

BARCELONE – Séances intercommunautaires : RGPD
Mercredi 24 octobre 2018 – 09h45 à 12h00 CEST
ICANN63 | Barcelone, Espagne

BRUCE TONKIN: Bonjour. Puis-je demander aux membres du panel de bien vouloir prendre place autour de la salle, nous sommes prêts pour commencer.

Greg, Milton, Chris, s'il vous plait.

Bien, nous allons commencer pour utiliser le temps qui nous est imparti ce matin.

Je m'appelle Bruce Tonkin. On m'a demandé de présider cette séance intercommunautaire sur le RGDP.

L'idée d'une séance intercommunautaire, c'est de réunir la communauté pour essayer de voir comment la communauté dans son ensemble peut se concentrer sur d'importants problèmes et essayer de les résoudre.

Donc lors de cette séance intercommunautaire, nous avons des représentants de plusieurs parties de l'organisation ICANN. Nous avons des représentants de la GNSO chargés des politiques concernant les noms de domaine GTLD. De la part de la chambre des parties contractantes, nous avons Nick Wenban-Smith. Il est le conseiller général de Nominet, chargé des extensions géographiques,

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

dans ce cas là .UK, ainsi que les domaines de premier niveau tels que .BLOG.

Également, Flip Petillion – j’ai bien prononcé votre nom ? Oui – qui vient d’une entreprise en Belgique, qui offre des services d’arbitrage. Donc il résout des litiges liés aux noms de domaine.

Du groupe des parties prenantes non commerciales, nous avons le professeur Milton Mueller qui nous vient de Georgia.

Et du SSAC nous avons Greg Aaron. Greg est vice-président du groupe cybernétique chargé des attaques en ligne. Et il est expert dans les utilisations malveillantes en ligne.

Nous avons Hadia Elminiawi de l’ALAC. Hadia est directrice du centre d’entrepreneuriat DNS en Égypte.

Du GAC, nous avons Hashley Heineman, elle est responsable de la politique de l’internet à l’intérieur de la NTIA aux États-Unis. Et lorsqu’elle se penche sur des problématiques qui touchent à plusieurs gouvernements, tels que tous les gouvernements représentés au GAC, et au niveau international, son point de vu est intéressant.

Nous avons également un représentant des autorités chargées de l’application. À savoir Chris Lewis-Evans. Chris travaille dans l’agence d’investigation criminelle au Royaume-Uni.

Et du côté de la protection des données, nous avons Cristina Monti. Cristina travaille à l’unité pour la protection des données et flux des

données au sein de la direction de la commission de l'Union Européenne pour la justice.

Donc nous avons tous, depuis de nombreuses années, travaillé sur la protection des données à caractère personnel.

Il m'a semblé intéressant de vous présenter un petit peu le contexte, en revenant au RFC-1591, qui date de mars 1994, et a été élaboré par John Postal. Puisque ça coïncide au 20^{ième} anniversaire de la mort de John Postal en 1998. Et c'est un document qui date d'il y a plus de 20 ans mais qui, à l'époque déjà disait que les gestionnaires de TLD sont dépositaires de la confiance de la délégation des noms et ils sont au service de la communauté. Il disait aussi que les préoccupations par rapport aux droits et aux titulaires de ces noms doivent se montrer responsables et être au service de la communauté.

Donc les titulaires de noms de domaine ont une responsabilité vis-à-vis de la loi, de la juridiction locale. Certains de ces titulaires de noms sont des personnes physiques. Dans le contexte des titulaires de noms de domaine, il s'agit en général de personnes physiques.

Et il peut aussi se passer que les données personnelles de ces personnes physiques sont protégées au titre des législations nationales et de par le monde.

L'ICANN a une mission, à savoir allouer les noms dans la zone racine. Donc gestion de la distribution des noms dans la zone racine du DNS, donc pour les noms de premier niveau. Et les noms de domaine pour les nouveaux gTLD.

L'ICANN ne doit pas réglementer des services qui utilisent des identifiants de l'internet, ou le contenu. Ça, c'est ce que l'ICANN ne fait pas. En général c'est les autorités chargées de l'application de la loi qui doivent le faire, qui doivent entreprendre des actions en cas d'infraction.

Il y a des organisations telles que des organisations de cyber-sécurité qui collectent des données, qui recensent les incidents, infractions et mènent les enquêtes pertinentes.

Il est également intéressant de penser à la dérivation de WHOIS. On va parler de la prochaine génération d'informations que nous fournissons dans les registres.

Et je vais vous lire le RFC original.

Il s'agissait d'un registre qui demandait le nom, l'adresse, le numéro de téléphone, l'adresse mail et également un courrier postal. Et à mesure que ça a évolué, c'est devenu un contexte pour les informations administratives pour les noms de domaines pour les grandes institutions connues de par le monde. Et dans ce cas-là il était très clair de quelle était l'entité légale qui était tenue pour responsable. Donc il n'était pas facile qui, dans une grande entreprise, avec des centaines de personnes était légalement responsable.

Donc maintenant il s'agit de registres gérés par des individus et des traders.

Mais il faut encore pouvoir identifier l'identité juridique de la personne responsable, et il faut pouvoir contacter le titulaire du registre en cas

de problèmes. Et c'est souvent le nom du titulaire du registre qui est la victime en cas d'incidents ou de délits.

Très souvent leur adresse, leur mail est piraté, et on s'aperçoit que cette personne a besoin d'aide pour résoudre ce problème, parce que ce titulaire de nom n'est pas forcément celui qui a commis le délit, mais son identité a été piratée.

Il est important également de penser à ce qu'il se passe du côté des registres publics, qui ont probablement des caractéristiques similaires aux autres registres. Beaucoup de pays ont des lois qui stipulent que ceux qui font affaire avec des registres, registres commerciaux, enregistrent leur entreprise et que les informations qui sont collectées dans le cadre du processus incluent les données personnelles, le nom, l'adresse, le numéro de téléphone des personnes physiques qui sont les directeurs de cette entreprise.

Autre exemple, l'enregistrement en cas d'achat de véhicule, dire de quelle marque il s'agit, quel modèle, etc., et également des données personnelles par rapport aux propriétaires du véhicule. Que ce soit une personne individuelle ou son entreprise.

Et on peut faire des analogies similaires avec l'ICANN. Si vous pensez à un organe d'enregistrement de véhicule, qui identifie un identifiant unique, c'est un petit peu l'étiquette qui figure l'identifiant d'un véhicule. Certaines personnes veulent avoir une plaque d'immatriculation personnalisée dans certains pays. Mais si quelqu'un veut être contacté, il peut faire de la pub aussi, en mettant des petites

affiches sur la voiture. Mais en aucun cas un nom personnel ou des données personnelles.

Mais en général, avec votre permis de conduire, vous pouvez conduire votre voiture comme bon vous semble, vous pouvez mettre ce que vous voulez sur votre voiture, dans votre voiture. Mais les agences qui sont responsables de la délivrance des plaques d'immatriculation ne s'en soucient pas. Tout ce qu'ils veulent c'est pouvoir identifier la personne qui est propriétaire de ce véhicule.

Donc si vous avez une voiture garée et quelqu'un s'aperçoit que cette voiture est pleine de drogue, alors la police va faire une enquête et va s'adresser à l'autorité chargée de l'enregistrement de la voiture pour voir qui est le propriétaire de la voiture.

Si vous êtes impliqué dans un accident de voiture, et quelqu'un prend votre voiture, a un accident et s'enfuit, on retrouve la plaque d'immatriculation, et cette plaque d'immatriculation est publique. Dans certains pays comme au Royaume-Uni, vous pouvez entrer la plaque d'immatriculation pour retrouver des informations sur la voiture. On va vous dire quel est le modèle de la voiture, quelle année, mais pas qui est le propriétaire de la voiture. Mais ça, ça vous permet d'être sûr qu'il s'agit de la bonne voiture. Parce que peut-être que vous vous souviendrez vaguement de la plaque d'immatriculation, plus des derniers chiffres, donc vous devez vous assurer que vous avez le bon véhicule. Une fois que vous en êtes sûr, vous allez voir la police en disant : voilà, on a utilisé ma voiture et la voiture a eu un accident.

Et on va chercher des informations sur la personne physique qui est propriétaire de cette voiture.

Donc il y a beaucoup d'analogies avec notre situation à nous. L'ICANN ne s'occupe pas de ce qu'il y a sur les emails, sur les sites web. La seule chose dont l'ICANN s'occupe, c'est les informations collectées par rapport aux parties qui détiennent les noms de domaine, qu'on puisse contacter ces parties, et ensuite, c'est aux autres de prendre des mesures en cas de délit.

Vis-à-vis des opérateurs ou des registres de numéros de téléphone, c'est un peu la même chose. Les registres d'extension géographiques fonctionnent un petit peu comme les gTLD. Le système veut qu'elles opèrent dans une seule juridiction. Et la plupart des extensions géographiques ont actualisé les annuaires de services pour être en conformité avec le RGPD.

Mais il faut encore trouver une solution qui fonctionne au niveau international et pas dans un seul pays.

On va regarder un exemple de Nominet, pour vous donner un exemple de la situation. En diffusant un niveau minimal d'informations au public, dans le WHOIS public, avec un accès authentifié pour les agences chargées de l'application de la loi, et ensuite, ils ont un formulaire sur leur site web où un utilisateur légitime peut demander à avoir accès à l'information. Mais il faut déclarer dans quels buts ils veulent le faire.

Et il faut nommer individuellement une personne chargée de chaque cas, en fonction de qui demande ce type d'information et quel en est le motif. Est-ce que c'est un motif juridique ? Juridiquement viable ou pas ? Légitime disons.

Donc c'est ainsi que ça fonctionne au Royaume-Uni et en général en Europe.

La plupart des opérateurs de registre ont des informations sur les entreprises de télécommunications, fournisseurs de services internet, avec toutes les données concernant les adresses IP. Donc dans ces organisations, ils ont tout ce genre de contexte.

Mais, en Europe, il faut avoir une solution qui soit conforme au RGPD.

Donc, il y a toute une série de codes qui fonctionnent, qui doivent être conformes aux législations en vigueur concernant la protection des données à caractère personnel. Et elles ont été actualisées afin d'avoir accès à des systèmes d'informations échelonné.

Il faut aller physiquement à la police, voir des microfiches, et vous allez passer des heures pour trouver une seule information. Maintenant, depuis ici à Barcelone, je peux avoir accès à ces archives du registre britannique.

Si on revient il y a des centaines d'années en arrière, il fallait aller dans les registres, les archives, à l'Église, retrouver la date de naissance, de mort, de mariage de la personne en question, et maintenant tout cela est archivé de manière numérique.

Donc ça, ça a été actualisé, ça a évolué en Europe. Je sais que dans les années 1950, après la Deuxième Guerre mondiale, il y a eu des préoccupations, beaucoup de mauvaises utilisations, puisqu'il y a eu des identités qui ont été dévoilées, et ça, ça enfreignait les droits de l'homme fondamentaux. Et donc il y a eu une convention pour éviter le traitement des données à caractère personnel.

Donc dans les années 80 l'Europe a adopté une convention qui a donné lieu, en 1990 à une directive.

Mais là, le défi pour les entreprises c'est qu'il faut voir la manière dont les législations sont appliquées dans chaque pays individuel de l'Europe. Et ça, ça représente un coût.

Donc ces règlements, qui sont apparus en 2016 nous ont fourni une approche uniforme pour tous les pays. Donc encore une fois, ces mises en application pourraient s'appliquer à tous les pays en Europe.

Donc c'est une standardisation de ces systèmes, et vis-à-vis de la vie privée.

Donc en 2016, ces lois sont arrivées, mais nous avons déjà des lois qui étaient liées à la confidentialité depuis des années.

Donc le défi pour l'ICANN, c'est que l'on a besoin d'une définition claire des motifs pour lesquels nous allons recueillir des données.

Donc il est important de distinguer les motifs de recueillement des données pour les opérateurs de registre publics. Et donc, ça représente un service à la communauté donc cette collecte, ce

recueillement de data, de données, pour les entreprises et pour les bureaux d'enregistrement qui recueillent ces informations à des fins commerciales.

Ce qu'on peut dire au niveau de l'ICANN, c'est que cette collecte d'information va faire part d'un registre public, et donc va faire part de dossiers, d'archives publiques.

Donc nous devons décider de ce qui va être recueilli et de ce qui va être diffusé donc vis-à-vis du public, et comment est-ce que ces informations vont être accessibles.

Qu'est-ce qui va correspondre à une utilisation légitime ? Et qu'est-ce qui va être illégitime ?

Nous avons des données à travers le globe sur des personnes physiques, et dans tous les pays d'ailleurs. Nous avons des utilisateurs dans beaucoup de pays, et nous avons donc des lois qui s'appliquent à toutes ces personnes physiques. Et ces lois sont souvent différentes quand il s'agit d'organisations ou d'entreprises.

Donc c'est très difficile de résoudre ce problème à partir de chaque région ou pays.

Donc voilà les principes sont dans le RGPD, ces principes sont communs par rapport à beaucoup de lois qui ont à voir avec la protection et la confidentialité. Donc on doit fournir des raisons pour lesquelles les données sont recueillies, quels sont les processus, comment se passent la publication de ces données par rapport à telle ou telle partie.

Donc on doit pouvoir collecter, recueillir des données pour certaines raisons. Donc il y a une limite qui doit être nécessaire. Et c'est pour ça que vous entendez des discussions diverses sur ce sujet. ;

Si un bureau d'enregistrement collecte des données pour fournir un service d'email, ce bureau n'a pas besoin d'adresse physique, puisque tout est livré d'une façon numérique. Donc si vous demandez à un bureau d'enregistrement, il va vous dire : tout ce qu'on a à faire, c'est de récupérer le numéro de carte de crédit, c'est tout ce qu'on a besoin. Pour un objectif public, vous allez peut-être demander plus d'informations. Et donc il faut savoir quelles informations doivent être recueillies.

Les données doivent être mises à jour. Les bureaux d'enregistrement doivent rappeler au titulaire de nom de domaine de mettre à jour les données dans le WHOIS. Il faut donc encore une fois s'assurer que ces données soient mises à jour, comme ça, les consommateurs peuvent se renseigner et obtenir les bonnes données. Donc, c'est ainsi qu'il faut que tout soit correct.

Dans des situations régulières, quand le consommateur commence à payer, donc avec une carte de crédit, ces chiffres ne vont pas être enregistrés. Donc si les bureaux d'enregistrement, les opérateurs de registres font face à des problèmes d'impôts ou des problèmes légaux, etc. puisque dans certains pays on exige des informations spécifiques, et ces informations devraient être conservées pendant un certain nombre d'années. Donc il faut savoir combien de temps ces données

pourront être conservées. Durant l'enregistrement, et après l'enregistrement.

Donc l'intégrité, la confidentialité, s'est pour s'assurer que toutes ces données soient sécurisées.

J'ai entendu souvent des idées dans ces panels, dans les différents panels au sujet des exigences. Et cela a été dit plusieurs fois. Et donc je vais demander aux membres du panel de résumer un peu ce qu'ils ont entendu.

Donc j'assume cette semaine, d'après ce que nous avons entendu, il nous faut des processus de développement de politique de réserves si vous voulez. Parce que souvent les choses fonctionnent très lentement. Nous devons donc à l'ICANN avoir les ressources et pouvoir contribuer à ces PDP.

Nous allons pouvoir ainsi développer des politiques de façon réussie.

Donc le RGPD doit appliquer donc les lois de confidentialité. Et il faut donc qu'il y ait des solutions pour que les forces de l'ordre puissent continuer à faire leurs enquêtes. Il faut donc fournir les informations sur les personnes qui sont à risque.

Il y a souvent des anecdotes telles que, bon il y a des couples qui se séparent, il y a des problèmes de violence, il y a des gens qui partent d'un pays à l'autre, donc il faut pouvoir absolument... Il y a des gens qui se séparent, donc encore une fois des gens qui partent dans un autre pays pour s'évader de cette violence, il faut pouvoir avoir ces données et les protéger.

Nous avons entendu beaucoup parler, la communauté technique qui pense que le RDAP est suffisant pour ces motifs, mais beaucoup de discussions ont été envisagées. C'est le langage que nous allons pouvoir utiliser pour échanger les informations.

Il y a des éléments, des caractéristiques qui sont importantes. Ces caractéristiques peuvent soutenir le concept pour la distribution des données, les informations, au lieu de les centraliser.

Donc il y a des tas de manières de procéder pour la mise en application.

Cela a été donc développé pour que les opérateurs de registre et les bureaux d'enregistrement communiquent. Il doit y avoir tout de même des politiques et pouvoir les mettre en œuvre.

On assume aussi que les opérateurs et les bureaux sont responsables. Ils recueillent les informations pour des motifs complètement différents. Ils sont responsables du processus. Ils doivent prendre leur responsabilité.

Donc la question qui va se poser au panel, en premier, c'est qu'il faut considérer l'historique des registres publics qui ont des problèmes pour protéger ces datas. Et il faut parler du concept de légitimité d'accès de ces datas qui ne sont pas disponibles pour le public en général.

Il faut essayer de comprendre le contexte des lois qui ont à voir avec la confidentialité.

Notre défi, c'est de trouver une solution opportune.

Donc la première question est celle-ci : quels sont les problèmes que l'on voit au niveau de l'ICANN, après cette semaine de discussion sur cette thématique, quelles sont donc les barrières, les obstacles qui nous empêcheraient de trouver une solution ? Que peut-on faire pour dépasser ces obstacles ?

Il y a beaucoup de personnes dans cette salle, il y a une centaine de personnes. Comment pouvez-vous aider ou aider les personnes qui font partie de différents groupes pour qu'ils trouvent une solution utile ?

Donc je vais demander aux personnes qui sont au panel de me faire part de leur opinion, pour donc dépasser ces obstacles.

ASHLEY HEINEMAN:

Je commence à un haut niveau.

Je ne vais pas rentrer dans tous les détails de notre discussion, mais beaucoup des obstacles auxquels j'ai fait face durant l'année passée sont ceux-ci.

Donc les gens viennent à la table avec des idées préconçues. Ils savent ce que les autres font, quelles sont leurs motivations, etc. Mais ce que j'ai appris, c'est que lorsqu'on se rassemble avec des personnes qui représentent des différents intérêts et perspectives, et qu'on commence à parler de ces questions, on se rend compte qu'on a des points de vue plus ou moins similaires.

Mais on a besoin d'avoir plus de possibilités de pouvoir dialoguer et de travailler ensemble pour un but commun. Et nous devons déclarer nos positions et essayer de travailler sur des points communs.

Je suis optimiste, je pense qu'on peut dépasser cela. J'ai vu qu'il y avait de bons résultats. Mais c'est vraiment une question à long terme, qui est très lourde.

Nous devons donc travailler ensemble de façon constructive.

BRUCE TONKIN:

Je pense que le défi, c'est que les gens questionnent votre motivation.

En réalité, les opinions de la plupart des gens sont assez équilibrées lorsqu'ils parlent en privé. Mais des fois ils viennent à ces forums publics et ils offrent des opinions complètement extrêmes.

Au lieu de rentrer dans une conversation avec quelqu'un d'un autre groupe et lui dire voilà, c'est ma position et j'ai raison, il vaudrait mieux leur poser plus de questions en leur demandant ce qu'ils veulent faire, ce qu'ils pourraient faire. Et peut-être qu'on pourrait trouver des points communs.

Donc il faudrait qu'il y ait une meilleure facilitation, arbitrage entre les gens, pour que les gens posent plus de questions au lieu de déclarer leurs positions fermes si vous voulez.

MILTON MUELLER:

Oui, je pense que l'obstacle le plus important est assez clair pour moi. Il s'agit... En tant que membre EPDP, je pense qu'on espère quand même pouvoir recréer l'ancien WHOIS, on aimerait avoir la même liberté qu'on avait auparavant.

Mais durant les dernières 20 années de l'existence du WHOIS, il y a eu un très gros intérêt sur l'égalité et l'accès de ces données. Parce que les affaires commerciales étaient basées là-dessus.

Des fois, on arrive à un débat sur l'accès et tout est lié à cet intérêt sur l'accès alors qu'on devrait discuter d'autre chose.

Donc je pense que l'obstacle peut être dépassé si on se concentrait en premier sur les premières étapes, c'est-à-dire finaliser les spécifications, pour voir ce qui pourrait être collecté, donc recueilli, quel en seront les motifs, quels sont les éléments qui sont nécessaires, comment ils seront transférés. Ainsi, on devrait pouvoir se mettre d'accord et de mettre de côté cette question sur l'accès, qui sera la prochaine étape.

Si on ne mélange pas les registres de l'ICANN et les buts des bureaux d'enregistrement dans la collecte de ces données, avec les intérêts légitimes des tierces parties, je pense que nous pourrions faire plus de progrès. Et cela plus rapidement.

Chaque discussion sur la collecte de ces données devient un problème. Nous n'avons pas résolu ce problème et nous allons continuer pendant longtemps sans avoir de résultats.

BRUCE TONKIN:

Vous nous avez dit que les gens pensent qu'on devrait revenir en arrière et revenir vers le WHOIS ? Combien de personnes dans cette salle pensent que c'est une question durable ? Qu'on revienne en fait vers le WHOIS tel qu'il l'était. Il n'y a qu'une personne. Je pense qu'on peut oublier ça, et nous allons donc de l'avant.

Je pense que vous avez raison Milton, si on revient sur le principe des lois sur la vie privée, on devrait répondre à cette question, quel est le motif de cette collecte de données. Et je pense que ce serait un bon point pour commencer.

FLIP PETILLION:

Oui, je voudrais vous rappeler ce qu'a dit Cherine : nous devons essayer de trouver un équilibre entre ce que nous avons besoin de façon collective et ce que nous voulons de façon individuel. Et je pense que c'était très bien dit. C'est ça le RGPD. J

Je pense que, tout le monde, nous devons nous souvenir de ce que veut dire le RGPD, et d'où il vient, et ce que cela veut dire.

Quand les gens discutaient de la première version du RGPD, ils ne pensaient pas à ce dont nous parlons aujourd'hui. Ils voulaient protéger les gens contre la publicité et le hameçonnage, etc. Mais pas avec ce dont on parle aujourd'hui.

Toutes les personnes qui sont incluses dans cette discussion aujourd'hui devraient comprendre quel est le vrai objectif. Voilà. On doit se dire qu'est-ce qu'on veut, et on doit équilibrer cela avec l'intérêt des autres.

Certaines personnes pensent que c'est un choix entre la peste et le choléra. Nous avons un déséquilibre, et ce n'est pas confortable, ce déséquilibre ne met pas à l'aise les gens dans la communauté. Il faut retrouver un équilibre.

Quand on va pouvoir comprendre cela, on va pouvoir avoir un vrai dialogue. Et encore une fois, il s'agit d'équilibre.

BRUCE TONKIN: Il faut donc accepter ce que dit la communauté, mais il faut un équilibre. C'est ça ?

FLIP PETILLION: À ICANN, nous nous basons sur un consensus. Il faut créer de la confiance pour tous. La confiance c'est la base du consensus. Et le consensus, c'est la base de l'équilibre.

BRUCE TONKIN: Qui dans la salle pense qu'on devrait se focaliser justement sur ce travail d'équilibre ?

Donc je vois qu'il y a la majorité dans la salle. C'est bien.

Donc le WHOIS tel qu'il était, on ne peut pas y revenir, mais on dit aussi qu'il faut aller de l'avant tout en trouvant un équilibre. Voilà.

Je pense, encore une fois, on assume tous qu'on doit... Bien sûr on comprend très bien tous qu'il faut équilibrer cet équilibre. Comment est-ce qu'on va en arriver à cet équilibre ?

FLIP PETILLON:

Oui, il faut beaucoup de bonne volonté. Il faut voir ce qui s'applique au RGPD, mais en externe. Par exemple par rapport aux forces de l'ordre, la protection des consommateurs. Ce sont des sujets très intéressants. La protection des enfants aussi.

Donc il y a d'autres lois qui sont applicables, pas seulement en Europe. N'oubliez pas que nous avons du e-commerce, en Europe, qui demande des dispositions obligatoires par rapport aux titulaires du nom de domaine, du site web pardon.

Donc, toutes les lois européennes, et toutes les directives, doivent toujours fournir que la mise en œuvre des réglementations, des directives, doit être équilibré avec tous les éléments du cadre de travail. Donc nous devons vraiment voir la vue d'ensemble, une vue d'ensemble mondiale.

BRUCE TONKIN:

Vous devez vous baser sur les différentes lois spécifiques, il doit y avoir donc cet équilibre. J'ai donné l'exemple des opérateurs de registre. Ils ont cet équilibre lorsqu'ils fournissent ces informations au public. Il faut savoir qui est responsable pour telle ou telle donnée, tel dossier. Hadia ? Vous voulez prendre la parole ?

HADIA ELMINIAWI: À mon avis, on devrait parler des défis d'une façon pratique. On sait tous maintenant que les données d'enregistrement ne sont plus ouvertes. C'est un portail fermé.

Ces données seront donc disponibles à la publication pour des parties tierces qui auraient donc un intérêt légitime.

Quand on parle de cet équilibre, donc il faut comprendre que cet équilibre sera exigé. Mais on doit aussi savoir que nous ne sommes pas les personnes qui vont mettre en place cet équilibre lorsqu'il s'agit de la mise en œuvre.

NON IDENTIFIE: Vous pensez qu'on va faire cet équilibre ? Qu'on va le faire ?

HADIA ELMINIAWI: Oui, nous savons qu'il est requis cet équilibre. Et donc on va le faire pour les personnes qui ont des intérêts légitimes.

Mais lorsqu'il s'agit de la mise en œuvre, nous ne sommes pas ceux qui vont mettre en œuvre cela. Et ce ne sont pas ceux qui vont faire cet équilibre en ce moment.

Donc dans certains cas, nous comprenons bien sûr les principes, les faits tels qu'ils sont, mais de façon pratique lorsqu'il s'agit de la mise en œuvre et de la distribution donc de ces données, nous ne sommes pas ceux qui vont décider dans ce cas si l'équilibre est réussi ou pas.

Donc nous devons garder ça en tête, à mon avis.

Je voudrais aussi parler des défis d'un autre point de vue. Le travail que nous faisons, les politiques que nous élaborons, ont besoin d'être pratiques, faciles à mettre en œuvre. En plus bien sûr, elles doivent être conformes au RGPD. Mais il faut donc qu'on mette en place des politiques, et ça c'est toujours un défi.

À mon avis, pour faire tout cela, il faut que des exigences soient nécessaires. Que ce soit pour les opérateurs ou les bureaux d'enregistrement ou les titulaires de noms de domaine, les services d'accréditation doivent savoir comment ils vont faire les choses, qui va faire les choses, qui va mettre en place ces exigences.

Il y a aussi un défi lié au risque de responsabilité des parties contractantes.

Si vous avez donc une politique qui ne prend pas telle ou telle chose en considération, vous n'aurez personne qui va mettre en œuvre cette politique. Donc à mon avis, voilà donc tous les défis qui ont besoin d'être traités maintenant et non après, donc en parallèle avec ce que nous faisons maintenant, au niveau des politiques. Bien sûr j'espère qu'on va obtenir un consensus, mais la question c'est comment on met en œuvre tout cela.

Travailler là-dessus maintenant plutôt qu'après, c'est qui est exigé. Donc pour moi, c'est le défi le plus important.

BRUCE TONKIN: Oui, donc vous dites qu'une partie de la communauté se concentre sur la politique, et qu'elle soit bonne. Mais pour obtenir une solution, il faut penser à la mise en œuvre aussi.

Donc il ne faut pas commencer à penser à la mise en œuvre après la politique. Il faut penser à ces deux choses en même temps.

Nick.

NICK WENBAN-SMITH: Bonjour, je suis ici comme représentant des parties contractantes.

Et je pense qu'il est très bon que quelqu'un ait parlé des risques des parties contractantes. Et j'aime que dans cette question le terme opportun, une solution opportune soit entre guillemets. Parce que là on parle de mai 2018. Donc on est 12 mois en retard.

Mais je pense que d'une manière générale, même si c'est arrivé très tard et ça a été très rapide, la spécification temporaire c'est quelque chose qui satisfait, d'une manière générale, les parties contractantes.

Ensuite, on pourra parler d'accès.

Mais ensuite, il faut appliquer nos propres politiques. Parce que depuis mai 2018 il faut être conforme avec la loi et donc ça inclut l'accès.

Et l'un des défis intéressants du RGPD concerne les principes. Donc il faut faire un équilibre entre les principes d'intérêts légitimes, et celui de la confidentialité. Et ça, c'est difficile. Mais en l'absence de

politiques mondiales formelles, il faut qu'on le fasse par nos propres moyens.

Donc nous avons un patchwork un peu, de politique, en termes de divulgations. Je sais que ce qu'on fait au Royaume-Uni c'est légal, parce qu'on reçoit des centaines de demandes d'accès, et des requêtes aussi. Parce que je sais que vous êtes conforme avec la législation sur la confidentialité.

Mais si quelqu'un n'aime pas ce que vous faites, alors ils vont porter plainte auprès de l'autorité chargée de la protection des données personnelles, et ils vont dire : voilà, on a reçu une plainte, et j'ai reçu une plainte sur la divulgation de données, de la part d'un organe chargé de la protection des droits de propriété intellectuelle. Et cette plainte a été rejetée. Donc je sais que ma politique sur la divulgation est suffisamment vigoureuse pour faire face à ce genre de défis qu'on reçoit.

Et c'est un exercice qu'ils ont le droit d'exercer, celui de porter plainte ; mais ensuite on peut rejeter cette plainte.

On a une expérience dans ce genre d'expérience post-RGPD. Ce qu'on sait c'est qu'on a une requête avec laquelle on ne peut pas être en conformité. Depuis 3 mois on a reçu environ 750 demandes. Donc on a reçu 750 demandes donc, et 96 % des gens ne disent pas clairement ce sur quoi porte la plainte.

BRUCE TONKIN: Il y a des décisions qui doivent être prises au niveau local, en fonction d'un type particulier de données.

Mais il doit y avoir également des mécanismes mis en place pour les deux côtés. C'est-à-dire celui qui demande les données et les données qui sont sujettes à la responsabilité de la partie qui les fournit.

NICK WENBAN-SMITH: Oui, le mécanisme est déjà mis en œuvre et appliqué dans la législation. Donc il existe déjà.

GREG AARON: Oui, une partie des conversations qu'on a cette semaine sur toutes ces responsabilités que le RGPD est en train de mettre sur tout le monde, ça donne lieu à des discussions intéressantes et c'est une bonne chose. Ça renforce la responsabilité.

Mais ça nous permet également de parler de la gestion des risques.

Tout le monde a des responsabilités bien sûr, et parfois il y a des pénalités qui sont associées, lorsque vous n'êtes pas à la hauteur, ou vous ne respectez pas ou n'honorez pas ces responsabilités.

Et le problème dans la gestion des risques, c'est que parfois ça devient une discussion qui se limite aux coûts. Qu'est-ce que je dois faire pour protéger dument les données ? À quoi est-ce que je m'expose si je partage ces données ?

Et dans la discussion, lorsqu'on parle de coûts, finalement, on limite et on cantonne à quelque chose de très simple la conversation.

Parce qu'effectivement, il y a un risque et ce que dit la loi, c'est que ces évaluations de risques sont très inégales. On le voit même au sein des ccTLD, RIR, au niveau européen qui prennent des décisions en fonction de leur appétit vis-à-vis du risque.

Et c'est ça, on commence à en parler et à dénouer un petit peu les choses. Parce qu'il peut y avoir une certaine confiance vis-à-vis du fait que les données sont bien gérées de la part de toutes les parties concernées, par rapport à toutes les parties qui l'utilisent. Et ça c'est l'équilibre qu'il faut trouver.

Parce que pour les experts en cyber sécurité, il est important de pouvoir utiliser ces données. Parce que les gens qui protègent la loi disent : on ne peut pas avoir cet accès, sauf si c'est fait correctement.

Donc on veut trouver ce bon équilibre. Mais pour cela, il faut arriver à un point on trouve le moyen d'y arriver.

BRUCE TONKIN: Quelqu'un d'autre ? Chris ?

CHRIS LEWIS-EVANS: Merci. Tout d'abord, j'aimerais souligner les progrès qui ont d'ores et déjà été faits dans ce groupe.

Et pour revenir à votre première question, c'était très bien, parce que si vous l'aviez posée à la conférence numéro 61 de l'ICANN, je pense que vous auriez reçu une réponse tout à fait différente de la part du public.

Je pense que le changement dans l'acceptation vis-à-vis de ce dont on a besoin est important parce qu'on comprend qu'il y a des exigences différentes qui viennent des différents groupes de l'ICANN. Non seulement concernant la protection des données, mais également de la part des parties qui ont la possibilité d'avoir accès aux données sur une base juridique.

Et donc cette compréhension est venue parce qu'on a compris quelles étaient les conditions requises et quelles étaient les solutions que les gens attendaient. Et, en fonction de ces exigences, on a pu trouver les solutions.

Et je pense que la meilleure manière de comprendre les réelles conditions requises aux gens, ça passe par le fait de comprendre réellement ces conditions qui sont requises. C'est un peu l'objectif de tout cela.

BRUCE TONKIN: Oui, c'est un petit peu l'objectif de tout cela.

CHRIS LEWIS-EVANS: Oui, et pour revenir à cette solution opportune, il faut revenir à cet équilibre entre les exigences et le fait de comprendre les besoins de tout le monde.

BRUCE TONKIN: Oui, si vous regardez les projets IT et les révisions, on s'aperçoit que c'est peut-être un point commun qu'on a. On a les mêmes difficultés.

CRISTINA MONTI: Oui, pour reprendre certaines des remarques qui ont déjà été faites, si on se penche vers l'avenir et on voit quelles sont les entraves, je pense qu'il est important de reconnaître que ce problème existe depuis longtemps.

Et peut-être que l'une des choses que le RGPD a pu faire, c'est amener ce sujet sur la table, et nous obliger tous à trouver une solution. Et dans un délai serré, limité dans le temps.

Je pense que beaucoup de choses se sont produites. On a vu dans le public que personne aujourd'hui ne pense que la confidentialité n'est pas importante. Tout le monde est d'accord pour dire que les données à caractère personnel c'est quelque chose d'important, et que ceux qui gèrent les données à caractère personnel devraient également être tenus pour responsables de leur utilisation, des données à caractère personnel.

Et je pense que ce qu'on entend aussi dans l'environnement ICANN, c'est qu'il y a eu beaucoup de progrès engrangés jusqu'à présent.

Parce que maintenant, tous nos canaux de communication sont ouverts, la question de la réforme de WHOIS fait maintenant partie des priorités dans beaucoup de discussions de haut niveau, également en dehors de l'ICANN. Donc, d'une certaine manière, des progrès ont été faits, et les discussions abordent une phase plus mure. Maintenant on arrive aux solutions plus concrètes. Et c'est là que le bât blesse.

Bien sûr, dans l'aspect opérationnel des principes que nous avons vu, c'est là qu'il y a un problème. Bien sûr dans le modèle de gouvernance multipartite, c'est difficile, parce que vous avez plusieurs intérêts en jeu et parfois les discussions peuvent être très polarisées. Mais je pense que ce n'est que dans un environnement multipartite qu'il est possible de trouver une solution durable.

Je pense aussi qu'à l'heure actuelle on sait que des étapes ont été franchies pour s'assurer que les registres, le registre WHOIS est en conformité avec le RGPD. Mais encore, il y a une étape prévisible et finale qu'il va falloir trouver et dépasser.

Et parfois, je pense que l'on a tendance à négliger un aspect important. Même les utilisateurs ou opérateurs de registres individuels ne sont pas complètement conscients de la manière dont les données sont gérées, qui ils doivent contacter s'ils veulent corriger les données, etc.

Donc nous sommes maintenant dans une situation où nous nous trouvons un petit peu au milieu.

BRUCE TONKIN:

Oui, je pense que ce que vous avez dit par rapport aux utilisateurs individuels est très bon. Parce que la plupart des gens ici dans la salle sont des professionnels de l'informatique, s'y connaissent.

Donc ils savent de quoi il retourne. Ce n'est pas le cas des utilisateurs individuels. Ils ne savent pas ce qu'est WHOIS. Ils ont probablement un jour eu une mauvaise expérience avec un site web, ils en auront fait un rapport, ils l'auront dénoncé. Et voilà, s'en est resté là.

Donc il faut faire ce travail de transparence. C'est important effectivement.

CRISTINA MONTI:

Oui.

Et pour compléter un petit peu ce qui a été dit par rapport aux risques, j'aimerais dire que le RGPD qui se fonde sur des règles qui existent depuis longtemps, devrait être vu et compris comme un encouragement pour tous les acteurs qui doivent gérer et administrer des données personnelles, pour qu'ils le fassent de manière juste, équitable et transparente. Et également avec des acteurs en dehors de l'Europe.

Et la situation s'est améliorée dans la mesure où maintenant il y a beaucoup plus d'uniformité dans la manière dont les règles sont appliquées, et parce qu'il y a des mécanismes qui sont maintenant en place pour le garantir.

Avant le RGPD, il y avait de nombreuses législations. Avec le RGPD, on a une plus grande uniformité. Donc pour les acteurs en dehors de l'Europe, ça va maintenant être beaucoup plus simple de gérer ou de faire face à ce problème.

BRUCE TONKIN: Oui, effectivement, il y a une sorte de normalisation au niveau international maintenant.

HADIA ELMINIAWI: Comme je l'ai dit auparavant, les défis ont à voir avec ce manque de compréhension, cette mauvaise compréhension.

J'aimerais maintenant dire rapidement que l'on ne collecte pas les données d'aucune manière pour les besoins des parties tierces ou de ceux qui ont un intérêt dans les accès aux données. Parce que ça c'est une mauvaise compréhension des choses, une idée erronée.

J'entends des gens qui disent : vous collectez des données pour les autorités chargées de l'application de la loi, ou pour telle ou telle personne. Et je veux rassurer toutes les personnes ici présentes. Toutes les données sont collectées uniquement pour les fins nécessaires pour remplir les services pertinents.

BRUCE TONKIN: Oui, ne collectez uniquement que les données nécessaires.

HADIA ELMINIAWI: Oui, collecter les données uniquement pour les fins qui sont évoquées.

BRUCE TONKIN: Oui. Par rapport à l'élément des données en particulier, on va y revenir par la suite. Nick ?

NICK WENBAN-SMITH: Oui, il y a un risque. Et le risque est toujours assumé par les parties contractantes. Ça, c'est l'une des choses qui nous amènent à appliquer une politique plus conservatrice.

Mais il y a quelque chose de plus général. Parce qu'il y a une préoccupation du fait que l'on parle de pénalités financières très importantes. Et pour une organisation responsable ça, ça ne me préoccupe pas.

Mais je pense au citoyen. Pour que l'on puisse être conforme à la loi et se montrer responsable, ça c'est un avantage compétitif au niveau commercial, pour quel qu'entreprise que ce soit.

Donc essayez de faire passer également ce message.

BRUCE TONKIN: Oui, ce dont vous parlez en fait, c'est la confiance, et les gens ont tendance à perdre cette confiance. Parce qu'ils souscrivent un service, et ensuite sans qu'ils le sachent leurs données sont données à des tiers.

Et pour revenir aux objectifs de haut niveau de l'ICANN, il faut que les gens aient confiance dans les noms de domaine, et aient confiance dans les gens qui les gèrent.

Parce que si vous ne faites pas confiance, alors autant utiliser les réseaux sociaux.

MILTON MUELLER:

Oui, je voulais revenir par rapport à ce qu'à dit Monti. Effectivement c'est un problème de très haut niveau le rôle de l'ICANN en tant qu'organisation et la conformité par rapport aux lois et à la législation internationale.

Oui, effectivement, moi je ne suis pas très fan de la législation européenne en matière de protection des données personnelles avant le RDPG. Mais je pense que ça nous a rendu service finalement. Parce que dans ce qu'on appelle l'effet Californie, lorsque l'État a dit que la pollution véhiculaire était beaucoup plus importante que dans le reste du pays. Donc, il fallait qu'en Californie... Est-ce qu'on allait construire et fabriquer des voitures différemment en Californie que dans le reste du Pays ?

Et je pense que c'est un petit peu la même chose. Avec le RGPD, on a fixé une norme, et lorsqu'on a une agence internationale comme l'ICANN qui puisse être conforme à une norme ? Ou bien est-ce qu'on essaye de mettre en place des normes concurrentielles ? Par exemple, aux États-Unis, on n'est pas content avec ce que l'Europe a décidé et on essaie de créer un autre système.

Je pense que c'est l'un des grands débats dont il faut être conscient s'agissant du RGPD.

Et je vous ai donné l'exemple des États-Unis, mais toute grande juridiction, que ce soit la Chine, l'Inde, peut-être le Canada, je n'en sais rien, pourrait tomber dans le même piège.

Parce que l'ICANN, en tant qu'une agence d'ordre privée et de gouvernance mondiale, qui avec une souveraineté territoriale fragmentée où vous pourriez avoir plusieurs systèmes.

BRUCE TONKIN:

Oui, si vous regardez un petit peu l'historique du RGPD, c'est effectivement ce qu'il s'est passé en Europe, avec plusieurs pays qui prenaient ce principe, mais l'interprétaient différemment.

Et j'imagine, pour un petit pays européen, essayer d'appliquer ces législations sur la confidentialité, c'est beaucoup plus difficile sur un petit marché que sur un grand marché. Et la même chose en termes de population.

Le cas de la Californie, c'est un marché énorme, et donc l'exemple que vous avez donné pour la fabrication des voitures, oui, il y a un rapprochement à faire.

FLIP PETILLION:

Oui, merci. Je voulais ajouter quelque chose.

Pour revenir à la question de la confiance. Il y a confiance lorsque vous donnez des informations, mais il devrait également y avoir de la confiance lorsqu'il y a une demande d'information. Et tout le monde devrait montrer un engagement pour contribuer à alimenter cette confiance. Et je pense que Nominet a donné un bon exemple.

Mais il y a un autre exemple qui a été donné par monsieur Noss, un bureau d'enregistrement particulier, et ça c'est un bon exemple de bonne volonté. C'est ce qu'on appelle bonne foi en Europe. C'est une volonté de parvenir à une solution viable.

BRUCE TONKIN:

Oui, je pense que par rapport à l'accès aux données, lorsqu'une partie demande l'accès aux données, ils sont ensuite tenus pour responsables, ils doivent rendre des comptes par rapport au fait qu'ils ont accès à ces données.

Il ne s'agit pas simplement d'avoir accès à ces données et qu'on n'en fait rien. Non. Ça doit faire partie du cadre de confiance. Les gens qui ont accès aux données ne doivent pas les utiliser à mauvais escient, c'est tout.

J'aimerais maintenant, j'ai d'autres questions à poser aux membres du panel, mais étant donné qu'il y a beaucoup de gens de la communauté dans la salle, j'aimerais me tourner vers la salle maintenant, et vous demander si vous avez des interventions dans la salle par rapport aux deux questions qui sont à l'écran, par rapport à une solution opportune, etc.

Est-ce qu'il y a des questions dans la salle ? Des demandes d'interventions ?

HOLLY RAICHE:

Une question. En termes d'objectifs, il faut que vous testiez les objectifs par rapport à l'ICANN. Mais la mission de l'ICANN est assez large.

Il y a des arguments qui disent que la mission est uniquement technique. Si vous regardez les missions de l'ICANN, ça va au-delà de l'aspect technique.

Si vous avez les données d'une personne, ce n'est pas simplement pour fournir un soutien technique, c'est également utilisable dans le cas d'arbitrage, etc.

Donc moi je serais préoccupée si ce n'est pas, si la mission de l'ICANN ça ne comprend pas la gestion de tout le système et sa stabilité.

ASHLEY HEINEMAN:

Oui, je pense que cela fait longtemps, mais nous avons compris cela. C'est une bonne chose.

Tout cela n'est donc pas finalisé, mais nous reconnaissons tout cela, surtout quand il s'agit de la sécurité et la stabilité, et la résilience du système de noms de domaine.

BRUCE TONKIN:

Vous avez une autre question ? Alors Rachel.

RACHEL POLLACK : Merci de nous avoir porté ces discussions aussi intéressantes. J'ai deux commentaires et une question.

Durant la dernière réunion où j'ai participé, c'est-à-dire il y a un an et demi à Copenhague, le conseil de l'Europe avait amené des commissionnaires, des commissaires du RGPD. Et donc il y a eu une réunion entre les membres de l'ICANN et ce conseil de l'Europe. Et il y a eu un guide qui a été publié cette année d'ailleurs sur les questions du RGPD et l'ICANN.

Je me demande si les membres du panel ont eu l'occasion de regarder et de lire ce guide, et s'ils ont continué leurs discussions avec ces commissaires du RGPD. Pour pouvoir comparer leurs données avec tous ces modèles.

Et moi je voudrais faire un petit lien avec ma propre organisation. Nous avons publié deux études qui expliquaient certaines questions, telles que la liberté d'expression, la vie privée et la transparence, afin de pouvoir donc parler d'un certain équilibre entre les droits de l'homme et tout cela d'ailleurs.

Donc je voudrais savoir s'il y a la même chose sur la liberté de l'internet.

BRUCE TONKIN: Juste un petit commentaire, avec respect des protections des données et de ces commissaires, ICANN les a donc contactés et il y a eu un événement parallèle la semaine dernière à ce sujet.

HADIA ELMINIAWI: En fait, nous avons pris en considération toutes les correspondances que nous avons eues avec le bureau du RGPD. Et des réponses ont été fournies à l'ICANN.

Durant cette phase de travail, quand nous avons développé cette politique, nous avons observé tout ce qui nous avait été fourni, et nous avons pris tout cela bien sûr en considération.

BRUCE TONKIN: Cristina.

CRISTINA MONTI: Oui, pour clarifier un peu cette question, bien sûr nous sommes tout à fait conscients du guide qui a été fourni par le conseil de l'Europe. C'est un document très utile.

Cependant, c'est lié aux principes. Et quand il s'agit du RGPD, le conseil de l'Europe travaille plutôt sur la convention 108.

En fait, elles [les autorités de protection des données du conseil de l'Europe] ne pouvaient pas venir à cette réunion car il y avait une réunion mondiale internationale, d'ailleurs en ce moment à Bruxelles.

Mais je voudrais tout de même réassurer tout le monde, les autorités de protection des données européennes sont tout à fait conscientes de cette discussion, ils suivent les progrès qui ont été faits. Ils ont aussi fourni des directives et des conseils, et nous ont demandé de fournir des informations sur toutes ces questions spécifiques. Ils sont vraiment ouverts à un dialogue continu avec nous. Ils sont aussi conscients de cette...

Encore une fois, il y a donc des pouvoirs plus importants. Ils ont des outils à leur disposition, et avant d'appliquer des frais, des cotisations ou des menaces de coûts et de frais, ils espèrent donc, encore une fois, un dialogue.

BRUCE TONKIN:

Oui, c'est un bon point. Nous avons donc maintenant une approche plus ou moins coopérative, et ainsi nous pouvons être tenus au courant de toutes les exigences.

Numéro 2.

NON IDENTIFIE:

Une question pour Nick, qui nous vient du Adobe à distance. L'expérience des parties contractantes sur l'accès est très valable, nous apporte beaucoup. Quels sont les chiffres, combien y a-t-il de requêtes d'accès de la part des tierces parties ?

BRUCE TONKIN:

Nick.

NICK WENBAN-SMITH: Nous allons voir, bien sûr nous allons aller vers, pour essayer de comprendre...

Nous avons donc des choses qui n'avaient pas été publiées dans le WHOIS. Et donc pour le .UK, qui est donc une des extensions géographiques les plus importantes, nous avons donc vu une certaine généralité dans toutes les demandes de données. Quand il s'agit des adresses mail et dans le WHOIS public.

Après le RGPD, nous sommes en train de recueillir tous ces numéros, et nous le faisons avec précaution, dans notre analyse de données. Nous avons donc eu 800 demandes pour des noms de domaine, des enregistrements de données pour des noms de domaine. Nous sommes arrivés à 6 mois, et maintenant nous pouvons voir un petit peu, étudier cette expérience.

Lorsque nous avons reçu ces exigences, nous les avons analysés, et nous avons étudié la raison pour laquelle ces données avaient été exigées pour nous assurer qu'il y ait de la transparence. Donc il y a beaucoup d'éléments qui sont rentrés en comptes dans ces données individuelles.

Et, en poursuivant, nous allons essayer de voir les choses d'une façon organisationnelle.

Du côté des parties contractantes, nous avons vraiment des dialogues intéressants. Nous collectons, nous recueillons toutes les informations

pour essayer de comprendre les expériences et de savoir ce qui fonctionne bien et ce qui ne fonctionne pas bien.

Les chiffres n'ont pas été si importants quand il s'agit des requêtes et demandes de données, comme le suggéraient beaucoup de personnes. Car nous avons déployé, nous avons demandé...

Je suis un petit nerveux, parce que techniquement, il faut fournir de l'accès aux parties contractantes, et à cause de mes expériences préalables, sur la façon dont ICANN met en œuvre les choses. Nous allons en arriver avec un système qui va être complexe, et qui est peut-être trop compliqué.

Il faut vous rappeler que même si le registre UK, par exemple, est très important, nous avons aussi un autre registre pour le Pays de Galles. Nous avons reçu zéro demande pour des données dans ce cas-là.

Donc pour les nouveaux gTLD, et ce nouveau programme, ce seront des chiffres qui seront très représentatifs.

Donc mettre en œuvre quelque chose qui est si compliqué et qui coûte beaucoup n'est pas forcément justifié. Donc il faut vraiment étudier la question.

Je serais très intéressé de savoir si les plus petits registres ont reçu des demandes ou pas.

BRUCE TONKIN:

Alors la question était celle-ci, si j'ai bien compris, vous aviez 800 demandes de la part des forces de l'ordre ?

NICK WENBAN-SMITH: Non, 800 par trimestre.

BRUCE TONKIN: 800 par trimestre, c'est ça ?

NON IDENTIFIE: Je voulais vous poser une question, car vous avez parlé des principes du RGPD sur l'exactitude.

Donc il y a des standards, des normes d'exactitudes qui sont mis à jour tous les ans, une fois par an, par encore une fois les opérateurs de registre. Donc c'est une discussion qui continue.

Je pense que nous ne sommes pas très loin d'une bonne solution.

Comment est-ce qu'on peut définir un motif si on a des fausses données ? Comment est-ce qu'on peut mettre en place un objectif, et je ne parle pas seulement du point de vue de l'Europe et des tierces parties, mais aussi pour les parties contractantes ou pour toutes les autres unités qui voudraient des informations afin qu'ils puissent savoir si les données sont exactes ou pas ?

Donc il faut qu'on mette cette question de côté, parce qu'il y a des coûts énormes qui sont... Il y aura donc des coûts énormes. Donc je pense qu'on n'a pas encore atteint une solution là-dessus.

BRUCE TONKIN: Y a-t-il d'autres commentaires ?

MILTON MUELLER: Donc le fantôme de l'ancien WHOIS nous hante encore.

Et donc le problème, ce problème d'exactitude en est un bon exemple. Donc quand il s'agit des données, des contacts personnels, on sait très bien qu'il y a des personnes bienveillantes et malveillantes.

Une fois que ces données deviennent protégées par rapport à un accès discriminatoire, le problème de l'exactitude devient différent. Il y aura donc des fausses informations, mais ce ne sera pas le cas pour tous les bureaux d'enregistrement légitimes.

Donc la discussion sur la vérification des données est un problème qui est lié au principe, par rapport ce qu'on recueille, les données qu'on recueille ou qu'on collecte ou pas. Il y a donc un ensemble de politiques qui sont déjà existantes quand il s'agit de l'exactitude.

C'est un bon exemple des obstacles que nous avons devant nous pour pouvoir progresser. Il faut essayer de décider ce que l'on va recueillir, ce qui sera conforme au RGPD, et cela est lié à la conformité, donc au RGPD.

BRUCE TONKIN: Numéro 2.

FIRDAUSI:

Je voudrais vous demander un exemple lorsqu'il s'agit du conflit de réglementation.

Quand vous parlez des principes juridiques, quand est-ce que ces réglementations spéciales repousseront, dépasseront les nouvelles régulations, quand est-ce que les nouvelles régulations dépasseront les anciennes réglementations ?

Il y a donc des choses qu'on pourrait... Il y a donc matière à investigation.

Quels principes vont être utilisés quand on sait que le RGPD s'applique à l'Europe, mais pas seulement à l'Europe ? Comment les gouvernements des autres régions, ou tout simplement une autre région qui a les mêmes institutions similaires telles que EU en Asie du Sud où nous avons un accord multi niveau ou bilatéral. Ou est-ce qu'on va faire face à ce problème cas par cas ?

[Note de transcription : le paragraphe précédent est l'exacte transcription de la traduction simultanée]

Il faut donc sensibiliser le consommateur sur le sujet.

Qu'est-ce que vous pensez du rôle d'administrateur sur la confidentialité, sur la protection des données dans l'avenir ? Parce qu'il serait bon pour toutes les organisations à travers le monde d'avoir un tel administrateur, et c'est urgent.

BRUCE TONKIN: Est-ce que vous recevez des réponses ou des demandes de données en externe du .UK ? Et comment est-ce que vous gérez cela ?

NICK WENBAN-SMITH: Oui, nous comprenons les processus. Peu importe où vous êtes, nous avons des requêtes, des demandes, en dehors du Royaume-Uni. Bon, bien sûr en recevons au Royaume-Uni parce que nos enregistrements sont faits au niveau du Royaume-Uni.

Nous avons bien sûr beaucoup de bureaux d'enregistrement qui se trouvent en dehors du Royaume-Uni. Les mêmes politiques s'appliquent, c'est une politique mondiale ;

Donc lorsqu'on essaye de comprendre comment on peut mettre en pratique le RGPD, c'est bon de voir qu'il y a une standardisation.

Donc c'est la même chose si les demandes viennent de l'intérieur ou de l'extérieur.

BRUCE TONKIN: En Europe, vous êtes liés par les lois européennes. Donc vous appliquez ces lois à toutes les demandes.

NICK WENBAN-SMITH: Oui, en termes d'application de ce système sur l'accès, il est donc plus facile de procéder de cette manière.

BRUCE TONKIN: [non traduit]

NICK WENBAN-SMITH: Oui, oui. Il faut que les lois soient appliquées pour les opérateurs de registre et les bureaux d'enregistrement.

ASHLEY HEINEMAN: Je ne vais pas parler de la part des États-Unis, mais avec ma position au GAC.

Il faut faire très attention quand on définit le RGPD en tant que règlement général sur la protection des données. Il y a beaucoup de réglementations.

Donc ce qui est devenu donc une question pour l'ICANN, c'est que ça fait partie des responsabilités des parties contractantes.

Donc nous espérons que tout ce qui concerne le RGPD sera en général lié aux autres lois concernant la protection des données.

On va voir comment cela rentre en jeux.

Je pense, ce qui intéresse les gouvernements, c'est la mise en œuvre et c'est aussi la capacité des forces policières en dehors de la zone Europe.

C'est donc plus facile pour les forces de police Européennes d'avoir accès. Tout cela n'est pas très clair pour le reste du monde, donc les forces policières à travers le reste du monde.

BRUCE TONKIN: Prochaine personne au micro.

NON IDENTIFIE: Je voudrais parler des commentaires que vous avez faits sur les 800 demandes que vous avez eues en trois mois.

Avant le RGPD, combien de demandes aviez-vous par mois ? Parce que cela pourrait être des informations intéressantes sur les vraies demandes, des demandes que la communauté en général vous fait passer.

NICK WENBAN-SMITH: Non, ce ne sont pas les mêmes chiffres mois par mois. Souvent nous avons un volume de demandes d'une agence particulière, qui demande plus d'investigations à telle ou telle période de l'année.

Donc l'ampleur du changement des demandes, on passe de 10 à 20 par mois, à 800. Donc ça fait à peu près 250 demandes de plus.

BRUCE TONKIN: Est-ce que c'est à travers vos propres services ou est-ce qu'il s'agit des demandes qui ont à faire au RGPD en général au Royaume-Uni ?

NICK WENBAN-SMITH: Oui, la chose la plus significative par rapport au RGPD, c'est que ça n'a pas vraiment changé les lois au Royaume-Uni, mais cela a permis aux

personnes physiques individuelles de se rendre compte qu'il y avait des différences.

Le 25 mai, c'était donc surtout les médias, on a parlé dans tous les journaux télévisés. Donc il y a une certaine prise de conscience par rapport à la population.

GREG AARON:

Depuis le RGPD, en mai, nous commençons tout juste à comprendre quels en sont les effets. Nous avons commencé à voir des informations qui en ressortent.

Donc ce qui s'est passé récemment, par exemple, il y a deux organisations qui sont composées de professionnels sur la cybersécurité et des opérateurs de réseau, donc des groupes dont les membres incluent des compagnies pour la sécurité, qui protègent donc des banques, des institutions, etc. Donc on nous a demandé : est-ce qu'il y a plus de demandes, est-ce qu'il y en a moins, comment ça se passe ? Donc il y a eu 300 réponses avec des informations.

Et on s'est rendu compte que certains d'entre eux ne savaient pas vraiment comment faire les demandes. Parce que les organisations qui sont titulaires des données font les choses de façon différentes, ils ont des procédures en place qui sont différentes, elles utilisent des mécanismes différents. Cela dissuade un petit peu les groupes dans leurs demandes.

S'il y a moins de demandes, ce n'est peut-être pas significatif par rapport à la vraie demande des données, parce qu'il y a des

institutions qui ont abandonné leurs demandes, comme ils le faisaient pour le WHOIS. Parce qu'ils ne nous disent plus ce dont ils ont besoin.

Donc, dans les mois à venir, nous aurons plus d'informations sur la manière, du moins sur l'impact que cela a sur les gens et les institutions.

DIRK KRISCHENOWSKI:

Dirk de .BERLIN. Je suis vice-président du ccTLD.

Nous avons publié quelque chose il y a peu de temps sur notre site. Nous avons publié donc une étude de 39 géo-TLD. Et de ces 39 cas, 25 géo-TLD venaient d'Europe, et le reste venait de l'extérieur de l'Europe. Et les résultats de cette étude ont démontré que les géo-TLD qui venaient d'Europe prenaient les choses sérieusement par rapport au RGPD, et le nombre de demandes d'accès aux données commence à diminuer. Et cette baisse a à voir avec cette efficacité.

Les études des opérateurs de registre face au RGPD montrent qu'il n'y a pas un besoin d'avoir des preuves ou des évidences pour demander l'accès.

Donc, les demandes à partir de mai jusqu'en septembre ont été de moins de 50 demandes à travers ces 39 géo-TLD. Et nous avons plus de 7000 enregistrements.

BRUCE TONKIN: Merci. Je pense qu'il est excellent que les gens partagent ces données et ceux qui gèrent les registres puissent le faire. Parce que ça aide beaucoup au développement de politiques.

JOHN LAPRISE: Bonjour. John Laprise, ALAC. Et je vais d'ailleurs retirer mon chapeau membre ALAC, parce que je travaille sur la recherche de marchés au département d'État aux États-Unis.

Et pour répondre à la question de Bruce par rapport à ce qu'il se passe aux États-Unis. J'ai participé récemment à un webinaire où on s'est aperçu qu'il y a beaucoup d'entreprises aux États-Unis qui sont conscients du RGPD et qui s'acheminent vers l'adoption.

Mais en fait, elles préfèrent attendre et voir ce qu'il se passe. Et, aux États-Unis, on dit : bon ce n'est pas la peine de se précipiter, laisse partir celui qui est devant toi pour voir comment ça se passe. Et c'est un peu ce comportement qu'on voit aux États-Unis, les gens attendent pour voir ce qu'il se passe.

Mais, d'une manière générale, sur le marché, il y a une attitude assez ouverte, il y a une nouvelle initiative qui va dans le droit fil du RGPD aux États-Unis.

Voilà un petit peu la tendance aux États-Unis.

BRUCE TONKIN: Merci.

THOMAS DE HAAN:

Thomas de Haan des Pays-Bas.

Je voulais revenir à l'intervention de Nominet parce que ça me semble très intéressant de voir quel mécanisme existe actuellement.

Bien sûr vous avez parlé de la juridiction au Royaume-Uni, qui est un peu moins complexe que l'échelle mondiale.

Mais j'aimerais savoir, vous avez fait référence aux requêtes d'accès futurs aux données. Qu'en est-il des accès groupés ?

Par exemple, aux Pays-Bas, on a les plus grands ccTLD au monde qui sont parvenus à un accord avec les autorités locales pour avoir un accès groupé limité.

Est-ce que mécanisme existe aussi au Royaume-Uni ?

Et, question suivante, est-ce que vos instruments ou ceux que vous avez mis en place répondent aux demandes ?

BRUCE TONKIN:

Oui, ici il y a un petit problème de terminologie. Est-ce que vous parlez de demandes groupées, pour toutes les parties ? Et ensuite il y a « groupé » pour certains groupes seulement ; alors... Accès groupé pour toutes les bases de données accessibles aux autorités chargées de l'application de la loi ?

Est-ce que vous voulez répondre par rapport à cette requête ?

NICK WENBAN-SMITH: Oui, je vais répondre par rapport à ce que vous avez demandé sur l'accès groupé.

Effectivement, les autorités basées au Royaume-Uni ont droit à un accès groupé. Les opérateurs de registre ont beaucoup plus de données que celles qu'on partage avec les autorités chargées de l'application de la loi, et que celles qui sont sur le WHOIS public.

Mais l'accord qu'on a convenu, c'est qu'ils auraient accès aux mêmes données WHOIS que celles auxquelles ils avaient publiquement accès avant le 25 mai de l'année dernière.

Donc on connaît ces agences, on sait comment elles fonctionnent, elles coordonnent toute une série d'actions, il s'agit de l'agence nationale de criminalité, etc.

Donc ça, c'est fait par un seul point d'accès. C'est-à-dire notre autorité locale.

Et par rapport à l'accès automatique, non, on n'en a pas d'accès automatique.

BRUCE TONKIN: Milton.

MILTON MUELLER: Oui, je pense que c'est une bonne discussion par rapport à l'accès. Mais je dois vous rappeler qu'on parle d'accès.

Donc ne perdons pas de vue, un que nous avons beaucoup de données intéressantes collectées par rapport aux effets actuels. Je pense que les informations des géo-TLD ont montré leur intérêt par rapport à l'étude sur les ccTLD et d'autres.

Mais vous avez bien pu observer la complexité lorsqu'on a entendu Nominet parler des différents types et niveaux d'accès. On voit la complexité là.

Et là, Dirk en a parlé, il a dit qu'on n'a pas besoin d'accès unifié, et certains disent au contraire qu'on en a besoin. Donc c'est un problème qu'il faut examiner.

Mais d'abord il faut décider de ce qu'il y a dans notre WHOIS, ce qui est publié, quelles sont les données collectées.

Et ne confondons pas les deux problèmes. On devrait pouvoir finaliser cette première partie. Je pense que c'est assez facile d'ici trois mois.

Et si on n'arrive pas à le faire, alors on est confronté à un gros problème, parce que les délais courent, et on a l'impression que ce processus va droit dans le mur.

Et il y a d'ailleurs beaucoup de gens qui aimeraient qu'on aille droit dans le mur, qui aimeraient intervenir et qu'il y ait une intervention gouvernementale, et une fragmentation.

Mais attention. Respectons les temps. Formulons une politique, et ensuite ayons un débat riche, du reste, sur l'accès.

BRUCE TONKIN: Oui. Vous pouvez essayer d'avancer progressivement, essayer de voir quel est l'objectif, quel est l'intérêt dans la collecte des données, et ensuite voir ce qu'il se passe. Parce que sinon, vous tournez en rond finalement.

BECKY BURR: Bonjour, Becky Burr. Je parle en tant que directrice de la confidentialité Neustar.

Lorsque Microsoft a mis en place sa plateforme RGPD au niveau mondial, a fait état du fait qu'ils reçoivent plus de requêtes et remplissent de requêtes de la part des États-Unis, plus que nulle part au monde.

Donc, [le fait est que] d'après notre expérience et le fait que tout le monde en Europe est conscient du RGPD depuis le 25 mai 2018, et de par le monde, donc mon expérience est la suivante - en tout cas dans cette entreprise nord-américaine et dans les autres entreprises qui essaient de se prêter au jeu et de rentrer dans les règles du RGPD - elles ont répondu et elles ont apporté une réponse rapide aux consommateurs.

BRUCE TONKIN: Merci Becky.

AMRITA CHOUDHURY: Bonjour Amrita Choudhury de l'Inde. Peut-être que je vais me tromper, mais n'hésitez pas à me corriger.

Je crois qu'il y a plus de 300 millions de registres enregistrés, et plus de 3 millions noms enregistrés dans les noms de domaine européens, ce qui est moins de la moitié des registres de domaines mondiaux.

Donc, ma question est la suivante : comment est-ce que les noms de domaine peuvent être en conformité avec le RGPD par rapport au registre WHOIS ?

Est-ce que l'ICANN est en train d'examiner aussi les lois des autres pays ? Parce que l'Europe c'est une zone, une région où les lois sont protégées, mais il y en a d'autres.

Deuxième question. Nous avons des pays qui sont relativement développés, qui ont un bon niveau de compréhension, et on a d'autres régions, comme l'Inde, qui sont émergentes. On a des noms de domaine qui ont été vendus par plusieurs entreprises, organisations, de l'Europe, des États-Unis et de l'Inde. Et les opérateurs de registre et bureau d'enregistrement n'ont peut-être pas le même niveau de compréhension et de capacité. Donc, est-ce qu'il y a quelque chose de prévu pour renforcer ces connaissances, pour que les utilisateurs finaux et leurs intérêts puissent être dûment pris en considération ?

Parce qu'on est assis ici pour parler des acheteurs de domaines et pas des utilisateurs finaux, en particulier dans les pays émergents.

BRUCE TONKIN:

Oui, donc vous demandez est-ce que les lois des autres pays sont également prises en considération, vous prenez l'exemple de l'Inde. Et

deuxièmement comment la prise de conscience est renforcée par rapport à toutes ces questions.

Donc, peut-être que je vais d'abord répondre à la deuxième partie de la question et ensuite, je vais demander à Hadia qui vient de l'ALAC, qui s'occupe de la prise conscience de par le monde de répondre à la première partie de la question.

HADIA ELMINIAWI:

Oui. Je vais parler en tant que membre de l'EPDP.

L'une des recommandations qui, nous l'espérons, va ressortir de l'équipe de l'EPDP, c'est de faire une recommandation pour sensibiliser et éduquer les titulaires de noms de domaine.

Et je pense qu'on va pouvoir le faire grâce à l'ICANN mais grâce à la collaboration des opérateurs de registre et des bureaux d'enregistrement. Parce que ça va dans le meilleur intérêt des bureaux d'enregistrement et opérateurs de registres que les titulaires de noms de domaines soient conscients de ce qu'il se passe vis-à-vis de cette nouvelle politique.

Si nous envisageons, dans notre travail, d'autres législations en termes de confidentialité, c'était la question, non. Parce qu'en fait l'équipe EPDP est chargée de voir la conformité de la spécification temporaire vis-à-vis du RGPD. Et j'espère qu'il n'y aura pas de conflit vis-à-vis d'autres législations en terme de confidentialité.

Mais à vrai dire, actuellement, on n'examine pas les autres législations en termes de confidentialité. Non.

ASHLEY HEINEMAN:

Pour parler au nom du GAC, oui, en termes de notre engagement dans l'EPDP, et dans les activités en cours par rapport à WHOIS, nous avons fait de notre mieux – peut-être que ce n'est pas le meilleur terme d'ailleurs, de notre mieux – mais nous avons fait notre possible pour voir quelles étaient les lois en vigueur dans le monde, en utilisant la structure RGPD.

Mais on essaie de ne pas se focaliser uniquement sur le RGPD, de ne pas faire un travail qui soit spécifique au RGPD, mais de voir également ce qu'il se passe dans les autres pays, dans les autres législations.

BRUCE TONKIN:

Merci ; Cristina.

CRITINA MONTI:

Je voulais aussi faire des commentaires sur cette question, une question récurrente par rapport aux tensions, aux tensions potentielles entre les différentes lois, les différentes juridictions, et la nature mondiale de l'internet.

On sait que c'est un défi, et on sait que c'est un défi qu'on va sans cesse devoir relever. Non seulement par rapport à la protection des données, mais dans d'autres domaines aussi.

C'est pourquoi il est important de ne pas se tromper ici à l'ICANN, de faire bien les choses. Parce qu'on va fixer un précédent pour l'avenir.

Pour ce qui concerne la protection des données, en général, j'aimerais aussi insister sur le fait que ce que l'on voit – et peut-être que là je suis un peu plus optimiste que mon collègue Milton Mueller – on voit une tendance vers la convergence. Ces principes, qui sont inscrits dans le RGPD et qui se fondent sur la protection des droits fondamentaux de l'être humain, sont finalement je dirais des principes de bon sens. À savoir bien gérer vos données.

Ensuite, et comme je le disais au début, le problème, ce sont les détails et la mise en œuvre. C'est là qu'il faut se concentrer.

Et il se peut que toutes les réponses ne soient pas là et qu'on puisse découvrir qu'il va nous falloir trouver des solutions novatrices pour que ce système fonctionne, et pour étendre un petit peu les limites de ce à quoi on a affaire.

Donc on a des processus en place, on a des parties prenantes autour de la table, et il faut que ça fonctionne.

Et mon point de vue sur les différents processus est le suivant : je comprends que certaines parties prenantes aimeraient avoir une approche séquentielle, tandis que d'autres ont un sentiment d'urgence et veulent tout de suite parvenir à une solution.

Personnellement, je ne vois pas en quoi ce serait un problème d'avoir des processus parallèles, mais c'est vrai qu'il faut avoir une bonne compréhension des problèmes, et c'est vrai que parfois on a de

mauvaises interprétations, des idées erronées, sur les choses. C'est quelque chose de récurrent.

D'où l'importance de travailler de manière collective, ensemble, dans les groupes de travail et autres pour tendre tous vers une solution unique.

Donc identifions ensemble comment est-ce que l'on va pouvoir surmonter cette difficulté et combler ce fossé.

BRUCE TONKIN:

J'aimerais revenir à une autre question, et je reviendrais ensuite vers la salle. Autre question à l'attention du panel.

Quelles sont les choses en termes de PDP qui ont été mises en œuvre, parce qu'il y a d'autres questions qui ont été liées à cette thématique.

L'une d'entre elles c'est les solutions que les bureaux d'enregistrement et opérateurs de registres ont mises en place pour protéger les données à caractère privé, ce qu'on a appelé service d'anonymisation ou d'enregistrement fiduciaire.

Et par rapport au WHOIS, il s'agissait d'une entreprise séparée, c'est ce qu'on appelait les services d'anonymisation où une entreprise qui opérait au nom du titulaire de nom de domaine, qui avait un intérêt dans le WHOIS et qui pouvait avoir accès à l'utilisateur final.

Donc ces services d'anonymisation et d'enregistrement fiduciaire faisaient un excellent travail pour donner au consommateur la possibilité de protéger ses propres données personnelles.

Ce qui n'était pas clair, c'était dans quelles circonstances les données personnelles sont ensuite divulguées aux autorités chargées de la loi, et ensuite à d'autres groupes.

Donc il y a un processus de discussion sur cette thématique.

Et donc ma question au panel est la suivante : est-ce qu'il faut revenir en arrière et revoir ces politiques ? Les politiques de l'EPDP.

Autre question qui s'est posée il y a quelques années par rapport au WHOIS détaillé. L'opérateur central a des données sur le DNS, sur le bureau d'enregistrement. Et ensuite il faut aller demander au bureaux d'enregistrement des informations sur le titulaire du nom de domaine. Et ça, c'est le système distribué.

Et il y a quelques années, l'idée c'était d'avoir tous ces systèmes séparés pour la demande, la requête. Donc le PDP voulait avoir toutes ces informations à un seul endroit. Mais, ce qui apparait avec la réglementation dans beaucoup de pays, c'est qu'il y a des restrictions pour le transfert de données transfrontalier.

Et le sentiment actuel c'est qu'on a les douanes en Australie qui conservent les données, et si vous opérez un registre en Allemagne ou dans un autre pays, vous conservez les données de votre client, si votre client est enregistré dans votre pays. Et ensuite vous divulguez les données par les voies conventionnelles et opportunes.

Donc ces deux choses pourraient aller à l'encontre de ce que fait l'EPDP. Donc j'aimerais savoir ce que pense le panel par rapport à ce qu'on doit faire par rapport au travail qui a été fait jusqu'à présent.

Est-ce qu'on a besoin d'une actualisation, d'une mise à jour, ou d'une nouvelle approche ?

ASHLEY HEINEMAN:

Je vais parler très brièvement parce que je pense que je ne suis pas la mieux placée pour y répondre.

Je voulais savoir, par rapport à l'équipe de révision des services d'anonymisation et d'enregistrement fiduciaire –j'en ai fait partie de cette équipe – je dirais que l'impact a été stoppé jusqu'à présent.

L'objectif c'était d'avoir accès à ces données, et les services d'anonymisation et d'enregistrement fiduciaire c'est une option disponible pour les données massives. Et il faut qu'il y ait des limites là aussi et des règles.

Donc si rien d'autre ne vient impacter ce travail, alors ce groupe de travail va certainement s'interrompre.

MILTON MUELLER:

Je ne vais pas répondre sur la première question, mais sur la deuxième, sur le WHOIS.

Je pense que le WHOIS détaillé ne sera plus nécessaire une fois que le RGPD sera pleinement mis en œuvre. Et qu'on a besoin que le RDAP soit remplacé... Non pardon le WHOIS détaillé sera remplacé par le RDAP. Et donc que les données soient gérées par les opérateurs de registre.

BRUCE TONKIN: Qu'est-ce que le RDAP ?

MILTON MUELLER : Le RDAP va donner lieu à une base de données fédérée où les gens pourront avoir accès sans avoir à le stocker dans deux endroits différents, à savoir l'opérateur de registre, et le bureau d'enregistrement. En tout cas c'est ainsi que je comprends les choses. Mais peut-être que je me trompe.

Mais je pense que la justification du WHOIS détaillé, c'est qu'au début ça simplifiait le transfert de domaines entre le bureau d'enregistrement et opérateur de registre. Mais il semblerait qu'on puisse le faire sans avoir à utiliser le WHOIS détaillé. Et également, le principe d'avoir à minimiser le transfert et la collecte de données qui semble impliquer des obligations de la part du bureau d'enregistrement et de l'opérateur de registre.

GREG AARON: Ce qu'on a vu dans notre expérience dans les deux derniers mois par rapport à la spécification temporaire, c'est que si le RGPD couvre une certaine partie des données, la spécification temporaire, elle, permet de couvrir des données qui ne sont pas couvertes par la loi.

Par exemple, le RGPD ne couvre pas les informations de ce qu'on appelle une personne morale. Ces données peuvent être rédigées au

titre de la spécification temporaire et ça permet de donner aux gens moins de données sur lesquelles travailler ;

Donc ce qu'a fait le SSAC, c'est qu'il faut rendre ces données disponibles, conformément aux lois, ça c'est très important, mais n'appliquez pas de manière excessive la loi.

Donc il faut l'appliquer, cette loi, mais pas outrepasser.

Donc, d'une certaine mesure, il y a des gens qui ne sont pas sujets au RGPD, et qui peuvent s'en prévaloir.

Par exemple, si je suis un individu et je dis moi je ne suis pas au RGPD, j'utilise un service d'enregistrement fiduciaire. Là il y a un chevauchement entre ces deux cas.

Je dois dire aussi que le SSAC a dit que les registres détaillés sont une bonne idée pour la sécurité et la stabilité et n'ont rien à voir, certains d'entre eux en tout cas n'ont rien à voir avec les dispositions des données.

Donc je ne suis pas d'accord avec ce qu'a dit Milton.

NICK WENBAN-SMITH:

Je pense que la question a à voir avec les spécifications temporaires. Nous allons voir si cela reste une politique permanente.

Donc, si les données des gens ne sont pas exposées dans le WHOIS, quelle est l'importance de la vie privée ? Beaucoup de personnes ont bénéficié de cette protection des données.

Il y a cependant toujours eu une demande pour ces services d'anonymisation et d'enregistrement fiduciaire. Beaucoup de personnes qui veulent lancer une nouvelle marque, ou qui veulent enregistrer un nouveau nom le font à travers ces services.

Donc je pense qu'au tout début, il y aura bien sûr ce genre de demandes. Mais il y aura aussi des demandes de moins haut niveau.

HADIA ELMINIAWI:

Je suis d'accord avec ce qui a été dit.

Je voudrais juste rajouter que tous ces fournisseurs de services légitimes qui peuvent et qui peuvent se permettre de donner, de divulguer certaines des données dans des circonstances spécifiques, là je ne suis pas sûre si nous avons besoin de ces services d'enregistrement fiduciaires.

BRUCE TONKIN:

Chris.

CHRIS LEWIS-EVANS:

Oui, ces services soulignent la question dont on parlait. Dans ces services, il n'y avait pas de façon uniforme de faire des demandes de données par rapport à ces services. Donc cela nous a amenés vers un montant de demandes qui est moindre. Donc je pense que la question a déjà été posée au niveau du nombre de requêtes ou de demandes.

Donc c'était la révision RDS2, et le groupe qui travaillait contre le hameçonnage, ils avaient indiqué qu'il y avait un manque de connaissances au niveau de l'accès et de l'obtention de l'accès.

Voilà donc la raison des problèmes que nous avons maintenant.

Pour toutes les personnes qui ne sont pas au courant de ce qu'il se passe par rapport au RGPS, nous ne voyons pas encore un impact complet par rapport aux spécifications temporaires. Donc pour l'instant, il n'est pas nécessaire de passer par là.

Donc il s'agit de créer les politiques en premier. Cela nous permettra d'avoir un accès uniforme, un modèle d'accès uniforme. Et donc cela nous donnera un bon modèle, un modèle juridique pour avoir l'accès aux données.

CYRUS NAMAZI:

Un commentaire sur la mise en œuvre de ces politiques d'enregistrement fiduciaire.

Je suis donc Cyrus, je fais partie du GDD à l'ICANN.

Je voudrais seulement clarifier quelque chose, en ce qu'il s'agit de la mise en œuvre des politiques par rapport au GDD.

Donc, nous n'avons rien arrêté. Surtout en ce qu'il s'agit du travail d'anonymisation et d'enregistrement fiduciaire.

Nous avons réalisé qu'en ce moment, il n'y a pas assez de clarification pour pouvoir mettre en œuvre un cadre de travail légal, juridique,

pour faire avancer ce modèle d'accréditation d'une façon qui serait justifiée, du moins en termes de travail efficace et applicable.

Il y a donc un manque de clarification sur le RGPD. On doit savoir comment faire face aux éléments qui sont inclus. Donc on ne sait pas de quoi va avoir l'air ce modèle d'accréditation.

Nous sommes dans une situation où le DoS n'est pas complètement réglé, on ne sait pas comment interpréter les implications du RGPD.

Nous essayons de temporiser le travail, et nous essayons donc de temporiser la vitesse avec laquelle les informations arrivent. Nous voulons donc pouvoir mettre en place quelque chose qui va changer dans un futur très proche.

Ce n'est pas limité au travail d'anonymisation et d'enregistrement fiduciaire, mais il s'agit aussi de l'implémentation du WHOIS détaillé. Les politiques ont été définies, ratifiées par le conseil d'administration il y a longtemps. Donc dans ce cas particulier, il s'agit opérateurs et des bureaux qui vont en arriver à un accord pour pouvoir gérer la situation entre eux. Donc c'est ce qu'on appelait le RAA.

Il y a d'autres programmes en cours. Nous en avons en fait 13 au sein de l'organisation qui sont liés à ces services d'enregistrement de données. Et certains de ces programmes vont être impactés, alors que nous apprenons à mieux comprendre le RGPD.

Donc tous les services qui sont liés au RDS vont peut-être avoir à changer dans l'avenir.

BRUCE TONKIN:

On ne peut pas vraiment parler du temps et des solutions parce qu'il faut laisser, il faut penser aux politiques qui ont été mises en place il y a à peu près 5 ans, peut-être même plus longtemps.

Donc je pense que le monde avance et les réglementations continuent à changer. Et elles changent depuis quelques années d'ailleurs ;

Je pense qu'en tant que communauté, qu'organisation, on doit être un peu plus agiles dans notre réponse vis-à-vis de ces changements.

Et par exemple le défi du WHOIS, en ce moment, est-ce que c'est la bonne chose à faire quand on pense au nouveau RGPD. On a l'impression que les efforts qui ont été faits vis-à-vis du PDP sont basés sur l'exactitude des exigences. On doit bien recevoir les données, on doit avoir des données qui sont exactes.

Et maintenant nous devons revenir vers les bases fondamentales, c'est-à-dire la façon avec laquelle on recueille les données.

Il y avait donc à l'époque, nous on avait donc étudié les transferts de toutes les informations. Si vous allez donc décrire quel était le motif en 2000, je pense qu'en tant que communauté, on peut se rendre compte qu'on n'avait pas les bonnes informations de suivi pour définir ce motif ou ce but.

Alors, il s'agit d'une discussion sur l'accès, et je pense que quand on parle du WHOIS, on sait très bien que maintenant on peut faire la

même chose, mais sans avoir à centraliser ou stocker de façon centralisée toutes les informations.

CYRUS NAMAZI:

Merci Bruce, vous avez souligné un des éléments de changement, changement de cet environnement qui change.

Comme vous le savez, nous sommes dans la phase de mise en œuvre du RDAP qui est une plateforme complètement différente du protocole du WHOIS préalable.

Cela a permis de nous poser la question que vous avez soulignée : où est-ce que l'on stocke les données ?

Et avec le RDAP, on arrive donc à une plateforme qui correspond au 21^{ème} siècle, une plateforme qu'on peut échelonner, une plateforme qui nous donne, disons, un écosystème dynamique à travers le globe. Cela nous permet d'avoir un système de services de données qui peut être ponctuel, avec les temps qui changent.

BRUCE TONKIN:

Vous pouvez venir au micro numéro 1 S'il vous plaît ?

VOLKER GREIMANN:

Je voudrais revenir sur ce que je considère, la distinction entre les entités juridiques et les personnes titulaires de noms de domaine.

Les spécifications temporaires ne devraient pas vraiment trop protéger, il faut vraiment comprendre ce que le RGPD protège. Cela ne

protège pas les données personnelles, cela protège aussi ces données qui sont incluses dans les données qui sont fournies par les entités légales.

Donc si une compagnie fournit les données personnelles d'un de leurs employés, avec leur email, le numéro de téléphone, cela correspond à des données personnelles. On ne peut pas faire cette distinction en tant que bureau d'enregistrement. Mais ces données doivent être protégées de la même façon que les données personnelles le seraient.

Donc, ces informations sont donc inutiles pour la détermination de la protection de telle ou telle donnée.

DEAN MARKS:

Je voudrais revenir en arrière sur ce que M. Monti a dit tout à l'heure à propos du RGPD qui correspond à des réglementations qui sont déjà en place depuis longtemps.

En respect des enregistrements fiduciaires et de l'anonymisation, en 2016 quand on parlait déjà du RGPD, il y avait déjà des inquiétudes sur les lois correspondant à la vie privée.

On ne savait pas si le RGPD allait être mis en œuvre.

Donc je ne sais pas pourquoi il y a eu une pause pour obtenir de la clarification. Je ne sais pas si tout le monde dans cette salle est d'accord, mais le RGPD n'amène aucune clarification, sur tous les détails.

Ce processus multipartite est donc un bon endroit dans lequel nous pouvons trouver un équilibre. Et nous avons déjà un équilibre par rapport au PDP des services d'anonymisation et d'enregistrement fiduciaire. Ça avait été approuvé par le conseil de la GNSO et par le conseil d'administration de l'ICANN.

C'est un très bon pas en avant pour en arriver à cet équilibre.

Quand est-ce qu'on va en arriver à cette clarté ? Et je pense que ça peut se faire si on continue avec ces services. La communauté multipartite pourra ainsi aider à mettre en place cette clarté.

Donc je pense qu'il faudrait appliquer ces services à tout ce modèle multipartite.

BRUCE TONKIN:

Est-ce que vous pouvez donner des exemples des obstacles auxquels vous faisiez face pour mettre en œuvre cela ?

CYRUS NAMAZI:

Oui. Dean, j'apprécie vraiment ce que vous venez de dire et je voudrais ajouter un point de clarification. Nous n'avons pas arrêté le travail d'élaboration de politique car nous travaillons dessus avec vous depuis quelque temps.

Ce n'est même pas une question, à mon avis, de la pertinence des politiques. C'est à la communauté de décider cela. Cela a à voir avec un bon cadre de travail juridique pour mettre les choses en œuvre.

Nous avons d'ailleurs des accords en place. Et en ce moment, il s'agit des choses dont nous ne sommes pas vraiment conscients, ce cadre de travail juridique qui est nécessaire pour le mettre en œuvre. Ça n'a rien à voir avec le reste.

Je pense qu'il n'y a pas de besoin de services d'anonymisation et d'enregistrement fiduciaire, après ce monde, ce nouveau monde RGPD. Mais ce n'est pas à nous de décider.

SEBASTIEN BACHOLLET:

Je vais parler en français. Vous allez dire comme d'habitude.

La question de savoir est-ce qu'il y a une différence entre les personnes physiques et les personnes morales, je suis encore étonné qu'on revienne sur.

Mais oui, il y a une différence. Moi, personne physique, j'ai un nom et une adresse mail. Et si j'ai besoin de mettre ces informations, bah j'en ai qu'une.

Une personne morale, une entreprise, elle peut décider de ce qu'elle met comme information. Et il serait intelligent qu'elle ne mette pas des informations personnelles dedans. Mais c'est son choix à elle.

Donc il y a une vraie différence. Il faut protéger les personnes physiques, les personnes morales peuvent s'organiser pour qu'il n'y ait pas d'informations sensibles dans les WHOIS qu'ils mettent.

Et ça permet que nous puissions accéder à ces informations, ce qui est normal pour des personnes morales.

Merci.

NON IDENTIFIE: Je suis tout à fait d'accord avec Sébastien. On a qu'à lire le texte de la régulation, et vous allez tout de suite comprendre. Il n'y a pas à interpréter le texte.

PETER KIMPIAN: Bonjour à tous. Peter, je viens du Conseil de l'Europe. Je vais être bref aujourd'hui.

Nous avons publié un guide sur la confidentialité des données. Nous attendons donc les opinions du EPDP.

Mais donc tous les membres de l'Union Européenne et les États membres participent. Et d'autres parties telles que la Fédération Russe, la Turquie, le Mexique, et certains pays d'Afrique y participent.

Donc il y a quelques indications et une compréhension commune sur ce sujet. Merci beaucoup.

BRUCE TONKIN: Y a-t-il des commentaires ? Il y a d'autres questions ?

Moi-même j'ai une question. On a couvert cela d'ailleurs. Mais nous devons parler de la conformité des solutions vis-à-vis des lois sur la vie privée. Nous avons bien sûr couvert cela, mais nous avons aussi une discussion avec l'audience, d'exemples qui pourraient nous amener sur d'autres sujets.

Donc est-ce qu'il y aurait d'autres commentaires sur la façon d'obtenir une solution opportune ? Comment est-ce que la communauté peut nous aider dans ce processus pour que l'on soit plus efficace ?

FLIP PETILLION:

Oui, il faut absolument augmenter la prise de conscience. Les gens qui partagent les données vont nous aider vraiment pour aller de l'avant dans la discussion.

Nous avons eu une réunion avec Goran, et il a dit quelque chose de très intéressant. Il disait : j'aurais aimé qu'on adresse ce problème il y a bien longtemps. C'est vrai. Mais voilà, ce sont les faits, il faut vivre avec.

Mais cela m'a fait pensé à l'avenir. Et je voudrais lancer une idée. Je voudrais penser un peu dans sa direction. La façon dont il pensait lui. Et voir ce qui nous manque maintenant. Peut-être aurons-nous de nouveaux éléments dans l'avenir quand il s'agit de l'accès, en supposant que nous aurons accès, en supposant que nous solutionnions cet accès. Cela veut dire que nous allons avoir à prendre plus de responsabilités dans l'avenir.

Vous savez, pendant 20 ans, nous avons eu un système UDRP qui a très bien fonctionné, qui protégeait les titulaires de droits, les droits de marques.

Il y a une solution et une inquiétude. S'il y a d'autres inquiétudes que nous devrions adresser, dans lesquelles nous aurions à suivre les mêmes approches dans l'avenir.

Donc l'inquiétude devrait être sur les dangers que pourraient causer tout cela vis-à-vis des enfants, vis-à-vis des gens en général.

Donc je préfère aujourd'hui recevoir un petit peu plus d'hameçonnage, mais tout en sachant qu'on pourrait combattre donc l'usurpation dans le EPDP.

ASHLEY HEINEMAN:

Représentant le GAC, je pense que cette conversation sur le fait qu'on ne devrait pas être distraits par d'autres choses – bien sûr il y a des domaines dans lesquels on ne pourrait pas être distrait – mais cela nous permet de faire les choses de façon opportune. Il ne faut pas se limiter au EPDP.

Je pense que de la part du GAC, nous soutenons ce modèle d'accès uniforme et cette conversation. Et nous apprécions vraiment que cette conversation ait eu lieu.

Cela nous permet de commencer notre processus de réflexion si vous voulez. Cela nous donne l'opportunité aussi de commencer à identifier les réponses aux questions.

Ça ne veut pas dire qu'on a commencé un développement technique ou quelque chose de ce genre, cela viendra bien sûr. Mais recevoir les questions comme les questions que nous avons reçues, par exemple de la part du conseil du RGPD, cela nous aide à aller de l'avant.

Et, encore une fois, il ne faut pas caractériser cet accès, ce modèle d'accès uniforme. Je pense qu'il y a des façons efficaces pour

commencer une conversation et dépasser les obstacles que nous avons devant nous.

CRISTINA MONTI:

Oui, très brièvement, je voulais insister – et c’est une suggestion – que pour moi le plus important pour avancer, c’est d’avoir un accord clair et être transparent par rapport aux différentes activités portant sur le processus et portant sur WHOIS et leurs objectifs fondamentaux.

Ça, c’est la base.

Et une fois qu’on aura cet accord sur les différentes activités en termes de processus, alors ce sera beaucoup plus simple de pouvoir traiter les autres aspects.

Et il faut également faire en sorte que ces activités portant sur les processus soient distinctes. Parce que peut-être qu’il y a des fondements juridiques différents qui s’appliqueront à chacun.

Donc Il faut être sûr qu’on avance dans la bonne direction. Voilà la suggestion que je voulais faire.

BRUCE TONKIN:

Merci.

GREG AARON:

Oui, c’est important de penser à l’avenir. On en est à la situation actuelle parce qu’on n’a pas suffisamment pensé à l’avenir. Donc penser à l’avenir c’est important.

Le groupe EPDP travaille d'arrache-pied sur des questions extrêmement complexes et difficiles. Et c'est probablement un bon moment pour que la GNSO et pour que l'organisation dans son ensemble, pense à ce qu'il va se passer en 2019, parce que la spécification temporaire va toucher à sa fin, à un moment donné.

Et, on va voir après le travail très dur de cet EPDP, les résultats que ça va donner.

Donc assurons-nous ensuite que le travail se poursuit et que les gens qui travaillent ont les ressources suffisantes pour l'achever ce travail.

HADIA ELMINIAWI:

Oui, en tant que membre ALAC, je pense que notre principale préoccupation, en tout cas notre principal intérêt, c'est de faire en sorte que l'internet continue d'être un espace sûr pour tous.

Détecter, prévenir la fraude, l'utilisation malveillante du DNS, voilà des choses qui nous semblent très importantes.

Cela étant dit, je dirais aussi qu'il est très important de regarder maintenant les processus normalisés de l'industrie et les services d'accréditation. Parce qu'on se demande combien de temps il va falloir attendre pour avoir quelque chose qui puisse être mis en œuvre et qui soit pratique et viable.

BRUCE TONKIN:

Il y a une question dans la salle ? Micro numéro1.

RUDY DANIEL: Bonjour. Je suis boursier de cette réunion ICANN63. J'ai une question.

Le RGPD, est-ce que le RGPD a mandaté l'ICANN et sa communauté à faire le ménage un petit peu par rapport au WHOIS et à mettre en place une méthodologie d'accès par rapport aux lois en vigueur et par rapport à l'avenir, étant donné que l'IPv6 est de plus en plus déployé et adopté ?

BRUCE TONKIN: Qui souhaite répondre ? Merci d'ailleurs à un boursier de s'être levé et d'avoir posé une question.

MILTON MUELLER: Oui, effectivement, le RGPD a forcé l'ICANN à faire un petit peu de ménage chez lui.

Vous avez raison, effectivement, on n'a pas su anticiper ce qui allait se passer, et regarder vers l'avenir. Ça fait maintenant 50 ans que certaines personnes nous disent que le WHOIS n'est pas juridiquement licite, conformément à la loi sur la protection des données. Et on n'a pas suffisamment prêté attention à cet avertissement.

Donc c'est plus politique, ça n'est pas forcément uniquement dû à une absence de prévision. Et le RGPD nous a obligés à revoir tout ça et à faire le ménage.

Donc une manière de voir le futur, l'avenir, et je suis tout à fait d'accord avec Madame Monti, la première chose à faire c'est identifier les objectifs et les données à collecter nécessaires pour réaliser cet objectif ;

Ensuite, quels éléments de ces données vont être diffusés publiquement et quelles sont les données qui ne vont pas l'être. Travailler sur l'accès, ça viendra ensuite.

Ce n'est pas forcément la tentative de Goran et du PDG d'explorer les questions juridiques pour voir si l'accès universel, ça sert de distraction ou si c'est prématuré. Non.

On ne sait pas vraiment ce que fera le modèle tant qu'on n'aura pas fait ce premier travail.

Donc je pense que la première discussion qu'on a eue sur cet accès unifié, c'est parce que ça a donné l'impression à certains que ce modèle universel ça allait permettre aux gens d'être accrédités. Et ça nous a distrait un petit peu, ça a distraie l'attention des gens de se concentrer sur le WHOIS tel qu'on l'a maintenant plutôt que de penser : comment je vais avoir accès et ne pas se préoccuper du WHOIS tel qu'il est actuellement.

RUDY DANIEL:

Je me demandais simplement si l'accès universel c'était finalement une solution temporaire ?

MILTON MUELLER: Oui, effectivement, d'un point de vu juridique, technique, politique, c'est compliqué.

Et je pense que c'est la principale justification qui a donné lieu à cette discussion. Ça ne doit pas être une solution temporaire, ça doit être compliqué.

Et Goran est en train d'essayer d'initier, de lancer ce genre de discussion. Mais en même temps, il essaye de pousser ces discussions dans une direction qui n'est peut-être pas la bonne.

Donc il faut essayer de repousser cette discussion sur l'accès universel jusqu'à ce qu'on ait résolu la première partie du problème.

Et une fois encore, ça devrait être rapide.

HADIA ELMINIAWI: Il ne s'agit pas de savoir si c'est une solution temporaire et rapide ou pas. Il faut résoudre tous les problèmes, c'est tout.

BRUCE TONKIN: Merci. J'aimerais remercier tous les membres du panel, parce qu'on a eu une discussion très constructive, on s'est posé les uns les autres des questions, on a commencé par les premières discussions, et on a vite compris quels étaient les enjeux, les problèmes. Et ça c'est un pas en avant positif.

Je pense qu'on a entendu clairement qu'on ne va pas revenir vers l'ancien WHOIS.

Et le concept qu'il faut retenir, c'est parvenir à un équilibre entre la protection des sujets de données et le fait de fournir un accès aux utilisateurs légitimes.

Donc merci à tous de votre participation. On attend avec impatience des résultats, on l'espère couronnés de succès, de l'EPDP.

Merci.

[FIN DE LA TRANSCRIPTION]