
BARCELONE – HLGM : Problématiques thématiques au sein de l'écosystème de la gouvernance de l'Internet :
cybercriminalité, protection des données/vie privée
Lundi 22 octobre 2018 – 12h15 à 13h30 CEST
ICANN63 | Barcelone, Espagne

FRANCISCO POLO : La deuxième séance va commencer d'ici très peu. Il n'y aura pas de pause-café. Nous vous avons pris un peu de retard et donc nous allons commencer notre travail dès maintenant. Merci.

Bienvenue. Nous sommes de retour de la pause-café. Nous passons à la deuxième partie de notre discussion. Dans cette partie, nous allons parler d'un sujet très intéressant, le cyber délit, la vie privée et la protection des données.

Notamment, nous allons parler des moyens dont nous disposons pour répondre à ces difficultés, ainsi que des moyens dont disposent les gouvernements pour lutter contre le cyber délit. Nous allons également parler des droits de l'homme dans un environnement où il y a de plus en plus de lois régionales et nationales. Je vais donner donc la parole au modérateur de ce panel. C'est un plaisir de donner la parole à Awa, présidente du Data Protection Act.

AWA N'DIAYE : Je vais, avec votre permission, parler en français, et nous allons, sans plus tarder, commencer notre session après avoir remercié,

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.

évidemment, le gouvernement espagnol et l'ICANN pour cette session de haut niveau.

Nous allons revenir, si je puis dire, parce qu'elle a été quelquefois assez largement abordée, à une question véritablement brûlante, une question très actuelle. Et cette question actuelle, certains en ont parlé déjà dans la précédente session, c'est le problème de la sécurité et de l'intégrité de l'Internet par rapport à la cybercriminalité.

ICANN, nous le savons, est le garant technique, le bras technique de cette sécurité et fait déjà un travail remarquable. Ce travail remarquable qui garantit la stabilité, l'ouverture et l'intégrité de l'Internet, malheureusement, n'est pas suffisant pour empêcher les dérives de toutes sortes et les menaces qui pèsent sur l'Internet. Cependant, nous allons d'abord commencer et demander à M. John Crain, qui est le responsable de la sécurité d'ICANN de revenir rapidement sur la gouvernance de l'ICANN. Il est le responsable des problèmes de sécurité et de résilience et donc il est une des chevilles ouvrières de l'ICANN qui maintient la stabilité d'un Internet ouvert, accessible et sécurisé.

Nous allons voir dans quelle mesure cet Internet-là peut être maintenu et conforté.

M. John Crain, vous avez la parole.

JOHN CRAIN :

Merci beaucoup. Merci à tous de me donner cette possibilité de

m'adresser à vous. Je vais vous parler un petit peu, de manière philosophique presque, sur la technologie et sur les principes à partir desquels l'Internet est conçu. L'Internet, ou l'ARPANET comme on l'appelait avant, est souvent décrit comme étant quelque chose de révolutionnaire et ça l'est, car c'est la façon dont fonctionne notre société. Il est fondé sur des principes établis par Jon Postel, que l'on appelle les lois de Jon Postel, établis en 1999. Les principes, c'est soit libre en ce que tu acceptes et conservateur en ce que tu envoies. Ce sont les principes qui ont été utilisés pour le développement des protocoles Internet.

Une grande partie la croissance de l'Internet est rattachée à ces principes, y compris les principes d'ouverture et de transparence. Ces technologies, ces premières technologies, ces premiers protocoles ont fait en sorte que le système fonctionne.

Le WHOIS dont vous avez entendu parler probablement faisait partie de ces premiers protocoles, et c'était une partie intégrante des éléments qui ont contribué à créer ce réseau pour résoudre les problèmes opérationnels.

Le WHOIS, au fil des années, a évolué pour pouvoir servir aux intérêts des différentes parties prenantes, comme les bureaux d'enregistrement de noms de domaine, les forces de l'ordre, les propriétés intellectuelles, les marques déposées et les individus. Mais le principe fondamental du protocole WHOIS reste le même.

Le fonctionnement stable de l'Internet est basé sur un concept très

simple. Vous ne pouvez pas faire fonctionner un système décentralisé — c'est l'Internet, un réseau de réseaux — si vous ne trouvez pas des gens qui puissent coordonner ces différentes parties et qui puissent coordonner les réponses à des problèmes rencontrés.

Lorsqu'il y a des abus ou des problèmes de sécurité, l'accès aux données est fondamental pour savoir qui est responsable de quoi et pour pouvoir restaurer le fonctionnement stable et sécurisé de l'Internet. Et cela a trait aux principes opérationnels de l'Internet. Un exemple de cela est, par exemple, le fait d'informer quelqu'un qu'un site Web a été compromis avec des contenus malveillants. Et donc il faut dire au fournisseur qu'il faut résoudre ce problème.

Mais l'Internet n'est pas seulement révolutionnaire, c'est aussi évolutionnaire, car il change. Il évolue et il s'adapte aux besoins des utilisateurs et de la société. L'Internet reflète, à bien des égards, les utilisateurs de la société qui s'en sert.

Les principes ont changé au fil du temps. Un des principes directeurs aujourd'hui, c'est, bien entendu, la sécurité. Et un exemple de la technologie, c'est ce qu'on appelle HTTPS. Ce système a été développé en 1999, il y a moins de vingt ans.

Cette technologie nous permet de chiffrer le trafic du Web, et c'est l'un des éléments essentiels derrière l'économie numérique, car sans ce chiffrement il est très difficile de pouvoir acheter des produits en ligne.

Au fil des années, la technologie a évolué pour adopter d'autres

principes. Un de ces principes, c'est la vie privée. Il est très connecté à la sécurité à bien des égards. Un exemple évident de cela dont vous avez probablement entendu parler, c'est le Règlement général européen sur la protection des données et la spécification temporaire qui a été développée à l'ICANN et sur laquelle travaille la communauté pour arriver à une solution plus stable. Et tout cela pousse le changement technologique. On voit le protocole WHOIS qui doit s'adapter et qui va vers le RDAP, le protocole RDAP. Ce sont des changements technologiques qui permettent de renforcer la protection des données et la vie privée, et qui adaptent donc ces principes pour qu'ils soient au service de la technologie Internet.

Cela est normal. Cela fait partie de l'évolution de la technologie. Le RDAP est en cours depuis plusieurs années. Ce n'est pas le RGPD qui l'a fait voir le jour, mais plutôt des questions ou des problèmes en matière de sécurité qui ont précédé le RGPD. Et c'est une progression normale.

Nous parlons beaucoup, aujourd'hui, de savoir comment nous, en tant que communauté, pouvons travailler ensemble pour répondre aux difficultés que posent ces changements technologiques. Il faut trouver un équilibre entre les différents principes qui parfois sont concurrents, sur lesquels est bâtie l'architecture de l'Internet.

Nous savons qu'il y a l'ouverture, mais il y a aussi la sécurité, la vie privée, et nous devons, en tant que communauté, nous devons travailler au nom de tous ceux qui utilisent Internet.

Maintenant je vais vous dire merci. Je vais passer la parole au modérateur. Merci beaucoup.

AWA N'DIAYE :

Voilà donc poser les bases mêmes de l'architecture de l'organisation ICANN. Vous avez parlé d'accès aux données et, à ce moment-là, le mot est dit : sécurité, oui, mais comment.

Comment préserver cette sécurité ? Comment la garantir ? Il faut forcément ouvrir pour pouvoir sécuriser.

À ce moment-là, nous allons nous tourner vers un de nos experts qui va apporter une autre perspective. C'est justement la perspective de la protection des données, protection légale des données, protection de la vie privée, qui apporte une perspective éthique, une perspective de droits inaliénables au problème que nous nous posons.

M. Enrique Factor, qui est le représentant donc de l'agence pour la protection de données personnelles de l'Espagne, vous avez la parole.

ENRIQUE FACTOR :

Merci, Madame. J'aimerais remercier l'ICANN et le gouvernement de l'Espagne de m'avoir donné l'occasion de participer à ce forum.

Messieurs, dames, chers délégués, je m'appelle Enrique Factor. Je travaille pour l'agence espagnole de protection de données, qui est l'agence nationale chargée de la protection de données. Elle fait partie

du Conseil européen de protection de données.

Mon travail consiste à protéger les droits de l'homme, plus spécifiquement, celui établi dans l'article 12 de la Déclaration universelle des droits de l'homme, qui est très similaire à celui établi dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne et l'article 18 de la Constitution de l'Espagne. Il s'agit du droit que nous avons tous à protéger notre vie privée.

Nous sommes tous d'accord pour dire que, aujourd'hui, tout est « donnée ». En fait, nous, nous sommes des données. Et les données qui nous définissent en tant qu'êtres humains sont ce que nous appelons les données à caractère personnel. Nous devons protéger les droits fondamentaux. Les forces de l'ordre s'en chargent. Mais qu'est-ce qui se passe dans le cyberspace ?

Dans le monde des ordinateurs, les agences d'application de la loi et les autorités de protection de données travaillent ensemble pour défendre nos droits.

Dans l'Union européenne, la vie privée et la protection des données ne sont pas des droits absolus. Ils sont limités à certaines conditions. Conformément à la Charte de l'Union européenne sur les droits fondamentaux. Le droit à la vie privée, la protection des données peuvent avoir besoin d'être confrontés à d'autres droits de l'homme comme les droits fondamentaux à la liberté d'expression, la liberté d'accès à l'information. Le droit à la vie privée et à la protection des données doit être considéré à la lumière d'autres intérêts en matière

de politiques publiques, la sécurité nationale.

Les membres de la communauté européenne souhaitent renforcer la coopération sur des affaires criminelles dans le domaine de la liberté, la justice. Nous faisons cela à travers des mécanismes, à travers des groupes de coordination et à travers des bases de données partagées, comme l'information — différents noms de bases de données — et avec l'Europol. Le cyber délit n'est pas seulement contrôlé à travers ces bases de données. Il y en a d'autres, comme le WHOIS qui est un élément essentiel pour combattre le cyber crime. Mais tous ces éléments doivent être conformes à la loi.

Nous nous battons tous pour défendre nos droits, mais cela ne peut pas se faire au détriment de la loi. Merci beaucoup.

AWA N'DIAYE :

Merci beaucoup, M. Factor. Donc, respecter les libertés individuelles, respecter les droits humains, respecter la loi qui protège les libertés individuelles, vous allez me dire, c'est ce que nous avons de plus précieux. Et c'est certainement le droit le plus inaliénable.

Cependant, il y a également une autre perspective qui est tout aussi précieuse, vous l'avez dit, M. Factor, c'est la sécurité publique. Comment faire pour prévenir et réprimer la cybercriminalité ? Comment faire pour ne pas porter atteinte à l'intégrité des informations ? Comment faire pour faire face à cette nouvelle délinquance ? Comment garantir la sécurité publique et la

coopération entre les États en matière d'investigation et d'échanges d'informations ?

Pour nous éclairer, nous avons un enquêteur hors pair, reconnu, trente ans d'expérience, chef du Centre européen de la cybercriminalité et qui est responsable d'un groupe de travail au sein de l'Union européenne qui définit les stratégies de menaces et les tendances dans ce cadre-là, M. Wilson, vous avez la parole.

STEVEN WILSON :

Merci, messieurs, dames, Monsieur le représentant du ministre de l'Espagne. Je remercie l'ICANN de m'avoir invité à parler à cette conférence. Je dois d'abord m'excuser. Mon collègue Tim Morris d'Interpol était censé être avec nous. Mais malheureusement, il a dû rester chez lui pour des questions très importantes relatives à l'Interpol.

Je ne suis pas expert technique parce que j'ai un personnel qui s'occupe de ce type de choses, mais j'ai un point de vue très stratégique du point de vue de l'Interpol, de l'application de la loi et l'impact du WHOIS sur notre travail et sur la sécurité publique. En fin de compte, l'intérêt public, la sécurité publique, ce sont des questions très importantes, et comment pouvons-nous nous assurer que l'Internet est sécurisé.

Tout d'abord, en ce qui concerne l'ECC, mon organisation, la cybercriminalité dans en Europe, nous avons donc plus de 200

enquêtes par an donc, en termes de paiement, de fraude relative au paiement dans le système bancaire. Il y a également le problème de l'exploitation des enfants avec la pédopornographie. Nous travaillons de près avec nos collègues. Nous avons également une unité d'investigation du Dark Net, et à Interpol, il y a également les problèmes de terrorisme, de traite des êtres humains.

Et la réalité, c'est que la cybercriminalité n'est pas uniquement affectée par le WHOIS. Toutes ces enquêtes sont affectées par le WHOIS. Donc ce dont on parle, et je remercie Enrique pour ses commentaires relatifs au droit privé, la protection des données et de la vie privée, c'est vraiment quelque chose de clé. C'est un droit fondamental.

L'Internet doit être un lieu sécurisé pour tous. Mais il faut également faire l'équilibre entre ceci et la victime de l'exploitation sexuelle des enfants, l'exploitation des personnes en ligne. Et donc, cet équilibre est difficile à trouver parfois.

Je crois qu'il est très important d'indiquer que, au niveau de l'application de la loi, notre intérêt cible les groupes criminels et les groupes terroristes. Si l'on considère le RGPD, il y a des principes fondamentaux très importants qui permettent de protéger nos données, et nous sommes moins en danger grâce à cette loi, mais il y a une conséquence pour les agents d'application de la loi. Elle a un impact sur les agents d'application de la loi et sur la sécurité publique. L'effet pratique n'est pas uniquement en lien avec la cybercriminalité,

mais également en lien avec le terrorisme, les abus d'enfants et les problèmes de blanchiment d'argent.

Le WHOIS est un point de départ pour beaucoup de nos enquêtes. L'idée de mettre en lien ceci avec les moyens est très importante ; identifier les liens- les enquêtes mondiales doivent être faites dans le respect des lois nationales. Le WHOIS a été vital dans ce domaine.

J'aimerais vous présenter en contexte certains exemples de nos travaux. Dans le domaine des abus d'enfants, cette année, il y avait un groupe pédophile organisé qui vendait l'accès à des sites pornographiques sur l'Internet. Nous avons rassemblé tous les noms de domaine reliés à ceci et ceci a été fondamental. Donc le croisement des données nous a permis d'y arriver, mais malheureusement, nous avons fait des erreurs. Ils ont fait des erreurs et c'est comme ceci que nous avons pu les attraper.

Deuxièmement, donc, Daesh, le réseau terroriste, nous avons pu éliminer un domaine qui distribuait des supports extrémistes et qui recrutait des militants pour cette organisation grâce à l'accès aux bases de données. Ceci a été fondamental pour la réussite de notre opération. Encore une fois, l'opération Avalanche, il y a quelques années.

Donc la cybercriminalité, c'est un réseau énorme mondial ; plus de 800 000 domaines compromis sont enregistrés. Il y a un groupe de personnes au premier niveau qui font partie de ce groupe.

Nous avons des investigations au niveau local. Nous essayons de comprendre exactement ce qui se passe.

Messieurs, dames, à l'avenir, selon moi, c'est un accès unifié, un modèle d'accès unifié. Ceci est fondamental dans notre travail d'interface d'utilisateur unique.

Interpol et Europol travaillent ensemble pour fournir les services que nous pouvons fournir. L'idée c'est de pouvoir attraper ces personnes. Les criminels n'ont pas de règles. Nous devons mettre en place des règles qui nous permettent de les empêcher de faire ce qu'ils souhaitent faire. Nous devons nous assurer que les bases de l'Internet sont maintenues. Je crois qu'il est extrêmement important de travailler ensemble pour avoir accès à cette base de données parce que l'intérêt public est la première considération. Merci beaucoup.

AWA N'DIAYE :

Je pense que tous les gouvernements ici présents, tous les gouvernements membres du GAC s'accordent sur l'importance de protéger les données personnelles et la vie privée de leurs citoyens. Mais tous, à mon avis, sont tout autant préoccupés par l'explosion des crimes sur l'écosystème numérique.

Comment mettre un terme à cela ? Quelle solution trouver et qui, quels sont les acteurs à mettre au-devant de la scène. Comment faire pour que, au niveau de nos États, on puisse réduire les débats citoyens qui explosent de toutes parts contre la diabolisation d'Internet, parce

qu'on a voulu réprimer les crimes contre l'intrusion dans la vie privée, parce qu'on a voulu être garant de la sécurité publique contre ce que nous appelons maintenant la surveillance de masse et que nous ressentons comme une intrusion dans nos libertés ? Comment faire ? Quelles solutions préconiser ?

Nous avons beaucoup parlé depuis ce matin de ce défi majeur qui est vraiment de s'unir, d'unir toutes les composantes de l'ICANN autour de ce que nous appelons l'avenir de l'Internet. Cet avenir-là, comment le bâtir ?

Nous avons avec nous un monsieur qui est à la fois diplomate de carrière, acteur de la société civile et entrepreneur technologique, donc un technicien, directeur exécutif et cofondateur des réseaux Internet et juridictions Policy Network Jurisdiction depuis 2012. Il a donc une expérience très diversifiée, cette expérience que justement l'ICANN appelle de tous ses vœux dans une symbiose multipartite pour nous permettre d'arriver à des solutions concernées et inclusives. M. de la Chapelle, M. Bertrand de la Chapelle, nous allons vous écouter. Vous allez peut-être nous apporter une solution globale de ce problème. Et ensuite, nous écouterons les différents pays pour avoir évidemment leurs remarques, leurs attentes et peut-être leur questionnement. M. de la Chapelle, vous avez la parole.

BERTRAND DE LA CHAPELLE : Merci beaucoup. Je suis très heureux d'être ici avec vous. J'en connais certains d'entre vous.

Alors rapidement, j'aimerais vous faire part de quelques points principaux. Les trois interventions qui m'ont précédé ont bien souligné les enjeux auxquels nous sommes confrontés, à savoir harmoniser trois objectifs, protéger les utilisateurs en respectant les nouveaux processus et les droits de l'homme et, en même temps, nous assurer que le développement de l'économie numérique n'est pas mis en risque. Ce sont des enjeux majeurs. Et comme j'ai dit, il faut trouver, il faut les harmoniser et non pas trouver un équilibre. Parce qu'on parle d'équilibre, et on a l'impression qu'on est en train de sacrifier les uns au détriment des autres.

La deuxième idée par rapport aux débats autour du WHOIS est une illustration de cette tension entre les trois dimensions et un exemple également des discussions qui se tiennent à l'ICANN.

Le troisième point que je voulais évoquer. Quand on parle du niveau technique du DNS, il y a un danger, à savoir celui de voir le DNS comme le dernier outil pour résoudre tous les problèmes. Et il faut bien distinguer le rôle des opérateurs Internet, le rôle qu'ils peuvent avoir dans les différentes dimensions.

Quand on parle de sécurité, de stabilité et des abus à la sécurité, comme par exemple l'hameçonnage, les logiciels malveillants, etc., il faut renforcer donc la coopération entre les acteurs pour lutter contre cette cybercriminalité. Autrement, lorsque l'on se bat contre les contenus malveillants, la couche DNS n'est pas l'outil approprié. Parce que lorsqu'on retire un nom de domaine, cela a un impact global et

peut souvent porter préjudice au niveau local.

Il y a des situations exceptionnelles qui doivent être corrigées où un nom de domaine est bien retiré à cause de contenus qui atteignent certains niveaux de malveillance. Et ensuite, ce qui est important, et j'ai fait partie du Ministère des affaires étrangères de France, l'exercice de la souveraineté dans l'ère digitale est confronté à de nouvelles difficultés. Pourquoi ? Parce que les décisions qui sont prises par un pays, au niveau national, peuvent avoir des répercussions sur le territoire d'un autre pays. Il est très important que, lorsque les lois sont développées, créées, les répercussions que ces lois peuvent avoir sur d'autres territoires doivent être prises en compte. Et cela nécessite une communication, une coopération entre les différents éléments.

Et qui plus est, les décisions qui sont prises nous ramènent au premier point que j'ai évoqué. Les décisions qui sont prises dans un silo en particulier ou dans une organisation internationale ou par rapport à un sous-thème en particulier du haut niveau technique ou sécuritaire, tout cela a un impact sur d'autres dimensions. Et trouver donc cette harmonisation dont je vous ai parlé est notre menace sous-jacente.

Pour finir, cette notion de permettre la coopération numérique, la coopération digitale, doit être considérée à partir de plusieurs domaines, plusieurs dimensions. Et l'institution que j'ai fondée a trois programmes dont un est lié directement à l'espace des noms de domaine, mais les deux autres programmes sont liés à l'accès transfrontalier à des pièces à conviction, ce qui constitue un défi

majeur. Et les gens de la communauté d'Internet peuvent ne pas être au courant qu'il y a des discussions en cours par rapport à cette question et qui peuvent avoir un impact sur nous. Par exemple, la proposition de l'Union européenne sur les pièces à conviction transfrontalière. Cela peut avoir un effet sur la vie privée.

Une autre dimension que vous connaissez peut-être, c'est de savoir dans quelles conditions il peut y avoir une demande transfrontalière de pièces à conviction dans une plateforme internationale. Par exemple, Facebook, etc., et ensuite, dans quelles conditions il est approprié de retirer un nom de domaine parce que les activités dans ce nom de domaine sont illégales.

Voilà les domaines sur lesquels je travaille. Je crois que, de manière fondamentale, le grand enjeu, c'est de voir quelle est la société numérique que nous voulons construire, comment pouvons-nous coopérer pour mettre en place des normes, comment nous les mettons en place, et comment nous attribuons les différents aspects de ce domaine.

AWA N'DIAYE :

Merci, M. de la Chapelle. On le voit donc le grand enjeu de ce problème. Le grand enjeu auquel nous sommes tous confrontés ne pourra pas se résoudre sans les États. Nous attendons donc des États qui vont prendre la parole qu'ils apportent des contributions, vu leur rôle critique dans cette gouvernance d'Internet.

Nous allons commencer tout de suite par l'Ouganda, l'honorable Frank Tumwebaze, Ministre de l'information et de la communication et de la technologie. Vous avez la parole.

FRANK TUMWEBAZE :

Madame la Présidente, chers délégués. Je voudrais d'abord remercier le gouvernement d'Espagne et l'ICANN de nous avoir donné quelques minutes pour présenter notre point de vue de la part du Ministre des TIC. Cette opportunité est la bienvenue du point de vue des gouvernements et dans le cadre de cette réunion de haut niveau pour parler des questions critiques.

L'Ouganda fait partie du GAC à l'ICANN depuis six ans. Mais nous avons dû parfois demander des solutions à l'ICANN dans le cadre de l'intérêt public. Nous reconnaissons malgré tout qu'il reste encore beaucoup de choses à faire.

Aujourd'hui, nous devons prendre en considération le sujet de la protection des données et de la vie privée, car ce sujet est d'importance cruciale. Alors le développement des services publics sur l'Internet, c'est une question critique dans cette ère de la mobilité des citoyens. La nature mondiale des services et des différents régimes de protection des données, à tout ceci s'ajoutent les capacités en matière de cybercriminalité. Il y a également les cadres de travail qui ont un impact sur le flot d'accès aux informations par les différents organes gouvernementaux.

L'Ouganda recommande donc que le processus d'élaboration des politiques et les exigences dans l'industrie en lien avec l'écosystème de l'Internet, auxquels nous contribuons tous, doivent assurer que les services publics et la sécurité nationale ne sont pas perturbés. Et donc il faudra reconnaître les différentes exigences des intérêts publics des différents pays.

Donc en conclusion, j'aimerais répéter encore une fois l'engagement de l'Ouganda à travailler avec les différents acteurs, pour assurer une croissance continue et l'inclusivité de l'écosystème de l'Internet pour un développement durable pour tous. Merci.

AWA N'DIAYE :

Merci beaucoup pour l'Ouganda pour la précision et la clarté, et surtout pour concision, parce que je voudrais rappeler à chaque intervenant qu'il a trois minutes au plus, donc moins c'est parfait.

Je donne maintenant la parole à Cook Islands, à Pua Hunter qui est le directeur TIC de Cook Islands.

PUA HUNTER :

Merci. J'aimerais donner la possibilité au pays de Tuvalu, au Ministre représentant du Ministère de transport et de la communication. Je donnerai donc la parole au représentant de Tuvalu.

MONISE LAAFAI :

Bonjour à tous. Chers collègues, messieurs, dames. Je m'appelle Monise Laafai, Ministère des communications et du transport de Tuvalu. C'est ma première réunion à l'ICANN et je suis tout à fait honoré de représenter ici mon pays. Merci, Madame la Présidente. Merci aux différents panélistes d'avoir partagé votre expertise et vos expériences dans l'écosystème de l'Internet.

Tout d'abord, j'aimerais exprimer nos remerciements au Ministère d'Espagne pour leur hospitalité. Nous tenons cette réunion dans un magnifique pays.

Les défis concernant la vie privée, le cyber délit, ne sont pas très importants dans mon pays ; nous avons d'autres difficultés. Et en tant que pays petit insulaire qui est isolé des autres centres d'entreprise, nous sommes extrêmement vulnérables aux effets du changement climatique. Il est très important pour nous de pouvoir renforcer le transport, car c'est un point crucial pour le développement économique. Pour cela, les télécommunications sont également très coûteuses.

Un monopole public soutient la population de 11 000 personnes. Nous avons une loi qui a été amendée pour pouvoir s'adapter au développement et au commerce électronique.

Notre expertise est limitée en matière de cybercriminalité. Les gens de notre ministère remplissent plusieurs tâches. Par exemple, notre représentant ici au GAC remplit beaucoup d'autres fonctions en matière d'application de la loi et autres, et il est aussi mon conseiller

en tant que ministre.

Malgré toutes ses difficultés, nous nous embarquons dans la mise en œuvre d'un câble de fibre optique qui permette de connecter nos communautés, les communautés de notre île. C'est un développement important, car il va encourager le développement et la mise en œuvre de mécanismes pour essayer de lutter contre les difficultés que j'ai déjà évoquées.

Trois minutes ne me permettraient pas suffisamment de temps pour faire un résumé de nos nombreuses difficultés, mais j'espère que la participation de mon pays aux réunions de l'ICANN va contribuer à réduire le fossé numérique entre mon pays et le monde en développement, le monde développé, et que cela va permettre de mieux faire comprendre quelles sont nos difficultés et nos contraintes.

Beaucoup d'entre vous ici connaissent les noms de domaine depuis longtemps. Nous voulons bien comprendre quelles sont les implications du RGPD pour notre pays ; il y a des actions que nous devons mettre en place. Il y a des mesures qui s'avèrent très coûteuses pour un pays comme le mien. Et j'invite l'ICANN et les acteurs de l'écosystème de considérer la possibilité de tenir des événements dans notre région pour promouvoir la participation et pour que nous puissions soutenir le travail de l'ICANN, notamment en ce qui concerne l'élaboration de politiques publiques. Merci de cette occasion et merci à tous. Gracias.

AWA N'DIAYE : La parole est à la République Dominicaine. M. Nelson Gullen, membre du conseil d'administration d'INDOTEL.

NELSON GULLEN : Merci beaucoup. Je vais commencer par remercier, au nom du gouvernement de la République dominicaine, le gouvernement espagnol de nous avoir accueillis dans cette belle ville de Barcelone. La République dominicaine s'est engagée à établir les mécanismes adéquats en matière de cybersécurité pour protéger les institutions de l'État, les citoyens, et les secteurs productifs. Ces mesures cherchent à garantir le développement fiable des activités de toute la population dans un cadre de respect des droits de l'homme.

Cependant, nous avons constaté que, pour lutter contre des groupes fondamentalistes qui utilisent Internet, beaucoup de gouvernements ont promu des lois qui combattent le terrorisme qui finissent par être utilisées pour réprimer les dissidents. Il est préoccupant de voir que la cyber sécurité, le cyber délit et des comportements abusifs ont servi d'excuses au législateur pour criminaliser ce qui est critique, la légitimité d'un gouvernement, ou pour attaquer et réprimer le discours politique qui s'avère critique.

Nous considérons que poursuivre et mettre en prison les utilisateurs Internet pour le seul fait de s'être exprimé librement ne permet pas de trouver une solution intégrale qui puisse nous permettre de lutter contre la menace du terrorisme.

Nous sommes préoccupés par les projets de loi qui, sous prétexte de la cyber sécurité, essayent d'accéder aux données WHOIS pour des bénéfices particuliers. Cela se traduit dans un conflit d'intérêts tout à fait clair qui doit être résolu au niveau global et auquel l'ICANN peut contribuer.

La République dominicaine souhaite contribuer à l'amélioration de la connectivité globale de l'Internet et souhaite soutenir les droits des individus, la liberté, l'Internet. Et c'est pour cela qu'elle refuse ce type d'intervention dans la gouvernance globale de l'Internet, car l'intérêt général doit toujours prévaloir sur les intérêts particuliers. Merci beaucoup.

AWA N'DIAYE :

Si je donne la parole à la Commission européenne, M. Pierce O'Donohue, qui est le directeur de Future Networks DJ Connect.

PIERCEO'DONOHUE :

Merci, Madame la Présidente. Donc la protection des données, cet intérêt est très compréhensible et donc la législation européenne à laquelle nous faisons référence, le RGPD est un excellent exemple de cette tendance. Enrique Factor a déjà remis cette législation dans son contexte de la protection des données et d'autres politiques d'intérêt public, de protection de l'intérêt public. Donc je ne vais pas parler de tout ceci.

Mais nous avons également parlé des menaces réelles en matière de

cybercriminalité, auxquelles sont confrontées les agences de protection et donc d'application de la loi. Et donc, dans le cadre de leur travail, il faut trouver l'équilibre entre la protection contre ces menaces et la protection des données.

Et bien sûr que Bertrand de la Chapelle l'a dit, ce n'est pas un choix. Il ne s'agit pas de choisir, il y a un paradoxe. Afin de pouvoir alimenter et protéger l'Internet, ce qui est la mission à laquelle vous êtes tous engagés, en tant que véhicule pour que tout le monde bénéficie du point de vue économique et social, pour protéger les données des personnes et pour que ces personnes puissent avoir confiance en l'Internet de manière suffisante pour pouvoir être présents et bénéficier du potentiel, afin de pouvoir y arriver à tout ceci, il faut également nous assurer que l'Internet est sécurisé et qu'il ne permet pas la criminalité. Et ce paradoxe, cet équilibre justement, c'est ce à quoi nous sommes confrontés au jour le jour.

Étant donné que ceci a été fait référence dans le cas du travail du GAC et de la communauté de l'ICANN au cours des semaines passées, au cours de cette même réunion, je dois parler de la question et de son impact sur le WHOIS de manière plus spécifique, comme nous l'avons déjà entendu mentionner dans différentes interventions. Le point de vue que je vous donne est celui de membres de l'Union européenne et de la Commission.

L'Union européenne reconnaît le rôle central de l'ICANN et sa responsabilité afin de garantir la sécurité, la stabilité et la résilience du

système des noms de domaine. Et dans le cadre de ce rôle, l'ICANN doit garantir le fonctionnement du service WHOIS, y compris la collection, le maintien et la collecte des données, juste des données précises et des titulaires de noms de domaine. Et ceci doit être fait dans le respect des lois en Europe, comme dans d'autres régions.

Nous soutenons le dialogue continu entre l'ICANN et les autorités de protection des données européennes. Et je vous rappelle, nous avons des représentants présents. Nous vous rappelons que ces unités de réglementation sont indépendantes et ne dépendent pas de l'influence des gouvernements.

Donc l'idée c'est d'assurer le respect de ces règles. Mais nous devons également souligner le fait que, nulle part dans le RGPD, il n'est indiqué que le traitement des données est interrompu pour des processus légitimes, pour des raisons d'application de la loi, de recherche sur la cyber sécurité ou pour des raisons de détection et de suivi en cas d'infraction à la propriété intellectuelle ou d'autres droits. L'idée c'est d'identifier les objectifs légitimes et de trouver l'équilibre entre les besoins légitimes et la protection des données à caractère personnel. Et donc, à mon avis, c'est quelque chose qui bénéficiera à tout l'ICANN, à toute la communauté de gouvernance de l'Internet, si nous arrivons à trouver une solution. C'est complexe certes, mais je crois que ce sera très utile à l'avenir puisque cela permettra de protéger les droits fondamentaux, qui sont fondamentaux, et également de s'assurer que les gouvernements pourront fonctionner à l'avenir. Merci.

AWA N'DIAYE : Merci beaucoup. Je donne la parole au gouvernement indien, Dr Gulshan Rai, coordonnateur de la cyber sécurité au niveau national.

GULSHAN RAI : Merci beaucoup. Je pense- je vais commencer par remercier le gouvernement de l'Espagne d'accueillir cette réunion.

Les économies numériques se développent très vite en Inde. Nous espérons atteindre 1,5 milliard de croissances économiques. Or, avec cette croissance économique, d'autres difficultés apparaissent : le cyber délit, la cyber sécurité, la vie privée, le libre flux d'informations commencent à avoir une place prépondérante.

Notre ministre a bien annoncé le lancement d'un cadre pour traiter de cette question et une stratégie de cyber sécurité. Pour ce qui est de la cyber sécurité, la vie privée et le libre flux d'informations, cela représente un défi très important, un défi non seulement pour l'Inde, mais aussi pour le monde entier. C'est pour cela qu'il nous faut avoir des cadres juridiques, des cadres juridiques qui peuvent ne pas être compatibles. Certains cadres qui ont été annoncés récemment ont suscité des inquiétudes et des difficultés qui ont été déjà évoquées par d'autres intervenants.

Aujourd'hui 90 % des cyber délits sont très spécifiques. Avec le

gouvernement, nous devons jouer un rôle pour pouvoir en venir à bout du problème de la cyber criminalité. Si nous regardons la carte du monde, nous voyons qu'il y a des frontières. Or si nous voyons l'Internet, l'Internet n'a pas de frontière. Cela nécessite donc, pour que cet Internet sans frontières fonctionne, il faut un fonctionnement sans frontières, interopérable et sûr.

Et l'Internet a un rôle fondamental. La communauté indienne est engagée à travailler pour la création d'un cadre interopérable qui puisse résoudre les problèmes que l'on retrouve dans ce domaine. La technologie comme Big Data, l'intelligence artificielle, l'Internet des objets jouent un rôle important et le GAC a un rôle-clé pour essayer de réunir les communautés afin qu'elles travaillent de manière interopérable pour résoudre ces problèmes qui évoluent très vite. Merci beaucoup et merci de m'avoir écouté.

AWA N'DIAYE :

Merci beaucoup, je donne la parole maintenant aux USA avec Monsieur David Redl, Secrétaire pour la communication et l'information et administrateur de la NTIA.

DAVID REDL :

Merci beaucoup, oui je vais me limiter à trois minutes.

Donc merci d'avoir donné cette opportunité de parler par rapport à ces sujets. Les États-Unis soutiennent l'approche multipartite en matière de développement de politiques.

Donc les processus ascendants créent des politiques auxquelles on fait confiance dans tout le système de l'Internet. Ceci informe différentes questions, la cybercriminalité et autres et la protection des données.

Les enjeux de la gouvernance de l'Internet ne sont pas faciles à résoudre. Il y a toujours des décisions qui sont difficiles, mais la NTIA s'engage à répondre à ces enjeux de manière assurer la prospérité et à donner la place à l'innovation. Pour bénéficier de cette approche, nous devons continuer de donner le feu vert aux innovateurs pour créer un Internet plus ouvert, plus sécurisé et plus prospère. Ceci s'applique aux enjeux pour l'accès aux données WHOIS avec l'application du RGPD. Comme vous le savez, les services du RGPD sont très utiles pour tous. Pour les objectifs légitimes des agences d'application de la loi et la protection de la propriété intellectuelle.

Les informations sur le WHOIS sont cruciales pour protéger l'intérêt public et pour assurer la stabilité, la sécurité et la confiance dans le DNS. Du point de vue des États-Unis, il est impératif de trouver la voie de l'avenir. Et le Comité européen de la protection des données a clarifié son point de vue. L'ICANN et les membres de la communauté de l'ICANN continuent de travailler avec intensité dans le cadre de l'EPDP sur cette question. Nous essayons de clarifier les points de vue des différentes parties prenantes de l'ICANN pour voir où sont les problèmes de conformité au RGPD, et le processus compliqué.

Cela veut dire qu'il y a des risques pour les sociétés qui sont

impliquées dans le DNS et la fourniture de services. Les parties doivent trouver une solution qui atténue tous les risques pour les sociétés, et cette tâche est immense. Voilà pourquoi les États-Unis soutiennent l'engagement d'ICANN org avec nos collègues européens, y compris avec le Comité européen de la protection de données, pour simplifier les enjeux auxquels nous sommes confrontés. L'ICANN assumera les risques et responsabilités d'accès au WHOIS conformément au RGPD. Si ceci est possible, eh bien, le problème sera simplifié.

Le temps avance rapidement par rapport à la spécification temporaire. Donc je demande au GAC d'avoir un rôle de leadership dans les discussions communautaires pour un modèle d'accès unifié. Les États-Unis sont prêts à travailler avec le GAC et le reste de la communauté sur ces questions. Merci beaucoup.

AWA N'DIAYE :

Merci beaucoup. Je donne maintenant la parole à la Malaisie, docteur Mohd Ali Mohammad, secrétaire général du Ministère de la communication et du multimédia. Merci.

MOHD ALI MOHAMMAD :

Merci, Madame la Présidente. Je vais être très bref.

En raison du développement et des changements dans le domaine technologique, les agences d'application de la loi en Malaisie sont confrontées à de nouvelles difficultés pour combattre le délit dans l'ère de la convergence. Les délinquants utilisent des techniques de

plus en plus sophistiquées. Les méthodes d'investigation commencent à ne plus avoir la même efficacité qu'avant.

Pour répondre à ces problèmes, les organismes d'application de la loi de Malaisie utilisent et mettent à profit toutes les informations disponibles, susceptibles de faire avancer les investigations, y compris les informations WHOIS. Les organismes d'application de la loi, à travers les mécanismes prévus par la loi, font aussi appel à l'aide de gestionnaires des noms de domaine pour obtenir des informations utiles pour leurs investigations. C'est pour cette raison que le rôle de la communauté du système des noms de domaine et du WHOIS est essentiel, et devrait être préservé pour répondre aux besoins en matière d'enquête et d'application de la loi. Merci beaucoup.

AWA N'DIAYE :

Merci beaucoup pour cette concision. Je vais profiter de cette confusion, puisqu'il vous restait encore quelques minutes pour donner la parole à John Crain. On a beaucoup parlé de noms de domaine, de WHOIS. Peut-être que John Crain pourra nous apporter quelques petites remarques supplémentaires par rapport à ces interrogations. Merci.

JOHN CRAIN :

Merci beaucoup. Donc si je peux me permettre, j'ai entendu beaucoup de mentions du WHOIS et de l'importance de cette base de données qu'est le WHOIS. Et donc, je souhaiterais clarifier pour ceux qui ne

connaissent pas nécessairement les détails techniques qui ont été présentés hier que lorsqu'on parle du WHOIS, eh bien, on parle du RDAP qui, en fait, remplacera le WHOIS.

Il s'agit de systèmes décentralisés, donc, il n'y a pas une seule base de données, il y a plusieurs bases de données qui se trouvent un peu partout dans le monde. Et c'est une composante importante à mentionner.

Il est excellent qu'on puisse avoir ce type de discussion ici à l'ICANN, où nous rassemblons les différents acteurs et où nous discutons de solutions possibles qui puissent faire l'équilibre entre ces principes, la sécurité, la vie privée et la robustesse du réseau. Ceci étant, je repasse la parole à notre présidente.

AWA N'DIAYE :

Merci beaucoup, M. Crain. Je vais passer toute la parole à Mexico, avec M. Victor Lagunes Soto Ruiz, qui est le chef de l'unité pour l'innovation et la technologie auprès du cabinet du président de la République.

VICTOR LAGUNES SOTO RUIZ : Merci beaucoup, Madame. Merci au gouvernement de l'Espagne de la ville de Barcelone et merci à l'ICANN de cette coopération continue en matière de digitalisation et de gouvernance de l'Internet.

Le rôle du Mexique bien entendu en ce qui concerne le numérique a été très ambitieux. La stratégie numérique de connectivité a été très

importante, et plus on connecte des Mexicains, plus on réduit la fracture numérique. Mais en même temps, nous sommes de plus en plus exposés aux risques du cyber délit.

Nous sommes inquiets ou préoccupés pour la protection des données à caractère personnel. Nous développons la stratégie nationale en matière de cyber sécurité en coopération avec tout l'écosystème, dans un environnement multipartite.

L'année dernière, nous avons pu publier cette stratégie en coopération avec l'industrie, le secteur universitaire, la société civile, mais aussi avec les observateurs, des experts internationaux, en coopération avec l'ONU, l'UNESCO, l'Organisation des États américains. Cette stratégie nous aide à renforcer le numérique, mais aussi à renforcer la protection des citoyens pour protéger notre économie, pour protéger l'innovation et les droits des citoyens, les institutions publiques, la sûreté publique, la sécurité nationale, tout cela par le biais de programmes de sensibilisation, des programmes de création et de renforcement d'une culture de cyber sécurité, création de capacités, recherche-développement, établissement de critères techniques et de normes techniques ainsi que protection des infrastructures critiques, renforcement du cadre juridique.

Tous ces éléments nous permettent de renforcer le développement durable en matière Internet.

Je suis fier de partager avec vous, le fait que le SMSI a qualifié la stratégie du Mexique comme championne l'année dernière. Merci.

AWA N'DIAYE : Je donne la parole maintenant au Brésil, à l'ambassadeur Benedicto Fronseca Filho, directeur du département pour les sciences et technologies.

BENEDICTO FONSECA FILHO : Merci, Madame la Présidente. J'aimerais mentionner l'importance qu'attache le Brésil à cette discussion sur la cyber criminalité, la protection des données. Il s'agit d'une priorité pour nous.

Le Brésil a adopté, en aout dernier, une nouvelle législation sur la protection des données qui, en grande partie, est inspirée par le RGPD. Cette législation devrait entrer en vigueur en février 2020.

Nous parlons également de l'élaboration d'une stratégie nationale de cyber sécurité. Comme vous le savez, au niveau mondial, nous avons beaucoup plaidé pour le droit de la vie privée dans l'espace numérique. Nous avons également promu des résolutions dans le contexte des Nations Unies. Et nous cherchons des moyens de mettre en place des outils qui permettent de lutter contre la cybercriminalité. Et d'ailleurs, j'aimerais mentionner une notion qui a été évoquée par Bertrand de la Chapelle, l'importance de la coordination, de la coopération et de la communication entre les gouvernements au sein de la communauté internationale, de manière à traiter de ces questions dans leur contexte.

Et j'aimerais également évoquer ce qu'a dit Bertrand. Il a attiré

l'attention sur le fait que le débat sur le WHOIS illustre les dimensions, donc, de la protection des données, de la lutte contre les abus, sans mettre en danger le développement des technologies numériques. Dans ce contexte, je souhaite également appuyer l'importance des réseaux de juridiction de l'Internet, qui fournissent des plateformes de discussion de ces questions, parce que nous n'avons pas de lieu pour s'occuper de la question des juridictions dans toutes ces discussions. Ces discussions se produisent dans un lieu, mais il faut qu'il y ait un lieu commun. Et donc nous serons très impliqués dans les discussions relatives aux débats du WHOIS dans le contexte de l'ICANN.

Nous sommes d'accord. Il faut absolument trouver le bon équilibre par rapport à ces préoccupations : la protection de la vie privée d'un côté et la sécurité de l'autre. Nous avons entendu le représentant d'Interpol. Nous avons entendu nos collègues brésiliens. Et il est vraiment dans notre intérêt, actuellement — encore une fois, je fais référence à ce qui a été dit — donc de réconcilier ces différentes dimensions de manière appropriée. Merci.

AWA N'DIAYE :

Merci beaucoup. Je donne la parole à Samoa, à l'honorable Afamasaga Lepuiai Rico Tupai, Ministre des communications et des technologies de l'information.

AFAMASAGA LEPUIAI RICO TUPAI : Madame la présidente, je souhaiterais pouvoir intervenir dans

la séance numéro quatre, s'il vous plait, si vous me permettez.

AWA N'DIAYE :

Donc je donne la parole à la Suisse, à Niklas Nilsson, premier secrétaire à l'ambassade de Suisse en Espagne.

NIKLAS NILSSON :

Merci, Madame la Présidente. Nous parlons au nom de la Suède, et non pas de la Suisse. Je voulais préciser cela. Merci beaucoup de cette opportunité de pouvoir vous présenter la perspective de la Suède en matière des droits de l'homme.

Nous adoptons une approche de respect des droits de l'homme, pour tout ce qui est numérique. Il s'agit d'un principe fondamental : les droits de l'homme doivent être respectés en ligne et hors ligne. La démocratie et le règne de la loi doivent être respectés dans le cyberspace aussi.

Pour ce qui est des droits de l'homme sur Internet, cela est déclaré partout, mais de plus en plus on voit des gouvernements appliquer des censures au nom de la sécurité. Il y a eu beaucoup de lois répressives pour contrôler la propagande, et ces mesures ne font que limiter la participation des citoyens à la société et vont à l'encontre des véritables fondements de la société démocratique.

On voit une tendance à un espace démocratique réduit. Ces législations limitent la liberté d'expression, mais aussi limitent la

possibilité des individus de participer à la prise de décision au sein des sociétés.

Messieurs, dames. Grâce à l'Internet et aux médias sociaux, les droits de l'homme sont mieux connus qu'avant. La place qu'ils occupent dans notre vie, dans notre société, doit être mise en exergue, et nous devons les protéger.

L'Internet a un grand potentiel pour promouvoir le développement économique et l'inclusion, la diversité. La capacité à rapprocher les gens ne doit pas être affaiblie ; en limitant la liberté de l'Internet, nous limitons le développement. C'est pour cela que nous croyons que les droits de l'homme doivent être la base des discussions pour pouvoir répondre aux défis que pose la numérisation, le numérique, pour que tout le monde puisse accéder à un Internet ouvert et sûr.

Et pour finir, le modèle multipartite avec des acteurs venant de l'industrie des gouvernements de la société civile, y compris les défenseurs des droits de l'homme, est un élément-clé pour développer un cadre de régulation de l'Internet. Je répète, quelle est l'ambition de la Suède ? Un Internet ouvert, inclusif, qui permet à tout le monde de participer sur un pied d'égalité. Merci.

AWA N'DIAYE :

Je donne la parole aux Pays-Bas, si je ne me trompe. M. Geert Moelker, membre du conseil d'administration pour l'économie digitale au Ministère de l'économie et du climat.

GEERT MOELKER :

Merci, Madame la Présidente. Je serai bref. J'aimerais simplement mentionner deux points sur le WHOIS.

On a déjà beaucoup parlé de l'équilibre ou de la réconciliation entre les différents droits fondamentaux en matière de vie privée, mais également en matière de droits de protection contre la criminalité. Nous sommes d'accord. Ce n'est pas soit l'un, soit l'autre. C'est un équilibre qu'il faut trouver, une solution.

Et ce que j'aimerais mentionner, c'est que s'il y a un organisme au sein duquel c'est possible, c'est au sein de l'ICANN puisque de multiples acteurs sont représentés. Donc c'est une immense tâche, mais nous pouvons y arriver.

Deuxième chose. L'urgence. Nous sommes confrontés à un besoin urgent de trouver des modalités pour accéder aux données du WHOIS. Depuis mai 2018, beaucoup d'accès au WHOIS ont été modifiés, beaucoup d'autorités de réglementation l'on fait. Et donc, si on ne trouve pas un modèle d'harmonisation, eh bien, la fragmentation aura lieu. Les autorités d'application de la loi seront confrontées à des obstacles et les utilisateurs n'auront plus aucune certitude par rapport à la sécurité de leurs données.

Encore une fois, nous voyons que l'ICANN a un rôle pivot à jouer. L'ICANN est la seule organisation qui, au niveau mondial, peut avoir une approche uniforme par rapport à cette question.

La réforme du WHOIS ne peut pas ne pas avoir de solution. Nous devons trouver des solutions également dans les délais impartis. Nous savons que ceci nécessitera l'implication de différents acteurs, le Conseil, les différents acteurs de l'ICANN, et ceux qui sont hors de l'ICANN. Nous soutenons le modèle multipartite de l'ICANN, mais je dois également dire qu'à mon avis ce débat sur le WHOIS est un test pour ce modèle suite à la transition IANA. Alors, assurons-nous de réussir ce test. Merci.

AWA N'DIAYE :

Merci beaucoup. Je donne la parole au dernier intervenant, l'Italie, pour trois minutes également, Mme Rita Forisi, directrice générale de l'Institut supérieur pour la communication et les technologies de l'information.

RITA FORSI :

Merci, Madame la Présidente. Chers délégués, messieurs, dames, tout d'abord je tiens à remercier le gouvernement de l'Espagne de nous avoir accueillis et d'avoir accueilli cette réunion gouvernementale de haut niveau.

Nous savons que le WHOIS c'est l'annuaire où sont collectées les données sur les titulaires des noms de domaine et que ces données ne sont plus accessibles. Les données sont utilisées à plusieurs fins, y compris pour trouver des noms qui peuvent être utiles aux forces de l'ordre, pour également protéger les droits des marques, etc.

L'Italie soutient le travail qui a été fait jusqu'à maintenant pour développer et mettre en œuvre une solution permanente, mais, en même temps, voudrait insister sur la nécessité d'accélérer les recherches d'un nouveau modèle unifié qui puisse être satisfaisant pour toutes les parties.

Trouver une solution qui puisse tenir compte des différents intérêts doit être un objectif que l'on doit atteindre. Il faut une coopération renforcée entre toutes les parties concernées du système des noms de domaine. En même temps, toute la communauté du DNS doit reconnaître qu'agir vite est un élément crucial lorsqu'on a trait au cyber délit.

Le dialogue en cours entre l'ICANN et les autorités de protection de données est très important. Le vrai défi auquel nous sommes confrontés est celui de protéger en même temps tous les aspects concernant les domaines Internet.

AWA N'DIAYE :

Merci beaucoup. Voilà. Je pense que nous sommes au bout de notre débat avec les États. Nous avons bien vu que, comme on dit, ce ne sont pas deux choses qui s'annulent l'une l'autre, ce sont deux choses qui doivent être prises ensemble, cette nécessité qui a été ici démontrée de rappeler les principes fondamentaux et l'importance de ces principes fondamentaux des droits de l'homme. Cette nécessité également de mettre en place des politiques concertées entre tous les acteurs de la cyber sécurité.

Je voudrais avant de terminer et pour clore ce panel, je voudrais revenir à M. de la Chapelle en lui demandant de nous dire à nouveau cette importance d'une solution globale et d'une solution multipartite. M. de la Chapelle, vous avez une minute.

BERTRAND DE LA CHAPELLE : Merci. Je ne souhaite pas vous décevoir, mais ce n'est pas vraiment une solution globale. C'est plutôt identifier les problèmes dans chaque domaine. J'ai écouté avec attention ce qui a été dit. Et sur le débat du WHOIS, il y a un lien très étroit avec ce dont on a parlé lors du premier panel, à savoir comment est-ce que l'interaction entre les gouvernements et le reste de la communauté a lieu au sein de l'ICANN, et dans quelle mesure la participation des gouvernements au GAC permet également d'organiser la discussion dans le cas de leur propre processus. Ça, c'est important.

Et la deuxième idée que je souhaite souligner, c'est que si certes l'ICANN est un espace important, sa mission est limitée. Et il y a un danger parce que, étant donné que la communauté est là, tout ce qui est relatif à l'Internet a tendance à retomber dans cette communauté. Mais il est important d'identifier quels sont les sujets qui sont traités, chacun des sujets avec chacune des questions individuelles. Par exemple, l'innovation des politiques. Certains des sujets en fait n'appartiennent pas à l'ICANN. Et donc il faut créer d'autres opportunités en dehors pour les questions qui émergent, pour qu'il y ait communication, coopération et coordination entre les différents

acteurs.

Donc il n'y a pas une seule solution mondiale. Mais il y a sans doute une approche mondiale en matière d'innovation de politiques pour permettre à des initiatives d'être mises en place et pour rassembler les différents acteurs. C'est ce que l'on fait à une petite échelle, mais il y en a d'autres qui font des choses tout à fait similaires.

AWA N'DIAYE :

Merci beaucoup, M. de la Chapelle. Donc je voudrais, pour finir, redonner la parole à M. le Président, et rappeler ici l'importance qui a été soulignée par tous et pour finir par M. de la Chapelle de renforcer la coopération entre les acteurs. La coopération multi parties prenantes est essentielle pour arriver à une solution, même cette solution est très complexe ; chacun l'a souligné. Et une des choses importantes que j'aimerais également rappeler, qui a été soulignée ici, c'est d'harmoniser les lois pour permettre justement d'arriver à ces solutions-là, harmoniser les lois pour que les lois nationales ne s'entrechoquent pas et ne soient pas également l'occasion de dérives contre la liberté d'expression sur Internet. Donc, harmoniser les lois pour arriver véritablement à un Internet de confiance, un Internet par lequel chacun peut bénéficier de son potentiel.

Je vous remercie et je vais redonner la parole à Monsieur le Président.

FRANCISCO POLO :

Merci beaucoup, Mme N'Diaye pour une séance excellente et merci

pour votre modération.

Merci beaucoup à toutes les personnes qui ont participé à cette séance. C'est notre dernière séance du matin. Nous allons nous réunir à 15 heures pour poursuivre notre travail. Merci beaucoup.

MANAL ISMAÏL :

Merci. Merci au modérateur. Merci aux experts. Merci à toutes les délégations qui ont participé. Comme Francisco l'a bien dit, c'est la pause-café pour les chefs de délégations qui ont le ruban orange. Le déjeuner est servi à la salle de banquet. S'il vous plait, suivez les panneaux et vous serez guidés par le personnel de l'ICANN. Pour tout le reste, profitez du déjeuner et assurez-vous d'être dans la salle de retour à 15 heures. Merci beaucoup,

[FIN DE LA TRANSCRIPTION]