l'équipe responsable de l'EPDP de poursuivre ses travaux sur deux sujets : 1) la distinction entre les données d'enregistrement des personnes morales et des personnes physiques, et 2) la possibilité que les contacts uniques aient une adresse e-mail anonymisée uniforme. Ces deux sujets constituent l'objet de l'étape 2A.

Plus précisément, l'équipe responsable de l'EPDP a reçu les instructions suivantes :

a) Personnes morales vs. personnes physiques - L'équipe responsable de l'EPDP devra se pencher sur l'étude menée par l'organisation ICANN (à la demande de l'équipe responsable de l'EPDP et avec l'approbation du conseil de la GNSO pendant l'étape 1), sur l'avis juridique fourni par le cabinet Bird & Bird, ainsi que sur les nombreux commentaires reçus à ce sujet pendant le forum de consultation publique sur le supplément et répondre :
   i. Si des mises à jour doivent être apportées aux recommandations relatives à ce sujet issues de la première étape de l'EPDP (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire ») ;
   ii. Établir quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la différence entre les enregistrements des personnes morales et celui des personnes physiques.
b) En ce qui concerne la possibilité que les contacts uniques aient une adresse e-mail anonymisée uniforme, l'équipe responsable de l'EPDP devra étudier l'avis juridique et réfléchir à des propositions spécifiques comportant des garanties suffisantes pour éviter

les problèmes identifiés dans le document initial. Les groupes qui ont demandé un délai supplémentaire pour examiner cette question, entre autres l'ALAC, le GAC et le SSAC, seront responsables de soumettre des propositions concrètes par rapport à ce sujet. Cet examen devrait déterminer :

i. S'il est possible que les contacts uniques aient une adresse électronique anonyme uniforme et, si possible, si cela devait être obligatoire.
ii. Si cela était possible, mais pas obligatoire, quelles directives devraient être fournies, le cas échéant, aux parties contractantes souhaitant mettre en place des adresses e-mail anynomisées uniformes.

1.2 Rapport initial

Le 3 juin 2021, l'équipe responsable de l'EPDP a publié son rapport initial pour consultation publique. Le rapport initial décrivait la réflexion de l'équipe jusqu'à ce point et était destiné à servir d'outil pour solliciter les commentaires de la communauté, en particulier dans les domaines où des divergences importantes subsistaient. Bien que des recommandations préliminaires aient été incluses dans le rapport initial, l'équipe responsable de l'EPDP a demandé que ces recommandations soient prises en considération en combinaison avec une série de questions soulevées pour aider à la finalisation de son rapport.

Après la publication du rapport initial, l'équipe responsable de l'EPDP : (i) a examiné attentivement les commentaires publics reçus en réponse à la publication du rapport initial (ii) a poursuivi l'examen du travail en cours avec les groupes de la communauté que représentent les membres de l'équipe (iii) a poursuivi ses délibérations pour l'élaboration d'un rapport final qui sera examiné par le conseil de la GNSO et, au cas où il serait approuvé, transmis au Conseil d'administration de l'ICANN pour approbation en tant que politique de consensus de l'ICANN. Comme requis par les directives des groupes de travail de la GNSO, le président de l'équipe responsable de l'EPDP a effectué des appels à consensus sur les recommandations contenues dans le présent rapport final. En bref :

1.3 Réponses et recommandations

Déclaration du président

Bien que ce rapport final et ses recommandations aient l'appui consensuel de l'équipe responsable de l'étape 2A de l'EPDP, il est important de signaler que certains groupes ont estimé que le travail n'était pas allé aussi loin que nécessaire, ou n'a pas inclus suffisamment de détails, tandis que d'autres groupes ont estimé que certaines recommandations n'étaient ni appropriées ni nécessaires. De surcroît, au cours de la dernière étape de notre travail, certains groupes auraient préféré avoir l'occasion de qualifier de manière plus détaillée le niveau de consensus dont faisaient l'objet les rubriques comprises dans les recommandations. Dans ce contexte, tous les lecteurs du

rapport final de l'étape 2A de l'EPDP devraient également lire les déclarations de la minorité soumises par chaque groupe, qui ont été annexées et font partie du rapport final et du registre historique de notre travail.

Au-delà du consensus atteint sur les recommandations du rapport final, il y a plusieurs domaines sur lesquels les groupes de l'EPDP 2A n'étaient pas pleinement d'accord, y compris si la différenciation entre les données d'enregistrement des personnes morales et physiques devrait être obligatoire ou facultative, et si l'avantage de la publication des données d'enregistrement de la personne morale était correctement équilibré par rapport au risque de divulgation involontaire des données à caractère personnel. Ces divergences d'opinion et de perspective restent largement inchangées par les recommandations du rapport final.

Ce rapport final constitue un compromis qui est le maximum qui a pu être atteint par le groupe à ce stade dans le cadre du temps et de la portée actuellement alloués, et il ne doit pas être considéré comme fournissant des résultats qui aient été pleinement satisfaisants pour tout le monde. Cela souligne l'importance des déclarations de la minorité pour comprendre le contexte complet des recommandations du rapport final.

Pour de plus amples détails sur ces qualifications, veuillez consulter l'article 3.6 des Directives de la GNSO pour les groupes de travail.

Consulter la section 3 pour voir le texte intégral des recommandations et des réponses.

Réponse à l'instruction (a)(i) du conseil.

L'équipe responsable de l'EPDP présente la réponse suivante à l'instruction du conseil indiquant si des mises à jour sont nécessaires à la recommandation de l'étape 1 de l'EPDP sur ce sujet (« les bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et ceux de personnes morales, mais ne sont pas tenus de le faire ») :

> L'équipe responsable de l'EPDP n'est pas parvenue à un consensus sur le fait de recommander des modifications à la Recommandation 17.1 de l'étape 1 de l'EPDP (« les bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et ceux de personnes morales, mais ne sont pas tenus de le faire »).

Proposition au conseil de la GNSO

> L'équipe responsable de l'EPDP reconnaît que les développements législatifs actuels et futurs pourraient nécessiter d'autres travaux de politique sur ce sujet, par exemple pour résoudre les conflits potentiels avec les exigences de politique existantes et/ou pour examiner s'il existe un risque de fragmentation des

marchés qui doive être résolu. En même temps, l'équipe responsable de l'EPDP reconnaît qu'il ne pourrait pas être possible d'évaluer l'impact de la législation avec précision avant son adoption. L'équipe responsable de l'EPDP recommande au conseil de la GNSO de suivre ces développements à travers les rapports législatifs / réglementaires élaborés par l'organisation ICANN.

Notant les discussions en cours et l'adoption attendue de la directive révisée sur la sécurité des réseaux et des systèmes d'information (« NIS2 »), l'équipe responsable de l'EPDP encourage fortement le conseil de la GNSO à suivre les procédures existantes pour identifier et déterminer la portée des futurs travaux politiques possibles à la suite de l'adoption du NIS2 afin d'évaluer si l'élaboration de politiques supplémentaires est jugée souhaitable et/ou nécessaire.

Guide de différenciation entre personnes physiques et personnes morales

Recommandation 1

L'équipe responsable de l'EPDP RECOMMANDE la création d'un ou de plusieurs champs afin de faciliter la distinction entre les données d'enregistrement des personnes morales et des personnes physiques et/ou si ces données d'enregistrement contiennent des données à caractère personnel ou non personnel. L'organisation ICANN DOIT coordonner avec la communauté technique, par exemple avec le groupe de travail consacré au RDAP, afin d'élaborer toutes les normes nécessaires associées à l'utilisation de ce ou de ces champs dans l'EPP et le RDDS.

Ce ou ces champs POURRAIENT être utilisés par les parties contractantes qui établissent une distinction entre les données d'enregistrement des personnes morales et des personnes physiques et/ou si ces données d'enregistrement contiennent des informations personnelles ou non personnelles. Pour plus de clarté, les parties contractantes POURRAIENT utiliser le ou les champs, ce qui signifie que si une partie contractante décidait de ne pas utiliser le ou les champs, ils pourraient être laissés vides ou ne pas exister. En outre, les parties contractantes POURRAIENT inclure le ou les champs dans une réponse RDDS.

Le SSAD, conformément aux recommandations de l'étape 2 de l'EPDP, DOIT appuyer le ou les champs afin de faciliter l'intégration entre le SSAD et les systèmes des parties contractantes. Ces champs doivent pouvoir contenir les valeurs suivantes :

Statut juridique

- La distinction de statut juridique n'a pas été faite (valeur par défaut)
- Non spécifié – le titulaire du nom enregistré et/ou l'agent d'enregistrement ne l'ont pas précisé
- Le titulaire du nom enregistré est une personne physique

- Le titulaire du nom enregistré est une personne morale

Données à caractère personnel

- La présence de données à caractère personnel n'a pas été déterminée (valeur par défaut)
- Non spécifié – le détenteur du nom enregistré et/ou l'agent d'enregistrement n'ont pas fait de spécification
- Les données d'enregistrement contiennent des informations à caractère personnel
- Les données d'enregistrement NE contiennent PAS d'informations à caractère personnel

Réponse à l'instruction (a)(ii) du conseil.

Recommandation 2

La recommandation de l'équipe responsable de l'EPDP est que les parties contractantes qui choisissent de se différencier en fonction du type de personne DEVRAIENT suivre les directives[1] ci-dessous et documenter clairement toutes les étapes de traitement des données. Cependant, il n'est pas du ressort ou de la responsabilité de l'équipe responsable de l'EPDP de prendre une décision finale concernant les risques juridiques, car cette responsabilité appartient en fin de compte à/aux autorité(s) de contrôle.

Le RGPD protège les personnes physiques en ce qui concerne le traitement de leurs données à caractère personnel. Le RGPD ne couvre pas le traitement de données à caractère personnel ayant trait aux personnes morales et notamment les entreprises établies comme des personnes morales y compris le nom et le type de personne morale et ses détails de contact. [Considérant 14, RGPD] Cette figure permet généralement la divulgation des données des personnes morales parce qu'elles ne relèvent pas de la compétence du RGPD ; toutefois, lors du traitement des données des personnes morales, les parties contractantes devraient mettre en place des mesures de protection pour garantir que les données d'identification personnelle concernant une personne physique ne soient pas divulguées dans des données marquées comme appartenant à une personne morale, car il s'agit d'un exemple d'information qui *entre* dans le champ d'application du RGPD. Pour plus d'informations sur cette distinction, veuillez vous référer à la lettre du Comité européen de la protection des données, à partir de la p. 4.

1. Les titulaires de noms de domaine devraient pouvoir s'auto-identifier en tant que personnes physiques ou morales. Les bureaux d'enregistrement devraient transmettre cette option d'autoidentification comme personne physique ou morale

[1] Veuillez noter que les agents de liaison de l'organisation ICANN ont fourni à l'équipe responsable de l'EPDP les commentaires suivants sur la façon dont cette orientation serait mise en œuvre une fois adoptée : https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html.

(i) au moment de l'enregistrement, ou sans délai indu après l'enregistrement,[2] et (ii) au moment où le titulaire de nom de domaine met à jour ses informations de contact ou sans délai indu après la mise à jour des coordonnées.

2. Tout processus de différenciation doit garantir que les données des personnes physiques soient expurgées par le RDDS public, à moins que la personne concernée n'ait donné son consentement à les publier ou que ces données puissent être publiées en raison d'une autre raison légale en vertu du RGPD, conformément à l'approche de « protection des données dès la conception et par défaut » énoncée à l'article 25 du RGPD.
3. Dans le cadre de la mise en œuvre, les bureaux d'enregistrement devraient envisager d'utiliser le(s) champ(s) décrit(s) dans la Recommandation 1 dans le RDDS, le SSAD ou dans leurs propres ensembles de données qui indiqueraient le type de personne (morale ou physique) et, s'il est légal, le type de données dont il s'agit (données à caractère personnel ou non personnel). Un tel marquage pourrait faciliter l'examen des demandes de divulgation et des exigences d'automatisation par le biais du SSAD et l'affichage des données à caractère non personnel des personnes morales par des systèmes autres que le SSAD (comme le Whois ou le RDAP). Un mécanisme de signalement pourrait également vous aider à indiquer les modifications apportées au type de données dans le(s) champ(s) de données d'enregistrement.
4. Les bureaux d'enregistrement devraient s'assurer qu'ils communiquent clairement la nature et les conséquences du fait qu'un titulaire de nom de domaine s'identifie comme personne morale. Ces communications devraient inclure :
    a. Une explication de ce qu'est une personne morale dans un langage simple et facile à comprendre.
    b. Des directives du bureau d'enregistrement à l'intention du titulaire de nom de domaine (personne concernée)[3] concernant les conséquences possibles de :
        i. L'identification de leurs données d'enregistrement de nom de domaine comme correspondant à une personne morale ;
        ii. La confirmation de la présence de données à caractère personnel ou non personnel, et ;
        iii. La fourniture de son consentement.[4] Cela est également conforme à l'article 3.7.7.4 du contrat d'accréditation de bureau d'enregistrement (RAA).
5. Si les titulaires s'identifient comme des personnes morales et confirment que leurs données d'enregistrement n'incluent pas de données à caractère personnel, les

[2] Pour plus de clarté, les bureaux d'enregistrement devraient s'assurer que si le titulaire n'a pas l'option de s'auto-identifier au moment de l'enregistrement, l'option devrait être fournie au plus tard 15 jours après la date de l'enregistrement.
[3] Remarque : le titulaire pourrait ne pas toujours être la personne concernée, mais dans toutes les circonstances, un avis ou un consentement approprié doit être fourni à toutes les parties et par toutes les parties, conformément à la loi sur la protection des données en vigueur.
[4] Voir aussi https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

bureaux d'enregistrement devraient publier les données d'enregistrement dans les services d'annuaire des données d'enregistrement accessibles au public.
6. Les titulaires de noms de domaine (personnes concernées) doivent avoir un moyen facile pour corriger les erreurs possibles.
7. La distinction entre les titulaires de noms de domaine qui sont des personnes morales et ceux qui sont des personnes physiques ne peut pas déterminer à elle seule la façon dont les informations devraient être traitées (rendues publiques ou masquées), car les données fournies par les personnes morales pourraient inclure des données à caractère personnel protégées par la législation sur la protection des données, comme le RGPD.

Recommandation 3
L'équipe responsable de l'EPDP recommande, conformément aux exigences de l'article 40 du RGPD en matière de codes de conduite, que les directives élaborées ci-dessus concernant la différenciation entre personne physique et personne morale soient prises en compte par tout travail futur possible au sein de l'ICANN par les autorités de contrôle et les responsables du traitement concernés en relation avec l'élaboration d'un Code de conduite du RGPD. Pour éviter tout doute, le présent Code de conduite est distinct du Code de conduite mentionné dans le RAA et/ou les contrats de registre. Conformément au considérant 99 du RGPD, « lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations ».

Réponse à l'instruction (b)(i) du conseil.

L'équipe responsable de l'EPDP reconnaît qu'il pourrait être techniquement possible d'avoir un contact e-mail par titulaire de nom de domaine ou un contact e-mail pour chaque enregistrement.[5] Certaines parties prenantes voient des risques et manifestent d'autres préoccupations[6] qui empêchent actuellement l'équipe responsable de l'EPDP de recommander d'exiger aux parties contractantes qu'une adresse électronique par titulaire de nom de domaine ou une pour chaque enregistrement soit accessible au public. L'équipe responsable de l'EPDP note en effet que certains groupes de parties prenantes ont exprimé les avantages de 1) un contact e-mail pour chaque enregistrement à des fins de joignabilité, car des préoccupations ont été exprimées

[5] Certains membres de l'équipe responsable de l'EPDP notent que, même si cela est techniquement possible, d'autres facteurs liés aux efforts requis pour mettre en œuvre une telle fonctionnalité devraient être pris en compte pour déterminer la viabilité globale.
[6] Tel que 1) il n'est pas clair que le travail de mise en œuvre d'un tel concept soit justifié par l'avantage potentiel. 2) de plus, il n'est pas clair que les objectifs, tels que présentés, soient effectivement atteints ou le plus atteints possible en exigeant des adresses e-mail pour chaque enregistrement ou par titulaire de nom de domaine.

quant à la convivialité des formulaires Web et 2) contact e-mail par titulaire de nom de domaine à des fins de corrélation.[7]

Réponse à l'instruction (b)(ii) du conseil.

Recommandation 4

La recommandation de l'équipe responsable de l'EPDP est que les parties contractantes qui choisissent de publier une adresse e-mail pseudonymisée par titulaire de nom de domaine ou pour chaque enregistrement dans le RDDS accessible au public devraient évaluer les directives juridiques obtenues par l'équipe responsable de l'EPDP sur ce sujet (voir Annexe F), ainsi que toute autre directive pertinente fournie par les autorités de protection des données pertinentes.

Lors de l'évaluation des risques, des avantages et des garanties associés à la publication d'une adresse e-mail pseudonymisée par titulaire de nom de domaine ou pour chaque enregistrement dans le RDDS accessible au public, les parties contractantes devraient au moins considérer :

- Les adresses e-mail des personnes physiques pour chaque enregistrement et par titulaire de nom de domaine sont probablement des données à caractère personnel (c'est-à-dire, aucune des deux approches ne crée de données anonymes telles que définies dans le RGPD). Ces données sont probablement des données à caractère personnel du point de vue de l'autorité de contrôle et de tiers.
- Toutefois, même si l'on considère les données à caractère personnel, le masquage des adresses e-mail offre des avantages par rapport à la publication des adresses e-mail réelles des titulaires de nom de domaine, notamment : (i) démontrer une technique d'amélioration de la protection des données dès la conception et par défaut (Article 25 du RGPD) ; et (ii) une certaine réduction des risques pertinente lors de la réalisation d'une analyse d'équilibre d'intérêt légitime pour la divulgation de l'adresse e-mail masquée à des tiers.
- En somme, la publication d'une adresse e-mail pour chaque enregistrement comporte probablement moins de risques que la publication d'adresses e-mail par titulaire de nom de domaine en raison de la quantité d'informations qu'une partie peut potentiellement lier à une personne concernée en fonction d'un contact e-mail par titulaire de nom de domaine.
- Pour la publication d'adresses électroniques pour chaque enregistrement et par titulaire de nom de domaine, les parties contractantes devraient adopter des mesures efficaces pour limiter la disponibilité des coordonnées aux spammeurs.

[7] La capacité d'identifier quels domaines un titulaire de nom de domaine particulier a enregistrés est importante pour les forces de l'ordre et pour les enquêtes de cybersécurité vis-à-vis des mauvais acteurs qui enregistrent souvent de nombreux domaines à des fins malveillantes.

1.4 Conclusions et prochaines étapes

Ce rapport final sera présenté au conseil de la GNSO à des fins d'examen et d'approbation.

1.5 Autres sections importantes de ce rapport

Pour un examen complet des questions et des échanges pertinents de cette équipe responsable de l'EPDP, les sections suivantes sont comprises dans le présent rapport final :

- Le contexte des questions à l'examen ;
- La documentation concernant les participants aux délibérations de l'équipe responsable de l'EPDP, les registres d'assistance et les liens vers les manifestations d'intérêt, le cas échéant ;
- Une annexe comprenant la mission de l'équipe responsable de l'EPDP comme définie dans la charte que le conseil de la GNSO a adoptée ; et
- Les documents concernant la demande de commentaires de la part de la communauté par le biais des canaux formels des SO/AC/SG/C, y compris leurs réponses.

2 Approche de l'équipe responsable de l'EPDP

La présente section donne un aperçu de la méthodologie de travail et de l'approche de l'équipe responsable de l'EPDP. Les points décrits ci-dessous visent à fournir au lecteur les informations de contexte pertinentes sur les processus et les délibérations de l'équipe responsable de l'EPDP et ne devraient pas être interprétés comme représentant la totalité des délibérations du groupe de travail.

2.1 Méthode de travail

L'équipe responsable de l'EPDP a commencé ses délibérations sur l'étape 2A le 17 décembre 2020. L'équipe a continué son travail principalement à travers des conférences téléphoniques tenues une fois par semaine ou plus, outre ses échanges par e-mail sur sa liste de diffusion. Toutes les réunions de l'équipe responsable de l'EPDP sont documentées sur son espace de travail wiki, y compris sa liste de diffusion, les documents préliminaires, les documents d'information et les contributions provenant des organisations de soutien et des comités consultatifs de l'ICANN, y compris les groupes de parties prenantes et les unités constitutives de la GNSO.

L'équipe responsable de l'EPDP a également préparé un plan de travail dans le cadre du projet de l'étape 2A de l'EPDP, qui a été examiné et mis à jour régulièrement, et partagé avec le conseil de la GNSO.

2.2 Document d'information de contexte et approche

Afin d'assurer une compréhension commune des sujets à traiter dans le cadre de ses délibérations de l'étape 2A, l'équipe de soutien du personnel a élaboré des documents d'information pour chacun des sujets. Les séances d'information ont inclus : 1) les instructions du conseil à l'équipe responsable de l'EPDP, 2) les recommandations pertinentes de l'étape 1 et de l'étape 2 de l'EPDP, 3) les études pertinentes ou les conseils juridiques obtenus précédemment, 4) les exigences de procédure, 5) les instructions de calendrier et 6) l'approche proposée. Ces documents d'information ont été distribués à l'équipe responsable de l'EPDP avant la première réunion et, avec les lectures obligatoires, ont constitué la base de la première affectation de l'équipe responsable de l'EPDP. Plus précisément, on a demandé à l'équipe responsable de l'EPDP d'examiner en profondeur les études attribuées et les conseils juridiques précédents et d'identifier toute question de clarification nécessaire.

2.3 Comité juridique

À l'instar des étapes 1 et 2, l'équipe responsable de l'EPDP s'est appuyée sur son Comité juridique pour examiner et peaufiner les questions identifiées par l'équipe responsable

de l'EPDP. Le Comité juridique est composé d'un membre de chaque SG/C/AC représenté au sein de l'équipe responsable de l'EPDP.

Le Comité juridique de l'étape 2 a collaboré dans l'examen des questions proposées par les membres de l'équipe responsable de l'EPDP afin d'assurer que :

1. Les questions soient de nature véritablement juridique, par opposition aux questions de politique ou de mise en œuvre des politiques ;
2. Les questions aient été formulées de manière neutre, évitant à la fois des résultats présumés et le positionnement des unités constitutives ;
3. Les questions soient à la fois posées de manière appropriée et en temps utile pour le travail de l'équipe responsable de l'EPDP ; et
4. Le budget limité des avocats externes ait été utilisé de manière responsable.

Le Comité juridique a transmis toutes les questions convenues à l'équipe responsable de l'EPDP avant d'envoyer des questions à Bird & Bird.

À ce jour, l'équipe responsable de l'EPDP a accepté d'envoyer à Bird & Bird quatre questions relatives à l'étape 2A. Le texte intégral des questions et des avis juridiques reçus en réponse aux questions se trouve à l'Annexe F.

2.4 Questions du conseil

Pour répondre aux questions posées par le Conseil de la GNSO, l'équipe responsable de l'EPDP a examiné (1) les commentaires fournis par chaque groupe dans le cadre des délibérations ; (2) les commentaires pertinents des étapes 1 et 2 ; (3) les commentaires fournis sur ces sujets par chaque groupe en réponse à la demande de participation précoce au cours des étapes précédentes ainsi que les commentaires pertinents fournis au cours du forum de commentaires publics sur le supplément de l'étape 2 de l'EPDP ;[8] (4) la lecture requise identifiée pour chaque sujet dans les documents de contexte, y compris l'étude de l'organisation ICANN sur « la différenciation entre les personnes morales et les personnes physiques dans les services d'annuaire de données d'enregistrement de noms de domaine (RDDS)», et (5) les commentaires fournis par Bird & Bird.

[8] Voir https://community.icann.org/x/Ag9pBQ, https://community.icann.org/x/Ag9pBQ, https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en ainsi que l'Outil de révision de commentaires publics vis-à-vis du supplément.

3 Réponses de l'équipe responsable de l'EPDP aux questions et aux recommandations du conseil

Après avoir examiné les commentaires publics sur le rapport initial, l'équipe responsable de l'EPDP présente ces réponses et recommandations au conseil de la GNSO pour examen. Ce rapport final indique le niveau de consensus atteint au sein de l'équipe responsable de l'EPDP eu égard aux différentes recommandations. En bref :

Déclaration du président

Bien que ce rapport final et ses recommandations aient l'appui consensuel de l'équipe responsable de l'étape 2A de l'EPDP, il est important de signaler que certains groupes ont estimé que le travail n'était pas allé aussi loin que nécessaire, ou n'a pas inclus suffisamment de détails, tandis que d'autres groupes ont estimé que certaines recommandations n'étaient ni appropriées ni nécessaires. De surcroît, au cours de la dernière étape de notre travail, certains groupes auraient préféré avoir l'occasion de qualifier de manière plus détaillée le niveau de consensus dont faisaient l'objet les rubriques comprises dans les recommandations. Dans ce contexte, tous les lecteurs du rapport final de l'étape 2A de l'EPDP devraient également lire les déclarations de la minorité soumises par chaque groupe, qui ont été annexées et font partie du rapport final et du registre historique de notre travail.

Au-delà du consensus atteint sur les recommandations du rapport final, il y a plusieurs domaines sur lesquels les groupes de l'EPDP 2A n'étaient pas pleinement d'accord, y compris si la différenciation entre les données d'enregistrement des personnes morales et physiques devrait être obligatoire ou facultative, et si l'avantage de la publication des données d'enregistrement de la personne morale était correctement équilibré par rapport au risque de divulgation involontaire des données à caractère personnel. Ces divergences d'opinion et de perspective restent largement inchangées par les recommandations du rapport final.

Ce rapport final constitue un compromis qui est le maximum qui a pu être atteint par le groupe à ce stade dans le cadre du temps et de la portée actuellement alloués, et il ne doit pas être considéré comme fournissant des résultats qui aient été pleinement satisfaisants pour tout le monde. Cela souligne l'importance des déclarations de la minorité pour comprendre le contexte complet des recommandations du rapport final.

Pour de plus amples détails sur ces qualifications, veuillez consulter l'article 3.6 des Directives de la GNSO pour les groupes de travail.

3.1 – Personne morale vs. personne physique

L'équipe responsable de l'EPDP a été chargée par le conseil de la GNSO de répondre aux deux questions suivantes :

i. Si des mises à jour doivent être apportées aux recommandations relatives à ce sujet issues de la première étape de l'EPDP (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire ») ;
ii. Établir quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la différence entre les enregistrements des personnes morales et celui des personnes physiques.

Pour répondre à ces questions, l'équipe responsable de l'EPDP a commencé par un examen de toutes les informations pertinentes, y compris (1) l'étude entreprise par l'organisation ICANN,[9] (2) les directives juridiques fournies par Bird & Bird, et (3) les contributions substantielles fournies sur ce sujet lors du forum de consultation publique. À la suite de l'examen de cette information, l'équipe responsable de l'EPDP a identifié un certain nombre de questions de clarification qui, après examen par le Comité juridique de l'équipe responsable de l'EPDP, ont été soumises à Bird & Bird (voir https://community.icann.org/x/xQhACQ). L'équipe responsable de l'EPDP a examiné les réponses du cabinet Bird & Bird et a appliqué les conseils reçus dans ses recommandations ci-dessous.

Réponse de l'équipe responsable de l'EPDP à la question i.

L'équipe responsable de l'EPDP a longuement discuté de cette question. Comme point de départ, l'équipe responsable de l'EPDP note que le RGPD et de nombreuses autres lois sur la protection des données définissent des exigences en matière de protection des données à caractère personnel des personnes physiques. Elles ne protègent pas les

[9] Dans le cadre de sa Recommandation de politique 17 de l'étape 1, l'équipe responsable de l'EPDP a recommandé que « l'organisation ICANN entreprenne dès que possible une étude pour laquelle les termes de référence soient élaborés en consultation avec la communauté, qui considère :

- La faisabilité et les coûts, y compris les coûts de mise en œuvre ainsi que les éventuels coûts de responsabilité découlant de la différenciation entre personnes morales et personnes physiques ;
- Des exemples d'industries ou d'autres organisations qui aient réussi à différencier les personnes morales des personnes physiques ;
- Les risques que pose la différenciation entre personnes morales et personnes physiques pour la vie privée des titulaires de noms enregistrés ; et
- D'autres risques potentiels (s'il en existe) qu'implique la non-différenciation pour les bureaux d'enregistrement et les opérateurs de registre ».

L'organisation ICANN a présenté l'étude à l'équipe responsable de l'EPDP en juillet 2020.

données à caractère non personnel des personnes morales.[10] En même temps, l'équipe responsable de l'EPDP reconnaît que le Comité européen de la protection des données (« CEPD ») a informé l'ICANN dans une lettre de juillet 2018 que « le simple fait qu'un titulaire de nom de domaine soit une personne morale ne justifie pas nécessairement la publication illimitée de données à caractère personnel concernant des personnes physiques qui travaillent pour cette organisation ou qui la représentent », et que « les données à caractère personnel identifiant des employés individuels (ou des tiers) agissant pour le compte du titulaire de nom de domaine ne devraient pas être rendues publiques par défaut dans le contexte du WHOIS ».[11] Pour obtenir de plus amples renseignements sur les différents points de vue à ce sujet, les lecteurs sont encouragés à examiner le rapport initial de l'équipe responsable de l'EPDP ainsi que les déclarations de la minorité qui ont été annexées au présent rapport.

L'équipe responsable de l'EPDP présente la réponse suivante à l'instruction du conseil indiquant si des mises à jour sont nécessaires à la recommandation de l'étape 1 de l'EPDP sur ce sujet (« les bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et ceux de personnes morales, mais ne sont pas tenus de le faire ») :

> L'équipe responsable de l'EPDP n'est pas parvenue à un consensus sur le fait de recommander des modifications à la Recommandation 17.1 de l'étape 1 de l'EPDP (« les bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et ceux de personnes morales, mais ne sont pas tenus de le faire »).

Proposition au conseil de la GNSO

> L'équipe responsable de l'EPDP reconnaît que les développements législatifs actuels et futurs pourraient nécessiter d'autres travaux de politique sur ce sujet, par exemple pour résoudre les conflits potentiels avec les exigences de politique existantes et/ou pour examiner s'il existe un risque de fragmentation des marchés qui doive être résolu. En même temps, l'équipe responsable de l'EPDP reconnaît qu'il ne pourrait pas être possible d'évaluer l'impact de la législation avec précision avant son adoption. L'équipe responsable de l'EPDP recommande au conseil de la GNSO de suivre ces développements à travers les rapports législatifs / réglementaires élaborés par l'organisation ICANN.
>
> Notant les discussions en cours et l'adoption attendue de la directive révisée sur la sécurité des réseaux et des systèmes d'information (« NIS2 »), l'équipe

[10] « Le RGPD ne s'applique pas au traitement des données à caractère personnel de personnes morales et notamment les initiatives constituées sous la forme de personnes morales, dont le nom et le statut de la personne morale et les coordonnées de cette personne ».
[11] Andrea Jelinek, Comité européen de la protection des données ; lettre à Goran Marby du 5 juillet 2018, disponible à l'adresse https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

responsable de l'EPDP encourage fortement le conseil de la GNSO à suivre les procédures existantes pour identifier et déterminer la portée des futurs travaux politiques possibles à la suite de l'adoption du NIS2 afin d'évaluer si l'élaboration de politiques supplémentaires est jugée souhaitable et/ou nécessaire.

Guide de différenciation entre personnes physiques et personnes morales

L'équipe responsable de l'EPDP reconnaît qu'il peut être nécessaire de faciliter et de normaliser les pratiques pour les parties contractantes qui décident de faire la distinction entre les personnes morales et les personnes physiques.

Pour faciliter la différenciation, l'équipe responsable de l'EPDP a élaboré les directives qui se trouvent dans la section ci-dessous. Dans cette directive, l'équipe responsable de l'EPDP suggère que les bureaux d'enregistrement pourraient envisager l'utilisation d'un champ qui indiquerait le type de titulaire de nom de domaine concerné (personne morale ou physique) et le type de données des titulaires de nom de domaine légaux qu'il concerne (personnelles/non personnelles). Ce concept d'identification du type de données d'enregistrement des noms de domaine en cause est également mentionné dans la Recommandation 9.4.4 de l'étape 2 de l'EPDP (réponse automatisée aux demandes de divulgation).

Dans la recommandation suivante, l'équipe responsable de l'EPDP décrit comment une partie contractante qui souhaite se différencier peut le faire en utilisant un ou plusieurs nouveaux champs pour saisir les résultats de cette différenciation.

Recommandation 1

L'équipe responsable de l'EPDP RECOMMANDE la création d'un ou de plusieurs champs afin de faciliter la distinction entre les données d'enregistrement des personnes morales et des personnes physiques et/ou si ces données d'enregistrement contiennent des données à caractère personnel ou non personnel. L'organisation ICANN DOIT coordonner avec la communauté technique, par exemple avec le groupe de travail consacré au RDAP, afin d'élaborer toutes les normes nécessaires associées à l'utilisation de ce ou de ces champs dans l'EPP et le RDDS.

Ce ou ces champs POURRAIENT être utilisés par les parties contractantes qui établissent une distinction entre les données d'enregistrement des personnes morales et des personnes physiques et/ou si ces données d'enregistrement contiennent des informations personnelles ou non personnelles. Pour plus de clarté, les parties contractantes POURRAIENT utiliser le ou les champs, ce qui signifie que si une partie contractante décidait de ne pas utiliser le ou les champs, ils pourraient être laissés vides ou ne pas exister. En outre, les parties contractantes POURRAIENT inclure le ou les champs dans une réponse RDDS.

Le SSAD, conformément aux recommandations de l'étape 2 de l'EPDP, DOIT appuyer le ou les champs afin de faciliter l'intégration entre le SSAD et les systèmes des parties contractantes. Ces champs doivent pouvoir contenir les valeurs suivantes :

Statut juridique

- La distinction de statut juridique n'a pas été faite (valeur par défaut)
- Non spécifié – le titulaire du nom enregistré et/ou l'agent d'enregistrement ne l'ont pas précisé
- Le titulaire du nom enregistré est une personne physique
- Le titulaire du nom enregistré est une personne morale

Données à caractère personnel

- La présence de données à caractère personnel n'a pas été déterminée (valeur par défaut)
- Non spécifié – le détenteur du nom enregistré et/ou l'agent d'enregistrement n'ont pas fait de spécification
- Les données d'enregistrement contiennent des informations à caractère personnel
- Les données d'enregistrement NE contiennent PAS d'informations à caractère personnel

• Réponse de l'équipe responsable de l'EPDP à la question ii

L'équipe responsable de l'EPDP a abordé sa tâche en examinant d'abord les directives qui seraient utiles aux bureaux d'enregistrement et aux opérateurs de registre qui choisissent de faire la distinction entre les enregistrements de personnes morales et de personnes physiques.
Définitions (à noter que ces définitions sont dérivées des travaux antérieurs liés à l'EPDP, comme indiqué ci-dessous) :

- EPDP-p1-IRT :[12] « publication », « publier » et « publié » signifie fournir des données d'enregistrement dans les services d'annuaire de données d'enregistrement accessibles au public.
- EPDP-p1-IRT :[13] « données d'enregistrement » désigne les valeurs des éléments de données recueillies auprès d'une personne physique ou morale ou générées par un bureau d'enregistrement ou un opérateur de registre, dans les deux cas en relation avec un nom enregistré conformément à l'article 7 de la présente politique.

[12] Voir https://docs.google.com/document/d/1SVFkoI6RmrVVz--RrVLSOj1bmz1qLb7_JTuvt7At4Uo/edit.
[13] Ibid.

- Rapport final de l'étape 1 de l'EPDP :[14] « divulgation » signifie l'activité de traitement aux termes de laquelle l'autorité de contrôle accepte la responsabilité de la divulgation d'informations à caractère personnel à des tiers sur demande.

Renseignements généraux et observations de l'équipe responsable de l'EPDP
En élaborant les directives ci-dessous, l'équipe responsable de l'EPDP tient à rappeler au conseil et à la communauté en général ce qui suit :

Portée du RGPD et d'autres lois sur la protection des données

A. Le RGPD et d'autres lois sur la protection des données définissent les exigences relatives à la protection des données à caractère personnel des personnes physiques. Il ne protège pas les données à caractère personnel des personnes morales et les données à caractère non personnel.
B. Le RGPD ne s'applique pas au traitement des données à caractère personnel de personnes morales et notamment les initiatives constituées sous la forme de personnes morales, dont le nom et le statut de la personne morale et les coordonnées de cette personne. Toutefois, lorsque les renseignements d'une personne physique sont utilisés en relation avec une personne morale, par exemple en tant que représentant d'une entreprise, les données de cette personne physique demeurent protégées en tant que données à caractère personnel en vertu du RGPD.
C. La distinction entre si les titulaires de nom de domaine sont des personnes physiques ou morales ne peut pas être déterminante quant à la façon dont les informations devraient être traitées (rendues publiques ou masquées), car les données fournies par les personnes morales pourraient inclure des données à caractère personnel protégées par les lois sur la protection des données, comme le RGPD.
D. Bien que le RGPD ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, les principes du RGPD, dont certains sont décrits ci-dessous, peuvent toujours s'appliquer si les données à caractère personnel d'une personne physique sont traitées dans le cadre du processus de différenciation et doivent être prises en compte, le cas échéant, par les parties contractantes. Conformément aux principes énoncés à l'article 5 du RGPD :
    a. Légalité, équité et transparence : « Tout traitement de données à caractère personnel doit être légal, équitable et transparent. Il devrait être clair et transparent pour les individus que les données à caractère personnel les concernant sont collectées, utilisées, consultées ou traitées de quelque manière que ce soit, et dans la mesure dans laquelle les données à caractère personnel sont, ou seront, traitées ». Le principe de transparence concerne, en particulier, les informations aux personnes concernées sur l'identité de l'autorité de contrôle et les objectifs du

[14] Voir https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf.

traitement[.][15] [. . .]
Si la base juridique est le consentement, « la mise à disposition d'informations aux personnes concernées avant d'obtenir leur consentement est essentielle pour leur permettre de prendre des décisions éclairées, de comprendre ce à quoi elles s'accordent et, par exemple, d'exercer leur droit de retirer leur consentement ».[16]

b. Limitation de l'utilisation à certaines fins : « Les données à caractère personnel devront être [. . .] collectées à des fins spécifiques, explicites et légitimes et traitées par la suite de manière compatible avec ces objectifs ».[17]

c. Minimisation de données : « Limiter la quantité de données à caractère personnel collectées à ce qui est nécessaire pour atteindre l'objectif ».[18]

d. Responsabilité : Le principe de responsabilité du RGPD « oblige les entreprises à démontrer (et, dans la plupart des cas, à documenter) la manière dont elles se conforment aux principes de protection des données lorsqu'elles effectuent des transactions commerciales ».[19]

Recommandations pertinentes de l'étape 1 de l'EPDP[20]

E. La Recommandation 6 de l'étape 1 de l'EPDP[21] stipule que, « dès que cela sera commercialement raisonnable, le bureau d'enregistrement devra donner la possibilité au titulaire d'un nom enregistré d'accorder son consentement à la publication des informations de contact expurgées ainsi que de l'adresse électronique, dans le RDS du bureau d'enregistrement parrain ».

[15]Consulter : Principes directeurs de la Commission irlandaise pour la protection des données sur le droit d'être informé. (https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-1 4-rgpd) et les directives du Groupe de travail Article 29 sur la transparence en vertu de la Règlementation 2016/679, sections 6 et 7 (telles qu'adoptées par le CEPD) (https://ec.europa.eu/newsroom/article29/items/622227).

[16] Voir les directives du CEPD, 05/2020, directives 05/2020 sur le consentement en vertu du la section 3.3 du règlement 2016/679.

[17] Voir l'article 5(1)(b) du RGPD ; voir aussi les directives du Bureau du Commissaire à l'information du Royaume-Uni sur la limitation de l'utilisation à certaines fins, (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulatio n-gdpr/principles/purpose-limitation/).

[18] Voir les directives du CEPD, 04/2019, protection des données dès la conception et par défaut, section 3.5 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_a nd_by_default_v2.0_en.pdf) et l'article 5.1 (c) du RGPD.

[19]Consulter : Directive de la Commission irlandaise pour la protection des données sur la responsabilité (https://www.dataprotection.ie/en/organizations/know-your-obligations/accountability-obligation) ; voir aussi les directives du CEPD, 04/2019, protection des données dès la conception et par défaut, section 3.9 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_a nd_by_default_v2.0_en.pdf.

[20] Note : la Recommandation 12 de l'étape 1 de l'EPDP concernant le champ « organisation » pourrait, une fois mise en œuvre, aider également les parties contractantes à faire la distinction entre personnes morales et personnes physiques, si elles le souhaitaient.

[21] Pour de plus amples renseignements sur l'état d'avancement de la mise en œuvre des recommandations de l'étape 1 de l'EPDP, veuillez consulter le site https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en.

F. En vertu de la Recommandation 17 de l'étape 1 de l'EPDP, les « bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et personnes morales sans, toutefois, être tenus de le faire ».

Recommandations pertinentes de l'étape 2 de l'EPDP

G. Selon l'étape 2[22] de la Recommandation 9.4.4 du rapport final qui traite de l'automatisation du traitement du SSAD : « L'équipe responsable de l'EPDP recommande que les types de requêtes de divulgation suivantes, désignées aptes du point de vue juridique à l'automatisation totale au titre du RGPD (saisie et traitement des décisions de divulgation) DOIVENT être automatisés dès le lancement du SSAD[.] [. . .] Aucune donnée à caractère personnel sur le registre d'enregistrement qui a été précédemment divulgué par la partie contractante ». La présente recommandation 9.4.4 porte généralement sur l'automatisation de la divulgation des registres qui ne comprennent pas de données à caractère personnel.[23]

H. Conformément à la Recommandation 8.7.1 du rapport final de l'étape 2, si la partie contractante reçoit une demande de l'administrateur de passerelle centrale du SSAD et que la partie contractante a déterminé qu'il s'agit d'une demande valide, « si, suite à l'évaluation des données sous-jacentes, la partie contractante détermine raisonnablement que la divulgation des éléments de données demandés n'entraînerait pas la divulgation de données à caractère personnel, la partie contractante DOIT divulguer les données, à moins que la divulgation ne soit interdite par la loi applicable ».

Modèles commerciaux des bureaux d'enregistrement

I. Les bureaux d'enregistrement utilisent différents modèles commerciaux (vente au détail, vente en gros, protection de la marque, autres), et les directives uniques ou excessivement normatives peuvent ne pas tenir compte correctement de la gamme de modèles commerciaux des bureaux d'enregistrement et des différents flux de processus que les différents modèles commerciaux pourraient exiger. Au lieu de cela, toute directive devrait permettre aux bureaux d'enregistrement de mettre en œuvre la différenciation d'une manière qui correspond le mieux à leur modèle commercial et de réduire les risques associés à la différenciation à un niveau acceptable pour ce bureau d'enregistrement en particulier. Par exemple, la différenciation au moment de l'enregistrement peut ne pas être pratique en toutes circonstances, y compris pour certains modèles commerciaux des bureaux d'enregistrement.

[22] Notez que les recommandations de l'étape 2 de l'EPDP sont soumises au Conseil d'administration de l'ICANN pour examen/approbation.

[23] Veuillez noter que les détails exacts de la mise en œuvre de cette recommandation doivent être déterminés par l'organisation ICANN en collaboration avec l'équipe de révision de la mise en œuvre, une fois que le Conseil d'administration de l'ICANN aura approuvé les recommandations.

Directives proposées

Recommandation 2

La recommandation de l'équipe responsable de l'EPDP est que les parties contractantes qui choisissent de se différencier en fonction du type de personne DEVRAIENT suivre les directives[24] ci-dessous et documenter clairement toutes les étapes de traitement des données. Cependant, il n'est pas du ressort ou de la responsabilité de l'équipe responsable de l'EPDP de prendre une décision finale concernant les risques juridiques, car cette responsabilité appartient en fin de compte à/aux autorité(s) de contrôle.
Le RGPD protège les personnes physiques en ce qui concerne le traitement de leurs données à caractère personnel. Le RGPD ne couvre pas le traitement de données à caractère personnel ayant trait aux personnes morales et notamment les entreprises établies comme des personnes morales y compris le nom et le type de personne morale et ses détails de contact. [Considérant 14, RGPD] Cette figure permet généralement la divulgation des données des personnes morales parce qu'elles ne relèvent pas de la compétence du RGPD ; toutefois, lors du traitement des données des personnes morales, les parties contractantes devraient mettre en place des mesures de protection pour garantir que les données d'identification personnelle concernant une personne physique ne soient pas divulguées dans des données marquées comme appartenant à une personne morale, car il s'agit d'un exemple d'information qui *entre* dans le champ d'application du RGPD. Pour plus d'informations sur cette distinction, veuillez vous référer à la lettre du Comité européen de la protection des données, à partir de la p. 4.

1. Les titulaires de noms de domaine devraient pouvoir s'auto-identifier en tant que personnes physiques ou morales. Les bureaux d'enregistrement devraient transmettre cette option d'autoidentification comme personne physique ou morale (i) au moment de l'enregistrement, ou sans délai indu après l'enregistrement,[25] et (ii) au moment où le titulaire de nom de domaine met à jour ses informations de contact ou sans délai indu après la mise à jour des coordonnées.
2. Tout processus de différenciation doit garantir que les données des personnes physiques soient expurgées par le RDDS public, à moins que la personne concernée n'ait donné son consentement à les publier ou que ces données puissent être publiées en raison d'une autre raison légale en vertu du RGPD, conformément à l'approche de « protection des données dès la conception et par défaut » énoncée à l'article 25 du RGPD.
3. Dans le cadre de la mise en œuvre, les bureaux d'enregistrement devraient envisager d'utiliser le(s) champ(s) décrit(s) dans la Recommandation 1 dans le

[24] Veuillez noter que les agents de liaison de l'organisation ICANN ont fourni à l'équipe responsable de l'EPDP les commentaires suivants sur la façon dont cette orientation serait mise en œuvre une fois adoptée : https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html.
[25] Pour plus de clarté, les bureaux d'enregistrement devraient s'assurer que si le titulaire n'a pas l'option de s'auto-identifier au moment de l'enregistrement, l'option devrait être fournie au plus tard 15 jours après la date de l'enregistrement.

RDDS, le SSAD ou dans leurs propres ensembles de données qui indiqueraient le type de personne (morale ou physique) et, s'il est légal, le type de données dont il s'agit (données à caractère personnel ou non personnel). Un tel marquage pourrait faciliter l'examen des demandes de divulgation et des exigences d'automatisation par le biais du SSAD et l'affichage des données à caractère non personnel des personnes morales par des systèmes autres que le SSAD (comme le Whois ou le RDAP). Un mécanisme de signalement pourrait également vous aider à indiquer les modifications apportées au type de données dans le(s) champ(s) de données d'enregistrement.

4. Les bureaux d'enregistrement devraient s'assurer qu'ils communiquent clairement la nature et les conséquences du fait qu'un titulaire de nom de domaine ne s'identifie comme personne morale. Ces communications devraient inclure :
    c. Une explication de ce qu'est une personne morale dans un langage simple et facile à comprendre.
    d. Des directives du bureau d'enregistrement à l'intention du titulaire de nom de domaine (personne concernée)[26] concernant les conséquences possibles de :
        i. L'identification de leurs données d'enregistrement de nom de domaine comme correspondant à une personne morale ;
        ii. La confirmation de la présence de données à caractère personnel ou non personnel, et ;
        iii. La fourniture de son consentement.[27] Cela est également conforme à l'article 3.7.7.4 du contrat d'accréditation de bureau d'enregistrement (RAA).
5. Si les titulaires s'identifient comme des personnes morales et confirment que leurs données d'enregistrement n'incluent pas de données à caractère personnel, les bureaux d'enregistrement devraient publier les données d'enregistrement dans les services d'annuaire des données d'enregistrement accessibles au public.
6. Les titulaires de noms de domaine (personnes concernées) doivent avoir un moyen facile pour corriger les erreurs possibles.
7. La distinction entre les titulaires de noms de domaine qui sont des personnes morales et ceux qui sont des personnes physiques ne peut pas déterminer à elle seule la façon dont les informations devraient être traitées (rendues publiques ou masquées), car les données fournies par les personnes morales pourraient inclure des données à caractère personnel protégées par la législation sur la protection des données, comme le RGPD.

Recommandation 3

L'équipe responsable de l'EPDP recommande, conformément aux exigences de l'article 40 du RGPD en matière de codes de conduite, que les directives élaborées ci-dessus

[26] Remarque : le titulaire pourrait ne pas toujours être la personne concernée, mais dans toutes les circonstances, un avis ou un consentement approprié doit être fourni à toutes les parties et par toutes les parties, conformément à la loi sur la protection des données en vigueur.

[27] Voir aussi https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

concernant la différenciation entre personne physique et personne morale soient prises en compte par tout travail futur possible au sein de l'ICANN par les autorités de contrôle et les responsables du traitement concernés en relation avec l'élaboration d'un Code de conduite du RGPD. Pour éviter tout doute, le présent Code de conduite est distinct du Code de conduite mentionné dans le RAA et/ou les contrats de registre. Conformément au considérant 99 du RGPD, « lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations ».

Trois exemples de scénarios

(Remarque : ces scénarios sont des illustrations de la façon dont un bureau d'enregistrement pourrait appliquer les directives ci-dessus. Ces scénarios NE doivent PAS être considérés comme des directives).

L'équipe responsable de l'EPDP a identifié trois scénarios de haut niveau différents pour déterminer comment la différenciation pourrait se produire en fonction de la personne responsable et du moment de cette différenciation. Il convient de noter que d'autres approches et/ou une combinaison de ces approches pourraient être possibles.

1. **Autoidentification de la personne concernée au moment de la collecte/de l'enregistrement des données**

a. Le bureau d'enregistrement informe le titulaire de nom de domaine (conformément à la directive 3 ci-dessus) et demande au titulaire (personne concernée) au moment de la collecte des données d'enregistrement de désigner le type de personne, morale ou physique. Le bureau d'enregistrement doit également demander au titulaire de confirmer si seules des données à caractère non personnel sont fournies pour le type de personne morale.[28]

b. Si le titulaire (personne concernée) s'est identifié comme une personne morale et a fourni une confirmation que les données d'enregistrement n'incluent pas de données à caractère personnel, le bureau d'enregistrement doit (i) communiquer avec les coordonnées fournies pour vérifier la réclamation du titulaire ;[29] (ii) inclure

[28] Notez que la confirmation que seules des données à caractère non personnel sont fournies peut également se produire à un autre moment. Toutefois, jusqu'à ce que le titulaire confirme qu'aucune donnée à caractère personnel n'apparaît parmi les données d'enregistrement, le bureau d'enregistrement n'inclut pas les données d'enregistrement sur la divulgation automatisée.

[29] Selon les directives fournies par Bird & Bird, « cette méthode de vérification est recommandée et contribuera à réduire les risques. Cette réduction des risques sera plus importante si un délai de grâce raisonnable est prévu dans lequel l'objection peut être déposée, avant que les données en question ne soient publiées dans les données d'enregistrement » et que « l'exigence d'une réponse affirmative aux courriers de vérification semble trop prudente, sauf si et jusqu'à ce que des études montrent que les mesures adoptées ne tiennent pas de quantités très importantes de données à caractère personnel en dehors des données d'enregistrement publiées. Toutefois, si un e-

l'ensemble de données d'enregistrement sur la divulgation automatisée en réponse aux requêtes du SSAD; et (iii) publier les données (pour fournir les données d'enregistrement dans les services d'annuaire de données d'enregistrement accessibles au public).

c. Si le titulaire (personne concernée) s'est autoidentifié comme une personne physique ou a confirmé la présence de données à caractère personnel, le bureau d'enregistrement n'inclut pas ces données d'enregistrement parmi les données divulguées et publiées automatiquement à moins que la personne concernée donne son consentement à la publication.[30]

2. Autoidentification de la personne concernée au moment de la mise à jour de l'enregistrement[31]

a. Le bureau d'enregistrement recueille les données d'enregistrement et les expurge provisoirement.

b. Le bureau d'enregistrement informe le titulaire de nom de domaine (conformément à la directive 3 ci-dessus) et demande au titulaire (personne concernée) de s'auto-identifier comme une personne morale ou physique. Le bureau d'enregistrement devrait également demander à un titulaire de nom de domaine auto-identifié comme une personne morale de confirmer qu'aucune donnée à caractère personnel n'a été fournie.[32]

c. Le titulaire de nom de domaine (personne concernée) s'identifie comme étant une personne morale ou personne physique et confirme qu'aucune donnée à caractère personnel n'a été fournie après la mise à jour. Par exemple, le titulaire de nom de domaine peut confirmer le type de personne au moment de la vérification initiale des données, en réponse à sa réception de l'e-mail de rappel de données Whois pour les enregistrements existants, ou par l'intermédiaire d'un avis distinct demandant l'autoidentification.[33]

d. Si la personne concernée s'auto-identifie comme une personne morale et confirme que les données d'enregistrement ne comprennent pas de données à caractère personnel, le bureau d'enregistrement devrait (i) communiquer avec les coordonnées fournies pour vérifier la réponse du titulaire ;[34] (ii) inclure l'ensemble

---

mail de vérification « a été retourné » (c'est-à-dire qu'une partie contractante sait qu'il n'a pas été livré), il serait préférable que la publication ne se produise pas ».

[30] Notez que la personne concernée n'est peut-être pas la partie qui exécute le processus, mais qu'elle a peut-être demandé à un tiers de le faire. Dans de telles circonstances, il pourrait ne pas être possible de documenter le consentement.

[31] On s'attend à ce que, pour ce scénario, un échéancier similaire soit suivi, comme c'est le cas actuellement dans la spécification de l'exactitude du WHOIS du contrat d'accréditation de bureaux d'enregistrement (voir https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy).

[32] Notez que la confirmation que seules des données à caractère non personnel sont fournies peut également se produire à un autre moment. Toutefois, jusqu'à ce que le titulaire confirme qu'aucune donnée à caractère personnel n'apparaît parmi les données d'enregistrement, le bureau d'enregistrement n'inclut pas les données d'enregistrement sur la divulgation automatisée.

[33] À noter que la mise en œuvre de la Recommandation 12 de l'étape 1 de l'EPDP (domaine de l'organisation) peut faciliter le processus d'autoidentification.

[34] Selon les directives fournies par Bird & Bird, « cette méthode de vérification est recommandée et contribuera à réduire les risques. Cette réduction des risques sera plus importante si un délai de grâce raisonnable est prévu dans

des données d'enregistrement dans la divulgation automatisée en réponse aux demandes du SSAD ; et (iii) publier les données.

3. Le bureau d'enregistrement détermine le type du titulaire de nom de domaine en fonction des données fournies

a. Le bureau d'enregistrement recueille les données d'enregistrement et les expurge provisoirement.
b. Le bureau d'enregistrement utilise les données recueillies pour déterminer s'il s'agit d'une personne morale ou physique.[35]
c. Si le bureau d'enregistrement déduit qu'il s'agit d'une personne morale et que, par la suite, le titulaire de nom de domaine (personne concernée) est informé (conformément à la directive 3 ci-dessus) et confirme qu'aucune donnée à caractère personnel n'est présente, le bureau d'enregistrement devrait (i) communiquer avec les coordonnées fournies pour vérifier la réponse du titulaire de nom de domaine[36] (ii) inclure l'ensemble de données d'enregistrement dans la divulgation automatisée en réponse aux demandes du SSAD et (iii) publier les données.
d. Si le bureau d'enregistrement a déduit que le titulaire de nom de domaine est une personne physique ou a détecté des données à caractère personnel, le bureau d'enregistrement ne devrait pas divulguer les données d'enregistrement à moins que le titulaire de nom de domaine ne donne son consentement à la publication ou que le bureau d'enregistrement divulgue les données en réponse à une demande de divulgation légitime.

L'équipe responsable de l'EPDP reconnaît que, dans tous les scénarios ci-dessus, il existe une possible erreur d'identification, ce qui pourrait entraîner la divulgation involontaire de données à caractère personnel. À cet égard, l'équipe responsable de l'EPDP encourage la révision du mémo de Bird & Bird, qui se trouve également à l'annexe F, en particulier aux sections 11.1-2, 13, 14.3 et 18.

lequel l'objection puisse être déposée, avant que les données en question ne soient publiées dans les données d'enregistrement » et que « l'exigence d'une réponse affirmative aux courriers de vérification semble trop prudente, sauf si et jusqu'à ce que des études montrent que les mesures adoptées ne tiennent pas de quantités très importantes de données à caractère personnel en dehors des données d'enregistrement publiées. Toutefois, si un email de vérification « a été retourné » (c'est-à-dire qu'une partie contractante sait qu'il n'a pas été livré), il serait préférable que la publication ne se produise pas ».

[35] Certains membres de l'équipe responsable de l'EPDP ont noté qu'il pourrait y avoir des risques pour le bureau d'enregistrement s'il devait déduire une différenciation sans la participation du titulaire de nom de domaine (personne concernée).

[36] Selon les directives fournies par Bird & Bird, « cette méthode de vérification est recommandée et contribuera à réduire les risques. Cette réduction des risques sera plus importante si un délai de grâce raisonnable est prévu dans lequel l'objection peut être déposée, avant que les données en question ne soient publiées dans les données d'enregistrement » et que « l'exigence d'une réponse affirmative aux courriers de vérification semble trop prudente, sauf si et jusqu'à ce que des études montrent que les mesures adoptées ne tiennent pas de quantités très importantes de données à caractère personnel en dehors des données d'enregistrement publiées. Toutefois, si un email de vérification « a été retourné » (c'est-à-dire qu'une partie contractante sait qu'il n'a pas été livré), il serait préférable que la publication ne se produise pas ».

3.2 Faisabilité de contacts uniques

L'équipe responsable de l'EPDP a été chargée par le conseil de la GNSO de répondre aux deux questions suivantes :

i. S'il est possible que les contacts uniques aient une adresse électronique anonyme uniforme et, si possible, si cela devait être obligatoire.
ii. Si cela était possible, mais pas obligatoire, quelles directives devraient être fournies, le cas échéant, aux parties contractantes souhaitant mettre en place des adresses e-mail anynomisées uniformes.

Le conseil a également indiqué que « les groupes qui ont demandé du temps supplémentaire pour examiner ce sujet, entre autres l'ALAC, le GAC et le SSAC, seront responsables de présenter des propositions concrètes pour aborder ce sujet ».[37]

Pour répondre à ces questions, l'équipe responsable de l'EPDP a commencé par un examen des directives juridiques reçues au cours de l'étape 1 et a examiné les propositions possibles qui pourraient fournir des garanties suffisantes pour traiter les questions signalées dans le mémo juridique.

L'équipe responsable de l'EPDP a noté comment une adresse électronique anonymisée a eu un impact sur les mesures de protection nécessaires et les impacts possibles sur les personnes concernées et donc sur la faisabilité. L'équipe a examiné les effets et les bénéfices de deux utilisations d'un tel contact, conformément aux deux objectifs distincts énoncés par ceux qui préconisent des contacts uniques, à savoir 1) la capacité de communiquer rapidement et efficacement avec le titulaire de nom de domaine, et 2) la corrélation entre les enregistrements enregistrés par le même titulaire de nom de domaine.

L'équipe responsable de l'EPDP a également observé que la terminologie utilisée dans le contexte de cette discussion pourrait bénéficier d'une plus grande précision. L'équipe responsable de l'EPDP a chargé le comité juridique de proposer une terminologie mise à jour et de passer en revue les questions de clarification à envoyer à Bird & Bird. Le Comité juridique a proposé un ensemble de définitions de travail, qu'il a soumis à l'équipe responsable de l'EPDP le 23 février 2021 (voir ici). En outre, le Comité juridique a élaboré un ensemble de questions de suivi qu'il a soumises à Bird & Bird, et ce dernier a fourni une réponse le 9 avril 2021. L'équipe responsable de l'EPDP a examiné ces directives juridiques dans l'élaboration de sa réponse aux questions du conseil.

[37] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf

Définitions

À la suite de l'examen initial de la première question de la charte, l'équipe responsable de l'EPDP a noté que le terme anonyme a été mal appliqué à cette question. L'équipe responsable de l'EPDP a noté que, pour que les données soient véritablement rendues anonymes en vertu du RGPD, la personne concernée ne pourrait pas être identifiable directement ou indirectement « par le contrôleur ou par quelqu'un d'autre ». (Voir l'article 26 du RGPD) Avec cette compréhension, l'équipe responsable de l'EPDP a choisi de concentrer sa question sur la pseudonymisation des données et a peaufiné davantage les définitions dans ses questions de suivi adressées à Bird & Bird.

« Contact e-mail par titulaire de nom de domaine », signifie « un e-mail pour tous les domaines enregistrés par un titulaire de nom de domaine unique [parrainé par un bureau d'enregistrement donné] OU [entre bureaux d'enregistrement], [38] qui se veut être des données pseudonymes[39] lorsqu'elles sont traitées par des parties non contractantes. [40]»[41]

« Contact e-mail pour chaque enregistrement », signifie « un e-mail à usage unique distinct pour chaque nom de domaine enregistré par un titulaire de nom de domaine unique, qui est destiné à être des données anonymes lorsqu'elles sont traitées par des parties non contractantes ». [42]

Notez, toutefois, que même en adoptant ces définitions, Bird & Bird a indiqué que les contacts par e-mail pour chaque titulaire ou pour chaque enregistrement créent « une

[38] Le Comité juridique a été chargé d'examiner les directives juridiques reçues au cours de l'étape 2 et de déterminer si des directives juridiques supplémentaires s'avéraient nécessaires. Dans un premier temps, le Comité juridique a choisi de peaufiner la terminologie utilisée dans sa question de l'étape 2 ; plus précisément, au lieu de se référer à « anonymisation » et « pseudonymisation », le Comité juridique a accepté d'utiliser les termes « contact e-mail pour chaque enregistrement » et « contact e-mail par titulaire de nom de domaine » parce que l'équipe responsable de l'EPDP a noté que l'utilisation précédente du terme « anonymisation » était incompatible avec la définition d'anonyme dans le RGPD. Dans sa formation de nouvelles définitions, le Comité juridique a noté qu'un contact par titulaire de nom de domaine pourrait exister au sein du bureau d'enregistrement parrain OU dans tous les bureaux d'enregistrement. Le Comité juridique a toutefois déterminé que la question de savoir si le contact pour le titulaire de nom de domaine devait exister au sein du bureau d'enregistrement parrain ou entre bureaux d'enregistrement était une question de politique pour l'équipe responsable de l'EPDP, et non une question juridique pour le Comité juridique ou Bird & Bird. En conséquence, le Comité juridique a choisi de laisser les deux options entre parenthèses, et Bird & Bird a présenté la légalité et les risques associés des deux options dans le mémo de l'étape 2A.

[39] Certains membres de l'équipe responsable de l'EPDP croient que le terme pseudonyme devrait être changé par anonyme. Cependant, il convient de noter que la définition fournie ci-dessus a été incluse dans la question et les directives de Bird & Bird.

[40] Certains membres de l'équipe responsable de l'EPDP estiment que « par des parties non contractantes » devrait être remplacé par « par des parties autres que l'autorité de contrôle ». Cependant, il convient de noter que la définition fournie ci-dessus a été incluse dans la question et les directives de Bird & Bird.

[41] Certains membres de l'équipe responsable de l'EPDP ont suggéré d'étendre la définition pour inclure « OU [dans les TLD exploités par le même fournisseur de services de registre] ». Cependant, il convient de noter que la définition fournie ci-dessus a été incluse dans la question et les directives de Bird & Bird.

[42] Certains membres de l'équipe responsable de l'EPDP estiment que « par des parties non contractantes » devrait être remplacé par « par des parties autres que l'autorité de contrôle ». Cependant, il convient de noter que la définition fournie ci-dessus a été incluse dans la question et les directives de Bird & Bird.

forte probabilité que la publication ou la divulgation automatisée de ces adresses e-mail soit considérée comme le traitement de données à caractère personnel ».

Renseignements généraux et observations de l'équipe responsable de l'EPDP

En élaborant sa réponse aux questions du conseil, l'équipe responsable de l'EPDP tient à rappeler au conseil et à la communauté en général ce qui suit :

Annexe à la spécification temporaire (« Questions importantes pour la considération de la communauté »)

- La spécification temporaire relative aux données d'enregistrement des gTLD, adoptée par le Conseil d'administration de l'ICANN le 17 mai 2018, incluait le libellé suivant dans l'annexe intitulé « questions importantes à prendre en considération par la communauté » :

  > « Aborder la faisabilité d'exiger des contacts uniques pour avoir une adresse e-mail anonyme uniforme dans tous les enregistrements de noms de domaine auprès d'un bureau d'enregistrement donné, tout en assurant la sécurité, la stabilité et le respect des exigences de l'article 2.5.1 de l'annexe A ».

  À titre de référence, la section 2.5.1 de l'annexe A stipule que : « Le bureau d'enregistrement DOIT fournir une adresse électronique ou un formulaire Web afin de faciliter la communication via e-mail avec le contact concerné, mais NE DOIT PAS indiquer l'adresse électronique du contact ou le contact lui-même ».

Recommandations pertinentes de l'étape 1 de l'EPDP

Recommandation 6 de l'étape 1 de l'EPDP
L'équipe responsable de l'EPDP recommande que, dès que cela sera commercialement raisonnable, le bureau d'enregistrement devra donner la possibilité au titulaire de nom enregistré d'accorder son consentement à la publication des coordonnées expurgées, ainsi que de l'adresse électronique, dans le RDS pour le bureau d'enregistrement parrain.

Recommandation 13 de l'étape 1 de l'EPDP
1) L'équipe responsable de l'EPDP recommande que le bureau d'enregistrement DOIVE fournir une adresse électronique ou un formulaire Web afin de faciliter la communication via e-mail avec le contact concerné, mais NE DOIVE PAS indiquer l'adresse électronique du contact ou le contact lui-même à moins que le titulaire du nom enregistré, conformément à la Recommandation 6, ait consenti à la publication de son adresse électronique.
2) L'équipe responsable de l'EPDP recommande que les bureaux d'enregistrement DOIVENT de tenir des fichiers journal qui ne devront contenir aucune information à caractère personnel, et qui devront contenir la confirmation qu'un relai de la

communication entre le demandeur et le titulaire du nom enregistré a eu lieu, sans inclure l'origine, ni le destinataire, ni le contenu du message. Ces dossiers seront mis à la disposition de l'ICANN à des fins de conformité, sur demande. Rien dans la présente recommandation ne devrait être interprété comme empêchant le bureau d'enregistrement de prendre des mesures raisonnables et appropriées pour prévenir l'utilisation malveillante du processus de contact du titulaire de nom de domaine.

> *Notez que, au cours des délibérations de l'étape 2A, certains membres de l'équipe responsable de l'EPDP ont soulevé la question des formulaires Web et des questions potentielles liées à l'utilisation de tels formulaires. Il a été noté que même si l'option d'un formulaire Web fait partie de la Recommandation 13 de l'étape 1 de l'EPDP, cette exigence est la même que dans la spécification temporaire qui est en vigueur depuis le 25 mai 2018. Les consultations avec l'organisation ICANN ont indiqué que les formulaires Web n'ont pas été une source importante de plaintes et que cela n'a pas été soulevé comme un problème dans le contexte de l'équipe de révision de la mise en œuvre chargée de mettre en œuvre la recommandation de l'étape 1.[43] Certains membres sont d'avis que, même s'il y a des problèmes, ceux-ci ne sont pas dans la portée de l'équipe responsable de l'EPDP, compte tenu de ses attributions limitées. L'équipe responsable de l'EPDP n'a pas été en mesure de s'entendre sur la façon de procéder à ce sujet.

Recommandation 14 de l'étape 1 de l'EPDP
Dans le cas d'un enregistrement de nom de domaine pour lequel un service d'anonymisation ou d'enregistrement fiduciaire « affilié » est utilisé (par exemple, lorsque les données associées à une personne physique sont masquées), le bureau d'enregistrement (et l'opérateur de registre, le cas échéant) DOIT inclure dans le RDDS public, et retourner en réponse à toute requête, les données à caractère non personnel complètes du RDDS sur le service d'anonymisation ou d'enregistrement fiduciaire, ce qui POURRAIT également comprendre l'adresse électronique pseudonymisée existante et fournie par ce service.
Considération de ce sujet à l'étape 2 de l'EPDP

Le rapport final de l'étape 2 de l'EPDP a signalé que :

> « La faisabilité d'une adresse e-mail anonymisée uniforme pour les contacts uniques : L'équipe responsable de l'EPDP a reçu des directives juridiques indiquant que la publication d'adresses e-mail masquées uniformes entraîne la publication de données à caractère personnel ; ce qui montre qu'il peut ne pas être possible de publier une grande échelle d'adresses e-mail masquées uniformes aux termes du RGPD. D'autres travaux sur cette question sont en cours d'examen par le conseil de la GNSO ».

[43] Voir https://community.icann.org/x/I4GBCQ.

L'équipe responsable de l'EPDP a proposé des réponses aux questions du conseil

i. S'il est possible que les contacts uniques aient une adresse électronique anonyme uniforme et, si possible, si cela devait être obligatoire.
ii. Si cela était possible mais pas obligatoire, quelles directives devraient être fournies, le cas échéant, aux parties contractantes souhaitant mettre en place des adresses e-mail anynomisées uniformes.

• Réponse de l'équipe responsable de l'EPDP à la question i.

L'équipe responsable de l'EPDP reconnaît qu'il pourrait être techniquement possible d'avoir un contact e-mail par titulaire de nom de domaine ou un contact e-mail pour chaque enregistrement.[44] Certaines parties prenantes voient des risques et manifestent d'autres préoccupations[45] qui empêchent actuellement l'équipe responsable de l'EPDP de recommander d'exiger aux parties contractantes qu'une adresse électronique par titulaire de nom de domaine ou une pour chaque enregistrement soit accessible au public. L'équipe responsable de l'EPDP note en effet que certains groupes de parties prenantes ont exprimé les avantages de 1) un contact e-mail pour chaque enregistrement à des fins de joignabilité, car des préoccupations ont été exprimées quant à la convivialité des formulaires Web et 2) un contact e-mail par titulaire de nom de domaine à des fins de corrélation de l'enregistrement.[46]

• Réponse de l'équipe responsable de l'EPDP à la question ii

Recommandation 4

La recommandation de l'équipe responsable de l'EPDP est que les parties contractantes qui choisissent de publier une adresse e-mail pseudonymisée par titulaire de nom de domaine ou pour chaque enregistrement dans le RDDS accessible au public devraient évaluer les directives juridiques obtenues par l'équipe responsable de l'EPDP sur ce sujet (voir Annexe F), ainsi que toute autre directive pertinente fournie par les autorités de protection des données pertinentes.

[44] Certains membres de l'équipe responsable de l'EPDP notent que, même si cela est techniquement possible, d'autres facteurs liés aux efforts requis pour mettre en œuvre une telle fonctionnalité devraient être pris en compte pour déterminer la viabilité globale.
[45] Tel que 1) il n'est pas clair que le travail de mise en œuvre d'un tel concept soit justifié par l'avantage potentiel. 2) de plus, il n'est pas clair que les objectifs, tels que présentés, soient effectivement atteints ou le plus atteints possible en exigeant des adresses e-mail pour chaque enregistrement ou par titulaire de nom de domaine.
[46] La capacité d'identifier quels domaines un titulaire de nom de domaine particulier a enregistrés est importante pour les forces de l'ordre et pour les enquêtes de cybersécurité vis-à-vis des mauvais acteurs qui enregistrent souvent de nombreux domaines à des fins malveillantes.

Lors de l'évaluation des risques, des avantages et des garanties associés à la publication d'une adresse e-mail pseudonymisée par titulaire de nom de domaine ou pour chaque enregistrement dans le RDDS accessible au public, les parties contractantes devraient au moins considérer :

- Les adresses e-mail des personnes physiques pour chaque enregistrement et par titulaire de nom de domaine sont probablement des données à caractère personnel (c'est-à-dire, aucune des deux approches ne crée de données anonymes telles que définies dans le RGPD). Ces données sont probablement des données à caractère personnel du point de vue de l'autorité de contrôle et de tiers.
- Toutefois, même si l'on considère les données à caractère personnel, le masquage des adresses e-mail offre des avantages par rapport à la publication des adresses e-mail réelles des titulaires de nom de domaine, notamment : (i) démontrer une technique d'amélioration de la protection des données dès la conception et par défaut (Article 25 du RGPD) ; et (ii) une certaine réduction des risques pertinente lors de la réalisation d'une analyse d'équilibre d'intérêt légitime pour la divulgation de l'adresse e-mail masquée à des tiers.
- En somme, la publication d'une adresse e-mail pour chaque enregistrement comporte probablement moins de risques que la publication d'adresses e-mail par titulaire de nom de domaine en raison de la quantité d'informations qu'une partie peut potentiellement lier à une personne concernée en fonction d'un contact e-mail par titulaire de nom de domaine.
- Pour la publication des adresses e-mail pour chaque enregistrement et pour chaque titulaire de noms de domaine, les parties contractantes devraient adopter des mesures efficaces pour atténuer la disponibilité des coordonnées aux spammeurs.

4 Prochaines étapes

4.1 Prochaines étapes

Ce rapport final sera présenté au conseil de la GNSO à des fins d'examen et d'approbation. Si le rapport final était adopté par le conseil de la GNSO, il serait ensuite transmis au Conseil d'administration de l'ICANN pour examen et, éventuellement, pour son approbation.

Glossaire

1. Comité consultatif
Un comité consultatif est un organe consultatif formel constitué de représentants de la communauté Internet et chargé de donner des avis à l'ICANN sur un sujet ou un domaine politique spécifique. Un certain nombre de ces comités sont prévus dans les statuts constitutifs de l'ICANN et d'autres peuvent être créés selon les besoins. Les comités consultatifs ne possèdent aucune autorité légale pour agir au nom de l'ICANN. Ils présentent leurs conclusions et formulent des recommandations au Conseil d'administration de l'ICANN.

2. ALAC - Comité consultatif At-Large
Le Comité consultatif At-large (ALAC) de l'ICANN a pour mission d'étudier et de proposer des avis sur les activités de l'ICANN qui se rapportent aux intérêts des utilisateurs individuels de l'Internet (la communauté « At-Large »). En tant qu'organisation privée à but non lucratif, responsable de la gestion technique du système des noms de domaine et d'adresses de l'Internet, l'ICANN s'appuiera sur ALAC et son infrastructure de soutien pour assurer la participation et la représentation d'un large éventail d'intérêts des utilisateurs individuels.

3. Unité constitutive des utilisateurs commerciaux (BC)
L'Unité constitutive des utilisateurs commerciaux représente les utilisateurs commerciaux de l'Internet. Elle est l'une des unités constitutives appartenant au Groupe des représentants des entités commerciales (CSG) visé au chapitre 11.5 des statuts constitutifs de l'ICANN. La BC est l'une de parties prenantes et unités constitutives de l'organisation de soutien aux extensions génériques (GNSO) chargée de conseiller le Conseil d'administration de l'ICANN sur les questions de politique relatives à la gestion du système des noms de domaine.

4. ccNSO - Organisation de soutien aux extensions géographiques
La ccNSO est l'organisation de soutien chargée d'élaborer et de recommander au Conseil d'administration de l'ICANN des politiques mondiales relatives aux noms de domaine de premier niveau géographique. Il s'agit d'un forum permettant aux gestionnaires des domaines de premier niveau géographique de se rencontrer et de discuter des questions d'ordre mondial d'intérêt commun. La ccNSO sélectionne un des membres du Conseil d'administration.

5. ccTLD - Domaine de premier niveau géographique
Les ccTLD sont des domaines à deux caractères, tels que .UK (Royaume-Uni), .DE (Allemagne) et .JP (Japon), que l'on appelle des domaines de premier niveau géographique (ccTLD) et qui correspondent à un pays, à un territoire ou à toute autre localisation géographique. Les règles et les politiques qui régissent l'enregistrement des

noms de domaine dans les ccTLD varient de manière significative. Les registres ccTLD limitent l'utilisation des ccTLD aux citoyens des pays concernés.

Pour plus d'informations sur les ccTLD et pour consulter la base de données complète des ccTLD avec leurs gestionnaires correspondants, veuillez consulter le site Internet http://www.iana.org/cctld/cctld.htm.

6. Données d'enregistrement de nom de domaine
Les données d'enregistrement de nom de domaine, également appelées des données d'enregistrement, concernent l'information qui est fournie par les titulaires de noms de domaine lors de l'enregistrement d'un nom de domaine, et qui est collectée par les bureaux d'enregistrement et les opérateurs de registre. Une partie de ces informations est disponible pour le public. Les éléments de données nécessaires pour l'interaction entre les bureaux d'enregistrement de noms de domaine génériques de premier niveau (gTLD) accrédités par l'ICANN et les titulaires de noms de domaine sont spécifiés dans le RAA en vigueur. Pour les domaines de premier niveau géographique (ccTLD), les opérateurs de ces TLD établissent leurs propres politiques ou suivent celles de leurs gouvernements concernant la collecte et l'affichage des informations d'enregistrement.

7. Nom de domaine
En tant que composante du système des noms de domaine, le nom de domaine identifie des ressources du Protocole Internet telles qu'un site Internet.

8. DNS - Système des noms de domaine
Le « DNS » fait référence au système des noms de domaine sur Internet. Le système des noms de domaine (DNS) permet aux utilisateurs de se repérer plus facilement sur Internet. Chaque ordinateur connecté à l'Internet possède une adresse unique, comparable à un numéro de téléphone, qui se compose d'une chaîne numérique relativement complexe, appelée « adresse IP » (IP signifiant « Protocole Internet »). Les adresses IP sont difficiles à mémoriser. Le DNS facilite l'utilisation de l'Internet en permettant de remplacer cette adresse IP obscure par une chaîne alphabétique familière (le « nom de domaine »). Ainsi, au lieu de taper 207.151.159.3, vous pouvez saisir www.internic.net. C'est un procédé « mnémonique » qui facilite la mémorisation des adresses.

9. EPDP - Processus accéléré d'élaboration de politiques
Il s'agit de l'ensemble d'étapes formelles, telles que définies dans les statuts constitutifs de l'ICANN, destinées à orienter la mise en place, la révision interne et externe, l'établissement d'un calendrier et l'approbation des politiques nécessaires pour coordonner le système mondial d'identificateurs uniques de l'Internet. Un EPDP peut être lancé par le conseil de la GNSO uniquement dans les circonstances particulières suivantes : (1) pour aborder une problématique de politique, étroitement définie, qui a été identifiée et cadrée soit après l'adoption par le Conseil d'administration de l'ICANN d'une recommandation de la GNSO en matière de politique, soit après la mise en œuvre

d'une telle recommandation adoptée ; ou (2) pour fournir une recommandation supplémentaire en matière de politique sur une problématique de politique spécifique dont la portée a été considérablement déterminée précédemment de manière à ce qu'une information exhaustive existe déjà sur le contexte pertinent, par ex. (a) dans un rapport thématique sur un PDP potentiel n'ayant pas été lancé ou (b) dans le cadre d'un PDP précédent n'ayant pas été complété ou (c) à travers d'autres projets tels que le processus d'octroi de directives de la GNSO.

10. GAC - Comité consultatif gouvernemental
Le GAC est un comité consultatif intégré par des représentants de gouvernements nationaux, des représentants d'organisations gouvernementales multinationales, d'organisations établies par des traités et des représentants d'entités autonomes. Sa mission est de conseiller le Conseil d'administration de l'ICANN sur des questions qui font l'objet d'inquiétudes de la part des gouvernements. Le GAC constitue un forum de discussion sur des inquiétudes ou des intérêts partagés par les gouvernements, y compris les intérêts des consommateurs. En sa qualité de comité consultatif, le GAC ne possède aucune autorité légale pour agir au nom de l'ICANN, mais il présente ses conclusions et ses recommandations au Conseil d'administration de l'ICANN.

11. Règlement général sur la protection des données (RGPD)
Le Règlement général sur la protection des données (UE) 2016/679 (RGPD) est un règlement de la législation de l'Union européenne relatif à la protection des données et de la vie privée pour toutes les personnes au sein de l'Union européenne (EU) et de l'espace économique européen (EEE). Il aborde également l'exportation des données à caractère personnel en dehors du territoire de l'Union européenne et de l'espace économique européen (EEE).

12. GNSO - Organisation de soutien aux extensions génériques
La GNSO est l'organisation de soutien chargée d'élaborer et de recommander au Conseil d'administration de l'ICANN des politiques de fond liées aux domaines génériques de premier niveau. Elle est intégrée par des représentants des opérateurs de registre gTLD, des bureaux d'enregistrement de gTLD, des organismes de protection des droits de propriété intellectuelle, des fournisseurs de services Internet, des entreprises et des organisations non commerciales.

13. Domaine générique de premier niveau (gTLD)
« gTLD » désigne le ou les domaines de premier niveau du DNS délégué par l'ICANN en vertu d'un contrat de registre qui est en vigueur, à l'exception des TLD géographiques (ccTLD) ou des TLD géographiques étant des noms de domaine internationalisés (IDN).

14. Groupe des représentants des opérateurs de registre (RySG)
Le Groupe des représentants des opérateurs de registre (RySG) est une entité reconnue au sein de l'Organisation de soutien aux extensions génériques (GNSO) constituée

conformément à l'article 5 du chapitre X (septembre 2009) des statuts constitutifs de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN).

Le rôle principal du RySG consiste à représenter les intérêts des opérateurs de registre gTLD (ou les parrains dans les cas des gTLD parrainés) (« opérateurs de registre ») (i) qui disposent actuellement d'un contrat avec l'ICANN pour fournir des services de registre à l'appui d'un ou plusieurs gTLD ; (ii) qui acceptent, dans ce contrat, de respecter les politiques de consensus ; et (iii) qui choisissent volontairement d'être membres du RySG. Le RySG est ouvert aux groupes d'intérêts visés au chapitre IV. Le RySG transmet ses points de vue au conseil de la GNSO et au Conseil d'administration de l'ICANN, en mettant l'accent particulièrement sur les politiques consensuelles de l'ICANN qui ont trait à l'interopérabilité, la fiabilité technique et le fonctionnement stable de l'Internet ou du système des noms de domaine.

15. ICANN - Société pour l'attribution des noms de domaine et des numéros sur Internet

L'ICANN est une association internationale de droit privé à but non lucratif qui est chargée de l'allocation de l'espace des adresses du protocole Internet (IP), d'attribuer des identificateurs de protocole, de gérer le système des noms de domaine génériques de premier niveau (gTLD), des domaines de premier niveau géographique (ccTLD), et d'assurer les fonctions de gestion du système des serveurs racine. Ces services étaient initialement assurés dans le cadre d'un contrat avec le gouvernement américain par l'IANA (Autorité chargée de la gestion de l'adressage sur Internet) et d'autres organismes. L'ICANN assume à présent les fonctions de l'IANA. En tant que partenariat public-privé, l'ICANN a pour mission de préserver la stabilité opérationnelle de l'Internet, de promouvoir la concurrence, d'assurer une vaste représentation des communautés Internet à l'échelle mondiale et d'élaborer des politiques relatives à sa mission moyennant des processus participatifs basés sur le consensus.

16. Unité constitutive des représentants de la propriété intellectuelle (IPC)

L'Unité constitutive des représentants de la propriété intellectuelle (IPC) représente les points de vue et les intérêts de la communauté de la propriété intellectuelle dans le monde entier, avec un accent particulier sur les marques de commerce, les droits d'auteur, les droits de propriété intellectuelle connexes et leur effet et leur interaction avec le système des noms de domaine (DNS). L'IPC est l'un des groupes constitutifs de l'Organisation de soutien aux extensions génériques (GNSO) chargée de conseiller le Conseil d'administration de l'ICANN sur les questions de politique relatives à la gestion du système des noms de domaine.

17. Unité constitutive des fournisseurs de services Internet et de services de connectivité (ISPCP)

L'Unité constitutive des fournisseurs de services Internet et de services de connectivité est une unité constitutive de la GNSO. Elle a pour objet de s'acquitter des rôles et responsabilités qui sont créés par les statuts constitutifs, les règles ou les politiques

pertinents de l'ICANN et de la GNSO au fur et à mesure que l'ICANN mène à bien ses activités d'organisation. L'ISPCP veille à ce que les points de vue des fournisseurs de services Internet et de services de connectivité contribuent à la réalisation des buts et objectifs de l'ICANN.

18. Serveur de nom

Un serveur de nom est une composante du DNS qui fait le stockage des informations sur une zone (ou plusieurs zones) de l'espace de noms du DNS.

19. Groupe des représentants des entités non commerciales (NCSG)

Le Groupe des représentants des entités non commerciales (NCSG) est l'un des groupes de parties prenantes de la GNSO. Le Groupe des représentants des entités non commerciales (NCSG) a pour objet de représenter, à travers ses représentants élus et ses unités constitutives, les intérêts et les préoccupations des titulaires de noms de domaine non commerciaux et des utilisateurs Internet non commerciaux de domaines génériques de premier niveau (gTLD). Il est le porte-parole et le représentant, dans les processus de l'ICANN, des organisations à but non lucratif qui servent des intérêts non commerciaux ; des services à but non lucratif tels que l'éducation, la philanthropie, la protection des consommateurs, l'organisation communautaire, la promotion des arts, la défense des politiques d'intérêt public, le bien-être des enfants, la religion, la recherche scientifique et les droits de l'homme ; les préoccupations liées aux logiciels d'intérêt public ; des familles ou individus qui enregistrent les noms de domaine à un usage personnel non commercial; et les usagers d'Internet qui sont principalement intéressés aux aspects non commerciaux, d'intérêt public, des politiques de noms de domaine.

20. Procédure de règlement de litiges après délégation (PDDRP)

Les procédures de règlement de litiges après délégation ont été élaborées pour fournir aux personnes lésées par la conduite d'un nouvel opérateur de registre gTLD une manière alternative de se plaindre de cette conduite. Ces procédures de règlement de litiges sont toutes administrées par des fournisseurs externes à l'ICANN et peuvent exiger que les plaignants prennent des mesures concrètes pour régler leurs problèmes avant de déposer une plainte officielle. Un panel d'experts déterminera si un opérateur de registre est en faute et recommandera des remèdes à l'ICANN.

21. Nom enregistré

« Nom enregistré » fait référence à un nom de domaine figurant dans le domaine d'un gTLD qui est composé de deux (2) ou plusieurs niveaux (par exemple : john.smith.name), pour lequel un opérateur de registre de gTLD (ou un affilié ou sous-traitant engagé dans la prestation de services de registre) maintient les données dans une base de données de registres, organise ledit maintien ou perçoit des revenus de ce maintien. Un nom figurant dans une base de données de registre peut être un nom de domaine enregistré même s'il n'apparaît pas dans un fichier de zone (par exemple : un nom de domaine enregistré, mais inactif).

22. Bureau d'enregistrement
Le terme « bureau d'enregistrement », lorsqu'il apparaît sans majuscule, fait référence à une personne ou à une entité qui s'engage par contrat avec les titulaires de noms de domaine enregistrés et un opérateur de registre, et qui collecte des données d'enregistrement sur les titulaires des noms de domaine enregistrés et envoie des informations sur l'enregistrement afin qu'elles puissent être saisies dans la base de données des registres.

23. Groupe des représentants des bureaux d'enregistrement (RrSG)
Le Groupe des représentants des bureaux d'enregistrement est l'un des nombreux groupes de représentants au sein de la communauté de l'ICANN, et est l'organe représentatif des bureaux d'enregistrement. Il s'agit d'un groupe diversifié et actif qui veille à ce que les intérêts des bureaux d'enregistrement et de leurs clients soient efficacement protégés. Nous vous invitons à en savoir plus sur les bureaux d'enregistrement de noms de domaine accrédités et sur le rôle important qu'ils jouent dans le système des noms de domaine.

24. Opérateur de registre
Un « opérateur de registre » est la personne physique ou morale couramment responsable, conformément au contrat conclu entre l'ICANN (ou son cessionnaire) et cette/ces personne(s) physique(s) ou morale(s) ou, si ce contrat est résilié ou expiré, conformément à un contrat conclu entre le gouvernement des États-Unis et cette/ces personne(s) physique(s) ou morale(s), pour la prestation des services de registre concernant un gTLD spécifique.

25. Services d'annuaire de données d'enregistrement (RDDS)
Le service d'annuaire des données d'enregistrement des noms de domaine, ou RDDS, fait référence au(x) service(s) proposé(s) par les registres et les bureaux d'enregistrement pour permettre l'accès aux données d'enregistrement des noms de domaine.

26. Procédure de règlement de litiges relatifs à des restrictions à l'enregistrement (RRDRP)
La procédure de règlement de litiges relatifs à des restrictions à l'enregistrement (RRDRP) a pour objet d'aborder des circonstances dans lesquelles un opérateur de registre d'un nouveau gTLD communautaire a dévié des restrictions à l'enregistrement prévues dans le contrat de registre.

27. SO - Organisations de soutien
Les SO se composent de trois organes consultatifs spécialisés, chargés de conseiller le Conseil d'administration de l'ICANN sur des questions relatives aux noms de domaine (GNSO et CCNSO) et aux adresses IP (ASO).

28. SSAC - Comité consultatif sur la sécurité et la stabilité
Comité consultatif du Conseil d'administration de l'ICANN constitué par des experts techniques issus de l'industrie et du secteur académique, ainsi que par des opérateurs des serveurs racine de l'Internet, des bureaux d'enregistrement et des registres TLD.

29. TLD - Domaine de premier niveau
Les TLD sont les noms situés au sommet de la hiérarchie de nommage du DNS. Dans les noms de domaine, ils représentent la chaîne de lettres qui suit le dernier « . » (le plus à droite). C'est le cas de « net » dans http://www.example.net. Le gestionnaire d'un TLD contrôle les noms de domaine de second niveau qui sont reconnus dans ce TLD. Les gestionnaires du « domaine racine » ou de la « zone racine » contrôlent les TLD qui sont reconnus par le DNS. Les TLD couramment utilisés sont, entre autres : .COM, .NET, .EDU, .JP, .DE, etc.

30. Politique de règlement uniforme de litiges relatifs aux noms de domaine (UDRP)
La politique de règlement uniforme de litiges relatifs aux noms de domaine (UDRP) est un mécanisme de protection des droits qui précise les procédures et les règles appliquées par les bureaux d'enregistrement dans le cadre de litiges survenant au cours de l'enregistrement et l'utilisation des noms de domaine gTLD. L'UDRP est une procédure administrative obligatoire visant surtout à résoudre des réclamations relatives à l'enregistrement malveillant ou de mauvaise foi de noms de domaine. Cette politique ne s'applique qu'aux litiges entre les titulaires de nom de domaine et les tiers, pas aux litiges entre un bureau d'enregistrement et son client.

31. Système uniforme de suspension rapide (URS)
Le système uniforme de suspension rapide est un mécanisme de protection des droits qui complète la Politique uniforme de règlement de litiges relatifs aux noms de domaine (UDRP) en vigueur en offrant aux détenteurs de droits une méthode plus efficace et économique pour résoudre les cas incontestables d'abus.

32. WHOIS
Le protocole WHOIS est un protocole Internet utilisé pour interroger des bases de données afin d'obtenir des informations sur l'enregistrement d'un nom de domaine (ou d'une adresse IP). Le protocole WHOIS a été initialement spécifié dans le RFC 954, publié en 1985. La spécification actuelle de ce protocole est décrite dans le document RFC 3912. Les contrats relatifs aux gTLD passés entre l'ICANN et les bureaux d'enregistrement et les opérateurs de registre exigent à ces derniers de permettre l'accès public aux données sur les noms enregistrés par le biais de pages Web interactives et des services WHOIS du port 43. Ces données, généralement dénommées « données WHOIS » incluent des éléments tels que la date de création et d'expiration des enregistrements de domaine, les serveurs de noms, l'information de contact du titulaire de nom de domaine ainsi que de ses représentants techniques et administratifs.

Les services WHOIS sont typiquement utilisés pour identifier les propriétaires de domaines à des fins commerciales et pour identifier les parties capables de corriger des problèmes techniques associés au domaine enregistré.

Annexe A - Information de contexte

Suite à la demande de certains membres de l'équipe responsable de l'EPDP, le conseil de la GNSO a demandé à l'équipe responsable de l'EPDP de poursuivre ses travaux sur deux sujets, après l'achèvement des étapes 1 et 2 de ses travaux, à savoir : 1) la distinction entre les données d'enregistrement des personnes morales et des personnes physiques, et 2) la possibilité que les contacts uniques aient une adresse e-mail anonymisée uniforme.

Données des personnes morales vs. données des personnes physiques - Instructions du conseil à l'équipe responsable de l'EPDP

Personnes morales vs. personnes physiques - L'équipe responsable de l'EPDP devra se pencher sur l'étude menée par l'organisation ICANN (à la demande de l'équipe responsable de l'EPDP et avec l'approbation du conseil de la GNSO pendant l'étape 1), sur l'avis juridique fourni par le cabinet Bird & Bird, ainsi que sur les nombreux commentaires reçus à ce sujet pendant la consultation publique sur le supplément du rapport initial de l'équipe responsable de l'EPDP :

i. Si des mises à jour doivent être apportées aux recommandations relatives à ce sujet issues de la première étape de l'EPDP (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire ») ;
ii. Établir quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la différence entre les enregistrements des personnes morales et celui des personnes physiques.

Faisabilité d'une adresse e-mail anonymisée uniforme pour les contacts uniques - Instructions du conseil à l'équipe responsable de l'EPDP

L'équipe responsable de l'EPDP devra étudier l'avis juridique et réfléchir à des propositions spécifiques comportant des garanties suffisantes pour éviter les problèmes identifiés dans le document initial. Les groupes qui ont demandé un délai supplémentaire pour examiner cette question, entre autres l'ALAC, le GAC et le SSAC, seront responsables de soumettre des propositions concrètes par rapport à ce sujet. Cet examen devrait déterminer :

i. S'il est possible que les contacts uniques aient une adresse électronique anonyme uniforme et, si possible, si cela devait être obligatoire.

   Si cela était possible mais pas obligatoire, quelles directives devraient être fournies, le cas échéant, aux parties contractantes souhaitant mettre en place des adresses e-mail anynomisées uniformes.

Annexe B – Contexte général

Contexte thématique et du processus

Le 19 juillet 2018, le conseil de la GNSO a lancé un processus accéléré d'élaboration de politiques (EPDP) et a formé l'équipe responsable de l'EPDP sur la spécification temporaire relative aux données d'enregistrement des gTLD. Contrairement à d'autres PDP de la GNSO qui sont ouverts à tous ceux qui souhaitent y prendre part, le conseil de la GNSO a décidé de limiter la composition de cet EPDP, essentiellement du fait de la nécessité de finir le travail dans un délai relativement court et du besoin de gérer de manière responsable les ressources destinées à cet effort. Les groupes de représentants de la GNSO, le Comité consultatif gouvernemental (GAC), l'Organisation de soutien aux extensions génériques (ccNSO), le Comité consultatif At-Large (ALAC), le Comité consultatif sur la sécurité et la stabilité (SSAC) et le Comité consultatif du système des serveurs racine (RSSAC) ont été invités à désigner chacun un nombre limité de membres et de suppléants, tel que décrit dans la charte. En outre, l'organisation ICANN et son Conseil d'administration ont été invités à désigner un nombre limité d'agents de liaison pour participer à cette initiative. Un appel à volontaires a été adressé aux groupes susmentionnés en juillet, et l'équipe responsable de l'EPDP a tenu sa première réunion le 1er août 2018.

Contexte de la problématique

Le 17 mai 2018, le Conseil d'administration de l'ICANN a approuvé la Spécification temporaire relative aux données d'enregistrement des gTLD. Le Conseil d'administration l'a approuvée dans le but d'établir les dispositions temporaires qui régiront la manière dont l'ICANN et ses parties contractantes continueront à respecter les obligations contractuelles et les politiques en matière de WHOIS élaborées par la communauté, tout en se conformant au Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). La spécification temporaire a été adoptée en vertu de la procédure prévue pour les politiques temporaires, décrite dans le contrat de registre (RA) et le contrat d'accréditation de bureau d'enregistrement (RAA). À la suite de l'adoption de la Spécification temporaire, le Conseil d'administration « devra mettre en œuvre immédiatement le processus d'élaboration de politiques de consensus prévu dans les statuts constitutifs de l'ICANN ».[47] Ce processus d'élaboration de politiques de consensus sur la Spécification temporaire devrait être achevé dans un délai d'un an. En outre, la portée du travail inclut des discussions sur un système normalisé d'accès aux données d'enregistrement non publiques.

Lors de sa réunion du 19 juillet 2018, le conseil de l'Organisation de soutien aux extensions génériques (GNSO) a lancé un EPDP sur la Spécification temporaire relative

[47] Consulter l'article 3.1(a) du Contrat de registre : https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

aux données d'enregistrement des gTLD et a adopté la charte de l'équipe responsable de l'EPDP. Contrairement à d'autres PDP de la GNSO qui sont ouverts à tous ceux qui souhaitent y prendre part, le conseil de la GNSO a décidé de limiter la composition de cet EPDP, essentiellement du fait de la nécessité de finir le travail dans un délai relativement court et du besoin de gérer de manière responsable les ressources destinées à cet effort. Les groupes de représentants de la GNSO, le Comité consultatif gouvernemental (GAC), l'Organisation de soutien aux extensions génériques (ccNSO), le Comité consultatif At-Large (ALAC), le Comité consultatif sur la sécurité et la stabilité (SSAC) et le Comité consultatif du système des serveurs racine (RSSAC) ont été invités à désigner chacun un nombre limité de membres et de suppléants, tel que décrit dans la charte. En outre, l'organisation ICANN et son Conseil d'administration ont été invités à désigner un nombre limité d'agents de liaison pour participer à cette initiative.

Le Conseil de la GNSO a voté l'adoption des 29 recommandations figurant dans le rapport final de l'étape 1 de l'EPDP lors de sa réunion du 4 mars 2019. Le 15 mai 2019, le Conseil d'administration de l'ICANN a adopté le rapport final de l'étape 1 de l'équipe responsable de l'EPDP, à l'exception de certaines parties de deux recommandations : 1) la finalité 2 de la Recommandation 1, et 2) la possibilité de supprimer des données dans le champ « Organisation » de la Recommandation 12. Conformément aux statuts constitutifs de l'ICANN, une consultation a eu lieu entre le conseil de la GNSO et le Conseil d'administration de l'ICANN pour discuter des parties des recommandations de l'étape 1 de l'EPDP qui n'ont pas été adoptées par le Conseil d'administration de l'ICANN. En même temps, une Équipe de révision de la mise en œuvre (IRT), composée par l'organisation ICANN (ICANN org) et par des membres de la communauté de l'ICANN, travaille sur la mise en œuvre des recommandations approuvées du rapport final de l'étape 1 de l'équipe responsable de l'EPDP. Pour de plus amples détails sur l'état de la mise en œuvre, veuillez consulter ici.

Le conseil de la GNSO a approuvé le Rapport final de l'étape 2 lors de sa réunion du 24 septembre 2020 par majorité qualifiée. Le rapport final contient les recommandations de l'équipe responsable de l'EPDP pour un Système normalisé d'accès et de divulgation (SSAD) pour les données d'enregistrement non publiques, ainsi que des recommandations et des conclusions par rapport aux questions dites « de priorité 2 », dont celle relative à l'expurgation du champ ville, entre autres.

Dans le cadre de cette approbation, le conseil de la GNSO a accordé de demander une consultation avec le Conseil d'administration de l'ICANN afin de discuter de la viabilité financière du SSAD et certaines des préoccupations exprimées dans les différentes déclarations de la minorité, y compris si une autre analyse coûts-bénéfices devrait être menée avant que le Conseil d'administration de l'ICANN ne considère toutes les recommandations relatives au SSAD pour leur adoption. Au cours de l'ICANN70, le Conseil a demandé à l'organisation ICANN de lancer une Étape de conception opérationnelle (ODP) pour les recommandations relatives au SSAD, et l'ODP est en cours. Pour de plus amples informations sur l'ODP relative au SSAD, rendez-vous à la page :

Comme la consultation demandée ne se rapporte qu'aux recommandations de la SSAD, le Conseil d'administration a choisi d'examiner les recommandations de priorité 2 séparément et a mené une période de consultation publique sur ces recommandations de décembre 2020 à janvier 2021. Le Conseil d'administration a mené une période distincte de consultation publique sur les recommandations relatives au SSAD de février à mars 2021.

Suite à la demande de certains membres de l'équipe responsable de l'EPDP, le conseil de la GNSO a demandé à l'équipe responsable de l'EPDP de continuer à travailler sur deux sujets dans le cadre d'une étape 2A, à savoir : 1) la distinction entre les données d'enregistrement des personnes morales et des personnes physiques, et 2) la possibilité que les contacts uniques aient une adresse e-mail anonymisée uniforme.

Annexe C – Adhésion et participation à l'équipe responsable de l'EPDP

Adhésion et participation à l'équipe responsable de l'EPDP

Résumé des activités de la réunion :

Séances plénières :

- 42 appels en plénière (5 annulés) pour 53,5 heures d'appel, pour un total de 1924,5 heures homme
- Taux de participation total de 85,3 %

Réunions du Comité juridique :

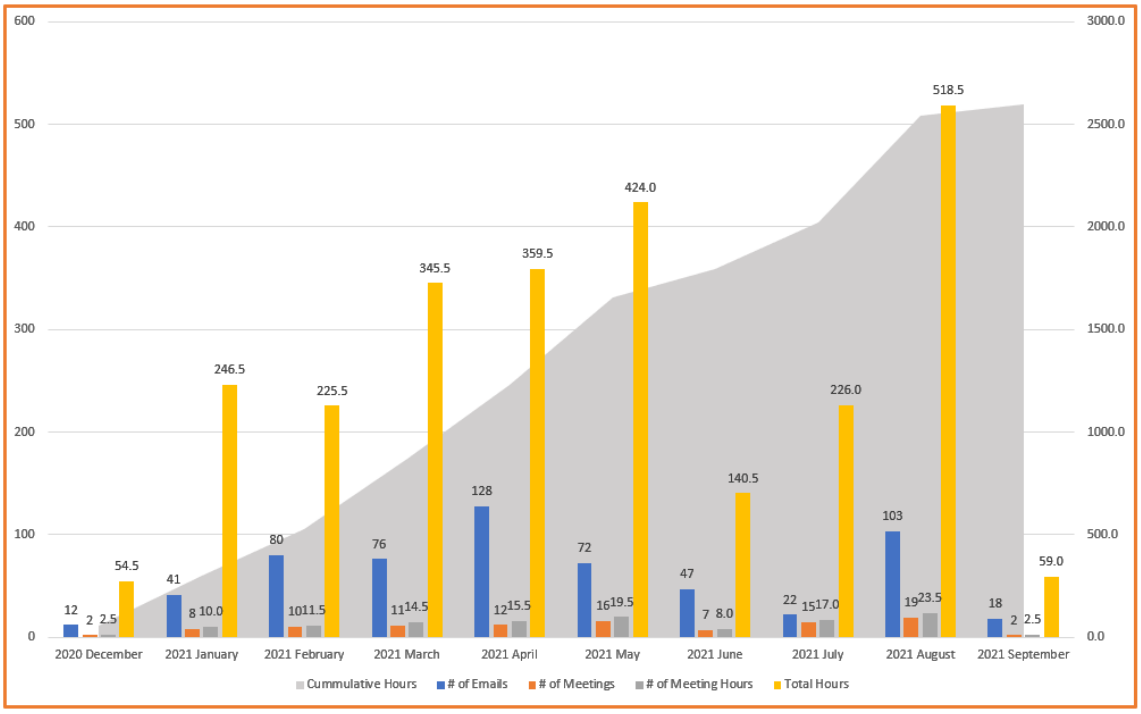
- 11 appels de sous-groupes pour 17,5 heures d'appel pour un total de 232,5 heures homme
- Taux de participation total de 89,2 %

Réunions en petites équipes :

- 16 appels de sous-groupes pour 17,5 heures d'appel pour un total de 180,0 heures homme
- Taux de participation total de 99,0 %

Réunions de l'équipe de direction :

- 51 appels de l'équipe de direction pour 39,0 heures d'appel, soit au total 268,5 heures homme



Les archives contenant les courriers électroniques de l'équipe responsable de l'EPDP peuvent être consultées sur https://mm.icann.org/pipermail/gnso-epdp-team/.

Les membres de l'équipe responsable de l'EPDP sont :

Groupe / membre représenté	SOI	Date de début	Date de départ	% de participation	Rôle
Comité consultatif At-Large (ALAC)				**>98,6 %**	
Alan Greenberg	SOI	15 nov. 2020		>97,2 %	
Hadia Elminiawi	SOI	15 nov. 2020		>100,0 %	LC
Unité constitutive des entreprises et des utilisateurs commerciaux (BC)				**>88,9 %**	
Margie Milam	SOI	15 nov. 2020		>86,1 %	LC
Mark Svancarek	SOI	15 nov. 2020		>91,7 %	
Conseil de la GNSO				**>88,7 %**	
Brian Beckham	SOI	18 fév. 2021		>86,2 %	Vice-président, LC
Keith Drazek	SOI	12 mars 2020		>97,2 %	Président, LC
Philippe Fouquart (UE)	SOI	26 janv. 2021		>81,3 %	Agent de liaison, LC
Comité consultatif gouvernemental (GAC)				**>74,1 %**	
Christopher Lewis-Evans	SOI	19 nov. 2020		>88,9 %	
Laureen Kapin	SOI	19 nov. 2020		>83,3 %	LC
Melina Stroungi	SOI	20 nov. 2020		>50,0 %	LC
Conseil d'administration de l'ICANN				**>73,6 %**	
Becky Burr	SOI	12 nov. 2020		>75,0 %	Agent de liaison, LC

Matthew Shears	SOI	12 nov. 2020		>72,2 %	Agent de liaison
Unité constitutive des représentants de la propriété intellectuelle (IPC)				**>84,7 %**	
Brian King	SOI	20 nov. 2020		>97,2 %	LC
Jan Janssen	SOI	20 nov. 2020		>72,2 %	LC
Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN)				**>93,1 %**	
Amy Bivins	SOI	12 juill. 2020		>88,9 %	Agent de liaison, LC
Brian Gutterman	SOI	12 oct. 2020		>97,2 %	Agent de liaison
Unité constitutive des fournisseurs de services Internet et de services de connectivité (ISPCP)				**>93,1 %**	
Christian Dawson	SOI	15 nov. 2020		>94,4 %	
Thomas Rickert	SOI	15 nov. 2020		>91,7 %	LC
Groupe des représentants des entités non commerciales (NCSG)				**>65,0 %**	
David Cake	SOI	12 mars 2020		>72,2 %	
Manju Chen	SOI	12 mars 2020		>97,2 %	
Milton Mueller	SOI	12 mars 2020		>58,3 %	
Stefan Filipovic	SOI	12 mars 2020		>13,9 %	LC
Stephanie Perrin	SOI	12 mars 2020		>83,3 %	LC
<Vacant>					
Groupe des représentants des bureaux d'enregistrement (RrSG)				**>70,4 %**	
James Bladel	SOI	15 nov. 2020		>27,8 %	
Sarah Wyld	SOI	15 nov. 2020		>94,4 %	
Volker Greimann	SOI	15 nov. 2020		>88,9 %	LC
Groupe des représentants des opérateurs de registre (RySG)				**>94,4 %**	
Alan Woods	SOI	15 nov. 2020		>91,7 %	LC
Marc Anderson	SOI	15 nov. 2020		>97,2 %	
Matthew Crossman	SOI	15 nov. 2020		>94,4 %	LC
Comité consultatif sur la sécurité et la stabilité (SSAC)				**>98,5 %**	
Ben Butler	SOI	15 nov. 2020	14 janv. 2021	>50,0 %	
Steve Crocker	SOI	2 oct. 2021		>100,0 %	
Tara Whalen	SOI	15 nov. 2020		>100,0 %	LC

LC – a participé au Comité juridique

Les suppléants de l'équipe responsable de l'EPDP sont :

Groupe représenté / suppléant	SOI	Date de début	Date de départ	% de participation	Rôle
Comité consultatif At-Large (ALAC)					
Holly Raiche	SOI	15 nov. 2020		>100,0 %	
<Vacant>					
Unité constitutive des entreprises et des utilisateurs commerciaux (BC)					
Steve Del Bianco	SOI	15 nov. 2020		>93,3 %	

Comité consultatif gouvernemental (GAC)					
Ryan Carroll	SOI	26 janv. 2021		>100,0 %	
Velimira Nemiguentcheva-Grau	SOI	26 janv. 2021		>100,0 %	
<Vacant>					
Conseil d'administration de l'ICANN					
León Felipe Sánchez Ambia	SOI	12 nov. 2020		>86,7 %	
Unité constitutive des représentants de la propriété intellectuelle (IPC)					
<Vacant>					
Unité constitutive des fournisseurs de services Internet et de services de connectivité (ISPCP)					
Suman Lal Pradhan	SOI	15 nov. 2020		>100,0 %	
Groupe des représentants des entités non commerciales (NCSG)					
Bruna Santos	SOI	12 mars 2020		>100,0 %	
<Vacant>					
<Vacant>					
Groupe des représentants des bureaux d'enregistrement (RrSG)					
Matt Serlin	SOI	15 nov. 2020		>100,0 %	
Owen Smigelski	SOI	15 nov. 2020		>97,0 %	
Theo Geurts	SOI	15 nov. 2020		>100,0 %	
Groupe des représentants des opérateurs de registre (RySG)					
Amr Elsadr	SOI	15 nov. 2020		>100,0 %	
Beth Bacon	SOI	15 nov. 2020		>100,0 %	
Sean Baseri	SOI	15 nov. 2020		>100,0 %	
Comité consultatif sur la sécurité et la stabilité (SSAC)					
Greg Aaron	SOI	15 nov. 2020		>100,0 %	
<Vacant>					

Le personnel de soutien de l'équipe responsable de l'EPDP comprend :

Groupe représenté / personnel affecté	SOI	Date de début	Date de départ	% de participation	Rôle
Andrea Glandon		15 nov. 2020			
Berry Cobb		15 nov. 2020			
Caitlin Tubergen		15 nov. 2020			LC
Julie Bisland		15 nov. 2020			
Marika Konings		15 nov. 2020			
Terri Agnew		15 nov. 2020			

Annexe E - Déclarations de la minorité

COMITÉ CONSULTATIF AT-LARGE
Rapport final de l'étape 2 A du processus accéléré d'élaboration de politiques sur la spécification temporaire relative aux données d'enregistrement des gTLD

Déclaration de la minorité de l'ALAC

L'ALAC reconnaît et apprécie le travail de l'équipe responsable de l'étape 2A de l'EPDP, les efforts du président, du vice-président et de l'agent de liaison auprès du conseil de la GNSO, ainsi que le dévouement et les efforts du personnel de soutien de l'organisation ICANN. Néanmoins, l'ALAC croit que l'étape 2A ne s'est pas correctement acquittée de son mandat. Le résultat net est que l'importance des données d'enregistrement pour les divers membres de la communauté tels que les agences de protection des consommateurs, les autorités d'application de la loi, les enquêteurs en matière de cybersécurité et le rôle crucial qu'ils jouent dans la protection des utilisateurs quotidiens de l'Internet, des titulaires de noms de domaine, des clients, des entreprises et de l'ensemble de la population en ligne ne sera pas correctement prise en compte.

Il est important de trouver un équilibre entre la protection des renseignements personnels des titulaires de noms de domaine et l'expérience, la sécurité et la sûreté des utilisateurs. L'expurgation de données qui ne sont pas protégées par les lois sur la protection des données ne permet pas de trouver le juste équilibre.

Dans cette déclaration de la minorité, l'ALAC s'inquiète des aspects suivants des recommandations du rapport final de l'étape 2A et de leur impact sur la sécurité des utilisateurs quotidiens de l'Internet :

- Omission de faire la distinction entre les données de personnes morales et des personnes physiques,
- Omission de mandater l'utilisation de l'élément de données commun par toutes les parties contractantes,
- Manque de moyens pour contacter les titulaires de noms de domaine
- « Processus »

Omission de mandater la distinction entre les données des personnes morales et des personnes physiques

Le RGPD ne protège pas les données à caractère non personnel des personnes morales. En outre, le considérant 14 du RGPD de l'UE dit « Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale. »

L'EPDP a reçu des directives juridiques selon lesquelles il était raisonnable de permettre aux titulaires de noms de domaine de s'auto-identifier comme des personnes physiques et, avec des précautions, des avis de non-responsabilité et des capacités de correction appropriés, le risque de le permettre était faible pour les parties contractantes. Cette position a été appuyée par la lettre de juillet 2018 du CEPD à Göran Marby. Cet avis a été ignoré par l'EPDP. Bien que la base installée d'enregistrements de 200 millions prenne du temps à traiter (par exemple au moment du renouvellement), l'EPDP n'a même pas recommandé que la différenciation des nouveaux enregistrements soit faite. ? Plus important encore, même le débat sur la prise de telles mesures (comme l'ont officiellement proposé les membres du GAC auprès de l'EPDP) a été sommairement rejeté au début de l'étape 2A, au lieu de se concentrer uniquement sur les « directives » qui pourraient être ignorées. Compte tenu de toutes les dispositions ci-dessus et du fait que le service d'annuaire des données d'enregistrement (RDDS) est un bien public qui protège les utilisateurs en ligne du monde entier et que les lois sur la protection de la vie privée et similaires sont un bien public qui protège les données d'enregistrement des titulaires de noms de domaine, un juste équilibre doit se produire. Ce juste équilibre ne peut pas être atteint si plus de données que ce qui est exigé par la loi et la législation sont expurgées, et l'EPDP n'a fait pratiquement aucun effort pour atteindre cet équilibre.

Omission de mandater l'utilisation de l'élément de données commun par toutes les parties contractantes

Le ou les éléments de données communs proposés dans la Recommandation 1 permettent huit valeurs différentes possibles, y compris « la distinction de statut juridique n'a pas été faite » et « la présence de données à caractère personnel n'a pas été déterminée ». Ces statuts permettent aux parties contractantes qui ne se différencient pas d'utiliser le champ nouvellement défini. Toutefois, l'EPDP n'a pas recommandé que les champs soient utilisés, même par les bureaux d'enregistrement qui choisissent volontairement de faire une distinction entre personne morale et physique ou d'identifier la présence ou l'absence de données à caractère personnel. L'utilisation des champs n'a point été exigée MÊME LORSQUE des données valides et utiles sont disponibles, ce qui n'a aucun sens. De plus, l'EPDP n'a pas désigné ces champs comme étant admissibles à la divulgation publique, même s'ils NE contiennent AUCUN renseignement personnel.

Conformément aux recommandations des rapports finaux des étapes 1 et 2 de l'EPDP, les parties contractantes (CP) doivent mettre à jour leur service actuel d'annuaire de données d'enregistrement (RDDS)

Le fait de mandater l'utilisation de l'élément de données commun par toutes les parties contractantes permettrait à des processus similaires d'être suivis par toutes les CP du monde entier, qu'elles fassent ou pas la distinction entre types de personnes et qu'elles soient soumises ou non aux réglementations de l'UE.

En conséquence, nous créons un élément commun que personne n'est tenu d'utiliser, ce qui va à l'encontre des raisons pour lesquelles il existe des façons communes de faire les choses et en ouvrant la porte à la fragmentation.

Manque de moyens pour contacter les titulaires de noms de domaine

L'ALAC regrette que l'EPDP n'ait pas réussi à mettre fin aux méthodologies visant à mieux traiter l'anonymisation ou la pseudonymisation des adresses e-mail de contact. Cela veut dire que nous sommes laissés avec les recommandations de l'étape 1 permettant l'anonymisation, mais en l'absence de cette dernière, permettant des formulaires Web pour le contact. Depuis la fin de l'étape 1, il est devenu évident que certains (principaux) bureaux d'enregistrement utilisent un type de formulaire Web qui ne permet effectivement pas de communications utiles avec un titulaire de nom de domaine. La résolution de cette lacune apparente dans le règlement a été jugée hors de portée, malgré les instructions de la GNSO de revoir cette recommandation de l'étape 1. L'effet net est que, pour une partie importante de la base d'enregistrements de gTLD, il n'existe aucun moyen efficace de réaliser des communications avec les titulaires de noms de domaine.

« Processus »

L'ALAC est préoccupée par le fait que tout au long de cet EPDP, l'accent a été mis exclusivement sur les processus projetés et les calendriers établis, avec un impact important sur la capacité de déterminer et de recommander une bonne politique.

En voici quelques exemples :

- Échéances qui ne permettent pas une délibération suffisante de la consultation avec les groupes qui appuient cet EPDP
- Les déterminations de portée qui excluent certaines choses hors de portée parce qu'elles ne sont pas explicitement mentionnées dans les instructions de la GNSO, mais permettant d'autres détournements (comme la recommandation sur le Code de conduite)
- Suspension de la discussion sur la différenciation en faveur de « l'orientation », avec la promesse du retour qui ne se concrétise jamais.
- Des normes incohérentes de « preuve » qui permettent de rejeter certains arguments alors que d'autres se tiennent.

Il semble qu'il y ait une réticence croissante des parties contractantes à accepter DE NOUVELLES obligations, quels que soient les bénéfices pour les autres parties ou le bien public. C'est troublant pour la direction.

Synthèse

L’étape 1 de l’EPDP a déterminé que l’étape 2 « déterminerait et réglerait le problème de la distinction entre personne morale et personne physique de l’étape 2 ». Cette étape a été reportée à l’étape 2A. Il est clair que nous n’y sommes pas parvenus. En outre, bien que nous ayons recommandé la création d’éléments RDDS critiques, nous leur donnons la possibilité d’être complètement ignorés. L’ALAC a beaucoup de difficultés à étiqueter cet effort comme un succès.

Déclaration de la minorité de l'Unité constitutive des utilisateurs commerciaux de l'ICANN sur le rapport final de l'étape 1 de l'équipe responsable de l'EPDP[48]
10 sept. 2021

Introduction

Cette déclaration de la minorité est soumise au nom de l'Unité constitutive des utilisateurs commerciaux de l'ICANN (BC).[49]

La BC défend vivement les droits à la vie privée et de l'intention protectrice du RGPD. Toutefois, dans le contexte du travail de l'équipe responsable de l'EPDP sur ce processus accéléré d'élaboration des politiques (EPDP) (une équipe qui a été explicitement enjointe de « préserver la base de données WHOIS dans la mesure du possible » tout en respectant la loi en matière de vie privée), la politique qui en résulte dépasse ce qui est nécessaire pour protéger les données des personnes physiques.

L'étape 2A de l'équipe responsable de l'EPDP a été chargée par le conseil de la GNSO de se concentrer sur deux sujets spécifiques : 1) la distinction entre les données d'enregistrement des personnes morales et des personnes physiques, et 2) la possibilité que les contacts uniques aient une adresse e-mail anonymisée uniforme. Notre commentaire se concentre sur la distinction entre personne morale et personne physique, sur l'absence de résultats exécutoires et, surtout, sur la nécessité critique de répondre aux progrès législatifs européens qui auront un impact sur les politiques élaborées, ou sur leur absence.

Comme indiqué précédemment, la BC croit fermement que la différenciation facultative entre personnes morales et personnes physiques est inadéquate et que la politique de l'ICANN doit exiger une telle différenciation afin d'assurer la sécurité et la stabilité du DNS mondial.

En somme, les recommandations de l'étape 2A, en ne faisant pas la distinction entre les personnes morales et les personnes physiques, donnent lieu à l'expurgation d'un nombre important de documents ou à leur indisponibilité. Cela est affligeant, et même frustrant, compte tenu de la prévalence bien connue des méfaits en ligne. Cette frustration a été bien documentée dans la récente enquête du Groupe de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (M3AAWG)[50], qui a détaillé les limites substantielles de l'accès actuel aux informations sur l'enregistrement

[48] 3-sept-2021, Rapport final de l'étape 2A de l'EPDP, à l'adresse https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20210903/4c231c0a/EPDPPhase2A-FINALREPORT-3September2021003-0001.pdf

[49] Les commentaires antérieurs de la BC et le rapport de la minorité sur l'étape 2 de l'EPDP comprennent :
- la présentation de la part de la BC et de l'IPC d'une déclaration conjointe de la minorité pour l'étape 2 de l'EPDP.
- Commentaires du BC sur le rapport initial de l'étape 2A

[50] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

de noms de domaine non publics et a affirmé que les solutions actuellement discutées par l'ICANN ne répondraient pas aux besoins des forces de l'ordre et de la cybersécurité.

Bien que l'équipe responsable de l'EPDP ait désigné ses recommandations comme étant soutenues par « consensus », la BC affirme qu'elle ne soutient pas les résultats de l'étape 2A, qu'elle ne soutient pas une désignation par « consensus » et qu'elle justifie ici sa dissidence.

Point de vue de la BC sur le Rapport final de l'étape 2A de l'EPDP

L'un des principes fondamentaux de la mission de l'ICANN est d'établir une politique de consensus qui contribue à la sécurité et à la stabilité du DNS et d'appliquer rigoureusement toutes les obligations résultant de cette politique. Toutefois, la BC observe une tendance récente (particulièrement prononcée dans les délibérations et les résultats du groupe de travail (WG) de l'étape 2A) vers le recours à des obligations « facultatives » (par exemple, l'utilisation de « devrait » et « pourrait » dans le libellé des recommandations) qui contourne les obligations et ne s'engage pas fermement à maintenir la sécurité et la stabilité. De plus, on s'appuie de plus en plus sur l'émission de conseils plutôt que sur une politique contraignante, laissant une marge considérable pour la conformité des parties contractantes et une politique faible, édulcorée et probablement inapplicable. Ce résultat est malheureux. La BC estime que la communauté de l'ICANN devrait dédier du temps à la politique qui s'appliquera uniformément à tous les bureaux d'enregistrement et à tous les opérateurs de registre (pas seulement à un sous-ensemble indéfini, agissant de manière arbitraire).

En fait, la BC note qu'à l'exception de la première partie de la Recommandation 1 (qui oblige l'ICANN à coordonner avec la communauté technique l'élaboration de normes techniques pour faciliter la différenciation entre les données d'enregistrement des personnes morales et des personnes physiques), le rapport final de l'étape 2A de l'EPDP ne contient aucune politique réelle et n'établit aucune obligation exécutoire sur les parties contractantes. Cela représente un échec malheureux du processus multipartite.

La désignation de « consensus » de l'équipe responsable de l'EPDP pour le rapport final ne reflète pas les divisions profondes dans les résultats des groupes de travail. Il est clair qu'une partie importante de membres du groupe de travail, ainsi que de la communauté de l'ICANN, trouve que les résultats de l'étape 2A sont inadéquats. Cette division ne doit pas être négligée, même si le groupe de travail insiste sur le positionnement de ce rapport comme ayant été décidé par consensus.

Exigence d'une distinction entre personne morale et personne physique

Nous réitérons que l'incapacité des utilisateurs de l'Internet à identifier avec qui ils font des affaires en ligne et l'incapacité croissante des forces de l'ordre, de la cybersécurité et des professionnels du droit à identifier les acteurs criminels en ligne par le biais de

leurs données d'enregistrement de noms de domaine, continuent de saper gravement le mandat de l'ICANN en matière de sécurité et de stabilité. Ainsi, les intérêts de ces utilisateurs ne sont pas reflétés adéquatement dans la politique.

L'incapacité de l'équipe de l'étape 2A de l'EPDP à parvenir à un consensus sur la recommandation de faire des changements à la Recommandation 17.1 de l'étape 1 et son échec à « déterminer et résoudre la question juridique par rapport à la distinction entre personne morale et personne physique » dans ses délibérations, comme l'exige la politique de l'étape 1, ne signifie pas que la politique définie dans la Recommandation 17.1 de l'étape 1 devrait rester ou devenir la politique de l'ICANN « par défaut ». En fait, c'est le contraire qui s'est produit. Comme l'équipe de l'étape 2A n'est pas parvenue à un consensus sur cette recommandation, nous pensons que le dossier devrait indiquer que l'opinion consensuelle n'existait pas et n'existe toujours pas, ce qui permettrait une différenciation juridique facultative par rapport à la distinction entre personnes morales et personnes physiques par les bureaux d'enregistrement et les opérateurs de registre.

Directive NIS2

La maturation de la directive NIS2 indique que le Parlement européen ne se contentera pas d'aborder et d'influer sur la question de la distinction entre personnes morales et personnes physiques, mais également sur d'autres politiques liées au WHOIS, notamment l'exactitude, les éléments de données critiques, la publication en temps opportun des données à caractère non personnel et la réponse en temps opportun aux demandeurs d'accès légitimes. L'ICANN doit être parfaitement consciente du fait que les principales parties prenantes, y compris les autorités de régulation d'Europe et des États-Unis, surveillent de près l'engagement du Parlement européen sur ces questions via la directive NIS2. Les futurs avis et décisions des tribunaux et des autorités de régulation de la protection de la vie privée sont probables et pourraient s'accélérer à la suite des procédures liées à la directive NIS2. Il est clairement possible que la progression de la directive NIS2 puisse rapidement dépasser l'élaboration des politiques de l'ICANN qui devra revoir l'impact de ladite directive une fois qu'elle sera adoptée.

L'ICANN devrait donc être tenue de répondre correctement à la directive NIS2 lorsqu'elle est adoptée par l'Union européenne. Cela donne le temps à l'ICANN de mettre à jour ses contrats et politiques avant que la directive NIS2 ne soit transposée pour la première fois dans les lois des États membres de l'UE. Le non-respect de cette directive entraînera probablement une approche sectorielle fragmentée et incohérente des obligations découlant de la directive.

Recommandation 1

La BC ne soutient pas cette recommandation. Alors que nous soutenons l'obligation pour l'ICANN de définir un mécanisme technique normalisé pour faciliter la différenciation entre les données d'enregistrement des personnes morales et des

personnes physiques, la BC regrette l'absence d'obligations des parties contractantes d'utiliser ce champ, ou même d'indiquer si la distinction a été faite. Le fait de ne pas exiger l'utilisation de ce mécanisme technique ne donnera pas lieu à un RDDS cohérent et fiable. Il s'agit d'une occasion manquée de réduire le nombre de demandes de données à caractère non personnel qui ont été inutilement traitées, telles que les données de contact pour les services d'anonymisation et d'enregistrement fiduciaire non affiliés. Ce résultat est bien en deçà des besoins des personnes impliquées dans les enquêtes sur l'utilisation malveillante du DNS, les activités liées à la cybercriminalité, les violations à la propriété intellectuelle et d'autres activités qui menacent le bien-être des consommateurs.

Comme indiqué ci-dessus, la BC est fermement convaincue que l'ICANN doit prendre des mesures pour mettre à jour la politique de l'EPDP lorsque la directive NIS2 a été adoptée par l'Union européenne.

Recommandation 2

La BC s'oppose à la recommandation 2 pour des raisons de procédure et en ce qui concerne sa recommandation spécifique.

Sur le plan procédural, en violation des statuts constitutifs de l'ICANN et de la Charte de l'étape 2 de l'EPDP, l'équipe responsable de l'étape 2A de l'EPDP a consacré inexplicablement beaucoup de temps à l'élaboration de politiques d'orientation plutôt que de politiques consensuelles contraignantes. Un sous-ensemble des membres du groupe de travail a effectivement « manqué le temps », consacrant la plupart de ses efforts à créer des directives, reportant ainsi jusqu'aux dernières semaines de l'étape 2A toute discussion significative et solide sur la manière de créer des politiques de consensus contraignantes.

L'annexe 2-A des statuts constitutifs de l'ICANN spécifie le processus de production des directives, qui nécessite le lancement officiel d'un processus d'orientation par le conseil de la GNSO. Ce processus n'a pas été suivi et, par conséquent, ne peut pas produire de directives de manière justifiée.

Pour cette raison, la politique définie dans la Recommandation 2 devrait être adoptée comme une politique consensuelle et non pas simplement comme une « orientation », et appliquée de manière appropriée.

En ce qui concerne les détails de la recommandation, la BC estime qu'elle est également faible et inapplicable, ce qui entrave davantage la convivialité des données d'enregistrement de noms de domaine à des finalités légitimes. La recommandation devrait obliger les parties contractantes à suivre les principes de la Recommandation 2.

Enfin, nous notons qu'il y a une erreur à la page 20 du rapport final, qui devrait être corrigée comme suit :

> « Cela permet généralement la publication ~~divulgation~~ des données des personnes morales parce qu'elles ne relèvent pas de la compétence du RGPD. Toutefois, lors du traitement des données des personnes morales, les parties contractantes devraient mettre en place des mesures de protection pour s'assurer que les données d'identification personnelle concernant une personne physique ne soient pas publiées ~~divulguées~~ dans les données marquées comme correspondant à une personne morale, car il s'agit d'un exemple d'information qui est dans le champ d'application du RGPD ».

Ces clarifications sont nécessaires pour assurer la cohérence avec les recommandations du rapport de l'étape 1 de l'EPDP, à savoir que l'information d'une personne physique ***peut être divulguée sur demande***, à des finalités légitimes, à condition qu'une base juridique appropriée existe en vertu du RGPD.

Recommandation 3

La BC observe que cette recommandation ne définit pas d'obligations exécutoires de la part d'une partie en particulier et n'encourage pas le développement de telles obligations. Recommander que le travail sur un code de conduite soit « considéré » par « tout travail futur possible au sein de l'ICANN » est vague et inapplicable, et laisse sans réponse les priorités de la communauté qui méritent une attention particulière.

En conséquence, la recommandation devrait encourager l'ICANN à commencer un processus pour établir un code de conduite. Si l'ICANN le faisait, la BC s'opposerait fermement à tout processus qui n'impliquerait pas toutes les parties prenantes de l'ICANN. La définition et le développement d'un code de conduite doivent être effectués de manière ouverte, transparente et inclusive et ne doivent pas être développés en dehors du processus multipartite de l'ICANN (par exemple, via des négociations à huis clos entre l'organisation ICANN et les parties contractantes).

Recommandation 4

Il est regrettable que l'équipe responsable de l'EPDP n'ait pas consacré suffisamment de temps pour aborder ce sujet important. La BC reste persuadée qu'une adresse e-mail pseudonymisée pour chaque titulaire de noms de domaine devrait être ***requise*** pour faciliter l'enquête sur l'utilisation malveillante du DNS en permettant la joignabilité et le référencement croisé des enregistrements par les titulaires de nom de domaine.

Encore une fois, la BC regrette que cette recommandation ne définisse aucune obligation exécutoire des parties contractantes, laissant des écarts importants entre la recommandation et la mise en œuvre pratique. La recommandation pour que les parties

contractantes évaluent les conseils juridiques et les risques, les avantages et les garanties est susceptible d’entraîner une politique trop prudente, faible et finalement inefficace.

Ce commentaire a été écrit par Alex Deacon, Margie Milam, Steve Del Bianco, Mark Svancarek, Drew Bennett et Mason Cole. Il a été approuvé en accord avec notre charte.

Déclaration de la minorité de l'IPC sur l'étape 2A de l'EPDP

La législation sur la protection des données, y compris le RGPD, ne s'applique pas aux données à caractère non personnel. En fait, bien que le RGPD soit certes quelque peu ambigu, il peut même ne pas s'appliquer aux données à caractère personnel relatives aux entités juridiques.[51] Par conséquent, les bases de données telles que le WHOIS/RDDS, qui servent de nombreux buts d'intérêt public, ne doivent expurger que les données qui sont manifestement des données à caractère personnel nécessitant un traitement différent en raison de la législation sur la protection des données. Cependant, l'étape 2A de l'EPDP a déplacé inexplicablement et de manière inappropriée la « charge de la preuve » ou du moins la « charge de la persuasion » vers ceux qui préconisent un résultat de bon sens : les données à caractère non personnel ne doivent pas être cachées. L'IPC note que l'étape 2A de l'EPDP a commencé son travail du mauvais pied entièrement en prenant cette charge inappropriée et en essayant de fournir des directives plutôt que de créer une politique consensuelle contraignante. Ce n'est pas le rôle du PDP, qui est conçu pour élaborer une politique de consensus liant toutes les parties contractantes sur un pied d'égalité. L'IPC note en outre une tendance troublante dans l'élaboration multipartite de politiques tout au long des nombreuses étapes de l'EPDP : il est possible qu'il y ait peu de succès lorsque certaines parties prenantes ne sont disposées qu'à agir exclusivement dans leurs propres intérêts, avec peu de considération pour le compromis dans l'intérêt du bien commun. Aujourd'hui plus que jamais, nous devons rassembler nos parties prenantes dans l'intérêt de la sécurité, la stabilité et la résilience du DNS et de la « promotion de l'intérêt public mondial », comme le stipule l'acte constitutif de l'ICANN. Enfin, nous notons que la désignation de « consensus » attribuée aux recommandations de l'étape 2A de l'EPDP reflète de manière inadéquate la division au sein du groupe de travail sur ces résultats, et ne reflète pas que la Recommandation 17.3 de l'étape 1 de l'EPDP, à savoir, « L'équipe responsable de l'EPDP déterminera et règlera la question de la distinction entre personne morale et personne physique à l'étape 2 » reste non résolue sans obligation de faire la distinction.

Ci-dessous, des commentaires spécifiques sur l'étape 2A de l'EPDP.

I. Se fier à l'autodésignation du titulaire de nom de domaine

L'une des déceptions les plus courantes dans les recommandations de l'étape 2A de l'EPDP est le concept selon lequel les parties contractantes ne devraient pas être tenues de se fier à ce qu'un titulaire de nom de domaine spécifie la nature des données du RDS et soit publie, soit expurge les données en conséquence. L'avis juridique a confirmé cette évaluation de bon sens, qualifiant les données de « faible sensibilité », de « faible

[51] Cette règlementation ne s'applique pas au traitement des données à caractère personnel de personnes morales et notamment les entreprises constituées sous la forme de personnes morales, dont le nom et le statut et les coordonnées de la personne morale. Considérant 14 du RGPD

risque », et même en cas d'une publication par négligence fondée sur l'autodésignation incorrecte d'un titulaire de nom de domaine, il semble fort probable que « l'ordre de corriger le problème » (probablement accompagné d'un délai raisonnable pour mettre en œuvre les changements), plutôt qu'une amende, ne trouve « aucun exemple d'application de la loi à cet égard ».[52]

Sur la base de ces conseils juridiques, un groupe qui travaille véritablement dans l'intérêt public aurait dû facilement accepter de publier des données identifiées par la personne concernée comme des données à caractère non personnel. Et pourtant, aucun accord de ce type n'a émergé.

II. Éléments de données communs

L'IPC appuie clairement le développement d'un ou plusieurs éléments de données communs pour indiquer si les données RDS se rapportent à un titulaire de nom de domaine qui est une entité juridique ou à un titulaire de nom de domaine qui est une personne physique et/ou si les données elles-mêmes contiennent des données à caractère personnel. Bien que décevant comme résultat le plus concret de l'étape 2A, l'IPC soutient et apprécie le fait que le modèle multipartite soit parvenu à un consensus sur cet élément de données normalisé.

Cela dit, l'IPC et ses collègues d'autres unités constitutives et comités consultatifs sont fermement convaincus qu'un tel élément de données normalisé devrait être obligatoire, en particulier en l'absence d'une publication de données de bon sens selon la représentation des titulaires de nom de domaine. Bien que nous soyons encouragés par l'accord pour développer cet élément de données, nous doutons du probable impact positif de ce compromis si un tel élément de données ne parvient jamais à une utilisation généralisée par les parties contractantes. En fait, l'IPC est franchement déçue et découragée du fait que l'équipe de l'étape 2A ne peut s'entendre sur une plus grande utilisation de cet élément de données. Les possibilités allaient de la collecte facultative pour les nouveaux domaines uniquement à la collecte et à la publication obligatoires du champ pour tous les domaines sous gestion. Pourtant, le strict minimum (la collecte facultative) a été le seul résultat susceptible de parvenir à un consensus. Cela est particulièrement décevant étant donné que le champ lui-même ne contient pas les données à caractère personnel et que, par conséquent il n'y a aucun risque au cas de les publier. En outre, les parties contractantes n'ont jamais fourni de motif d'opposition à la collecte ou à la publication obligatoire de cet élément de données. Elles se sont contentés de répéter « nous ne voyons pas la valeur » (vraisemblablement comme opérateurs de registre et bureaux d'enregistrement) lorsqu'elles ont reçu la justification fournie par les parties non contractantes, qui comprend : l'utilité pour le SSAD, l'indication de la soumission d'une demande SSAD ou d'une demande de registre/bureau d'enregistrement unique, les informations sur la décision d'expurger les

[52] https://community.icann.org/display/EOTSFGRD/EPDP+-P2A+Legal+subteam

données traitées pour cause ou pour des raisons de commodité pour la partie contractante, entre autres.

III. Travail du futur code de conduite

Enfin, bien que cela ait potentiellement été hors de portée pour cette étape 2A de l'EPDP, le rapport final contient une disposition exigeant que l'ICANN considère les directives présentées vis-à-vis d'un code de conduite dans tout engagement futur avec le Comité européen de la protection des données. Dans un premier temps, la recommandation est faible dans la mesure où elle n'impose pas la création d'un code de conduite. En outre, la recommandation est formulée de manière ambiguë pour inclure les autorités de contrôle et les responsables du traitement, avec une phrase distincte faisant allusion à « la communauté ». Plus inquiétant encore, lorsque l'IPC a insisté pour que le rapport final précise que les groupes représentant les demandeurs de données RDS doivent être inclus explicitement en tant qu'autorités de contrôle et les responsables du traitement (à leurs propres fins), certaines parties contractantes ont présenté des objections, se référant aux demandeurs comme des « intérêts de tiers ». Dans l'environnement multipartite de l'ICANN, la communauté, en particulier la communauté diversifiée représentée au sein et à travers la GNSO, ne doit pas être reléguée au statut « d'observateur » sur quelque chose d'aussi impactant que le statut juridique des données RDS qui est si fondamental pour la sécurité, la stabilité et la résilience du DNS.

IV. Adresse e-mail pseudonymisée par titulaire de nom de domaine

L'IPC reste convaincue qu'une adresse e-mail pseudonymisée du titulaire de nom de domaine devrait être publiée obligatoirement dans le WHOIS/RDDS. Les conseils juridiques obtenus par l'équipe responsable de l'étape 2A de l'EPDP ont identifié le risque de publication comme « modéré » étant donné que de telles données pourraient être utilisées pour identifier un titulaire de nom de domaine d'une personne physique lorsqu'elles sont combinées à d'autres données à caractère personnel. Cependant, les bénéfices d'intérêt public d'une telle publication l'emportent sur les droits de protection de la vie privée de la personne concernée, car la capacité d'utiliser des adresses e-mail pseudonymisées basées sur le titulaire de nom de domaine est essentielle pour faciliter la corrélation entre les propriétaires de domaines afin de traiter les réseaux qui menacent la sécurité à grande échelle, les programmes d'hameçonnage et les sites contrefaisants de la propriété intellectuelle. Nous remarquons que la publication d'adresses e-mail basées sur un nom pseudonymisé semblerait conforme au RGPD, et notons que plusieurs entités européennes de la chaîne d'approvisionnement du DNS publient en fait les adresses e-mail *réelles* du titulaire de nom de domaine sans être en mesure de s'en tenir au RGPD, comme indiqué dans les directives juridiques fournies à

l'EPDP.[53] Si le Comité européen de la protection des données ou une autorité de protection des données considère que cette approche n'est pas conforme au RGPD, la politique pourrait être rétablie à l'exigence actuelle de publication d'une adresse e-mail anonymisée ou d'un lien vers un formulaire Web, avec la divulgation de l'adresse électronique réelle en réponse à des demandes de tiers valides.

V. Conclusion

En conclusion, bien que l'IPC appuie le consensus obtenu pour créer un élément de données normalisé qui reflète la nature (morale ou physique) du titulaire de nom de domaine et/ou des données d'enregistrement, le rapport final de l'étape 2A de l'EPDP ne parvient pas à atteindre son objectif ultime. La Recommandation 17.3 de l'étape 1 de l'EPDP exigeait que, outre la différenciation facultative, « l'équipe responsable de l'EPDP détermine et résolve la question de la distinction entre personne morale et personne physique au cours de l'étape 2 ». Malheureusement, cette question n'a pas encore été résolue. Exiger que l'ICANN coordonne la communauté technique dans la création d'un élément de données que les parties contractantes sont libres d'ignorer est tout à fait loin de « résoudre » la question de la distinction entre personne morale et personne physique. Et ne pas exiger la différenciation des données à caractère personnel et non personnel ne parvient pas à atteindre l'objectif global de l'EPDP de « préserver la base de données WHOIS dans la mesure du possible » tout en respectant la loi en matière de vie privée.

[53] « Dans sa base de données Whois, EURid publie les adresses e-mail des titulaires de noms de domaine dans le TLD .eu (de personnes physiques et/ou d'entités étant des personnes morales) .... De même, bien que RIPE-NCC s'appuie sur le consentement pour publier des renseignements à caractère personnel sur les contacts tech/admin, il publie des informations à caractère personnel sur les titulaires de ressources au motif que « faciliter la coordination entre les opérateurs de réseaux est le seul but qui justifie la publication de données à caractère personnel dans la base de données de RIPE-NCC et qu'il est clair que le traitement des données à caractère personnel se rapportant à un titulaire de ressources est nécessaire pour l'exécution de la fonction de registre, qui est effectuée dans l'intérêt légitime de la communauté RIPE et du bon fonctionnement de l'Internet dans le monde (et qui est donc conforme à l'article 6.1.f du RGPD) ». Note de Bird & Bird du 27 avril 2021, rapport initial de l'étape 2A de l'EPDP, pages 56 et 57.

Déclaration de la minorité du Comité consultatif gouvernemental portant sur le rapport final de l'étape 2A du Processus accéléré d'élaboration de politiques (EPDP) au sujet des données d'enregistrement des gTLD

Remarque : le Comité consultatif At-Large (ALAC), l'Unité constitutive des utilisateurs commerciaux (BC) et l'Unité constitutive des représentants de la propriété intellectuelle (IPC) soutiennent les positions exprimées dans ce commentaire.

Introduction et commentaire général

Le GAC apprécie le temps et l'engagement considérables de l'équipe responsable de l'étape 2A de l'EPDP, de ses dirigeants et du personnel de soutien de l'ICANN pour l'élaboration de ces recommandations de politique complexes et importantes concernant le traitement des données d'enregistrement de noms de domaine des entités juridiques et des contacts e-mail pseudonymisés. Bien que le GAC reconnaisse l'utilité de nombreuses composantes des recommandations finales, ce comité reste préoccupé par le fait que presque aucune des recommandations finales ne crée d'obligations exécutoires. Elles ne répondent donc pas aux attentes du GAC en matière de politiques qui exigeraient la publication de données d'enregistrement de noms de domaine non protégées par le Règlement général sur la protection des données (RGPD) de l'UE et la création d'un cadre approprié pour encourager la publication de contacts e-mail pseudonymisés avec des garanties appropriées.

Pour ce qui est du contexte, comme l'a souligné le GAC dans ses contributions précédentes,[54] les autorités d'application de la loi, la protection du consommateur et d'autres personnes chargées de protéger le public contre les actions malveillantes facilitées par le DNS, ont besoin d'un accès rapide et efficace aux données d'enregistrement de noms de domaine. Jusqu'en mai 2018, cet accès était disponible au public via le système WHOIS. En réponse au RGPD, l'ICANN a mis en œuvre des politiques qui permettent de masquer une grande partie de ces données, même celles qui ne sont pas protégées par le RGPD. Comme le RGPD ne protège pas les informations de contact des personnes morales, de nombreux groupes de parties prenantes, y compris le GAC, ont demandé pourquoi les politiques de l'ICANN permettaient l'expurgation d'informations non protégées dans les résultats du RDS/WHOIS. Par conséquent, le GAC et d'autres groupes de parties prenantes ont encouragé l'élaboration de politiques plus précises qui protégeraient les données à caractère personnel tout en publiant des données à caractère non personnel, y compris les données d'enregistrement liées aux entités juridiques, reconnaissant ainsi que la

[54] Voir les commentaires du GAC sur le rapport final de l'étape 1 de l'EPDP (20 février 2019), le commentaire du GAC sur le rapport initial de l'étape 2 (24 mars 2020) et le commentaire du GAC sur le supplément au rapport initial de l'étape 2 (5 mai 2020). Voir aussi le communiqué du GAC d'Abou Dhabi (1er novembre 2017), le communiqué du GAC de San Juan (15 mars 2018) et le communiqué du GAC de Barcelone (25 octobre 2018).

publication de données d'enregistrement de noms de domaine non protégées est en faveur de l'intérêt public.

La portée des travaux dans le cadre de l'étape 2A de l'EPDP a donné suite à ces préoccupations et s'est concentrée sur deux sujets, à savoir :

1. La différenciation des données d'enregistrement entre personnes morales et personnes physiques ;
2. La faisabilité d'une adresse électronique anonymisée[55] uniforme pour les contacts uniques.

Dans le premier sujet, les questions abordées étaient les suivantes :

i. Établir si des mises à jour doivent être apportées aux recommandations de l'étape 1 de l'EPDP à ce sujet (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire » ;[56]
ii. Établir quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la différence entre les enregistrements des personnes morales et celui des personnes physiques.

Sous le deuxième thème « faisabilité d'une adresse électronique anonymisée uniforme pour les contacts uniques », l'équipe responsable de l'EPDP a abordé les questions suivantes :

i. Évaluer s'il est possible ou non pour les contacts uniques d'avoir une adresse électronique anonymisée uniforme et, dans ce cas, si cela devrait être une exigence ; et,
ii. Si cela était possible, mais pas obligatoire, quelles directives devraient être fournies, le cas échéant, aux parties contractantes souhaitant mettre en place des adresses e-mail anynomisées uniformes.

Le GAC croit que les recommandations finales de l'étape 2A fournissent plusieurs éléments constructifs, notamment :

1. La création de champs de données pour signaler/identifier les titulaires de noms de domaine légaux et les données à caractère personnel ;
2. Des directives spécifiques sur les garanties qui devraient s'appliquer pour protéger les informations à caractère personnel lorsqu'il s'agit de différencier les enregistrements de noms de domaine des personnes morales et des personnes physiques ;
3. L'encouragement pour la création d'un code de conduite qui inclurait le traitement des données d'enregistrement de noms de domaine provenant d'entités juridiques ;

[55] L'équipe responsable de l'EPDP a par la suite conclu que le terme « pseudonymisé » était le plus précis. Voir « Définitions » à la p.24 du Rapport final de l'étape 2A de l'EPDP.
[56] Voir la recommandation 17 du rapport final de l'étape 1 de l'EPDP à : https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.

4. L'encouragement pour que la GNSO fasse le suivi des développements législatifs pouvant exiger des révisions aux recommandations politiques actuelles, et
5. Le contexte et les conseils utiles pour ceux qui souhaitent publier des e-mails pseudonymisés.

Néanmoins, les recommandations finales ne sont pas à la hauteur parce qu'elles proposent principalement des mesures facultatives plutôt que des mesures obligatoires, même si elles s'appliquent à des informations qui ne sont pas protégées par le RGPD, comme les données à caractère non personnel des entités juridiques. Les actions facultatives peuvent conduire à un système fragmenté et incertain pour les demandeurs et les personnes concernées, avec différentes stratégies sur différents bureaux d'enregistrement pour la manière dont les données sont protégées ou divulguées.[57]

Pour rappel, un pourcentage important de noms de domaine est enregistré par des entités juridiques et le RGPD ne protège généralement pas leurs données d'enregistrement de noms de domaine à caractère non personnel. Certaines analyses montrent qu'un ensemble considérablement plus important d'informations d'enregistrement a été rédigé par rapport à ce qui est exigé par le RGPD, c'est-à-dire « peut-être cinq fois plus que ce qui est nécessaire ».[58] Par exemple, les données disponibles suggèrent que seulement 11,5 % environ des domaines appartiendraient à des personnes physiques soumises au RGPD, alors que les coordonnées de 57,3 % de tous les domaines ont été expurgées.[59] Ce masquage de nombreuses données d'enregistrement, sans doute inutile, entrave un grand nombre d'avantages associés à la transparence concernant la propriété des noms de domaine.

En ce qui concerne le traitement des données des personnes morales, le GAC estime qu'une telle différenciation devrait être nécessaire pour de nombreuses raisons différentes (comme indiqué ci-dessous) qui bénéficient le public.

Tout d'abord, la publication de données d'enregistrement de noms de domaine non publics concernant les entités juridiques augmenterait l'information disponible pour les entités chargées de protéger le public. Compte tenu de la prévalence des délits sur Internet, la publication des données d'enregistrement des entités juridiques aiderait les agences d'application de la loi et de protection du consommateur et la capacité des professionnels de la cybersécurité à enquêter rapidement et plus efficacement sur les activités illicites facilitées par le DNS, y compris les efforts de lutte contre la

[57] Le GAC a exprimé ses préoccupations concernant les politiques qui risquent la fragmentation des contributions précédentes, y compris le Communiqué du GAC de Barcelone (25 octobre 2018). Voir aussi la Déclaration de la minorité du GAC à propos du Rapport final de l'étape 2 de l'EPDP sur les données d'enregistrement des gTLD (24 août 2020)

[58] Voir le résumé analytique de l'étude du WHOIS sur la disponibilité des données de contact et la classification des titulaires de noms de domaine (25 janvier 2021) à l'adresse https://www.icann.org/en/system/files/correspondence/chapin-to-botterman-25jan21-en.pdf.

[59] Ibid.

cybercriminalité. En outre, la publication permet aux agences d'application de la loi ou aux équipes d'intervention informatique d'urgence de 1) identifier rapidement la juridiction ou l'emplacement des entreprises victimes de cybercriminalité et 2) fournir à grande échelle, aux entités juridiques, des notifications et des messages de protection en cas de compromission de leurs domaines.

Deuxièmement, l'exigence pour que les bureaux d'enregistrement publient les données d'enregistrement de noms de domaine des entités juridiques réduirait de manière significative le nombre de demandes de divulgation de données d'enregistrement de noms de domaine et les défis associés à l'obtention de réponses à la divulgation,[60] car cet ensemble de données serait déjà accessible au public. Troisièmement, la mise à la disposition du public de données à caractère non personnel accroît généralement la confiance dans le DNS en permettant la transparence quant à la propriété des noms de domaine, y compris les domaines qui facilitent les communications et les transactions sensibles en ligne.

Enfin, les conseils juridiques reçus soulignent les faibles risques associés aux données d'enregistrement des entités juridiques. Dans la mesure où les informations personnelles sont incluses dans les données d'enregistrement d'une entité juridique, elles sont susceptibles d'être « peu sensibles » parce qu'elles concernent les détails de travail d'un employé plutôt que sa vie privée.[61] En outre, si les garanties appropriées sont suivies, les risques juridiques associés à cette publication, même en cas d'erreurs involontaires, semblent faibles.[62]

En résumé, nous soutenons qu'un processus de différenciation par les parties contractantes entre les données des personnes morales et celles des personnes physiques doit être rendu obligatoire. Le rapport final ne reflète pas suffisamment les divers intérêts en jeu dans la discussion sur la différenciation et la publication ultérieure d'informations non protégées. Le GAC estime que l'intérêt public l'emporte sur les préoccupations commerciales, notamment parce que la disponibilité publique de l'information favoriserait la stabilité, la sécurité et la résilience du DNS.

Les commentaires suivants identifient des préoccupations spécifiques concernant les recommandations finales.

Recommandation 1 - Champs pour faciliter la différenciation entre les données d'enregistrement des personnes morales et des personnes physiques

[60] Voir article 5.3.1 du rapport préliminaire de l'équipe de révision du service d'annuaire de données d'enregistrement (31 août 2018) et l'enquête commune des groupes de travail anti-hameçonnage, et anti-abus pour la messagerie, les programmes malveillants et les mobiles (18 octobre 2018)

[61] Voir la Note de Bird & Bird du 6 avril 2021.

[62] Ibid

Le GAC a encouragé la création et l'utilisation de champs de données pour signaler les titulaires de noms de domaine étant des personnes morales et la présence ou l'absence de renseignements personnels dans leurs ensembles de données. De tels mécanismes de signalisation fourniraient une première étape nécessaire à la différenciation. La Recommandation 1 comprend plusieurs obligations en ce qui concerne la création de champs afin de faciliter la différenciation entre les données d'enregistrement des personnes morales et des personnes physiques et d'identifier si ces données d'enregistrement contiennent des données à caractère personnel ou non personnel. Outre la création de ces champs, il existe d'autres obligations :

- Que l'ICANN coordonne la communauté technique, par exemple le groupe de travail RDAP, afin de développer les normes nécessaires associées à ce(s) domaine(s) ;
- Que le SSAD, conformément aux recommandations de l'étape 2 de l'EPDP, soutienne les champs afin de faciliter l'intégration entre le SSAD et les systèmes des parties contractantes ; et
- Que les champs prennent en charge des valeurs spécifiques liées au statut des personnes morales et à la présence ou l'absence de données à caractère personnel.

Le GAC apprécie particulièrement la précision de cette recommandation en spécifiant précisément les valeurs à inclure dans ces champs. Le GAC estime toutefois que la Recommandation 1 serait plus efficace pour créer l'infrastructure nécessaire à la différenciation si :

1. Il est demandé aux parties contractantes non seulement de créer, mais également d'utiliser ces champs ;
2. Des délais précis sont définis pour rendre ces champs opérationnels ; et
3. Il est garanti que les champs fonctionneront dans le cadre des systèmes actuels et envisagés de collecte et de divulgation de données.

Pour plus de clarté, le GAC estime que l'obligation pour les parties contractantes de remplir ces champs pour tous les enregistrements futurs, sans tenir compte du fait que les parties contractantes choisissent ou non de différencier dans leur traitement des données des entités morales et des entités physiques, est efficace et dans l'intérêt public parce qu'elle fournirait une base pour signaler et identifier les données qui pourraient faire l'objet de futures demandes accélérées du SSAD ou d'obligations juridiques futures.[63]

Le GAC note également qu'une utilisation volontaire d'un tel champ est incompatible avec les étapes précédentes de l'EPDP, où des mesures telles que des expurgations de

[63] À cet égard, le GAC se félicite que le rapport final encourage la GNSO à évaluer si des travaux politiques futurs sont nécessaires à la lumière des développements législatifs. Par exemple, l'EPDP a pris note des discussions en cours et de l'adoption prévue de la Directive révisée sur la sécurité des réseaux et des systèmes d'information (« NIS2 »). Voir la « proposition au conseil de la GNSO » à la p.15 du Rapport final de l'étape 2A de l'EPDP.

données ont été appliquées à l'ensemble du système plutôt que de s'appuyer sur des décisions individuelles des parties contractantes.

Recommandation 2 - Orientation pour les parties contractantes qui choisissent de se différencier

L'équipe responsable de l'EPDP a créé les directives pour la différenciation en fonction des principes applicables du RGPD et des conseils juridiques approfondis. Notamment, le conseil juridique a identifié des garanties très spécifiques pour atténuer le risque de divulgation illicite et a observé que, en tout état de cause, les données en cause n'étaient pas aussi sensibles que d'autres catégories d'informations personnelles parce qu'elles étaient liées au travail, plutôt qu'à la vie privée. Enfin, le conseil juridique a fait observer que si les garanties étaient respectées, il est peu probable que la divulgation accidentelle d'informations personnelles aboutirait à des mesures d'exécution. Comme les directives ont adopté les garanties conseillées, les risques de responsabilité sont faibles et discutés précédemment, alors que les avantages pour le public sont élevés.

Pour les raisons évoquées ci-dessus, le GAC estime que la recommandation aurait dû faire en sorte que les parties contractantes établissent une distinction entre les entités juridiques et physiques. En conséquence, il aurait également dû demander aux parties contractantes d'appliquer les directives applicables identifiées dans la Recommandation 2 et de publier toutes les données à caractère non personnel des entités juridiques dans les données accessibles au public. Le GAC estime également que les garanties reflétées dans la Recommandation 2 sont plus justement appelées « Meilleures pratiques ».

Recommandation 3 - Codes de conduite et exemples de scénarios

Le GAC se félicite de la recommandation de l'équipe responsable de l'EPDP selon laquelle les directives de l'équipe énoncées dans la Recommandation 2 devraient être prises en considération dans tout travail futur possible au sein de l'ICANN par les autorités de contrôle et les responsables du traitement concernés en relation avec l'élaboration d'un code de conduite du RGPD. Le GAC note que les parties prenantes concernées par un tel code devraient avoir la possibilité de participer à l'élaboration de ce code, y compris les demandeurs potentiels (et donc les responsables potentiels du traitement) de données d'enregistrement de noms de domaine.

Le GAC apprécie également les conseils fournis par les scénarios spécifiques. Le GAC croit que la logique et la clarté de ces trois scénarios seraient améliorées si la publication ou la non-divulgation dans le cadre des scénarios applicables était exigée. Chaque scénario énonce des conditions spécifiques qui, logiquement, exigent la publication ou la non-divulgation des données d'enregistrement de noms de domaine et, par conséquent, l'utilisation du mot « devrait » plutôt que « doit » dans ces scénarios est déplacée.

Recommandation 4 - Adresses e-mail pseudonymisées

En ce qui concerne les contacts uniques et les adresses e-mail pseudonymisées, le GAC salue les mesures à prendre pour fournir des conseils sur la publication d'une adresse e-mail par le biais de la méthode de protection des données qui utilise des techniques d'anonymisation et note les niveaux de risque réduits que cela représente pour la publication, comme indiqué dans les notes juridiques reçues par l'équipe responsable de l'EPDP.[64] Bien que le GAC reconnaisse qu'il existe certains risques liés à la publication d'informations, même pseudonymisées, le considérant 28 du RGPD souligne l'utilisation de la pseudonymisation comme méthode pour réduire ces risques pour les personnes concernées et aider les autorités de contrôle et les responsables du traitement à respecter leurs obligations en matière de protection des données. En outre, les e-mails pseudonymisés sont largement utilisés par les services d'anonymisation et d'enregistrement fiduciaire avec peu ou pas d'impact sur un grand nombre de personnes concernées. Le GAC note également les avantages qu'une telle publication d'e-mails pseudonymisés fournirait, en particulier en ce qui concerne la facilitation de communications rapides et efficaces avec les titulaires de nom de domaine. Il a été signalé que certains formulaires Web n'avaient pas été des mécanismes efficaces pour communiquer avec les titulaires de noms de domaines.

[64] Voir la Note de Bird & Bird du 9 avril 2021sur les options de masquage des adresses de contact et la Note de Bird & Bird du 4 février 2020 sur les questions concernant un système normalisé d'accès et de divulgation (« SSAD »), les services d'anonymisation et d'enregistrement fiduciaire et les e-mails pseudonymisés.

Déclaration de la minorité du NCSG sur le rapport final de l'étape 2 de l'EPDP

Le NCSG est heureux de voir que les tâches finales des étapes 1 et 2 de l'EPDP sont achevées. Le NCSG est également heureux que l'ICANN se conforme enfin à la loi sur la protection des données, ce à quoi nous avons insisté depuis les premiers jours des discussions sur les politiques relatives au WHOIS. Toutefois, le processus de cet EPDP a été inutilement long et douloureux et ne reflète pas une appréciation de la responsabilité de l'ICANN de se conformer à la loi sur la protection des données, mais plutôt la difficulté à amener de nombreuses parties prenantes à adopter le concept de respect des droits des titulaires de nom de domaine. Nous pensons également que la prolifération des déclarations de la minorité, réitérant des positions qui ont été débattues à plusieurs reprises au cours des neuf derniers mois, voire des trois dernières années, est inutile. Cependant, il est loin de l'intention du NCSG de se fonder sur ce principe et de refuser de reformuler nos propres arguments.

Nous avons maintes fois évoqué les droits du titulaire de nom de domaine. D'habitude, nous étions les seuls à souligner les droits du titulaire de nom de domaine ; nous devrions avoir été rejoints par au moins l'ALAC, le SSAC et le GAC, qui ont des rôles clairs dans la représentation des droits des titulaires de noms de domaine. Heureusement, les parties contractantes soutiennent également leurs clients et leur font régulièrement part de leurs propres obligations. L'ICANN devrait également insister sur les droits des clients dans son rôle d'intermédiaire neutre de l'accord de MS pour gérer les gTLD.

Le manque de clarté concernant le rôle de l'organisation ICANN en tant qu'autorité de contrôle dans une relation de co-contrôleur a également embrouillé les eaux et rendu plus complexe l'idée de la politique. Nous avons souvent déclaré que la nature précise des rôles de l'ICANN et des parties contractantes aurait dû être clarifiée, sans doute avec l'aide d'un avocat externe, au début de cet effort. La nature des arrangements du co-contrôleur est importante ; beaucoup de temps aurait été économisé, et des confusions évitées, si nous avions été plus conscients de ces relations contractuelles éventuelles.

Plusieurs parties ont soulevé la question des projets de règlementation en Europe qui pourraient avoir un impact sur l'application du RGPD, ce qui a ralenti la procédure. Notre position est que nous ne devrions pas essayer de modifier le travail accompli dans les deux premières étapes de cet EPDP en nous basant sur des spéculations sur la réglementation potentielle. Encore une fois, le désir de freiner la mise en œuvre du RGPD avant que de telles réglementations ne soient promulguées et intégrées dans les lois nationales indique le manque de considération de la loi sur la protection des données et les droits à la vie privée des titulaires de noms de domaine.

En ce qui concerne les questions précises abordées dans le présent rapport, nous avons souligné tout au long de cet EPDP, et dans un PDP précédent sur les services d'anonymisation et d'enregistrement fiduciaire que la distinction entre personne morale

et personne physique n'est pas une distinction utile à faire lorsqu'il s'agit de décider de la nécessité de protéger les données dans le RDS. Comme nous l'avons répété à maintes reprises, c'est la mauvaise question à poser, parce que de nombreux travailleurs employés par une personne morale ou une entreprise ont des droits à la vie privée en ce qui concerne la divulgation de leurs informations personnelles et de leurs données de contact. La personne morale n'a pas de droits à la vie privée, mais les personnes physiques en ont.
Même si nous suivons la question « personne morale vs. personne physique » avec une question de clarification exigeant que le titulaire de nom de domaine témoigne qu'aucune information personnelle n'est incluse dans les informations qu'il fournit, cela n'élimine en aucun cas les risques de divulgation d'informations personnelles. De nombreuses organisations ont du mal à répondre à ces deux questions, en particulier les organisations que représente le NCSG, qui comprennent les organisations à but non lucratif, les organismes bénévoles, les clubs et les groupes d'intérêt, les groupes religieux, les organisations de défense des droits humains, etc.

Cela est également vrai pour les entrepreneurs uniques, certains types de professionnels et les travailleurs indépendants qui sont traités comme des entrepreneurs, mais qui fonctionnent réellement dans une relation employeur/employé. Bien que ce soit assez facile pour les grandes entreprises dotées d'équipes juridiques, même celles qui ont des activités dispersées dans le monde entier, de s'assurer qu'elles puissent répondre à cette question, cela n'est pas facile pour les petites entités ayant des budgets plus réduits et une manière non corporative de s'engager avec leurs bénévoles et leurs membres.

Notre position est donc que, du fait que la distinction n'est pas claire pour de nombreuses entités, il n'est pas pratique ou souhaitable de mandater la distinction, et bien que les parties contractantes aient développé d'excellentes directives pour leurs membres afin de les aider à décider comment traiter cette distinction, cette orientation ne doit pas faire partie de la politique. Si elle en fait partie, elle devient une orientation sur les questions juridiques et ce n'est pas quelque chose que l'ICANN devrait faire. Les parties contractantes sont parfaitement capables de publier ces directives par elles-mêmes, et l'ICANN est parfaitement capable de les faire remarquer comme étant les meilleures pratiques du secteur privé, et non comme des directives dans le cadre de leur politique et appliquées par l'ICANN. Les parties contractantes doivent connaître au mieux leur propre risque juridique et, puisqu'elles sont les autorités de contrôle et responsables de toute amende pouvant résulter d'une action de mise en application, elles doivent être libres de décider de la manière de gérer la divulgation des informations des clients.
Nous notons que les parties qui ont le plus insisté à faire cette distinction entre personnes morales et personnes physiques ont également insisté pour avoir un ou plusieurs champs pour saisir les données. Étant donné que la recommandation établit qu'il s'agit d'un champ volontaire du ressort des parties contractantes, dont les modèles commerciaux et la manière d'utiliser les champs varient énormément, nous ne pensons

pas que les recommandations concernant la précision du champ soient utiles. Si l'ICANN s'engage à instruire l'IETF, par exemple, sur la manière de normaliser le champ, comment la distinction, la collecte et la divulgation des données pertinentes sont-elles nécessaires pour rendre cette distinction encore volontaire ? C'est une question à laisser aux meilleures pratiques du secteur privé.

Nous avons également parlé des droits des travailleurs indépendants, des entrepreneurs uniques, des artistes indépendants, des vendeurs et des commerçants, même si nous avons explicitement pour mission de représenter les parties prenantes non commerciales. Personne d'autre ne représente ces gens, dont le nombre augmente de plus en plus rapidement alors que les modèles d'emploi se transforment avec l'économie mondiale de l'Internet. Cette lacune est révélatrice de l'accent mis sur les grandes entreprises et du manque de concentration sur les questions concurrentielles qui sont exacerbées par la politique du DNS. Nous espérons que les parties contractantes aborderont les droits de ces personnes et veilleront à ce qu'elles soient traitées équitablement et dans le respect des normes de respect à la vie privée lorsque cette politique sera mise en œuvre.

Groupe des représentants des bureaux d'enregistrement

Les représentants du groupe des représentants des bureaux d'enregistrement (RrSG) auprès du groupe de travail (WG) de l'étape 2A de l'EPDP souhaitent remercier le personnel de l'ICANN et tous les autres membres du groupe de travail de l'EPDP pour leur travail acharné tout au long de cette étape de l'EPDP. La déclaration suivante vise à compléter notre vote consensuel et notre contribution tout au long du travail de l'étape 2A de l'EPDP.

Commentaires d'ordre général

Tout au long des délibérations de l'étape 2A de l'EPDP, l'équipe du RrSG a souligné que chaque bureau d'enregistrement individuel doit être en mesure de déterminer le niveau de risque qu'il assume, dans le cadre d'une base de référence qui permette le respect des obligations légales pertinentes. De même, chaque bureau d'enregistrement individuel doit être en mesure de déterminer ce qu'il considère être commercialement et techniquement faisable pour sa propre activité commerciale unique.

Bien que les recommandations présentées par ce groupe de travail de l'étape 2A de l'EPDP permettent l'autodétermination, en fournissant des options et des conseils aux bureaux d'enregistrement et aux opérateurs de registre qui choisissent de faire la distinction pour évaluer la présence de données à caractère personnel dans le dossier d'enregistrement, ou qui choisissent de publier un e-mail de contact par titulaire de nom de domaine ou pour chaque enregistrement, il est décevant que l'obtention de ce résultat ait été le produit d'une lutte importante. Tout au long du travail sur cette étape, le groupe de travail a réexaminé les questions à plusieurs reprises sans ajouter quoi que

ce soit de nouveau à la discussion, et a discuté de sujets qui étaient en dehors de sa portée. Peut-être plus important encore, très souvent le groupe de travail n'était ni intéressé ni préoccupé par les risques juridiques et financiers que certaines obligations proposées créeraient pour les parties contractantes dans différentes juridictions ou de modèles commerciaux différents, ou les risques pour les titulaires de noms de domaine eux-mêmes.

Enfin, nous notons que tous les avantages potentiels des obligations politiques dans ces domaines, qui annuleraient la capacité cruciale des bureaux d'enregistrement à choisir leurs propres obligations juridiques, commerciales, et les risques techniques, n'ont pas été démontrés clairement ou de manière assez convaincante pour montrer un besoin absolu de telles obligations par opposition à des options moins problématiques suggérées par l'équipe des représentants des bureaux d'enregistrement. Les obligations politiques suggérées ne sont pas fondées sur une nécessité stricte ou sur des améliorations largement acceptées de l'écosystème des noms de domaine, ce qui peut justifier leur exigence. L'équipe du RrSG est donc convaincue que le résultat du travail de l'étape 2A, y compris les directives et les exigences facultatives pour la différenciation et l'utilisation d'une adresse électronique par titulaire de nom de domaine ou pour chaque enregistrement, est approprié.

Entités juridiques vs. personnes physiques

L'équipe du RrSG appuie le maintien de la Recommandation 17 (1) de l'étape 1 et considère que cela résout la question mentionnée dans la recommandation 17 (3) de l'étape 1. Bien que les divers groupes représentés dans le groupe de travail de l'étape 2A de l'EPDP ne soient pas arrivés à un accord sur la question, tous les apports pertinents ont été examinés et traités en détail au cours des délibérations et aucune autre délibération n'est prévue ou attendue ; dans ce cadre, la question a été résolue. De plus, c'est la *bonne* résolution. Chaque bureau d'enregistrement individuel doit contrôler sa propre analyse des risques et des avantages et tenir compte de sa propre réalité juridictionnelle afin de déterminer si et comment il se différenciera, et le résultat auquel nous sommes parvenus maintient la capacité de le faire.

L'équipe des bureaux d'enregistrement souligne que la méthode de différenciation variera d'un bureau d'enregistrement à l'autre. L'utilisation « d'indicateurs » ou de « champs » pour n'indiquer le type de personne ou la présence de données à caractère personnel ainsi que le contenu de l'orientation elle-même a été abordée dans cette étape comme étant facultative, plutôt qu'obligatoire pour tous les bureaux d'enregistrement. Cette orientation de haut niveau est le produit d'un compromis important ; elle est utile, mais ne s'applique pas dans toutes les situations ou à tous les bureaux d'enregistrement dans le monde entier. À ce titre, elle *doit* demeurer facultative. Toute directive ou code de conduite obligatoire ne peut être créé que par les parties contractantes concernées elles-mêmes, en tenant dûment compte des commentaires de la communauté.

Faisabilité de contacts uniques

L'équipe RrSG convient que la publication d'une adresse électronique basée sur l'enregistrement ou sur le titulaire de nom de domaine dans le RDDS public est une activité de traitement de données et apprécie les commentaires utiles et minutieux fournis par Bird & Bird sur ce sujet. Bien que certaines mises en œuvre de cette option de publication puissent présenter un risque plus faible que d'autres, nous notons à nouveau que chaque bureau d'enregistrement individuel doit être en mesure de déterminer le degré auquel il assume des risques juridiques, plutôt que de céder la prise de cette décision au groupe de travail de l'étape 2A de l'EPDP. Par conséquent, nous encourageons tous les lecteurs de ce rapport final à examiner les directives juridiques fournies à ce sujet (incluses à l'annexe F du présent rapport), et nous prévoyons que des directives et un soutien supplémentaires seront mis à la disposition des membres du Groupe de représentants des bureaux d'enregistrement, le cas échéant.

Pour de plus amples informations sur les points de vue de l'équipe RrSG à cet égard, veuillez voir également notre article sur Circle ID : La vie privée, personnes morales vs. personnes physiques, et l'EPDP de l'ICANN sans fin. Merci.

Groupe des représentants des opérateurs de registres

Déclaration de la minorité au rapport final de l'étape 2A du processus accéléré d'élaboration de politiques sur les données d'enregistrement des gTLD

Après plus de trois ans de diligence, le RySG est heureux de célébrer la résolution du processus accéléré d'élaboration de politiques sur la spécification temporaire pour les données d'enregistrement de gTLD (« EPDP »). Il s'agissait d'un effort presque sans précédent, déclenché par la promulgation du RGPD, qui a exigé que la communauté de l'ICANN se réunisse pour résoudre les incompatibilités de longue date avec les obligations en matière de protection des données. Le RySG est extrêmement reconnaissant pour le travail et l'engagement de nos présidents et vice-présidents, de l'infatigable équipe de soutien de l'ICANN et des membres de l'équipe responsable de l'EPDP qui se sont engagés de bonne foi à trouver un terrain d'entente et à comprendre ces sujets certes complexes.

Le RySG est convaincu que, comme dans les étapes précédentes de ce travail, nous sommes parvenus au juste équilibre entre la protection des droits à la vie privée de la personne concernée par les données, le respect de nos obligations légales et la non-création d'obstacles inutiles ou de défis opérationnels pour nos clients ou nos entreprises.

I. La question personne morale vs. personne physique est résolue

L'étape 2A a résolu la question de la différenciation entre personne morale et personne physique. Un PDP n'est pas obligé à donner lieu à des recommandations consensuelles pour résoudre un problème. Le fait que le groupe de travail ne se soit pas mis d'accord sur les changements apportés à la recommandation précédente (Recommandation 17 de l'étape 1) sur la distinction entre personne physique et personne morale est un résultat de grande valeur et acceptable. Après trois étapes de délibération de l'EPDP, une étude réalisée par l'organisation ICANN, et des conseils juridiques d'un avocat externe sur la différenciation entre personne morale et personne physique, il est bien temps de reconnaître que ce problème est clos.

En effet, l'équipe responsable de l'EPDP a suivi avec diligence les instructions du conseil de la GNSO pour « répondre . . . si des mises à jour doivent être apportées aux recommandations relatives à ce sujet issues de la première étape de l'EPDP (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire) » ;[65] Pour répondre à cette question

[65] Instructions du conseil de la GNSO pour la question de la distinction entre personne morale et personne physique dans l'étape 2A : « L'équipe responsable de l'EPDP devrait examiner l'étude entreprise par l'organisation ICANN (comme demandé par l'équipe responsable de l'EPDP et approuvé par le conseil de la GNSO au cours de l'étape 1) ainsi que les conseils juridiques fournis par Bird & Bird et les contributions substantielles fournies à ce sujet lors du forum de consultation publique sur le supplément et la réponse :

précise, il fallait tenir compte des trois parties de la Recommandation 17 de l'étape 1 dans son intégralité.[66] Les arguments selon lesquels l'équipe responsable de l'EPDP n'a pas satisfait à la Recommandation 17.3 (« l'équipe responsable de l'EPDP déterminera et réglera la question des personnes morales vs. les personnes physiques à l'étape 2 ») adoptent une vision délibérément étroite du texte de la recommandation, ignorant le langage clair des instructions du conseil de la GNSO. Le RySG s'inquiète du fait que certains aient suggéré que ce problème n'est pas résolu. Cette question a été abordée dans trois étapes distinctes de l'EPDP et, à chaque fois, le résultat a été que les parties contractantes pourraient faire la distinction, mais ne sont pas tenues de le faire. Cela démontre clairement que cette question a été traitée de manière appropriée et cohérente. La perception que ce travail n'a pas en quelque sorte été résolu pourrait nuire à la communauté de l'ICANN et être considérée comme une atteinte à l'efficacité du modèle multipartite. Cela serait également injuste pour les membres du groupe de travail et pour les innombrables heures qu'ils ont dédiées à délibérer et à régler la question.

II. La différenciation facultative reste un bon résultat

Le RySG croit fermement que le maintien des recommandations de politique de l'étape 1, permissives, mais non obligatoires[67], pour les données d'enregistrement des personnes morales et des personnes physiques est un résultat objectivement bon de notre travail d'élaboration de politiques. Ce résultat ne consiste pas simplement à

I. Si des mises à jour doivent être apportées aux recommandations relatives à ce sujet issues de la première étape de l'EPDP (« Les bureaux d'enregistrement et les opérateurs de registre ont le droit d'établir une différence entre les enregistrements de personnes morales et ceux de personnes physiques, mais ne sont pas tenus de le faire » ;

II. Quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la différence entre les enregistrements de personnes morales et ceux de personnes physiques ».

[66] Le rapport final de l'étape 1 de l'EPDP contient la recommandation suivante sur la question concernant les personnes morales et les personnes physiques : **Recommandation 17,1 :** « L'équipe responsable de l'EPDP recommande que les bureaux d'enregistrement et les opérateurs de registre soient autorisés à différencier entre les enregistrements de personnes physiques et ceux de personnes morales sans, toutefois, être tenus de le faire ». **Recommandation 17,2 :** « L'équipe responsable de l'EPDP recommande que l'organisation ICANN entreprenne dès que possible une étude pour laquelle les termes de référence soient élaborés en consultation avec la communauté et qui porte sur :

- La faisabilité et les coûts, y compris les coûts de mise en œuvre ainsi que les éventuels coûts de responsabilité découlant de la différenciation entre personnes morales et personnes physiques ;
- Des exemples d'industries ou d'autres organisations qui aient réussi à différencier les personnes morales des personnes physiques ;
- Les risques que pose la différenciation entre personnes morales et personnes physiques pour la vie privée des titulaires de noms enregistrés ; et
- D'autres risques potentiels (s'il en existe) qu'implique la non-différenciation pour les bureaux d'enregistrement et les opérateurs de registre ».

Recommandation 17,3 : « L'équipe responsable de l'EPDP se penchera sur la question des personnes morales et physiques pour arriver à une solution à l'étape 2 ».

[67] Recommandation 17,1 : « L'équipe responsable de l'EPDP recommande que les bureaux d'enregistrement et les opérateurs de registre soient autorisés à différencier entre les enregistrements de personnes physiques et ceux de personnes morales sans, toutefois, être tenus de le faire ».

maintenir le statu quo. Nous croyons fermement que l'équilibre atteint (après une analyse poussée) dans le langage de la Recommandation 17 de l'étape 1 est d'une importance cruciale, surtout compte tenu de l'incertitude réglementaire que beaucoup de membres de l'équipe responsable de l'EPDP invoquent à maintes reprises comme justification pour modifier la recommandation de l'étape 1. Au lieu de cela, cette incertitude est en partie la raison pour laquelle la Recommandation 17 est une solution appropriée, souple et élégante à la question de la différenciation entre personne morale et personne physique.

a. Les parties contractantes doivent avoir le droit de contrôler leurs propres risques juridiques

Comme le RySG l'a expliqué tout au long de l'étape 2A, la flexibilité inhérente d'autoriser la différenciation sans l'exiger est importante pour permettre aux parties contractantes de contrôler leurs propres risques juridiques et de limiter les risques pour leurs clients. Les opérateurs de registre et les bureaux d'enregistrement ont déclaré à maintes reprises pendant la durée de l'EPDP qu'il s'agissait d'une prémisse fondamentale.

Les notes juridiques établissent clairement que « Si les parties pertinentes n'avaient aucune raison pour douter de la fiabilité de l'autoidentification d'un titulaire de nom de domaine, elles pourraient alors compter sur l'autoidentification seule, sans confirmation indépendante. Toutefois, nous comprenons que les parties s'inquiètent du fait que certains titulaires de noms de domaine ne comprendront pas la question et s'auto-identifieront à tort. Par conséquent, il y aurait un risque de responsabilité si les parties pertinentes ne prenaient pas d'autres mesures pour garantir l'exactitude de la désignation du titulaire de nom de domaine ».[68] De même, « le risque raisonnable que les personnes concernées s'auto-identifient à tort et ne parviennent pas à faire connaître les conséquences de l'autoidentification aux personnes concernées pourrait entraîner une responsabilité du fait de ne pas respecter le principe de légalité, d'équité et de transparence ».[69]

Le RySG apprécie le fait que Bird & Bird ait fourni des conseils sur la façon d'atténuer ces risques. Toutefois, la question de savoir comment et de quelle manière adopter ces procédures, sans parler de déterminer ce qui est et ce qui n'est pas un risque acceptable, doit être la responsabilité exclusive des parties contractantes qui assument ce risque. Dans tout autre arrangement commercial, ce serait une proposition incontestable. Comme nous l'avons dit depuis le début de ce PDP, où les parties contractantes sont responsables du traitement des données, les décisions relatives à ces

[68] « Conseil sur la responsabilité en rapport avec l'autoidentification d'un titulaire de nom de domaine en tant que personne physique ou personne morale conformément au Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD ») », par Ruth Boardman & Gabe Maldooff, en date du 25 janvier 2019 : https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx

[69] Id

données doivent être du ressort des opérateurs de registre et des bureaux d'enregistrement plutôt que de tiers qui ne présentent aucun risque eux-mêmes, et n'ont pas d'intérêts communs en termes de protection des données de nos clients.

b. La flexibilité est souhaitable

Le maintien de politiques flexibles plutôt que prescriptives sur la différenciation entre personne morale et personne physique garantit que les bureaux d'enregistrement et les opérateurs de registre soient agiles et capables de réagir rapidement aux futures modifications règlementaires qui puissent avoir un impact sur la publication des données de la personne morale sans nécessiter de l'élaboration de politiques supplémentaire. Le RySG reconnaît que la directive révisée sur la sécurité des réseaux et des systèmes d'information (« NIS 2 ») a le potentiel, une fois adoptée, d'influer sur la façon dont les bureaux d'enregistrement et les opérateurs de registre traitent les données des personnes morales. L'incertitude quant à la manière et au moment auquel les États membres de l'UE mettront en œuvre la directive NIS 2 est précisément la raison pour laquelle il est impératif que les opérateurs de registre et les bureaux d'enregistrement aient la flexibilité de déterminer eux-mêmes leur conformité avec l'environnement juridique et réglementaire changeant. L'environnement changeant et en évolution de la protection de la vie privée renforce la recommandation de l'étape 1 qui confirme l'option des parties contractantes de faire la distinction entre les personnes morales et les personnes physiques.

c. Justification insuffisante de la nécessité ou même du bénéfice des exigences supplémentaires

Bien que le RySG ait des convictions profondes au sujet de la Recommandation 17 de l'étape 1 par ses propres mérites, nous notons également qu'aucune justification convaincante n'a été fournie quant à la raison pour laquelle la différenciation obligatoire serait nécessaire, voire souhaitable. Sans plus d'informations, nous ne comprenons pas avec précision quel est le problème de la différenciation obligatoire entre les enregistrements de personnes morales et personnes physiques que l'on tente de résoudre.

III. Le RySG fait confiance au processus de la GNSO pour déterminer quand des travaux futurs de politique seront nécessaires

Le RySG soutient que la NIS 2 soit signalée au conseil de la GNSO pour en faire un suivi continu. Toutefois, nous ne pensons pas que la directive NIS 2 préliminaire exige de nouveaux travaux de politique et nous hésitons à prédéterminer un résultat. Le RySG soutient et s'en remet au rôle du conseil de la GNSO pour déterminer le moment auquel un travail politique s'avère nécessaire. Les pratiques et procédures de la GNSO établissent clairement que la politique de l'ICANN n'est pas requise pour diriger ou dupliquer les obligations auxquelles les parties contractantes sont soumises en vertu de

la loi. L'ICANN a lancé cet EPDP pour traiter de la promulgation du RGPD, le travail politique dans ce cas étant nécessaire en raison de conflits directs entre les exigences de nos accords avec l'ICANN et les exigences du RGPD. On ne peut pas en dire autant pour un projet de loi sur la directive NIS 2. Entre-temps, des lois sur la protection des données ont été adoptées ou sont entrées en vigueur en Californie, en Virginie, au Japon, en Inde et en Chine (pour n'en nommer que quelques-unes), que certaines ou toutes les parties contractantes doivent respecter. Personne n'a suggéré (à juste titre) que l'ICANN impose des politiques pour assurer le respect de ces obligations, car il n'y a pas de conflits directs avec nos accords. En fin de compte, la décision de savoir si et quand initier de nouveaux travaux sur les politiques doit être laissée au conseil de la GNSO, conformément aux processus existants.

IV. La Recommandation 1 est hors de portée et soulève des questions de mise en œuvre importantes

Pour rappel, sur la question de la différenciation entre personne morale et personne physique dans l'étape 2A, le conseil de la GNSO a chargé l'EPDP de répondre à deux questions manifestement limitées : (1) savoir s'il est nécessaire de faire des mises à jour à la recommandation de l'étape 1 de l'EPDP sur ce sujet (« Les bureaux d'enregistrement et les opérateurs de registre sont autorisés à différencier entre les enregistrements de personnes physiques et morales sans, toutefois, être tenus de le faire ») ; et (2) quelles directives, le cas échéant, peuvent être fournies aux bureaux d'enregistrement et/ou aux opérateurs de registre qui font la distinction entre les enregistrements de personnes morales et ceux de personnes physiques.[70]

Le respect de la portée convenue d'un PDP est d'une importance fondamentale pour l'élaboration d'une bonne politique. Malheureusement, le travail de l'étape 2A a subi des tentatives constantes d'élargir la portée de notre tâche, ce qui a abouti à une recommandation pour la création d'un élément de données qui, nous l'avons signalé à plusieurs reprises, est bien au-delà des instructions du conseil de la GNSO. La création obligatoire d'un nouvel élément de données n'a aucun lien avec le langage de la Recommandation 17 de l'étape 1 et n'est donc pas justifiée comme réponse à la première partie de la tâche qui nous a été confiée par la GNSO. Au lieu de demander des éclaircissements sur la portée au début de l'analyse de cette question, le président de l'EPDP a déterminé que la création d'un élément de données se rapporte à des directives dans la portée de l'EPDP. De plus, « si le conseil de la GNSO estime que notre travail est en dehors de la portée, ils le communiqueront ».[71]

[70] La Charte de l'étape 2A de la GNSO est disponible à l'adresse https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf

[71] « Sur votre point concernant la portée, l'équipe de direction et le personnel en ont discuté. Je suis d'avis que ce dont nous discutons ici est dans la portée de la charte de l'EPDP et de la directive qui nous a été donnée, ainsi que des questions auxquelles nous sommes chargés de répondre, étant donné que ça constitue des orientations. Je pense que si le conseil de la GNSO a l'impression que ce que nous produisons est hors de portée, ils le communiqueront. Nous avons ici Philippe comme agent de liaison. Il est également le président de la GNSO et gèrera toutes les questions liées à la portée ». Président de l'EPDP, réunion de l'étape 2A, 5 août 2021.

Par conséquent, le RySG demande respectueusement au conseil de la GNSO d'examiner d'abord la Recommandation 1 pour savoir si la proposition est en fait dans le cadre de la portée du travail de l'étape 2A avant de considérer s'il convient d'approuver la recommandation. Comme nous l'expliquons, nous croyons que ce n'est pas le cas. Si la GNSO déterminait que la Recommandation 1 est dans la portée, le RySG aurait encore des préoccupations importantes quant à la pertinence et à la mise en œuvre pratique de cette recommandation.

a. La Recommandation 1 n'est pas liée aux instructions reçues du conseil

Nous pensons que la création obligatoire proposée d'un nouvel élément de données, qui nécessite un engagement avec l'IETF, et probablement un engagement supplémentaire dans d'autres domaines, ne représente pas la « directive » mentionnée dans les instructions de la GNSO. L'existence (ou non) d'un élément de données normalisé ne fait rien pour aider les parties dans le processus de différenciation, elle ne fait que saisir le résultat de ce processus. Se concentrer sur le résultat plutôt que sur le processus n'est pas une directive, du moins pas une directive pratique significative et qui n'est donc pas conforme aux instructions reçues par l'EPDP de la part du conseil.

De même, nous ne convenons pas, en considérant la possibilité d'un élément de données normalisé, que la recommandation d'un nouvel élément de données soit liée à la directive, simplement parce que l'élément de données est référencé dans cette directive. Nous ne pouvons pas faire entrer des éléments dans la portée du PDP de cette manière. L'EPDP ne devrait pas dépasser la portée des instructions reçues, et nos recommandations doivent être tout aussi ciblées.

b. La création d'un nouvel élément de données soulève d'importants problèmes de mise en œuvre

Si la GNSO détermine que la Recommandation 1 est dans la portée du travail de l'étape 2A, le RySG croit toujours qu'il existe d'importants problèmes de mise en œuvre que la GNSO et l'ICANN doivent examiner attentivement avant d'adopter cette recommandation.

L'élément de données proposé n'est pas quelque chose que l'ICANN puisse créer par elle-même. Les normes Internet EPP et RDAP (les spécifications techniques), qui sont à la base de la plupart des canaux de communication utilisés pour les données d'enregistrement, sont contrôlées par l'IETF. L'IETF dispose d'un processus indépendant de l'ICANN au sein d'une communauté technique composée de plus de parties que celles liées à l'ICANN, ce qui pourrait créer des défis pour la mise en œuvre.

Compte tenu des préoccupations importantes soulevées concernant l'adoption de cet élément de données, nous notons qu'aucune justification convaincante n'a été fournie quant à la raison pour laquelle cet élément de données est nécessaire ou bénéfique, en particulier dans le cadre du RDDS public. Les justifications avancées (y compris (i) suivre la mesure dans laquelle les parties contractantes mettent en œuvre la différenciation ; (ii) permettre au public de vérifier l'exactitude d'une désignation « personne morale vs.

personne physique » ;(iii) déterminer la conformité avec les lois applicables (iv) faire référence à la « cohérence », et (v) savoir « quel préjudice » y a-t-il dans l'adoption de l'élément de données ? manquent d'avantages spécifiques, et sont probablement réalisables via les mécanismes existants. Aucune des raisons présentées n'a de sens pratique, encore moins elles sont nécessaires ou suffisamment convaincantes pour justifier des changements aussi importants et en dehors de la portée de la politique existante.

Comme indiqué ci-dessus, l'existence (ou non) d'un élément de données normalisé ne fait rien pour aider les parties contractantes qui souhaitent faire la différentiation entre les enregistrements des personnes morales et des personnes physiques ; elle ne fait que saisir le résultat de ce processus. En considérant la possibilité d'un élément de données normalisé, les opérateurs de registre ont convenu qu'aux fins de l'intégration à un futur système éventuel du SSAD, comme recommandé dans l'étape 2, il peut être logique d'utiliser une méthode normalisée pour indiquer si un enregistrement contient des données à caractère personnel ou non. Bien que nous reconnaissions qu'il peut y avoir un cas d'utilisation lié aux décisions de divulgation dans le SSAD, nous préférerons reporter ces décisions, le cas échéant, au développement du SSAD plutôt que de prendre des mesures maintenant qui puissent limiter l'utilité de cet élément de données une fois que le SSAD sera fonctionnel.

La recommandation va bien au-delà, exigeant à l'ICANN de créer ce champ en coordination avec la communauté technique pour une utilisation avec l'EPP et le RDDS. Pour être clair, le RySG ne prend pas en charge l'utilisation de ce champ ni dans l'EPP ni dans le RDDS. En tant que compromis, nous avons convenu qu'il s'agit d'un champ totalement facultatif où les parties contractantes qui le choisissent peuvent faire la distinction entre les personnes morales et les personnes physiques et/ou indiquer si un enregistrement contient des données à caractère personnel ou non susceptibles d'être utilisées, mais qui ne sont requises en aucun cas.

Dans l'intérêt d'une collaboration de bonne foi en vue d'une solution de compromis, les opérateurs de registre ont convenu de la création d'un élément de données normalisé et que les parties contractantes pourraient, si elles le décident, utiliser cet élément de données normalisé. Nous avons beaucoup de doutes quant à l'utilisation d'un tel domaine dans l'EPP ou le RDDS et nous devons préciser que nous ne soutenons pas son utilisation avec l'un ou l'autre. Nous n'avons pas entendu de justification convaincante pour expliquer pourquoi un tel champ devrait être utilisé dans les deux cas et notre soutien à la création d'un tel champ n'indique pas une directive ou une recommandation disant qu'il devrait être utilisé.

V. La directive élaborée sur la différenciation entre personne morale et personne physique est insuffisante

Le RySG soutient le concept de directive qui aide les parties contractantes à surmonter les défis juridiques et techniques complexes auxquels les opérateurs de registre et les

bureaux d'enregistrement sont régulièrement confrontés dans l'exploitation de nos activités. D'après notre expérience, les meilleurs conseils sont rédigés par les personnes ayant l'expertise et les intérêts appropriés pour faire face à la complexité et offrir de la clarté sur les questions difficiles ou ambiguës. Malgré les objections et suggestions d'amélioration continue des parties contractantes, les directives figurant dans ce rapport sur la différenciation entre personne morale et personne physique ne répondent à aucun de ces critères.

Lors de l'élaboration de la directive contenue dans la Recommandation 2, le groupe de travail a convenu qu'il s'agit d'une directive facultative dont les parties contractantes qui choisissent de différencier les enregistrements de personnes morales et physiques peuvent tirer parti à leur discrétion. Toutefois, le langage du rapport final de la Recommandation 2 indique que les parties contractantes qui choisissent de faire la distinction DEVRAIENT suivre cette directive. Le RySG estime que l'utilisation du mot DEVRAIT ou DEVRAIENT ici ne reflète pas exactement ce qui a été convenu par le groupe de travail. Selon le document RFC 2119, « DEVRAIT . . . signifie qu'il peut exister des raisons valables dans des circonstances particulières pour ignorer un point particulier, mais que toutes les conséquences doivent être comprises et soigneusement considérées avant de choisir une voie différente ». Puisque le fait de suivre ces directives pour la différenciation est facultatif, le terme le plus approprié ici est PEUT (« un élément est vraiment facultatif »). Dans l'intérêt d'une collaboration de bonne foi vers une solution de compromis, les opérateurs de registre ont choisi de soutenir la recommandation. Nous devons noter que nous ne sommes pas d'accord avec l'utilisation du verbe DEVRAIT et que les parties contractantes doivent examiner si les directives leur sont utiles et applicables avant de décider s'ils les adoptent.

En bref, les directives incluses dans ce rapport sur la différenciation entre personne morale et personne physique sont malheureusement insuffisantes si leur but est d'aider une partie contractante qui veut se différencier. Les directives ne sont pas à la hauteur pour plusieurs raisons. Premièrement, les directives sont délibérément et déraisonnablement axées sur les résultats. Ceux qui ont préconisé la nécessité de cette directive ont minimisé le processus par lequel la différenciation se produit, ainsi que les exigences et considérations juridiques connexes. Cette approche complique presque intentionnellement plutôt que de lutter contre les complexités et les risques impliqués dans le processus de différenciation et ne fait rien pour aider l'utilisateur de la directive à comprendre et à traiter ces complexités et ces risques.

Deuxièmement, les directives ne sont pas pratiques. Encore une fois, en échouant à gérer les complexités et les risques inhérents à la différenciation, les directives qui en résultent ne sont guère plus qu'une réaffirmation de la loi et des résultats attendus. Par exemple, la directive établit que :

> *« Les bureaux d'enregistrement devraient s'assurer qu'ils communiquent clairement la nature et les conséquences d'un titulaire de nom de domaine qui s'identifie comme une personne morale. Ces communications devraient inclure :*

- *Une explication de ce qu'est une personne morale dans un langage simple et facile à comprendre.*
- *Des directives à l'intention du titulaire de nom de domaine (personne concernée)35 641 par le bureau d'enregistrement concernant les conséquences possibles de :*
    - *L'identification de leurs données d'enregistrement de nom de domaine comme correspondant à une personne morale ;*
    - *La confirmation de la présence de données à caractère personnel ou non personnel, et ;*
    - *La fourniture de son consentement. Cela est également conforme à l'article 3.7.7.4 du contrat d'accréditation de bureau d'enregistrement (RAA) ».*

Malheureusement, pour un utilisateur de cette directive, cette brève section soulève plus de questions qu'elle n'apporte de réponses. Qu'est-ce qu'une personne morale ? Que se passe-t-il si le titulaire de nom de domaine n'est pas la personne concernée ? Quelles sont les conséquences qui devraient être expliquées à la personne concernée ? Quelles sont les étapes nécessaires pour s'assurer que la personne concernée comprend ce message (par exemple, test A/B, panels d'utilisateurs) ? Quels sont les risques si ces étapes ne sont pas suivies ? Comment obtient-on un consentement significatif, surtout lorsque le titulaire de nom de domaine n'est peut-être pas la personne concernée ? L'éducation ou la notification au titulaire de nom de domaine est-elle suffisante pour atténuer le risque ? Le simple fait de répéter des obligations qui sont largement imposées par la loi ne fait pas grand-chose ici pour aider réellement un utilisateur des directives à suivre ces questions.

De même, les directives indiquent dans le tout dernier paragraphe que :

> *La distinction entre les titulaires de noms de domaine qui sont des personnes morales et ceux qui sont des personnes physiques ne peut pas déterminer à elle seule la façon dont les informations devraient être traitées (rendues publiques ou masquées), car les données fournies par les personnes morales pourraient inclure des données à caractère personnel protégées par la législation sur la protection des données, comme le RGPD.*

C'est en fait la question la plus difficile et la plus risquée pour différencier les enregistrements de personnes morales et physiques. Comme le CEPD l'a indiqué à l'ICANN, « le simple fait qu'un titulaire de nom de domaine soit une personne morale ne justifie pas nécessairement la publication illimitée de données à caractère personnel relatives aux personnes physiques qui travaillent pour cette organisation ou qui la représentent ».[72] Cette directive ne fait rien pour envisager ou même pour expliquer de

[72] La lettre du CEPD adressée à Goran Marby, datée de juillet 2018, est disponible à l'adresse https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

façon minimale comment un bureau d'enregistrement pourrait commencer à aborder la question. La résolution de ce défi majeur, presque en passant, compromet gravement l'utilité de ces directives et accroît notre inquiétude quant à l'aspect pratique global de ce conseil.

Dans l'intérêt d'une collaboration de bonne foi, le RySG a accepté de soutenir la publication de cette directive malgré les préoccupations décrites ci-dessus, car la recommandation indique clairement que la directive est vraiment facultative et les parties contractantes (même celles qui choisissent de se différencier) ne sont en aucun cas tenues de suivre la Recommandation 2. Nous sommes sceptiques quant à l'adoption généralisée de ces directives, non pas parce qu'elles ne sont pas souhaitées, mais parce qu'elles ne font rien pour guider la mise en œuvre pratique et n'offrent aucun réconfort aux parties qui supportent les risques juridiques.

VI. Conclusion

Pour toutes les raisons susmentionnées, compte tenu du soutien continu des différentes parties de l'équipe responsable de l'EPDP pour la publication de ce rapport final et des recommandations énoncées, et malgré nos préoccupations concernant la portée des recommandations, le RySG ne s'oppose pas à l'adoption du présent rapport et des recommandations énoncées. Il est toutefois noté que cet appui est fondé sur la conviction de bonne foi que toutes les parties maintiennent le niveau de consensus convenu. Bien que le RySG n'appuie pas un certain nombre d'aspects de ce rapport, dans l'esprit et l'appui du modèle multipartite, nous avons fait des compromis.

Déclaration de la minorité du SSAC sur les spécifications temporaires pour les données d'enregistrement des gTLD - Rapport final de l'étape 2A du processus accéléré d'élaboration de politiques [73]

1 Introduction

Le Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC) apprécie la diffusion du rapport initial de l'étape 2A de l'équipe responsable du processus accéléré d'élaboration de politiques (EPDP) sur la spécification temporaire relative aux données d'enregistrement des gTLD (ci-après dénommé « rapport initial de l'étape 2A de l'EPDP »),[74] et nous remercions le groupe de travail de nous avoir donné l'occasion de faire des commentaires à ce sujet.

Dans le présent document, le SSAC présente à la fois des commentaires généraux sur le processus accéléré d'élaboration de politiques et des commentaires spécifiques sur les recommandations individuelles contenues dans le rapport initial de l'étape 2A de l'EPDP. Le SSAC se ferait un plaisir de discuter de ces commentaires avec l'équipe responsable de l'EPDP à sa convenance pour expliquer tout élément qui puisse être peu clair et qui nécessite davantage d'explications.

Le SSAC tient à souligner le temps et les efforts considérables consacrés par les membres de l'équipe responsable de l'EPDP et les remercie pour leur contribution à ce sujet important.

2 Contexte

Dans cette section, nous passons en revue les questions à l'étude par le groupe de travail (WG) de l'étape 2A de l'EPDP. Nous faisons quelques observations sur le processus accéléré d'élaboration de politiques dans son ensemble, puis nous décrivons notre approche. Dans la section suivante, nous présentons nos recommandations, dont certaines s'appliquent à l'effort global et certaines sont spécifiques à l'effort de l'étape 2A.

2.1 Questions à prendre en considération par le groupe de travail de l'étape 2A de l'EPDP

2.1.1 Distinction entre personnes morales et personnes physiques

Le Règlement général sur la protection des données (RGPD) offre une protection spécifique aux personnes physiques (c'est-à-dire les humains) et aucune protection aux

[73] Le document a été publié comme SAC118 et est disponible à l'adresse suivante : https://www.icann.org/en/system/files/files/sac-118-en.pdf

[74] Voir le rapport initial de l'étape 2A du processus accéléré d'élaboration de politiques (EPDP) sur la spécification temporaire relative aux données d'enregistrement des gTLD à l'adresse https://www.icann.org/en/system/files/files/epdp-phase-2a-initial-report-02jun21-en.pdf

personnes morales (c'est-à-dire les entreprises).[75][76] Le groupe de travail responsable de l'EPDP, et en particulier le groupe de travail de l'étape 2A de l'EPDP, a accordé une attention considérable à cette distinction. Parmi les questions que le groupe de travail responsable de l'EPDP a examinées, on peut citer :

1. Devrait-il y avoir un élément de données précis pour indiquer si le titulaire de nom de domaine est une personne physique ou une personne morale ?
2. Est-ce que chaque bureau d'enregistrement devrait être tenu de faire cette détermination pour chaque enregistrement ?
3. Quels sont les critères utilisés pour prendre sa décision ?
4. Quels sont les risques si la détermination du bureau d'enregistrement est incorrecte ?
5. Le titulaire de nom de domaine devrait-il être tenu de déclarer s'il s'agit d'une personne physique ou morale et le bureau d'enregistrement devrait-il s'appuyer sur cette attestation ?
6. Les données de contact des titulaires de noms de domaine classés comme personnes morales devraient-elles toujours être accessibles au public ?[77]
7. Les données de contact des titulaires de noms de domaine classés comme personnes physiques ne devraient-elles jamais être accessibles au public ?
8. Le statut du titulaire de nom de domaine devrait-il être disponible publiquement ?
9. Comment procéder lorsque les données personnelles identifiables (PII) d'une personne physique sont incluses dans l'enregistrement d'une personne morale ?

2.1.2 Faisabilité des contacts uniques

L'équipe responsable de l'EPDP a été invitée à prendre en considération les questions suivantes :

- Un contact unique sous la forme d'une adresse e-mail anonymisée uniforme est-il réalisable, et si oui, cela devrait-il être une exigence ?
- Si cela était possible, mais pas obligatoire, quelles directives peuvent être fournies, le cas échéant, aux parties contractantes qui pourraient souhaiter mettre en place l'adresse e-mail anonymisée uniforme ?

[75]Voir le considérant 14 du RGPD : « La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale. ». https://gdpr-info.eu/recitals/no-14/

[76] Voir l'article 4 du RGPD, disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1

[77] Le groupe de travail de l'EPDP traite généralement le processus de demande et de réponse comme si les données « publiques » étaient publiées pour que tout le monde puisse les voir. Dans tous les scénarios prévus, tout accès aux données d'enregistrement se fait par le biais d'un processus de demande-réponse. C'est-à-dire que les données d'enregistrement ne sont pas publiées dans le sens où la publication est généralement comprise. Dans ce document, nous utilisons les mots « disponible publiquement » pour désigner les données disponibles à toute personne qui les demande sans restriction d'utilisation et sans attribution.

L'équipe responsable de l'EPDP a observé que « contacts uniques » est un terme vague, et qu'il existe deux objectifs distincts énoncés par ceux qui préconisent des contacts uniques. À savoir : (1) la capacité de communiquer rapidement et efficacement avec le titulaire de nom de domaine sans divulguer des données à caractère personnel, et (2) un identificateur commun qui aide les enquêteurs à mettre en corrélation les enregistrements de domaine avec un contact commun.

L'équipe responsable de l'EPDP a tenté de dissiper ces ambiguïtés en proposant deux termes :

- **Contact e-mail par titulaire de nom de domaine** - un e-mail pour tous les domaines enregistrés par un titulaire de nom de domaine unique [parrainé par un bureau d'enregistrement donné] OU [entre les bureaux d'enregistrement], qui est destiné à être des données pseudonymes lorsqu'elles sont traitées par des parties non contractantes.
- **Contact e-mail pour chaque enregistrement** - un e-mail à usage unique distinct pour chaque nom de domaine enregistré par un titulaire de nom de domaine unique, qui est destiné à être des données anonymes lorsqu'elles sont traitées par des parties non contractantes.

Après quelques délibérations, l'équipe responsable de l'EPDP n'a pas fourni de réponse concluante sur la faisabilité d'un contact par titulaire de nom de domaine ou pour chaque enregistrement. L'équipe responsable de l'EPDP a recommandé que « les parties contractantes qui choisissent de publier une adresse électronique basée sur le titulaire de nom de domaine ou sur l'enregistrement dans le service d'annuaire des données d'enregistrement (RDDS) accessibles au public veillent à ce que la personne concernée soit protégée de manière appropriée, conformément aux directives pertinentes sur les techniques d'anonymisation fournies par leurs autorités de protection des données et les directives juridiques annexées ».
Le SSAC note que certains bureaux d'enregistrement ont déjà déployé quelques méthodes différentes pour prendre en charge le contact e-mail par titulaire de nom de domaine. Par exemple, les adresses e-mail par titulaire de nom de domaine ont été créées de manière unique par titulaire de nom de domaine, hébergées dans un domaine du bureau d'enregistrement. Les messages dirigés vers ces adresses e-mail sont redirigés dès leur réception par le bureau d'enregistrement vers le véritable destinataire. Certains bureaux d'enregistrement fournissent un formulaire Web qui peut être utilisé pour envoyer un message au titulaire de nom de domaine d'un nom de domaine particulier. Dans la plupart des cas, l'expéditeur du message d'origine ne sait pas si le message transféré a été remis ou ouvert. La spécification temporaire ne fournit aucune exigence de niveau de service pour les e-mails transférés.[78][79]

[78]Spécification temporaire pour les données d'enregistrement des gTLD ; Annexe A : Services d'annuaire de données d'enregistrement, paragraphe 2. https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[79] Il y a eu des problèmes documentés avec les mises en œuvre de la joignabilité au niveau des bureaux d'enregistrement. Voir p. 55 à 59 de

Le SSAC ne connaît actuellement aucune solution déployée qui soit capable de satisfaire aux exigences de contact e-mail pour chaque enregistrement, telles que définies ci-dessus. À titre d'anecdote, un petit nombre de solutions ont été proposées, mais aucune n'a obtenu de consensus.

2.2 Observations du SSAC

Sur la base de la participation à l'EPDP, le SSAC offre deux commentaires sur l'effort global visant à atteindre un système d'accès différencié qui réponde à de multiples objectifs. Par système d'accès différencié, le SSAC désigne un système qui permet de conditionner la réponse en fonction du demandeur et de l'objet de la demande. Le système normalisé d'accès et de divulgation (SSAD) est un exemple précis d'un tel système.

2.2.1 Intérêts concurrents

Du point de vue du SSAC, trois intérêts concurrents sont en jeu dans les délibérations sur les politiques.

1. **Défenseurs de la vie privée.** Certaines parties veulent s'assurer que les données de contact pour les personnes physiques ne sont pas disponibles publiquement, à moins que la personne physique ne donne son consentement explicite et éclairé pour permettre la disponibilité publique. Elles souhaitent également que cette protection s'applique aux personnes morales si les données de contact incluent des PII ou si des PII peuvent être déduites des données de contact.
2. **Demandeurs de données.** Les demandeurs souhaitent disposer du maximum de données qu'ils peuvent obtenir. Les demandeurs veulent que la protection de la vie privée soit aussi proche que possible de ce qui est légalement requis. Ils veulent que les requêtes soient satisfaites de manière fiable, rapide et économique.
3. **Autorités de contrôle.**[80] Ceux qui collectent les données et les rendent accessibles au public, à savoir les bureaux d'enregistrement et les opérateurs de registre, veulent réduire les coûts et les risques.

Certaines personnes ou organisations peuvent incarner plus d'un de ces intérêts concurrents.

2.2.2 Une préoccupation non exprimée

Le SSAD est le mécanisme proposé pour la gestion centralisée des demandes d'accès à des données d'enregistrement non publiques, défini dans les Recommandations 1 à 18 du rapport final de l'étape 2 du processus accéléré d'élaboration de politiques (EPDP) de

« Données d'enregistrement des noms de domaine au carrefour : l'état de la protection des données, de la conformité et de la joignabilité à l'ICANN ». http://www.interisle.net/domainregistrationdata.html

[80] Le terme comprend également d'autres personnes qui collectent ou traitent les données collectées lors de l'enregistrement (c'est-à-dire, les revendeurs).

la GNSO sur la spécification temporaire relative aux données d'enregistrement des gTLD.[81]

Un système d'accès bien conçu permettra aux demandeurs ayant des besoins légitimes d'accéder à des données non publiques, et de le faire de manière fiable, rapide et à faible coût.

À l'heure actuelle, il est incertain que nous puissions parvenir à un système de contrôle d'accès différencié qui soit satisfaisant. Actuellement, le Conseil d'administration de l'ICANN a demandé une évaluation de six mois de l'étape de conception opérationnelle (ODP) pour éclairer ses délibérations sur les recommandations politiques. Le SSAD proposé n'a pas encore de date de livraison prévue. L'estimation initiale des coûts a été critiquée par la communauté comme étant trop élevée. Il y a également un manque de définition quant aux données qui seront disponibles pour quels demandeurs, et dans quelles circonstances. Enfin, les parties contractantes peuvent effectuer des révisions manuelles des demandes de données, car l'EPDP n'a pas été en mesure de se mettre d'accord sur les cas d'automatisation.

En raison du manque de clarté sur le SSAD, certains des participants à l'EPDP semblent supposer que les seules données auxquelles ils sont susceptibles d'accéder dans un avenir prévisible sont des données accessibles au public et qu'ils sont pressés de maintenir la protection de la vie privée au minimum requis par la loi. Il en résulte une incapacité à résoudre de nombreuses questions dans l'EPDP.

2.3 Approche du SSAC

Le SSAC croit qu'il est très important pour les enquêteurs de sécurité d'avoir accès aux données d'enregistrement de noms de domaine. En même temps, il est également important que ceux qui méritent une protection puissent l'avoir. Ces deux alternatives peuvent coexister. Mais elles ne peuvent pas le faire dans le contexte d'un argument contradictoire sur la question de savoir si chaque contact doit être public ou non comme le seul choix à faire.

Il devrait être possible que les informations de contact considérées comme personnelles soient détenues en privé et mises à la disposition, dans des circonstances appropriées, des personnes qui en ont besoin. Du point de vue du SSAC, un système d'accès différencié opportun, fiable, efficace et efficient permettrait d'obtenir un résultat qui serait une amélioration pour tous les intérêts concurrents.

Ainsi, le SSAC estime que l'objectif de la communauté de l'ICANN et de l'organisation ICANN devrait être de construire et de faire fonctionner un SSAD efficace.

[81] Voir le rapport final du processus accéléré d'élaboration de politiques concernant l'étape 2 de l'EPDP sur la spécification temporaire relative aux données d'enregistrement des gTLD, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

Au stade actuel des choses, la discussion sur l'accès aux données non publiques est en dehors de la portée de l'étape 2A de l'EPDP, et la discussion des rapports des étapes 1 et 2 est considérée comme close. Par conséquent, dans ce rapport, nous formulons deux sortes de recommandations.

1. Recommandations générales sur l'accès différencié et le SSAD.
2. Dans le cadre de l'étape 2A de l'EPDP, nous proposons des recommandations détaillées qui, si elles sont adoptées, tirent le meilleur parti d'une situation imparfaite.

3 Recommandations

3.1 Recommandation à la GNSO et à l'organisation ICANN

Recommandation 1 : Le SSAC recommande à l'Organisation de soutien aux extensions génériques (GNSO) et à l'organisation ICANN de concentrer leur attention sur la construction et l'exploitation d'un système d'accès différencié efficace.

Un système d'accès différencié avec les propriétés suivantes est nécessaire :

Opportun	Il doit entrer en service rapidement
Fiable	Il doit fonctionner de façon prévisible et cohérente, tant dans le fonctionnement du système que dans la prise de décisions par les participants au système.
Utile	Il doit fournir des résultats qui soient bénéfiques pour les demandeurs.
Efficient	Il doit fournir rapidement des réponses à des demandes de données légitimes et à un coût qui soit acceptable pour toutes les parties à cette fin.
Facilement accessible	L'obtention et le maintien des informations d'identification doivent fonctionner suffisamment bien pour faciliter, plutôt que pour entraver, l'utilisation.

Le présent document utilise le terme « efficace » pour désigner un système d'accès différencié répondant à toutes les exigences ci-dessus, et bien entendu, incluant la fonctionnalité requise pour gérer des demandes et des réponses distinctes à diverses combinaisons de demandeurs et de fins, comme indiqué à la section 2.2.

3.2 Recommandations à l'étape 2A de l'EPDP

3.2.1 Personne morale vs. personne physique

Du point de vue d'un professionnel de la sécurité, la quantité maximale possible de données d'enregistrement doit être disponible pour enquête, soit par le biais d'un système d'accès différencié efficace, soit en les rendant disponibles dans le RDDS public.

Recommandation 2 : La SSAC recommande les points suivants concernant les personnes morales et les personnes physiques :

A. Il faudrait définir un élément de données qui indique le statut juridique du titulaire de nom de domaine. Au départ, nous proposons trois valeurs admissibles : Personne physique, personne morale et personne non spécifiée. « Non spécifiée » serait la valeur par défaut jusqu'à ce que le titulaire de nom de domaine s'identifie comme une personne physique ou morale. Ce champ doit pouvoir prendre en charge les valeurs d'état en fonction des décisions futures de la politique.
B. Cet élément de données doit être affiché dans le cadre des données accessibles au public.
C. Les titulaires de noms de domaine doivent être classés comme personnes physiques ou morales. Cela devrait être exigé au moment de l'enregistrement, pour tous les nouveaux enregistrements de domaine. Pour les enregistrements existants, la valeur peut rester « non spécifiée » jusqu'à ce qu'elle soit remplie ultérieurement. Les bureaux d'enregistrement devraient être tenus de demander à des moments pertinents, par exemple lors du renouvellement du domaine et/ou de l'enquête annuelle sur l'exactitude, si le titulaire de nom de domaine est une personne morale ou physique, dans le but d'obtenir éventuellement ces données pour tous les titulaires de nom de domaine, et de réduire la valeur « non spécifiée » au niveau pratique le plus bas.
D. Les titulaires de noms de domaine sont actuellement en mesure de le faire et devraient continuer à avoir la possibilité de rendre publiques leurs données de contact. Les titulaires de noms de domaine qui sont personnes morales devraient également avoir la possibilité de protéger leurs données par le biais de services d'anonymisation et d'enregistrement fiduciaire.

Ces recommandations sont conformes aux conseils précédents du SSAC.[82]

3.2.2 Faisabilité d'un contact e-mail pseudonymisé

Recommandation 3 : Le SSAC recommande ce qui suit en ce qui concerne la faisabilité d'un contact e-mail pseudonymisé :

A. Les deux objectifs de la politique, à savoir (1) la capacité de communiquer rapidement et efficacement avec le titulaire de nom de domaine sans divulguer des données à caractère personnel, et (2) un identificateur commun qui aide les enquêteurs à mettre en corrélation les enregistrements avec les contacts communs, devraient être considérés séparément.
B. Pour atteindre l'objectif de la politique (A1), les bureaux d'enregistrement devraient déployer (ou continuer à déployer) des méthodes pour prendre en charge les contacts e-mail basés sur les titulaires de noms de domaine (voir la

[82] Voir la section 3.6 du rapport SAC104. https://www.icann.org/en/system/files/files/sac-104-en.pdf

discussion sur les deux méthodes à la section 2.1.2). Le SSAC recommande en outre que des exigences uniformes soient élaborées pour les mesures de protection pour le contact e-mail par titulaire de nom de domaine. Les exigences devraient inclure le maintien de la vie privée du titulaire de nom de domaine, le cas échéant, et les engagements de niveau de service visant à établir des attentes quant à l'utilisation du service. Ces mesures de protection sont indépendantes de la méthode choisie (par exemple, adresses électroniques uniques ou formulaires Web).

C. Pour atteindre l'objectif de politique générale (A2), des recherches supplémentaires sont nécessaires sur les méthodes, leur efficacité et leurs compromis. Nous recommandons que l'étape 2A de l'EPDP *ne spécifie pas* de méthode pour établir une corrélation entre les enregistrements et un contact commun en ce moment.

Annexe C - Contributions de la communauté

E.1. Appel à contributions

Selon le manuel PDP de la GNSO, une équipe consacrée à un PDP devrait solliciter formellement des déclarations de chaque groupe de représentants et de chaque unité constitutive de la GNSO dans les premières étapes de ses délibérations. L'équipe responsable de l'EPDP est également encouragée à rechercher l'opinion d'autres comités consultatifs et organisations de soutien de l'ICANN ayant l'expertise, l'expérience ou un intérêt particulier dans la problématique examinée.

L'équipe responsable de l'EPDP a sollicité des commentaires sur ces deux sujets dans le cadre des premiers commentaires demandés au cours des étapes 1 et 2, et par conséquent, l'équipe responsable de l'EPDP a examiné et considéré les commentaires fournis à ce moment-là (voir https://community.icann.org/x/Ag9pBQ et https://community.icann.org/x/Ag9pBQ) dans le cadre de ses délibérations.

E.2. Forum de consultation publique sur le rapport initial

Le 3 juin 2021, l'équipe responsable de l'EPDP a publié son rapport initial pour consultation publique. Le rapport initial décrivait la réflexion de l'équipe jusqu'à ce point et visait à servir d'outil pour solliciter les commentaires de la communauté, notamment dans les domaines où des divergences importantes subsistaient. Bien que des recommandations préliminaires aient été incluses dans le rapport initial, l'équipe responsable de l'EPDP a demandé que ces recommandations soient prises en considération en combinaison avec une série de questions soulevées pour aider à la finalisation de son rapport.

L'équipe responsable de l'EPDP a utilisé un formulaire Google pour faciliter l'analyse des commentaires publics. Seize contributions ont été reçues des groupes de représentants et des unités constitutives de la GNSO, des comités consultatifs de l'ICANN, d'entreprises et d'organisations, en plus d'une contribution individuelle. Les commentaires reçus se trouvent à l'adresse suivante : https://docs.google.com/spreadsheets/d/1aRxF19pd5tEyO07__zaj7YvzOPjfIBfgi4WRy-nx8yY/edit?resourcekey#gid=1754667842.

Afin de faciliter son analyse des commentaires publics, l'équipe responsable de l'EPDP a mis au point un ensemble d'outils d'analyse des commentaires publics (PCRT) et des tables de discussion (voir https://community.icann.org/x/coMZCg). À travers l'examen en ligne et les séances plénières, l'équipe responsable de l'EPDP a terminé son analyse

et son évaluation des commentaires reçus et convenu des modifications à apporter aux recommandations et/ou au rapport.

Annexe F – Notes juridiques de Bird & Bird

Réponse à la Question 1 2 (personne morale vs. personne physique)

N O T E

Pour :	Société pour l'attribution des noms de domaine et des numéros sur Internet, équipe responsable de l'EPDP
De :	Ruth Boardman et Phil Bradley-Schmieg
Date :	6 avril 2021
Objet :	Questions de mars 2021 concernant le statut juridique, le consentement, *etc.*

Contexte

1. Le CEPD, dans une lettre de juillet 2018 à Göran Marby, a déclaré que :

   « *Les données à caractère personnel identifiant les employés individuels (ou les tiers) agissant pour le compte du titulaire du nom de domaine ne devraient pas être rendues publiques par défaut dans le contexte du WHOIS* ».

Consentement

2. Annexe A de la spécification temporaire indique que

   « En réponse aux requêtes de noms de domaine, le bureau d'enregistrement et l'opérateur de registre DOIVENT traiter les champs suivants comme « expurgés » à moins que le contact (par exemple le contact administratif ou technique) n'ait consenti à publier les données du contact : (…) ».

3. La Recommandation 6 du rapport final de l'étape 1 de l'EPDP, adoptée par le Conseil d'administration de l'ICANN en mai 2019, indique :

   « Dès que cela sera commercialement raisonnable, le bureau d'enregistrement doit donner la possibilité au titulaire de nom enregistré d'accorder son consentement à la publication des coordonnées expurgées, ainsi que de l'adresse électronique, dans le RDS pour le bureau d'enregistrement parrain ».

4. Le rapport final de l'étape 2 de l'équipe responsable de l'EPDP, daté du 31 juillet 2020, a également noté à la note 83 que :

   « *Une autre piste à explorer afin d'encourager la réduction du traitement manuel serait de déterminer quels mécanismes juridiquement acceptables les parties contractantes pourraient mettre en œuvre afin de permettre aux personnes*

concernées soit de donner leur consentement libre soit de s'opposer à la divulgation de leurs données au moment de l'enregistrement du nom de domaine. Cela faciliterait la maintenance de bases de données d'informations protégées et d'informations non protégées, permettant ainsi d'assurer un traitement automatisé à plus faibles coûts des bases de données non protégées ».

5. Bird & Bird a fourni des conseils à ce sujet, notamment dans notre Note du 13 mars 2020, intitulée « *Avis sur les options de consentement pour rendre les données à caractère personnel publiques dans le RDS et exigences en vertu du [RGPD]* » (la «**Note sur le consentement** »).

Personnes morales versus personnes physiques

6. En mai 2019, le Conseil d'administration de l'ICANN a également adopté la Recommandation 17 du rapport final de l'étape 1 de l'EPDP, qui stipule :

« 1) L'équipe responsable de l'EPDP recommande que les bureaux d'enregistrement et les opérateurs de registre puissent différencier entre les enregistrements de personnes physiques et ceux des personnes morales sans, toutefois, être tenus de le faire.

2) L'équipe responsable de l'EPDP recommande que l'organisation ICANN entreprenne dès que possible une étude pour laquelle les termes de référence soient élaborés en consultation avec la communauté et qui porte sur :

- *La faisabilité et les coûts, y compris les coûts de mise en œuvre ainsi que les éventuels coûts de responsabilité découlant de la différenciation entre personnes morales et personnes physiques ;*
- *Des exemples d'industries ou d'autres organisations qui aient réussi à différencier les personnes morales des personnes physiques ;*
- *Les risques que pose la différenciation entre personnes morales et personnes physiques pour la vie privée des titulaires de noms enregistrés ; et*
- *D'autres risques potentiels (s'il en existe) qu'implique la non-différenciation pour les bureaux d'enregistrement et les opérateurs de registre.*

3) Au cours de l'étape 2, l'équipe responsable de l'EPDP se penchera sur la question des personnes morales et physiques pour arriver à une solution ».

7. Bird & Bird a fourni des conseils sur ce problème, notamment dans :

7.1 Notre note du 25 janvier 2019, « *Avis sur la responsabilité en relation avec l'autoidentification d'un titulaire de nom de domaine en tant que personne physique ou morale conformément au [RGPD]*» (la « **Note sur la distinction entre personne physique et personne morale** ») ; et

7.2 Notre note du 9 avril 2020, « *Avis sur le principe de l'exactitude dans le cadre du [RGPD] : questions de suivi sur les notes « distinction entre personne*

physique et personne morale » et « exactitude » (la « **Note de suivi sur l'exactitude** »).

8. Les membres de l'EPDP pourraient également se rappeler que l'article 83(2) du RGPD énumère les facteurs à prendre en considération lorsqu'une autorité de surveillance décide d'imposer une amende administrative (et, dans l'affirmative, quels montants). Il s'agit notamment du nombre de personnes concernées touchées, de la nature des données, du caractère intentionnel ou négligent de l'infraction, des mesures prises par le contrôleur pour atténuer les dommages et du degré de responsabilité du contrôleur en tenant compte des mesures techniques et organisationnelles mises en œuvre par le contrôleur conformément aux articles 25 et 32 du RGPD.

9. Dans ce contexte, vous avez soulevé un certain nombre de questions y afférentes.

Question 1

Question posée : En vertu de la politique de consensus adoptée, les bureaux d'enregistrement donneront aux titulaires de noms de domaine la possibilité de consentir à la publication de données à caractère personnel incluses dans leurs données d'enregistrement. Veuillez comparer les risques juridiques pour les parties contractantes associés à :

1) la publication des données à caractère personnel sur la base du consentement du titulaire, d'une part,

Et

2) la publication des données sur la base de (i) l'autoidentification des données par le titulaire de nom de domaine comme des données relatives à une personne morale uniquement ou contenant également des données d'une personne physique (organisation ou personne physique) avant la publication et (ii) la vérification des procédures présentées dans la note de Bird & Bird du 25 janvier 2019 (c'est-à-dire notifier/expliquer ; confirmer ; vérifier ; possibilité de corriger) d'autre part.

Analyse

10. Nous supposons que cette question, et celles qui suivent portent sur le scénario soulevé comme une question par le CEPD dans sa lettre à Göran Marby au paragraphe 1 ci-dessus ; à savoir lorsque le titulaire est une personne morale et que l'un de ses employés (ou ses représentants) effectue un enregistrement au nom du titulaire et fournit ses propres données à caractère personnel et/ou celles d'autres personnes concernées (par exemple, en indiquant un collègue comme contact administratif).

11. Dans un tel cas, de ces deux mesures, cette dernière (qui, aux fins de la présente note, représente l'autodésignation vérifiée, « VSC ») représente un risque juridiquement moins élevé pour les parties contractantes. Il peut être possible de combiner les deux.

Consentement

11.1 Une personne concernée doit décider elle-même si elle souhaite prêter son consentement. Cela signifie que dans le scénario analysé, la personne qui effectue un enregistrement de domaine au nom du titulaire (personne morale) ne peut consentir qu'à la publication de ses propres données à caractère personnel. Elle ne peut pas consentir au nom de ses collègues ou d'autres personnes (« personnes concernées tierces »), si des détails à leur sujet sont fournis. Dans ce cas, elle ne pourrait que *transmettre* à une partie contractante le résultat de la décision de consentement de ce tiers.

11.2 Dans une telle situation, dont nous espérons qu'elle ne sera pas rare, la première option (recours au consentement du titulaire) pourrait ainsi laisser les parties contractantes dans l'incapacité de démontrer concrètement que (i) le tiers étant une personne concernée a effectivement consenti ; et/ou (ii) que ce consentement satisfaisait à toutes les exigences du RGPD en matière de validité du consentement (qui sont expliquées aux paragraphes 13 à 18 de la Note sur le consentement).

11.3 La Note sur le consentement présentait cinq options d'approches fondées sur le consentement (Note sur le consentement, par. 24). Il n'est pas évident de savoir laquelle de ces options est envisagée aux fins de la présente question.

11.4 La Note sur le consentement explique que :

11.4.1 Un système dans lequel les contrôleurs demandent le consentement valide direct de toutes les personnes concernées (contrairement à ce que la question actuelle semble proposer) serait moins risqué que de simplement compter sur des affirmations du titulaire de nom de domaine selon lesquelles un consentement valide aurait été obtenu auprès des personnes concernées ; et

11.4.2 Si, néanmoins, le système était conçu autour de la confirmation du titulaire de nom de domaine qu'un consentement valide a été obtenu des personnes concernées, les parties contractantes feraient mieux de vérifier le consentement directement avec les individus, ou d'exiger que le titulaire de nom de domaine fournisse *des preuves* qu'un consentement valide a été obtenu.

Autodésignation vérifiée

11.5 La deuxième option proposée dans la question présentée, la VSC, suggère vraisemblablement que, en règle générale, les données à caractère personnel **ne seront pas** publiées parmi les données d'enregistrement (et, au cas où elles seront incluses par défaut, un contrôle sera effectué en contactant les coordonnées fournies).

11.6 Par conséquent, *si* des données à caractère personnel sont en fait incluses parmi les données d'enregistrement, il s'agit d'un événement, espérons-le, rare et non

intentionnel.[83] En bref, le RGPD devrait, pour la plupart, être inapplicable sauf dans les cas limites accidentels.

11.7 Dans ces cas limites théoriquement rares, plusieurs facteurs atténueraient la responsabilité de la partie contractante (en particulier à la lumière de l'article 83(2) du RGPD, discuté au paragraphe 8 ci-dessus), que ce soit pour l'inexactitude, ou le traitement des données à caractère personnel sans fondement juridique (par exemple, le consentement). En particulier :

11.7.1 Des mesures importantes ont été prises pour vérifier que les données ne soient pas des données à caractère personnel ; et

11.7.2 Un moyen facile de corriger les erreurs a été fourni.

11.8 Il peut même y avoir un argument, fondé sur la jurisprudence de la Cour de justice de l'UE (« CJUE »), qu'il s'agit d'une situation dans laquelle les parties contractantes ne devraient généralement être responsables que si elles ne traitent pas correctement une plainte concernant les données – c'est-à-dire une fois qu'elles sont mises au courant de l'illégalité présumée et qu'elles ont ainsi la possibilité de « vérifier » le bien-fondé de la plainte.[84] Cela comporte un parallèle avec d'autres régimes de responsabilité de l'UE pour les opérateurs de services en ligne qui traitent – involontairement – du contenu qui viole la législation de l'UE.[85] Comme mentionné dans la note en bas de page 87 ci-dessous, cela est sans doute reconnu dans (au moins certaines) décisions des autorités de surveillance du RGPD.

Combinaison

11.9 Bien que la VSC présente un risque moindre pour les parties contractantes, elle présente un inconvénient : cela signifie que les données à caractère personnel ne sont pas (normalement) publiées. Certaines parties prenantes sont d'avis que cela semble être une occasion manquée de maximiser la disponibilité des données d'enregistrement publiquement disponibles.

---

[83] Attribuable à une erreur propre du titulaire de nom de domaine et/ou à l'échec des mécanismes de vérification déployés par une partie contractante.

[84] Dans son arrêt dans l'affaire C-136/17 *GC et autres*, la CJUE a expliqué que les obligations en vertu du RGPD relatives à une demande d'effacement (« droit d'être oublié ») s'appliquent « *à l'opérateur d'un moteur de recherche dans le contexte de ses responsabilités, pouvoirs et capacités en tant que contrôleur du traitement effectué dans le cadre de l'activité du moteur de recherche, à l'occasion d'une vérification effectuée par cet opérateur, sous le contrôle des autorités nationales compétentes, à la suite d'une demande de la personne concernée* ». Comme l'a expliqué l'avocat général dans cette affaire, « *un tel opérateur ne peut agir que dans le cadre de ses responsabilités, de ses pouvoirs et de ses capacités. Autrement dit, un tel opérateur pourrait être incapable d'assurer le plein effet des dispositions de [la loi de l'UE sur la protection des données], précisément en raison de ses responsabilités, pouvoirs et capacités limités. . . Un contrôle ex ante des pages Internet qui sont référencées à la suite d'une recherche ne relève pas des responsabilités ou des capacités d'un moteur de recherche* ». Il ne pouvait pas savoir, à partir du moment où il a indexé une page Web, que le contenu de cette page était (par exemple) obsolète (comme dans la décision originale de l'affaire *Google Espagne / Costeja*), ou (dans *l'affaire GC et autres)* des données de « catégorie spéciale » ou « d'infraction pénale » pour lesquelles il a exigé un consentement.

[85] Voir, par exemple, l'article 14 de la directive sur le commerce électronique 2000/31/EC et sa transposition dans les législations nationales des États membres de l'UE/EEE et du Royaume-Uni.

11.10 Les parties contractantes pourraient donc souhaiter envisager une combinaison de mécanismes : demander à la personne qui complète l'enregistrement si les données qu'elle fournit sont des données à caractère personnel. Si elle dit non, vérifier cette réponse en contactant les coordonnées fournies (VSC). Si, au contraire, elle dit oui, demander si les données à caractère personnel la concernent, et si c'est le cas, si elle est d'accord pour que ces informations soient publiées.

11.11 L'exactitude est parfois présentée comme une préoccupation du RGPD à l'égard de la publication des données d'enregistrement. Bien que nos enquêtes n'aient pas identifié de précédent substantiel en matière d'application de la loi dans une situation telle que celle qui est abordée ici, il nous semble que dans le cadre de ce modèle combiné (VSC + consentement) :

11.11.1 si (la personne représentant le) titulaire de nom de domaine identifie de manière incorrecte les données à caractère personnel comme étant non-personnelles, alors le processus de vérification que cela déclencherait devrait conférer une protection raisonnable contre la responsabilité des parties contractantes en vertu du principe du RGPD sur l'exactitude, comme expliqué au paragraphe 11.7 ci-dessus, comme le pourrait soutenir l'argument juridique énoncé au paragraphe 11.8 ci-dessus.

11.11.2 Autrement, si (la personne représentant) le titulaire de nom de domaine qualifiait de manière incorrecte les données à caractère non personnel comme étant des données à caractère personnel, qu'elle consente ou non ultérieurement à leur publication, les données ne seraient toujours pas des données à caractère personnel, de sorte que la responsabilité ne pourrait pas être réclamée telle que définie dans le RGPD.

QUESTION 2

Question posée : Les paragraphes 17 à 25 de la note de Bird & Bird datée du 25 janvier 2019 [la Note sur la distinction entre personne physique et personne morale] traitent des risques potentiels pour les bureaux d'enregistrement associés à la dépendance à l'égard de (1) l'autodésignation d'un titulaire comme étant une personne morale, et (ii) la confirmation que les données d'enregistrement ne contiennent pas de données à caractère personnel. La note a identifié diverses mesures que les bureaux d'enregistrement pourraient prendre pour atténuer le risque de publication involontaire de données à caractère personnel.

Par exemple, la note suggérait que les bureaux d'enregistrement pourraient prendre certaines mesures pour améliorer l'exactitude de l'autodésignation/attestation, par exemple : fournir des divulgations distinctes et claires, y compris des descriptions des conséquences de l'autodésignation en tant que personne morale, et demander aux titulaires de noms de domaine de confirmer qu'ils ne soumettent pas de données à caractère personnel ; tester la clarté et la lisibilité de telles divulgations ; effectuer un suivi périodique par e-mail avec les titulaires de noms de domaine et/ou les contacts techniques ; et fournir un mécanisme pour modifier l'autodésignation, ou corriger ou s'opposer à la publication des données à caractère personnel.

Q2(1) : En supposant qu'un bureau d'enregistrement prend les mesures d'atténuation identifiées par Bird & Bird, et en fonction de votre expérience et des précédents applicables, veuillez décrire le niveau de risque, la probabilité de mesures d'application de la loi, les amendes, les conseils, etc. résultant de la publication accidentelle subséquente de données à caractère personnel contenues parmi les données d'enregistrement d'une personne morale.

Q2(2) : En détaillant davantage la question [2(1)], veuillez aborder le niveau de risque (par exemple, mesures d'application de la loi, amendes, conseils, etc.) qu'affronte une partie contractante face à la publication de données à caractère personnel si un e-mail de confirmation envoyé par un bureau d'enregistrement au titulaire de nom de domaine et/ou aux contacts techniques du titulaire (i) indique clairement que le titulaire s'est autodésigné comme une personne morale et a déclaré affirmativement qu'aucune donnée à caractère personnel n'avait été incluse parmi ses données d'enregistrement ; ii) explique qu'en fonction de ces deux représentations, tous les champs des données d'enregistrement seront publiés sur Internet ; et (iii) fournit un mécanisme facile à utiliser par lequel l'autodésignation puisse être annulée et qui permette à une personne qui reçoit l'e-mail de s'opposer à la publication de ses données à caractère personnel et/ou corriger toute date inexacte ? Le bureau d'enregistrement doit-il exiger la réponse affirmative du titulaire de nom de domaine et/ou de son contact technique à son e-mail de confirmation ? La réponse varie-t-elle en fonction du support de la notification (par exemple, courrier postal ou e-mail) ?

Q2(3) : Existe-t-il des mesures d'atténuation et/ou de vérification supplémentaires ou alternatives disant qu'une partie contractante pourrait prendre pour réduire/éliminer davantage la responsabilité liée à la publication involontaire de données à caractère personnel en relation avec l'utilisation de l'autodésignation d'un titulaire de nom de domaine, par exemple la confirmation de l'existence d'identificateurs d'entreprise (Inc., GmbH, Ltd., etc.), l'examen des données du titulaire du compte pour des indices de personnalité juridique, etc. ? Dans quelle mesure chacune de ces mesures supplémentaires réduirait-elle la responsabilité ?

12. En ce qui concerne la Q2(1) (*niveau de risque, généralement, si les mesures décrites dans la VSC sont adoptées*) : malgré notre recherche de précédents dans plusieurs États membres de l'UE/EEE, nous ne sommes pas au courant d'un précédent comparable. De surcroît, il convient de noter que les tendances en matière d'application de la loi et les politiques d'action réglementaire évoluent en permanence, tout comme la viabilité des poursuites civiles par les parties en litige.

13. Toutefois, à notre avis, le risque pour les parties contractantes semble faible, si elles prennent les mesures décrites dans la question présentée pour éviter que les données à caractère personnel soient (ou si elles sont déclarées, restent) publiées parmi les données d'enregistrement.

14. Notre point de vue est basé sur les facteurs suivants (compte tenu également du paragraphe 83(2) du RGPD, dont il est question au paragraphe 8 ci-dessus) :

14.1 L'inclusion par négligence de données à caractère personnel, malgré les mesures décrites dans ce document (en supposant qu'elles sont bien mises en œuvre), semble ne se produire que sur une base exceptionnelle. Comme nous l'avons indiqué dans la Note sur la distinction entre personne physique et personne morale, il serait conseillé à l'ICANN et aux parties contractantes d'étudier (par exemple, de recueillir des statistiques) afin de contrôler si les mesures fonctionnent comme prévu.

14.2 Si les données à caractère personnel sont incluses par négligence dans les données d'enregistrement publiées, cela se produirait malgré les mesures importantes (VSC) prises par les parties contractantes dans ce scénario, et seraient principalement attribuables aux actions/omissions du titulaire de nom de domaine. Cela sera probablement pris en compte par les personnes concernées, les autorités de surveillance de la protection des données et les tribunaux.

14.3 Les données en question sont probablement de faible sensibilité. Le scénario envisagé ici (inclusion de données à caractère personnel parmi les données d'enregistrement publiées par négligence) semble être le plus susceptible de se produire lorsqu'une entité juridique (par exemple, une entreprise ou une organisation à but non lucratif) enregistre/entretient ses propres domaines. Dans ces scénarios, nous supposons que les données à caractère personnel qui pourraient être divulguées concernent habituellement les coordonnées professionnelles d'un employé (par exemple, l'adresse électronique d'une entreprise), et non la vie privée d'un individu. Bien que le RGPD confère une protection même sur le lieu de travail, les données en question peuvent sans doute être moins susceptibles de nuire à un individu que les données relatives à la vie privée de la personne concernée.[86]

14.4 Dans les cas plus sensibles (par exemple, s'il était déclaré qu'une personne travaille pour une entreprise dans un secteur sensible ou « embarrassant »), un titulaire de nom de domaine risquerait sérieusement de se soumettre à des plaintes de la part de ses propres employés. Les titulaires de noms de domaine ont donc déjà une incitation suffisante pour éviter les erreurs qui pourraient avoir de graves conséquences pour leur propre personnel.

14.5 Les mesures envisagées incluent la capacité de corriger l'erreur. Bien sûr, la nature de l'Internet mondial implique qu'il pourrait être difficile de supprimer complètement les données publiées par négligence des miroirs / caches / archives, si des services sont mis en place pour le faire. Nous encouragerions donc les mesures supplémentaires envisagées pour la Q2(2) ci-dessous.

[86] Comme expliqué ci-dessus, nous avons interprété cette question comme étant relative à des scénarios dans lesquels les titulaires sont des personnes morales, conformément à la citation du CEPD qui apparaît au paragraphe 1. En ce qui concerne les personnes titulaires de noms de domaine (personnes physiques), les questions seront largement similaires : si une personne physique déclare à tort que ses données ne sont pas des données à caractère personnel (i) les mesures de vérification devraient empêcher la publication des données, puisqu'elles donneront à la personne concernée la possibilité de corriger son erreur ; (ii) les facteurs atténuants et les arguments juridiques décrits aux paragraphes 11.7 et 11.8 aux paragraphes 14.1 - 14.6 dans ces présentes devraient conférer une protection juridique raisonnable aux parties contractantes.

14.6 Enfin, comme il a été mentionné ci-dessus, il pourrait être possible de fonder des arguments sur l'*affaire GC et autres* et considérer que cette responsabilité ne doit être engagée auprès d'une partie contractante que si et lorsqu'elle ne parvient pas à traiter correctement les plaintes concernant l'inclusion de données à caractère personnel dans les données d'enregistrement publiées (et non à partir du point précédent de la publication involontaire des données). Ceci étant, cela semble conditionné à ce que le ou les contrôleurs aient pris des mesures raisonnables pour empêcher une telle inclusion (par exemple, les mesures VSC discutées dans le présent document).

En ce qui concerne la Q2(2) (*niveau de risque si un e-mail de confirmation est envoyé, offrant un moyen facile d'annuler l'autodésignation / corriger les inexactitudes*) :

15. À notre avis, cette méthode de vérification est recommandée et contribuera à réduire les risques. Cette réduction du risque sera plus importante s'il existe un délai de grâce raisonnable dans lequel l'objection puisse être déposée, *avant* que les données en question ne soient publiées parmi les données d'enregistrement.

16. Les parties contractantes devraient prendre en compte les délais postaux (« courrier postal ») si ce moyen est utilisé. Il faudra peut-être du temps pour que le courrier soit livré à l'organisation, puis se retrouve face à la bonne personne (qui n'est peut-être pas en fonction, par exemple en congé annuel), puis soit traité par cette personne. L'e-mail ne souffrirait au moins pas habituellement des retards de livraison ; le délai de grâce ne devrait alors envisager qu'une possible absence et/ou l'incapacité temporaire du destinataire à traiter l'e-mail pour d'autres raisons.

17. À notre avis, il semble trop prudent d'exiger une réponse affirmative aux courriers de vérification, à moins que et jusqu'à ce que des études montrent que les mesures adoptées ne parviennent pas à maintenir des quantités très importantes de données à caractère personnel hors des données d'enregistrement publiées. Toutefois, si un e-mail de vérification était « retourné » (c'est-à-dire qu'une partie contractante sait qu'il n'a pas été livré), il serait préférable que la publication ne se poursuive pas (c'est-à-dire que le contrôle VSC devrait être traité comme ayant échoué dans ce cas).

18. Nous ne pouvons point exclure la possibilité que certains tribunaux ou organismes de réglementation voient les choses différemment. Même dans ce cas, un ordre pour corriger la question (probablement accompagné d'un délai raisonnable pour mettre en œuvre les changements), plutôt qu'une amende, semble plus probable, au vu des facteurs de l'article 83(2) du RGPD discutés au paragraphe 8 ci-dessus. Après avoir vérifié dans une sélection d'États membres, nous n'avons pu trouver aucun exemple d'application à cet égard. Par conséquent, il y a peu de directives disponibles outre ce qui est énoncé dans le RGPD lui-même.

19. *En ce qui concerne la Q2(3) (mesures supplémentaires ou alternatives pour réduire la responsabilité en vertu de la VSC)* : notre avis aux paragraphes 21 à 25 de la Note de suivi sur l'exactitude est particulièrement pertinent ici. Une grande partie de cette discussion, ainsi que le tableau des 16 mesures supplémentaires possibles qui pourraient être prises pour minimiser ou compenser les éventuelles inexactitudes dans les données d'enregistrement, restent pertinents ici.

20. La question, tel que vous l'avez posée, réitère déjà un grand nombre de ces mesures, à savoir : « *Fournir des divulgations distinctes et claires, y compris des descriptions des conséquences de l'autodésignation en tant que personne morale, et demander aux titulaires de noms de domaine de confirmer qu'ils ne soumettent pas de données à caractère personnel ; tester la clarté et la lisibilité de telles divulgations ; effectuer un suivi périodique par e-mail avec les titulaires de noms de domaine et/ou les contacts techniques ; et fournir un mécanisme pour modifier l'autodésignation, ou corriger ou s'opposer à la publication des données à caractère personnel* ».

21. La présente question suggère également de « *confirmer l'existence d'identificateurs d'entreprise (Inc., GmbH, Ltd., etc.)[et/ou] examiner les données du titulaire du compte pour des indices de personnalité juridique* ». En outre, la saisie d'un numéro d'enregistrement d'entreprise peut être un autre moyen de vérifier la personnalité juridique.

22. Ceci dit : la plupart des employeurs pourront fournir un numéro d'entreprise et/ou un nom d'entreprise se terminant par Ltd., PLC, SA, BV, GmbH, *etc.* ; et pourtant, ils pourraient également fournir des données à caractère personnel sur leurs employés, par exemple en tant que contacts pour le domaine. En conséquence, une telle vérification (même si elle s'avère viable) confirme seulement que le titulaire du nom de domaine est une personne morale. Elle *ne confirme pas* qu'un titulaire de nom de domaine qui est une personne morale n'a pas (en même temps) fourni des données à caractère personnel, par exemple sur ses employés. Cette mesure permet ainsi d'éviter que les titulaires de noms de domaine qui sont des personnes physiques identifient incorrectement leurs propres données, mais cela ne constitue pas un risque majeur (du point de vue du RGPD), puisque ces personnes sont en tout état de cause incitées à déclarer correctement leur statut de personne physique, et leur déclaration peut être vérifiée en les contactant. L'alternative, qui est peut-être un plus grand risque qu'un employeur comprenne les données à caractère personnel de ses employés n'est pas affectée par une telle mesure. Une telle mesure comporte donc des avantages limités en vertu du RGPD.

23. Ce qui pourrait être utile, si cela était possible, serait peut-être d'utiliser un outil technique pour évaluer si les adresses e-mail incluent le nom d'une personne ou semblent être génériques. À elle seule, cette mesure ne serait pas suffisante ; les adresses e-mail pourraient concerner une personne identifiable (c'est-à-dire, être des données à caractère personnel) même si leur nom n'est pas utilisé. Un tel outil ne devrait donc être considéré que comme faisant partie d'un ensemble de mesures. En ce qui concerne les numéros de téléphone : si ces derniers sont collectés, un outil technique pourrait vérifier les préfixes typiques associés aux téléphones portables (qui sont généralement liés à une seule personne, probablement plus souvent que les numéros de téléphone fixes).

24. De telles caractéristiques devraient être soigneusement mises à l'essai, puisque le taux de faux positifs et de faux négatifs pourrait être important, en particulier compte tenu de la nature très internationale du système des noms de domaine supervisé par l'ICANN (même en anglais, nous supposons que les adresses e-mail qui suivent le format « @johndeere.com » ou « @annsummers.com » pourraient présenter des difficultés).

25. Plutôt que d'agir automatiquement sur les conclusions de ces outils, certaines parties contractantes seraient prêtes à évaluer « manuellement » les données suspectes, bien que cela impliquerait probablement un effort substantiel de la part des parties contractantes. Il semble plus probable qu'un tel outil présente plutôt un rappel au titulaire de nom de domaine déclarant (« *il semble que vous pourriez avoir fourni les coordonnées d'une personne* (…) »), lui demandant s'il veut rejeter ce rappel ou poursuivre compte tenu de cela.

26. Par conséquent, ces outils pourraient être plus efficaces si le déploiement agit comme un « coup de pouce » supplémentaire (intelligent, conscient du contenu) pour les titulaires de noms de domaine, et non comme un déterminant automatisé de la possibilité de publier des données.

27. Compte tenu de la viabilité et des mérites peu clairs d'une telle approche, elle pourrait, par exemple, être considérée comme un élément plus à moyen/long terme pour l'exploration et les essais ; son développement et son déploiement complets pourraient être conditionnés à montrer non seulement qu'elle est techniquement viable, mais aussi que l'expérience montre que des mesures supplémentaires sont en fait nécessaires.

28. En fin de compte, nous ne pouvons donc pas actuellement prévoir d'autres mesures nécessaires ou attendues de la part des parties contractantes, outre celles qui sont déjà examinées dans la question posée.

29. Des divergences d'opinions sur ce point sont possibles. En outre, beaucoup pourrait dépendre de *la façon* dont les mesures proposées, y compris celles proposées dans la question posée, sont mises en œuvre. Par exemple, il existe un précédent en Hongrie selon lequel, lorsque l'exactitude des données est contestée, le traitement des données (par exemple, leur publication) pourrait devoir être temporairement interrompu, mais dans la mesure nécessaire pour vérifier et agir sur l'inexactitude signalée[87] ; apparemment pour savoir si la personne concernée a explicitement invoqué l'article 18(1) du RGPD (droit de demander la limitation du traitement des données pendant que des inexactitudes sont vérifiées). Bien que la conception suggérée ici ne semble pas exiger ou se prêter à une telle suspension temporaire (puisque les personnes concernées seraient en mesure de corriger instantanément une autocaractérisation qu'elles considèrent inexacte, c'est-à-dire que les rapports et les rectifications devraient normalement être simultanés), nous vous recommandons de garder cela à l'esprit si les plans évoluent et, en fin de compte, si les données inexactes pouvaient générer un retard potentiel entre le rapport et la rectification.

30. Au paragraphe 21 de la Note de suivi sur l'exactitude, nous avons expliqué que « *L'ICANN et/ou les parties contractantes seront les mieux placées pour évaluer*

[87] Décision de la NAIH dans l'affaire NAIH/2019/363/2 ; disponible en ligne à l'adresse https://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf. Une traduction automatique du passage en question dit : « *l'Autorité convient avec le [défendeur] que le contrôleur n'est pas tenu d'effacer des données dans un cas où l'exactitude des données précédemment fournies par le client est remise en question par un tiers et qu'il n'est pas démontré que les données ne sont plus à la disposition du client, mais à la disposition du notifiant. Toutefois, les mesures prises par le contrôleur sur la base de la notification devraient promouvoir le principe de l'exactitude et éviter l'utilisation de données inexactes. Dans ce cas, l'Autorité estime que le contrôleur devrait limiter temporairement le traitement des données inexactes en prenant des mesures raisonnables* ».

si les procédures actuellement en vigueur sont suffisantes ou s'il serait raisonnable de prendre des mesures supplémentaires pour se conformer au principe d'exactitude ; dans l'affirmative, il leur appartiendra d'évaluer les mesures qui seraient les plus appropriées ». Cette même note a indiqué au paragraphe 24 que « *[L]'utilisation de statistiques et le suivi du nombre de demandes de correction des personnes concernées sont également des mesures qui pourraient contribuer à assurer un niveau de précision approprié. Par exemple, le suivi des tendances au niveau des demandes de rectification pourrait permettre d'identifier un écart de précision ou lorsqu'une mesure peut ne pas être entièrement efficace et prendre des mesures pour couvrir l'écart ou remplacer la mesure par une autre plus appropriée* ».

* * *

Réponse à la Question 3 (personne morale vs. personne physique)

NOTE

Pour :	Société pour l'attribution des noms de domaine et des numéros sur Internet, équipe responsable de l'EPDP
De :	Ruth Boardman et Phil Bradley-Schmieg
Date :	27 avril 2021
Objet :	Question de mars 2021 concernant la reconnaissance par l'UE et par les tiers des intérêts relatifs à la publication des données d'enregistrement

Contexte

31. Dans une lettre du CEPD en date de juillet 2018 adressée à Göran Marby (la « lettre du CEPD de juillet 2018 »), [88] il a été déclaré ce qui suit :

> « Les données à caractère personnel identifiant les employés individuels (ou les tiers) agissant pour le compte du titulaire du nom de domaine ne devraient pas être rendues publiques par défaut dans le contexte du WHOIS ».

32. Cela a suscité plusieurs questions liées au RGPD, plus récemment dans notre note du 6 avril 2021 (la « **Note sur la VSC et les options de consentement** »), qui a abordé deux questions (les « **questions 1 et 2** ») traitant de différentes approches (et des risques qui en découlent) en ce qui concerne (i) la publication des données d'enregistrement conditionnée au consentement ; et (ii) la publication des données d'enregistrement si elles concernent (uniquement) une personne morale (par exemple, une entreprise), plutôt que d'être des données à caractère personnel (et comment cela peut être vérifié) ; c'est-à-dire, si elles font l'objet d'une autocaractérisation vérifiée, « VSC ».

33. Vous avez également demandé, dans la question présentée ci-dessous, si certaines dispositions de la législation de l'UE et/ou les pratiques de deux tierces parties (EURid et RIPE-NCC) créent un précédent utile dans ce domaine. La présente note se penche sur cette troisième question.

Question présentée : Le règlement de la Commission (CE) nº 874/2004 du 28 avril 2004 établissant des règles d'ordre public concernant la mise en œuvre et les fonctions du domaine de premier niveau .eu ainsi que les principes régissant l'enregistrement (« règlement .eu ») définit les règles de politique publique concernant la mise en œuvre et les fonctions du domaine de premier niveau .eu (TLD) et les principes de politique publique relatifs à l'enregistrement des noms de domaine dans le TLD .eu.

[88] Lettre du CEPD à Göran Marby en date du 5 juillet 2018 ; disponible en ligne à l'adresse https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf

L'article 16 du règlement de .eu est intitulé « base de données Whois » et prévoit :

> *« La finalité de la base de données WHOIS est de fournir des informations raisonnablement exactes et à jour sur les points de contact techniques et administratifs qui gèrent les noms de domaine enregistrés sous le TLD .eu.*
>
> *La base de données WHOIS doit contenir des informations sur le titulaire d'un nom de domaine pertinentes et non excessives par rapport à l'objet de la base de données. Dans la mesure où les informations ne sont pas strictement nécessaires en relation avec l'objet de la base de données, et si le titulaire du nom de domaine est une personne physique, les informations qui doivent être rendues publiques sont soumises au consentement sans équivoque du titulaire du nom de domaine. La présentation délibérée d'informations inexactes constituera un motif pour considérer que l'enregistrement du nom de domaine a enfreint les conditions de l'enregistrement ».*

À partir du 13 octobre 2022, le règlement de .eu sera abrogé par le règlement 2019/517, qui prévoit, en vertu de son article 12, intitulé base de données WHOIS :

> « *1. Le registre met en place et gère, avec toute la diligence requise, une base de données WHOIS dans le but de garantir la sécurité, la stabilité et la résilience du TLD .eu en fournissant des informations exactes et actualisées concernant les noms de domaine enregistrés dans le TLD .eu*
>
> *2. La base de données WHOIS contient des informations pertinentes concernant les points de contact qui gèrent les noms de domaines dans le TLD .eu et concernant les titulaires des noms de domaine. Les informations contenues dans la base de données WHOIS ne sont pas excessives par rapport à la finalité de la base de données. Le registre respecte le règlement (UE) 2016/679 du Parlement européen et du Conseil ».*

La base de données Whois est actuellement administrée par EURid, un organisme à but non lucratif désigné par la Commission européenne pour gérer le registre .eu. Dans sa base de données Whois, EURid publie les adresses e-mail des titulaires de noms de domaine enregistrés sous le TLD .eu (personnes physiques et morales). EURid fait la distinction entre les personnes physiques et les personnes morales en publiant l'adresse postale des personnes morales, alors que cette information n'est pas publiée pour les personnes physiques.

Par l'intermédiaire de l'article 16 du règlement de .eu, EURid peut se fonder sur l'article 6(1)(e) du RGPD, qui fournit une base juridique pour le traitement des données à caractère personnel qui est nécessaire pour l'exécution d'une tâche effectuée dans l'intérêt public ou dans l'exercice de l'autorité officielle dévolue au contrôleur. Bien que nous comprenions que la base d'intérêt public prévue à l'article 16 n'est pas disponible en dehors du domaine .eu, l'existence de cette base légale pour

le traitement d'EURid pourrait être interprétée de manière à suggérer que la législature de l'UE aurait reconnu que la divulgation des données enregistrées d'un titulaire de nom de domaine sert un intérêt légitime à la stabilité, à la sécurité et à la résilience. En outre, dans l'exercice de son mandat en vertu de l'article 16, EURid a déterminé que la publication de l'e-mail du titulaire de nom de domaine « n'est pas excessive par rapport à l'objet de la base de données ».

De même, bien que RIPE-NCC s'appuie sur le consentement pour publier des renseignements à caractère personnel vis-à-vis des contacts tech/admin, il publie des informations personnelles sur les détenteurs de ressources au motif que « faciliter la coordination entre les opérateurs de réseau est la seule finalité qui justifie la publication de données à caractère personnel dans la base de données de RIPE-NCC et qu'il est clair que le traitement des données à caractère personnel se rapportant à un détenteur de ressources est nécessaire pour l'exécution de la fonction de l'opérateur de registre, qui est exécutée dans l'intérêt légitime de la communauté RIPE et le bon fonctionnement de l'Internet dans le monde (et est donc conforme à l'article 6.1.f du RGPD) ».

Nous comprenons que la base d'intérêt public fournie par l'article 16 n'est pas disponible pour les parties contractantes en dehors du domaine de premier niveau .eu. Sur la base de votre expérience et du précédent applicable, dans quelle mesure (le cas échéant) : (i) l'existence de l'article 16 du règlement de l'UE ; (ii) la décision d'EURid de publier les adresses e-mail des titulaires conformément à l'article 16 ; (iii) la décision de RIPE-NCC de publier les adresses électroniques des détenteurs de ressources ; et (iv) un texte préliminaire concernant l'accès aux données d'enregistrement de la directive NIS2 récemment proposée créent-ils un précédent qui réduirait le risque des parties contractantes en relation avec la publication de l'adresse e-mail d'un titulaire de nom de domaine qui est une personne morale, même si les informations contenues étaient personnelles ? Ces faits affectent-ils vos réponses aux questions [1 et 2] ? Si cela n'affecte pas vos réponses, veuillez expliquer pourquoi.

34. Nous croyons que, dans l'ensemble, les documents cités n'affectent pas nos réponses aux questions 1 et 2 contenues dans la note vis-à-vis de la VSC et des options de consentement. Plus précisément, nous pensons que les documents cités ont un impact limité sur le risque pour la partie contractante en ce qui concerne la publication de l'adresse e-mail d'un titulaire de nom de domaine qui est une personne morale, même si ladite adresse contenait des données à caractère personnel. Notre point de vue est basé sur les raisons indiquées ci-dessous.

Règlement (UE) 2019/517, qui remplace le règlement (CE) n° 874/2004 de la Commission (le « nouveau règlement de .EU »)

35. Lorsque le Règlement (UE) 2019/517 (le « nouveau règlement de .EU ») remplacera le règlement (CE) n° 874/2004 de la Commission (l'« ancien règlement de .EU »), il supprimera une disposition de l'ancien règlement de .EU qui autorise la publication « non strictement nécessaire » de données à caractère personnel parmi les données d'enregistrement (si la personne concernée y consent

expressément). Les dispositions pertinentes sont citées dans la question présentée.

36. Le nouveau règlement de .EU ne dit pas expressément qu'une approche basée sur le consentement se soit avérée peu pratique ou non conforme ; il ne propose tout simplement aucun commentaire sur une telle approche. En fait, le nouveau règlement de .EU ne fait aucun commentaire spécifique sur la publication de données à caractère personnel, que ce soit « strictement nécessaire » ou autrement. Il se limite à exiger que le traitement des données soit conforme au RGPD (le cas échéant), sans dire comment. En particulier, le considérant 22 du règlement (UE) 2019/517 exige expressément que l'opérateur de registre de .EU choisisse une mise en œuvre de la base de données WHOIS et des systèmes connexes conformes aux normes de « protection des données à caractère personnel dès la conception et protection des données par défaut », par « nécessité » et par « proportionnalité ».

37. La référence la plus directe à la distribution des données d'enregistrement, s'il s'agit de données à caractère personnel, se trouve au considérant 21. Cela ne concerne que le partage des données avec les *organismes chargés de l'application de la loi* et leur accès, agissant en vertu de « la législation [de l'UE] ou nationale », *et non* le grand public *ni* les parties intéressées telles que les titulaires de droits de propriété intellectuelle :[89]

> « 21. Le registre devrait soutenir les services répressifs dans le cadre de la lutte contre la criminalité en mettant en œuvre des mesures techniques et organisationnelles visant à permettre aux autorités compétentes d'avoir accès aux données figurant dans le registre aux fins de la prévention et de la détection des infractions, ainsi que des enquêtes et des poursuites en la matière, comme le prévoit le droit de l'Union ou le droit national ».

38. En substance, le nouveau règlement de .EU parvient ici à une position généralement neutre et peu concluante. Il s'en remet généralement aux exigences du RGPD, et il évoque *expressément* le besoin de respecter la proportionnalité et la vie privée par défaut. Le fait qu'il traite de l'accès légitime par des groupes de parties prenantes *spécifiques* n'exclut pas nécessairement un système dans lequel certaines données à caractère personnel sont rendues publiques, par exemple avec le consentement d'une personne concernée. Néanmoins, le nouveau règlement de .EU a abandonné le libellé (trouvé dans son prédécesseur) qui acceptait explicitement une approche fondée (en partie) sur le consentement ; il est possible qu'une autorité de surveillance ou un tribunal puisse chercher à en tirer une conclusion défavorable.

[89] D'autres références à des intérêts plus larges ne traitent pas du partage des données du titulaire de nom de domaine avec elles. Par exemple, le considérant 20 dit que « [L]e registre devrait adopter des mesures claires visant à garantir l'identification en temps utile des enregistrements abusifs de noms de domaine et, si nécessaire, coopérer avec les autorités compétentes et d'autres organismes publics compétents en matière de cybersécurité et de sécurité de l'information qui participent spécifiquement à la lutte contre ces enregistrements, tels que les équipes nationales d'intervention informatique d'urgence (CERT) ». La « coopération » *pourrait* impliquer le partage de données à caractère personnel, mais (peut-être délibérément) la nouvelle réglementation de .EU ne dit rien sur ce point.

Fondement d'EURid sur la base juridique de la « tâche publique » du RGPD

39. La question posée suggère qu'EURid s'appuie sur l'article 16 de l'ancien règlement de .EU pour affirmer que sa publication (partielle) des données à caractère personnel des titulaires de noms de domaine soit autorisée par l'article 6(1)(e) du RGPD.

40. L'article 6(1)(e) permet le traitement nécessaire à l'exécution d'une tâche nécessaire pour l'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le contrôleur. Ces derniers doivent être prévus dans le droit de l'UE ou des États membres de l'UE.

41. Si la suggestion de la question est correcte,[90] alors EURid affirme implicitement qu'une telle publication est « strictement nécessaire par rapport à l'objectif de la base de données ». Si ce n'était pas le cas, alors EURid serait en infraction de l'article 16 de l'ancien règlement de .EU, qui stipule que « dans la mesure où l'information n'est pas strictement nécessaire en relation avec l'objet de la base de données, et si le titulaire du nom de domaine est une personne physique, les informations qui doivent être rendues publiques seront soumises au consentement sans équivoque du titulaire du nom de domaine ». À partir de la question posée, nous comprenons qu'EURid n'obtient pas ce consentement.

42. D'une part, cette position présumée indique qu'au moins un opérateur de registre (EURid) confirme l'importance (« stricte nécessité ») de publier (certaines) données dans le WHOIS, même s'il s'agit de données à caractère personnel, et sans consentement ou sans mesures telles que la VSC (à condition, au moins, que certaines données à caractère personnel soient expurgées, conformément à la politique d'EURid en la matière).[91]

43. Toutefois, le point de vue d'EURid ne reflète pas nécessairement le point de vue des tribunaux ou des autorités de surveillance qui font appliquer le RGPD et n'est pas contraignant pour eux. C'est le point de vue d'un opérateur de registre, entre autres. Le fait que les politiques de ce registre particulier soient également

[90] Nous n'avons pas été en mesure de le confirmer ; la politique actuelle de protection de la vie privée d'EURid ne précise pas expressément quelle est la base juridique du RGPD qui justifie la publication des données d'enregistrement, bien qu'elle indique que « nous sommes tenus de maintenir une base de données complète et précise de tous les noms de domaine enregistrés. La finalité de la fonction de recherche du WHOIS (https://whois.eurid.eu/en/ est de fournir des informations précises et à jour sur les personnes à contacter, tant sur le plan technique que sur le plan administratif, qui gèrent les noms de domaine. Cela nous aide à créer et à maintenir un environnement Internet sûr et fiable ». La référence aux publications « requises » semble compatible avec l'article 6(1)(e) (mission d'intérêt public) ou l'article 6(1)c) (obligation légale) du RGPD.

[91] Nous notons avec intérêt que la question posée affirme qu'EURid invoque l'Article 6(1)(e) du RGPD (mission d'intérêt public / autorité publique) *et non* l'Article 6(1)(f) du RGPD (intérêts légitimes). EURid n'est pas une autorité publique, et en principe est donc capable d'invoquer des intérêts légitimes pour publier des données à caractère personnel. Nous ne sommes pas au courant du raisonnement d'EURid pour éviter la base des « intérêts légitimes », et ne pouvons donc pas formuler de commentaires substantiels sur cette observation ; cela dit, il pourrait ne pas être utile/rassurant pour les autres parties contractantes. Contrairement à EURid, la plupart des parties contractantes ne peuvent pas se fonder sur l'article 6(1)(e) du RGPD parce que, à la différence d'EURid, il n'existe pas de droit de l'UE ou des États membres qui sous-tendent leur propre traitement lié au WHOIS.

assujetties à la surveillance de la Commission européenne[92] a une valeur de précédent tout aussi limitée : même si, d'un point de vue hypothétique, il s'agit d'une question qui a été discutée entre EURid et la Commission européenne, cette dernière ne s'occupe pas de faire appliquer le RGPD et ne parle pas non plus de ceux qui le font.

44. La question présentée précise en outre que « EURid distingue les personnes physiques des personnes morales en publiant l'adresse postale des personnes morales, alors que ces informations ne sont pas publiées pour les personnes physiques ». La politique actuelle relative à l'enregistrement des noms de domaine d'EURid (v.11) explique que "Si aucun nom de société ou d'entreprise n'est spécifié, la personne physique déposant la demande d'enregistrement est alors considérée comme étant le Titulaire ; si le nom de la société ou de l'entreprise est spécifié, cette dernière est alors considérée comme étant le Titulaire ».

45. Cela peut signifier qu'il est supposé que les coordonnées postales fournies par une organisation (un titulaire de nom de domaine qui est une personne morale) *ne contiennent pas* de données à caractère personnel ; ou simplement que, dans l'affirmative, cela est strictement nécessaire et/ou représente un risque moindre pour les personnes physiques. EURid (en tant qu'autorité de contrôle de la plupart des données en question) sera mieux placé que nous ne le sommes pour déterminer si cette hypothèse est vraie dans la pratique.

46. Même supposant que cette hypothèse est vraie dans la pratique pour EURid et les adresses postales qu'il publie dans le cadre des données d'enregistrement des personnes morales sous .EU, nous notons qu'à la lumière des commentaires du CEPD à l'ICANN,[93] il peut être déconseillé d'extrapoler ceci à d'autres informations de contact (par exemple, les adresses e-mail, qui peuvent se référer spécifiquement à une personne facilement identifiable au sein de l'organisation).

47. Sur la base de ces observations, et de l'appréciation du fait qu'EURid fonctionne dans un cadre législatif quelque peu unique qui lui donne la possibilité de s'appuyer sur quelque chose d'autre que le consentement ou les intérêts légitimes (contrairement à d'autres parties contractantes), il est difficile de tirer des conclusions générales de l'approche d'EURid.

La décision de RIPE-NCC de publier les adresses e-mail des détenteurs de ressources

48. La question a évoqué des citations d'un article de blog de 2018 écrit par le chef du service juridique de RIPE-NCC intitulé « Comment nous mettons en œuvre le

[92] Par exemple, le considérant 11 du nouveau règlement de .EU stipule : « La Commission devrait conclure avec le registre désigné un contrat, dans lequel devraient être précisés les procédures et les principes qui sont applicables au registre en matière d'organisation, d'administration et de gestion du TLD .EU ».

[93] « Le simple fait qu'un titulaire de nom de domaine soit une personne morale ne justifie pas nécessairement la publication illimitée de données à caractère personnel concernant des personnes physiques qui travaillent pour ou représentent cette organisation, comme les personnes physiques qui gèrent des questions administratives ou techniques pour le compte du titulaire du nom de domaine. Par exemple, la publication de l'adresse e-mail personnelle d'une personne qui est le contact technique composée de prénom.nom@société.com peut révéler des informations concernant son employeur actuel ainsi que son rôle au sein de l'organisation. Ensemble avec l'adresse du titulaire du nom de domaine, cela pourrait également révéler des renseignements sur son lieu de travail ». Lettre du CEPD de juillet 2018, à la page 5.

RGPD : fondements juridiques pour le traitement légal des données à caractère personnel et la base de données de RIPE ».

49. Dans cet article de blog, comme la question posée l'indique correctement, RIPE-NCC affirme qu'il s'appuie sur des intérêts légitimes (la base juridique de l'article 6(1)(f) du RGPD) pour la publication de données à caractère personnel (principalement les coordonnées) pour aider au bon fonctionnement d'un important système Internet.

50. Cependant, il convient de noter que l'article de blog indique également :

> « Toutefois, lorsque le détenteur de la ressource désigne une autre personne pour remplir ce rôle [c'est-à-dire, comme point de contact], il doit obtenir le consentement de la ou des personnes dont les données à caractère personnel seront insérées dans la base de données de RIPE avant de procéder à l'insertion de leurs données (conformément à l'article 6.1.a du RGPD) ».

51. Autrement dit, il nous semble que lorsque le détenteur de la ressource lui-même est une personne morale (i) RIPE-NCC considère les intérêts légitimes comme une base juridique appropriée dans les paramètres de la première partie (c'est-à-dire lorsque la personne qui effectue/met à jour un enregistrement fournit ses propres coordonnées et est donc la personne concernée par les données), mais (ii) RIPE-NCC avait préféré (au moins en 2018) de le faire uniquement avec le consentement d'une personne concernée dans des paramètres d'un tiers (par exemple, lorsque les coordonnées sont celles d'un collègue de la personne qui a complété/mis à jour l'enregistrement).

52. Cette distinction peut être due à des craintes qu'il soit plus difficile d'affirmer que les intérêts propres du tiers sont suffisamment alignés avec ceux du détenteur de la ressource et/ou de RIPE-NCC (et des parties prenantes connexes) ; et/ou des craintes qu'il y ait des risques plus importants pour les tiers qui sont des personnes concernées (par exemple, parce qu'il est plus difficile de leur faire parvenir un avis de confidentialité du RGPD, de sorte qu'ils peuvent être moins conscients de leurs droits). De telles préoccupations pourraient donc avoir motivé RIPE-NCC à préférer de se fier plutôt au consentement dans ces situations de « tiers ».

53. Bien que RIPE-NCC doive se procurer ses propres conseils juridiques sur la question, notre point de vue en ce qui concerne l'EPDP de l'ICANN est que cette distinction pourrait ne pas être légalement requise. L'article 6(1)(f) (la condition des intérêts légitimes) du RGPD n'exige pas que les intérêts de la personne concernée par les données soient alignés avec ceux des contrôleurs. Il suffit simplement d'établir un équilibre approprié entre les intérêts en jeu (ceux du contrôleur et/ou des tiers), par opposition aux « droits et libertés fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel ». Dans ce cas, RIPE-NCC et ses propres conseillers juridiques seront les mieux informés des divers intérêts et risques, mais il nous semble que :

    53.1 Les intérêts *du contrôleur et des parties prenantes au sens large* sembleraient être globalement les mêmes, que ce soit pour traiter les coordonnées d'une première partie ou d'un tiers : par exemple, l'ensemble de données correspondant à l'un ou à l'autre est vraisemblablement important

pour la correcte évaluation et résolution des perturbations d'un système Internet clé ;

53.2 En ce qui concerne les risques, les coordonnées de la première partie ou d'un tiers pourraient également être utilisées à des fins de marketing non sollicité ; il pourrait y avoir d'autres types de risques, mais une fois de plus, celles-ci semblent être similaires, que ce soit pour des personnes concernées qui sont des premières parties ou des tiers ;

53.3 En ce qui concerne la question de la notification, le RGPD accepte expressément qu'il y ait des situations dans lesquelles les données ne seront pas recueillies directement auprès d'une personne concernée et qu'une notification ne leur soit donc pas fournie (voir, en particulier, l'article 14(5) du RGPD). Il ne s'agit donc pas d'une raison pour rejeter automatiquement l'utilisation potentielle d'intérêts légitimes dans le cas où il y aurait des tiers impliqués ; et

53.4 C'est peut-être pour cette raison que la lettre du CEPD à l'ICANN de juillet 2018 a appuyé la possibilité d'un recours à des intérêts légitimes, même pour les données de tiers, à condition que les titulaires de noms de domaine ne soient pas *obligés* de fournir ces données de tiers, mais puissent plutôt fournir les leurs.[94] Nous comprenons que c'est effectivement le cas du système supervisé par RIPE-NCC.

54. RIPE-NCC estime probablement que les régulateurs et les tribunaux accueilleraient à première vue favorablement l'autonomie et le contrôle offerts par le recours au consentement, plutôt qu'une base juridique non consensuelle du RGPD, comme des intérêts légitimes. Toutefois, ces autorités pourraient également reconnaître les inconvénients pratiques d'une telle approche :

54.1 Le propre blog de RIPE-NCC reconnaît les doutes qui entourent parfois les consentements obtenus dans des contextes d'emploi (c'est-à-dire que de tels consentements, à la demande d'un employeur, peuvent ne pas avoir été librement donnés par un employé).

54.2 RIPE-NCC finit également par se fonder sur les déclarations de la première partie selon lesquelles elle aurait obtenu un consentement valide du tiers (« RIPE NCC considère qu'il est de la responsabilité de celui qui insère les données dans la base de données de RIPE (c.-à-d. le responsable) de s'assurer qu'elle a obtenu un consentement valide pour que le traitement ait lieu »). En théorie, cela pourrait impliquer une difficulté pour RIPE-NCC (en tant que contrôleur) de démontrer que ces consentements répondaient à toutes les exigences du RGPD.

54.3 Les parties contractantes pourraient être confrontées aux mêmes questions de RGPD en ce qui concerne les données d'enregistrement de noms de domaine.

[94] Lettre du CEPD de juillet 2018, aux pages 2 et 3.

55. Les opinions de RIPE-NCC ne reflètent pas nécessairement, comme dans le cas d'EURid, celles des autorités chargées de l'application du RGPD, et ne sont certainement pas contraignantes.

56. En outre, l'exercice d'équilibrage des intérêts légitimes qui doit être mené par RIPE-NCC est différent de celui de l'ICANN et des parties contractantes ; les données en question concernent des ressources différentes (IPv4, IPv6 et ressources de numéros AS, souvent allouées par RIPE-NCC (en blocs) à de très grandes organisations ; contrairement à l'enregistrement de noms de domaine spécifiques par des individus spécifiques pour un usage privé).

57. Il est donc difficile de tirer des conclusions générales vis-à-vis de l'approche de RIPE-NCC.

Projet de texte concernant l'accès aux données d'enregistrement dans la directive NIS2 récemment proposée

58. En décembre 2020, la Commission européenne a publié son projet de Directive révisée concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (« NIS2 »).

59. Les considérants de la directive NIS2 proposée stipulent que :

> « 15. Le fait de maintenir et préserver un système de noms de domaine (DNS) fiable, résilient et sécurisé constitue un facteur crucial pour la protection de l'intégrité d'Internet et est essentiel à son fonctionnement continu et stable, dont dépendent l'économie numérique et la société. Par conséquent, la présente directive devrait s'appliquer à tous les fournisseurs de services DNS, y compris les opérateurs de serveurs racine de noms de domaines, aux serveurs de noms de domaine de premier niveau (TLD), aux serveurs faisant autorité pour les noms de domaines et aux résolveurs récursifs.
>
> (…)
>
> (59) Le maintien à jour des bases de données précises et complètes de noms de domaines et de données d'enregistrement (appelées « données WHOIS ») ainsi que la fourniture d'un accès licite à ces données sont essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaine (DNS), lequel contribue en retour à assurer un niveau élevé commun de cybersécurité dans l'Union. Lorsque le traitement comprend des données à caractère personnel, ce traitement doit s'effectuer conformément à la législation de l'Union en matière de protection des données.
>
> (60) La disponibilité de ces données, et leur accessibilité, en temps opportun, pour les autorités publiques, y compris les autorités compétentes en vertu de la législation de l'Union ou du droit national en matière de prévention d'infractions pénales, d'enquêtes et de poursuites en la matière, les CERT (ou CSIRT) et, en ce qui concerne les données de leurs clients, pour les fournisseurs de réseaux et de services de communications électroniques et les fournisseurs de technologies et de services de cybersécurité agissant pour le compte de ces clients, sont essentielles pour prévenir et combattre l'utilisation abusive des noms de domaines, en

particulier pour prévenir, détecter et répondre aux incidents de cybersécurité. Cet accès doit être conforme à la législation de l'Union en matière de protection des données dans la mesure où il concerne des données à caractère personnel.

(61) Afin d'assurer la disponibilité de données exactes et complètes sur l'enregistrement des noms de domaine, les registres des noms de domaine de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaine pour le registre de noms de domaine de premier niveau (appelées « bureaux d'enregistrement ») doivent collecter et garantir l'intégrité et la disponibilité des données relatives à l'enregistrement des noms de domaine. En particulier, les registres de noms domaine de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaine pour le registre de noms de domaine de premier niveau devraient établir des politiques et des procédures aux fins de collecter et maintenir des données d'enregistrement exactes et complètes, ainsi que pour prévenir et corriger les données d'enregistrement inexactes, conformément aux règles de l'Union en matière de protection des données.

(62) Les registres des noms de domaine de premier niveau ainsi que les entités leur fournissant des services d'enregistrement de noms de domaine devraient rendre publiques les données relatives à l'enregistrement de noms de domaine qui ne relèvent pas du champ d'application des règles de l'Union en matière de protection des données, telles que les données concernant les personnes morales. Les registres des noms de domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaine pour le registre de noms de domaine de premier niveau devraient également permettre aux demandeurs d'accès légitimes d'accéder légalement à des données spécifiques d'enregistrement de noms de domaine concernant des personnes physiques, conformément à la législation de l'Union sur la protection des données. Les États membres devraient veiller à ce que les registres des noms de domaine de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaine répondent dans les meilleurs délais aux demandes de divulgation de données d'enregistrement de noms de domaine émanant de demandeurs d'accès légitimes. Les registres des noms de domaine de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaine devraient établir des politiques et des procédures entourant la publication et la divulgation des données d'enregistrement, y compris des accords de niveau de service régissant la gestion des demandes d'accès des demandeurs d'accès légitimes. La procédure d'accès peut également inclure l'utilisation d'une interface, d'un portail ou d'un autre outil technique afin de fournir un système efficace de demande et d'accès aux données d'enregistrement. En vue de promouvoir des pratiques harmonisées dans l'ensemble du marché intérieur, la Commission peut adopter des lignes directrices eu égard à ces procédures sans préjudice des compétences du Comité européen de la protection des données.

(…)

69. Le traitement de données à caractère personnel, dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité devrait constituer un intérêt

légitime du responsable du traitement concerné, tel que visé dans le règlement (UE) 2016/679. Cela devrait comprendre des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. Ces mesures peuvent nécessiter le traitement des types de données à caractère personnel suivants : Adresses IP, adresses universelles (URL), noms de domaines et adresses électroniques.

60. Les considérants du 59 au 62 y compris sont ensuite largement reflétés dans l'article 23 du projet de la directive NIS2.

61. Les considérants 15, 59 à 61 y compris et 69, ainsi que les articles 23 (1 à 3) de la directive NIS2 préliminaire sont largement favorables à un traitement complet et excessif des données d'enregistrement, à condition qu'il soit conforme au RGPD. La dernière phrase du considérant 61 soutient également expressément les mesures visant à promouvoir le respect du principe d'exactitude du RGPD, comme celles mentionnées dans nos notes précédentes.

62. Toutefois, le considérant 62 et les articles 23(4-5) sont plus particulièrement pertinents pour les questions en discussion dans la présente note, car ils concernent la publication/diffusion des données d'enregistrement, et pas seulement leur simple collecte et conservation. Ces dispositions de la directive NIS2 établissent une distinction claire entre les données à caractère personnel et les données à caractère non personnel et ne soutiennent expressément que la publication de données à caractère non personnel. En ce qui concerne les données à caractère personnel, la directive NIS2 s'en tient à discuter de ce qui semble être un *accès restreint* par les « demandeurs d'accès légitimes, conformément à la législation de l'Union en matière de protection des données » (et d'une formulation équivalente à l'article 23(5)).

63. À notre avis, par conséquent, la directive NIS2 préliminaire actuelle ne semble pas considérer un système dans lequel certaines données à caractère personnel pourraient être publiées (légitimement) de manière générale, par exemple avec le consentement du titulaire. Il n'est pas clair si cela correspond simplement au fait que cette option n'a pas été envisagée par les rédacteurs, *ou* parce que les rédacteurs n'ont pas considéré une telle approche comme valable et/ou conforme. Toutefois, cela signifie que la directive NIS2 préliminaire actuelle n'offre pas de soutien/réduction des risques importants pour un système fondé, par exemple, sur le consentement des titulaires de noms de domaine (mais il ne mine pas non plus une telle approche).

* * *

Réponse à la Question 4 (concernant les options de masquage des adresses de contact)

NOTE

Pour :	Société pour l'attribution des noms de domaine et des numéros sur Internet, équipe responsable de l'EPDP
De :	Ruth Boardman et Phil Bradley-Schmieg
Date :	9 avril 2021
Objet :	Question de mars 2021 concernant les options de masquage des adresses de contact

---

Contexte

64. Dans une lettre de juillet 2018 adressée à Göran Marby, le Comité européen de la protection des données (« CEPD ») a déclaré que :

> « *Les données à caractère personnel identifiant les employés individuels (ou les tiers) agissant pour le compte du titulaire du nom de domaine ne devraient pas être rendues publiques par défaut dans le contexte du WHOIS* ».

65. Dans ce contexte et en vous appuyant sur les conseils précédents que vous avez reçus à ce sujet, vous avez soulevé la question suivante.

Question posée : La note de B&B en date du 4 février 2020 concernant les informations de contact par e-mail se penchait sur deux options : (a) un « contact e-mail pseudonymisé » où la même chaîne unique serait utilisée pour plusieurs enregistrements de la personne concernée ; et (b) un « contact e-mail anonymisé » où une chaîne e-mail unique distincte serait utilisée pour chaque enregistrement. B&B a estimé que la publication de (a) ou (b) serait traitée comme la publication de données à caractère personnel sur le Web car l'objectif de la mise à disposition de cette adresse e-mail masquée est de permettre à des tiers de contacter directement la personne concernée et parce que des tiers avec des intérêts légitimes et proportionnés auraient accès aux données sous-jacentes.

Après examen, l'équipe juridique de l'EPDP a proposé que dès à présent les options (a) et (b) soient décrites de la manière suivante :

- L'expression « contact e-mail pseudonymisé » (option (a)) doit être remplacée par l'expression « **contact e-mail par titulaire de nom de domaine** », définie comme suit : « une adresse e-mail pour tous les domaines enregistrés par un titulaire de nom de domaine unique, *qui est sensée devenir des données pseudonymisées lorsqu'elles seront traitées par des utilisateurs tiers* (c'est-à-dire, des parties non contractantes) ». (La question de savoir si l'e-mail doit être

commun à tous ces enregistrements auprès de tous les bureaux d'enregistrement accrédités par l'ICANN constitue une détermination de politique à définir).

- L'expression « contact e-mail anonymisé » (option (b)) devrait être remplacée par l'expression « **contact e-mail pour chaque enregistrement** », définie comme « une adresse e-mail distincte à usage unique pour chaque nom de domaine enregistré par un même titulaire de nom de domaine, *qui est censée être des données quasi « essentiellement » anonymes lorsqu'elles seront traitées par des utilisateurs tiers* (c'est-à-dire, des parties non contractantes) ».

À des fins de discussion, veuillez supposer que dans les réponses aux questions ci-dessous les utilisateurs tiers des informations de contact e-mail pour chaque enregistrement ne peuvent pas identifier la personne concernée sans un effort disproportionné, de sorte que le risque d'identification semble en réalité négligeable.

1. En fonction de votre expérience et des précédents applicables, veuillez comparer le niveau de risque, la probabilité de mesures d'application de la loi, les amendes, les conseils, etc. associés (a) à la publication sur le Web ou (b) à la divulgation automatisée (i) d'un contact e-mail par titulaire de nom de domaine d'une part et (ii) d'un contact e-mail pour chaque enregistrement d'autre part. À cette fin, veuillez prendre en compte les points suivants :
    a. Le fait que le risque d'identification d'une personne concernée par un tiers (c'est-à-dire une partie non contractante) à travers un contact e-mail pour chaque enregistrement semble négligeable rendrait-il ces e-mails effectivement « anonymes » par rapport à ces tiers en vertu de la norme *Breyer* ?
    b. Dans la négative, quelle serait l'incidence du choix du contact e-mail (un pour chaque titulaire ou un pour chaque enregistrement) sur le résultat du test d'équilibre des intérêts légitimes prévu à l'article 6(1)(f) ? Dans quelle mesure l'utilisation d'un contact e-mail pour chaque enregistrement réduirait-elle l'impact de la publication sur les intérêts ou les droits et libertés fondamentaux de la personne concernée ?

La réponse à ces questions change-t-elle si la finalité principale de la publication d'un e-mail masqué est de soutenir la recherche et l'analyse statistiques, et non de communiquer avec la personne concernée ?

Analyse

66. Notre réponse commence par répondre à votre sous-question « *le fait que le risque d'identification d'une personne concernée par un tiers (c'est-à-dire une partie non contractante) à travers un contact e-mail pour chaque enregistrement semble négligeable rendrait-il ces e-mails effectivement « anonymes » par rapport à ces tiers en vertu de la norme Breyer ? »* pour expliquer pourquoi nous considérons que le RGPD resterait applicable dans un scénario d'un contact e-mail pour chaque enregistrement. Nous nous tournons ensuite vers les aspects plus généraux de la conformité avec le RGPD compris dans votre question.

Anonymat

67. Nous maintenons notre point de vue, exprimé dans notre note du 4 février 2020, selon lequel, avec l'une ou l'autre option (un contact e-mail par titulaire de nom de domaine ou un pour chaque enregistrement), il reste fort probable que la publication ou la divulgation automatique de telles adresses e-mail soit considérée comme le traitement de données à caractère personnel.

68. Pour que le RGPD s'applique au traitement des données électroniques (supposant que le critère de territorialité du RGPD soit respecté et que ses exclusions thématiques ne soient pas applicables), un test en deux parties est applicable :

68.1 Premièrement, il doit y avoir un traitement d'information qui se rapporte à une *personne en particulier*, compte tenu des données et du « contenu, finalité ou effet » (de leur traitement). Il s'agit / concerne le test « *Nowak* »[95].

68.2 Deuxièmement, cet individu particulier doit être « identifié ou identifiable », ce qui signifie qu'il doit exister « des moyens raisonnablement susceptibles d'être utilisés, comme le fait de se distinguer, soit par le contrôleur, soit par une autre personne, pour que la personne physique puisse être identifiée directement ou indirectement ».[96] Le terme « identification » ne signifie pas nécessairement trouver le vrai nom d'une personne ; il a plutôt une signification plus générale, qui porte sur la capacité de « distinguer » spécifiquement une personne pour un traitement différent (distinction),[97] et/ou être en mesure de recueillir/connecter plus de données à leur sujet (inférence et/ou association).[98] Un identificateur technique (même généré de manière aléatoire) peut suffire à de telles fins, en particulier s'il est lié à d'autres informations sur la personne, ce qui permet de les distinguer plus facilement d'une autre personne.[99] Il n'existe aucun « moyen raisonnablement probable » de réidentification si une telle activité est « interdite par la loi ou pratiquement impossible du fait qu'elle requiert un effort disproportionné en termes de temps, de coût et de main-d'œuvre, de sorte que le risque d'identification semble en réalité insignifiant »[100]. Il s'agit du test « *Breyer* » / « possibilité d'identifier ».

---

[95] Arrêt de la CJUE dans l'affaire C-434/16 *Nowak,* ECLI:EU:C:2017:994, au paragraphe 35.
[96] Considérant 26 du RGPD.
[97] Comme mentionné ci-dessus, le considérant 26 du RGPD fait spécifiquement référence à la « distinction » lorsqu'il s'agit de discuter de moyens raisonnablement susceptibles d'être utilisés pour identifier la personne concernée.
[98] La distinction, l'association et l'inférence sont trois parties du test d'anonymisation proposé par le Groupe de travail Article 29 dans son Avis 05/2014 sur les techniques d'anonymisation (« WP 216 »), disponible en ligne à l'adresse https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[99] Sur ce point, voir le considérant 30 du RGPD (« Les personnes physiques peuvent se voir associer, par les dispositifs, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes »).
[100] Arrêt de la CJUE dans l'affaire C-582/14 *Breyer,* ECLI:EU:C:2016:779, aux paragraphes 45 et 46.

69. Notre point de vue, exprimé ci-dessus, est que le traitement de ces alias d'e-mail serait toujours probablement considéré comme répondant aux deux tests, dans la mesure où la finalité du traitement est de fournir un moyen pour contacter les personnes concernées.

Test *Nowak*

70. En ce qui concerne le *test Nowak* : lorsqu'un contact est une personne physique, ces adresses seront des alias masqués correspondant à une vraie adresse e-mail utilisée par cette personne. À la lumière de cela :

70.1 Lorsque la finalité / l'effet prévu du traitement de ces données est de permettre la correspondance avec le destinataire (c'est-à-dire, souvent avec un personne concernée spécifique), compte tenu du critère de la Cour de justice de l'UE (« CJUE ») dans l'affaire *Nowak*, cette « finalité » et/ou cet « effet » signifie qu'il existe un lien avec une *personne physique en particulier*.[101]

70.2 En revanche, le traitement purement statistique visant à créer *des mesures globales* (décrivant des cohortes relativement importantes), par exemple, le nombre de ces alias de contact créés peut sans doute *ne pas* être soumis au RGPD. En effet, étant donné que le *contenu* d'un alias de contact généré de manière aléatoire ne permet pas d'en faire le lien spécifiquement avec une personne spécifique, du moins dans le cas d'un contact e-mail pour chaque enregistrement ; et (encore une fois, sans doute) ni la *finalité* ni l'*effet* de la création de résultats globaux de recherche statistique ne sont liés à un *individu en particulier* ; au contraire, les statistiques globales décrivent et différencient les *cohortes/groupes* (par exemple, par nation, par opérateur de registre, par bureau d'enregistrement, etc.). Le *test de Nowak* peut ne pas être satisfait à l'égard de cette classe de traitement (mais notez qu'il faut le distinguer des statistiques visant à générer de nouvelles informations sur, ou la classification de toute personne concernée spécifique (par exemple, le nombre de noms de domaine associés à un contact e-mail par titulaire de nom de domaine pour un titulaire donné).

70.3 Cependant, dans la pratique, nous ne pensons pas qu'il serait raisonnablement possible de dire que la seule finalité de créer et de publier les alias de contact est le traitement statistique global que nous venons de décrire. Dans ce cas, il ne serait point nécessaire de fournir une adresse e-mail. Le fait qu'une adresse e-mail soit fournie suggère qu'une finalité importante pour la création et la publication d'alias de contact sera toujours de fournir un moyen pour contacter des personnes spécifiques. Par conséquent, bien qu'un *certain degré* de traitement (pour les statistiques globales) puisse être hors de la portée du RGPD selon *le test Nowak*, il semble probable que le RGPD aille continuer à poser de préoccupations au niveau de la conformité à tout le moins en ce qui a trait à *l'autre* but du traitement.

[101] Dans certains cas, une adresse de contact du destinataire peut être une boîte de réception partagée (par exemple enquiries@example.com), auquel cas l'adresse de contact masquée ne représente sans doute *pas* des données à caractère personnel, que ce soit par l'application des *tests Nowak* ou *Breyer*.

70.4 Nous devrions également faire preuve de prudence contre toute dépendance excessive à l'égard *des arguments basés sur Nowak*. Malgré le fait que la décision se fait l'écho des premières directives du Groupe de travail Article 29,[102] que nous sachions le *test Nowak* n'est pas appliqué systématiquement dans les analyses et les directives des tribunaux et des autorités de surveillance qui appliquent le RGPD. Par exemple, au début du mois d'avril 2021, une recherche sur le site Internet de l'autorité belge de protection des données, dans toutes les langues disponibles, a trouvé que (i) seulement deux références directes à l'*affaire Nowak*, et uniquement sur des points sans rapport entre eux ; et (ii) il semble ne pas y avoir de citations de la phrase clé « contenu, finalité ou effet » tirées de *Nowak*. L'explication de cette autorité (dans son Lexique) du terme « données à caractère personnel » se concentre exclusivement sur le *test Breyer* (c'est-à-dire, la possibilité d'identifier une personne concernée).[103] D'autres autorités peuvent adopter un point de vue différent (par exemple, l'autorité britannique discute du « contenu, finalité ou effet » du test et en résume l'impact comme suit : « les informations doivent être « liées » à la personne susceptible d'être identifiée pour être considérées des données à caractère personnel. Cela signifie que les données ne se limitent pas à l'identification : elles doivent concerner la personne physique d'une manière ou d'une autre. (…) Les données peuvent faire référence à une personne susceptible d'être identifiée sans être des données à caractère personnel de cet individu, car elles ne sont pas liées à cette personne »).[104]

70.5 En outre, les autorités en la matière non seulement ne mettent pas toujours l'accent sur *Nowak*, mais *si* elles le faisaient, elles pourraient aussi adopter des approches très différentes de son interprétation. En particulier, la partie « contenu » du test de « contenu, finalité ou effet » pourrait susciter des divergences d'opinions. Le Groupe de travail Article 29, dans son *Avis 4/2007 sur la notion des données à caractère personnel* (WP 136)[105] a expliqué que « [l]'élément « contenu » est présent dans les cas où (suivant l'interprétation la plus évidente et habituelle du mot « relier ») des informations sont fournies à propos d'une personne particulière, quelle que soit la finalité de l'autorité de contrôle ou d'un tiers et, quel que soit l'impact de ces informations sur la personne concernée ». Si cette explication est correcte, un tribunal ou un organisme de réglementation pourrait alors conclure que la publication d'une adresse e-mail (même générée de manière aléatoire) pour un contact associé à l'enregistrement d'un nom de domaine est *intrinsèquement* une publication d'informations « à propos de » cette personne, car elle nous indique comment la contacter. Toutefois, il s'agit d'un point de vue problématique, car il « emprunte » le raisonnement des *tests de finalité* et *d'effet* (il examine une finalité possible du partage de l'information, *et non* le contenu de l'information elle-même), et se fonde sur une finalité/effet *hypothétique*, et non sur la finalité/effet *concret* du

[102] WP 136, à la page 10.
[103] https://www.autoriteprotectiondonnees.be/citoyen/vie-privee/lexique
[104] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/#pd5
[105] Groupe de travail Article 29, *Avis 4/2007 sur la notion de données à caractère personnel* (WP 136), à la page 10. Disponible en ligne à l'adresse https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

traitement, ce qui court-circuite ainsi complètement les deux tiers du test de « contenu, finalité ou effet ». Du point de vue de la logique et de la primauté du droit (clarté/certitude), cela pose problème. D'un point de vue plus simple, quelque chose générée de manière aléatoire (as876bnk@example.com) est une expression pure de « bruit » aléatoire, un instantané de l'état électrique du circuit du « générateur de numéros aléatoires » d'un ordinateur. Elle ne contient donc pas et ne peut en soi « *contenir* » aucune information sur une personne. Si elle *communiquait* en soi des informations sur une personne, elle ne serait logiquement pas aléatoire. De ce point de vue, une adresse générée de manière aléatoire ne passe ainsi pas le test du « contenu » ; il faudrait plutôt se concentrer sur la finalité et/ou l'effet du traitement des données.

70.6 Par conséquent, il est clair qu'il existe un risque considérable de désaccord avec certaines autorités si les arguments reposent sur l'*affaire Nowak*.

Test de *Breyer*

71. En ce qui concerne le test de *Breyer* : dans ce cas, la CJEU a mené un exercice de réflexion, à savoir qu'en cas de cyberattaque, une autorité qui contrôle une adresse IP (et, bien que le tribunal ne soit pas explicite sur ce point, nous supposons que l'autorité aurait un horodateur indiquant quand cette adresse IP était utilisée par un dispositif/une personne d'intérêt) pourrait communiquer ces informations aux autorités policières/judiciaires. La CJUE prévoyait que les autorités seraient alors souvent habilitées à demander des informations correspondantes au fournisseur d'accès à Internet qui a attribué cette adresse IP, et donc à engager des poursuites (bien que la CJUE ait demandé aux tribunaux nationaux de référence de vérifier cette hypothèse). La CJUE a alors considéré que, à moins que ce scénario ne soit interdit par la loi ou pratiquement impossible, il existait des « moyens raisonnablement probables » pour identifier une personne concernée.

72. Le point clé ici est que, bien qu'un tiers puisse uniquement connaître le contact e-mail par titulaire de nom de domaine ou pour un enregistrement, les autorités compétentes pourraient établir une corrélation avec les données d'enregistrement non publiques détenues par les parties contractantes, ce qui permettrait une réidentification. Pour autant que nous le savons, cela n'exigerait pas toujours des niveaux d'effort « pratiquement impossibles » ni ne serait universellement interdit par la loi.

73. Ainsi, même du point de vue *des tiers*, la distribution et l'utilisation de ces alias de contact pourraient être traitées comme un traitement de données à caractère personnel.

74. Du point de vue *d'une partie contractante* qui sait quel alias de contact elle a attribué à un titulaire de nom de domaine ou à son contact désigné, la création et l'hébergement de telles adresses, et leur mise à disposition pour utilisation par d'autres, est presque certainement un traitement de données à caractère personnel (lorsque les personnes de contact sont des personnes physiques).

Risque des différentes options présentées

75. Ayant expliqué notre point de vue que le RGPD demeure pertinent pour l'une ou l'autre option, nous passons maintenant à votre demande de comparaison des risques associés à (a) la publication sur le Web ou (b) la divulgation automatisée (i) d'un contact e-mail par titulaire de nom de domaine d'une part et (ii) d'un contact e-mail pour chaque enregistrement d'autre part.

76. Notre résumé (qui reflète les hypothèses et les mises en garde importantes fournies plus loin dans cette réponse) est le suivant :

	Un contact e-mail par titulaire de nom de domaine	**Un contact e-mail pour chaque enregistrement**
Publication Web	Moyen	Faible
Divulgation automatisée	Faible	Le plus faible

77. Selon l'application des principes du RGPD, le partage (soit par le biais de la publication Web, soit de la divulgation automatisée) des alias des adresses e-mail pour chaque enregistrement implique un risque moindre aux alias des adresses e-mail pour chaque enregistrement.

78. Cela correspond au fait qu'une personne possédant une adresse e-mail par titulaire de nom de domaine pourrait être en mesure d'en savoir plus sur la personne concernée, en particulier quant aux autres noms de domaine auxquels cette dernière est associée. La raison pour cela est que, à moins qu'une adresse de contact réelle différente n'ait été fournie par cette personne concernée pour chaque nom de domaine qu'elle a enregistré, chaque enregistrement aurait le même alias d'adresse e-mail.

79. La publication Web de ces détails pourrait faciliter relativement la création de tels profils, voire éventuellement créer un outil de recherche inverse (« pour le contact e-mail d'un enregistrement donné, quels sont les noms de domaine y associés ? »).

80. La divulgation automatique, à elle seule, compliquerait probablement cette tâche, car à moins que les outils de divulgation automatique *ne fournissent spécifiquement* une fonctionnalité de recherche inverse, [106] les demandeurs auraient probablement besoin d'interroger des nombres de noms de domaine potentiellement assez grands afin de recueillir suffisamment d'informations pour pouvoir établir des correspondances et commencer à développer une fonction de recherche inverse (incomplète). Cela dit, les demandeurs qui ont une liste

[106] Avant d'être déployées, de telles caractéristiques exigeraient un examen attentif. Pour des directives plus anciennes à ce sujet, voir l'Avis 5/2000 du Groupe de travail Article 29 relatif à l'utilisation des services de recherche des répertoires publics pour des recherches inverses ou multicritères (répertoires inversés) (« WP 33 »), disponible en ligne à l'adresse https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf

préétablie de noms de domaine spécifiques (par exemple, les versions « miroir » présumées d'un site Web hébergeant des contenus illégaux) pourraient déterminer si la même adresse e-mail a été fournie pour certains de ces sites ou pour tous. Ainsi, même dans un scénario de divulgation automatique, l'utilisation d'un système de contact par e-mail avec une adresse par titulaire de nom de domaine comporte des risques supplémentaires pour la vie privée, à comparaison du système de contact par e-mail ayant une adresse pour chaque enregistrement.

81. En conséquence, compte tenu des considérations suivantes :

81.1 La nécessité de se conformer à la règle de minimisation de données du RGPD ;

81.2 La nécessité de se conformer à une règle de « respect de la vie privée dès la conception et par défaut » ;

81.3 Le fait que le recours à l'article 6(1)(f) du RGPD (la base juridique des intérêts légitimes) soit plus robuste lorsque la conception du système minimise le préjudice aux « intérêts ou droits et libertés fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel » ; et

81.4 Que, pour déterminer si et dans quelle mesure des amendes devraient être appliquées à un contrôleur, les autorités doivent prendre en considération, *entre autres,* la « gravité » d'une infraction, la « portée » du traitement, le « niveau de dommage subi par » les personnes concernées, « toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées » et « le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 » (voir l'article 83 du RGPD),

Par conséquent, nous considérons qu'un système de contact par e-mail avec une adresse pour chaque enregistrement revêt un risque moindre à celui d'un système de contact par e-mail avec une adresse par titulaire de nom de domaine.

82. Après avoir expliqué l'équilibre des risques selon l'axe « système de contact par enregistrement vs. par titulaire de nom de domaine », nous nous tournons maintenant vers les risques contrastés pour la publication sur le Web par rapport à la divulgation automatisée.

83. Le spam ou d'autres e-mails non sollicités représentent un risque commun à un système de contact par e-mail avec une adresse pour chaque enregistrement et un système de contact par e-mail avec une adresse par titulaire de nom de domaine ; cette « adressabilité » est, sans doute, un aspect de la vie privée.[107] Le spam est une préoccupation de longue date des systèmes WHOIS ; elle a fait l'objet d'une étude du Comité consultatif sur la sécurité et la stabilité de l'ICANN en 2007, qui

[107] Le considérant 40 de la directive 2002/58/ce (la « directive vie privée et communications électroniques » de l'UE) stipule : « Des garanties devraient être prévues pour protéger les abonnés contre toute violation de leur vie privée par des communications non sollicitées effectuées à des fins de marketing direct, en particulier au moyen d'automates d'appel, de télécopies et de courriers électroniques, y compris les messages SMS ».

a conclu que « l'apparition d'adresses e-mail en réponse à des requêtes WHOIS contribue en effet à la réception de spam, bien qu'il ne s'agisse que d'un seul parmi plusieurs ».[108]

84. Par conséquent, que le système employé utilise un contact e-mail pour chaque enregistrement ou un par titulaire de nom de domaine, des mesures efficaces devraient être prises pour traiter la disponibilité d'adresses aux spammeurs (par exemple, utiliser des fonctions techniques pour empêcher la « collecte » de telles adresses ; et/ou le filtrage des communications inappropriées avant qu'elles ne soient livrées au destinataire prévu).

85. Par rapport à la publication sur le Web, nous présumons que la divulgation automatisée permet d'évaluer les motifs d'une demande, les sources de cette demande, et de surveiller / vérifier et appliquer des mesures de protection (par exemple, limitant les taux) sur de telles demandes ; c'est-à-dire une plus grande marge pour déployer les types d'atténuations qui réduiront la responsabilité en fonction des facteurs énoncés au paragraphe 81 ci-dessus. Il semblerait donc que, sur ce front, la divulgation automatisée présente intrinsèquement moins de risques sur ce plan que la publication sur le Web.

86. Ces avantages potentiels de la divulgation automatisée par rapport à la publication sur le Web présentent également, en théorie, des avantages en vertu de l'article 25 du RGPD (respect de la vie privée dès la conception et par défaut). En particulier, il faudrait réfléchir à ce que la publication sur le Web soit conçue de manière à ce qu'elle soit conforme à l'article 25(2) du RGPD, « ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».[109]

87. Cela dit, si des mesures efficaces contre le spam sont utilisées, et si une approche de contact par e-mail pour chaque enregistrement est adoptée (en raison de ses avantages discutés précédemment), puis, étant donné la faible utilité des données qui en résulte, il est difficile de voir comment leur publication sur le Web présenterait des risques significatifs pour la confidentialité ou la sécurité des données.

* * *

[108] *SAC 023 : Le service WHOIS est-il une source d'adresses e-mail pour les spammeurs ?* Résumé analytique. Disponible en ligne à l'adresse https://www.icann.org/en/system/files/files/sac-023-en.pdf

[109] Dans *ses Directives 4/2019 sur l'article 25 Protection des données dès la conception et protection des données par défaut, v2.0*, au paragraphe 56, le CEPD explique que cela signifie que « [l]e contrôleur doit limiter par défaut l'accessibilité et donner à la personne concernée la possibilité d'intervenir avant de publier ou de mettre à disposition des données à caractère personnel sur la personne concernée à un nombre indéfini de personnes physiques ». Disponible en ligne à l'adresse https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf