DUBLIN – Séance ouverte du groupe de travail du GAC sur la sécurité publique
Lundi 19 octobre 2015 – 15h00 à 16h30 IST
ICANN54 | Dublin, Irlande

LAUREEN KAPIN : … beaucoup de travail a été fait pour faire en sorte que ce communiqué du GAC puisse être accepté par le Conseil d'administration et puisse être mis en œuvre.

Bobby va nous parler un petit peu plus des améliorations qui ont été faites au niveau des contrats.

ROBERT FLAIM : Avant la création de ce groupe, il y avait les recommandations d'application de la loi. Cela a fonctionné pendant un certain nombre d'années, de 2009 jusqu'à 2013. Nous avons participé à ce type de politiques, les spécifications en matière de WHOIS, les services d'enregistrement fiduciaire d'anonymisation.

Notre travail, donc, au sein de ce groupe de travail concerne la sécurité publique. Et je vais vous montrer les améliorations en matière d'exactitude du WHOIS. Nous allons, par la suite, en reparler. Catherin va nous donner un aperçu par rapport à cette exactitude de WHOIS et pourquoi cela est important au niveau de la sécurité publique. Je vais vous donner un avant-goût de ce

que fait l'Europe par rapport à la protection de données au niveau des lois européennes et en matière d'exactitude du WHOIS. Nous avons travaillé dans ce domaine pendant dix ans dans différents groupes de travail, auxquels j'ai participé.

LAUREEN KAPIN : L'une des grandes leçons à tirer de ce travail, c'est que même si nous sommes un petit groupe au sein du GAC, nous – cela fait longtemps que nous travaillons dans ce type de domaine. Et maintenant, nous travaillons au sein du GAC.

Voyons notre travail récent. Comme Alice l'a dit au départ, si vous, vous êtes intéressé à connaître plus en profondeur le travail que nous avons fait, le site du GAC contient ces informations. Le site du GAC a une espace publique, il ne faut pas être membre du GAC pour accéder à ces informations. Et là, vous trouverez le travail du groupe ainsi que d'autres informations sur les représentants du groupe de travail ainsi que des commentaires que nous avons présentés. Voilà l'endroit où vous trouverez davantage d'informations, si vous voulez en savoir plus sur notre groupe.

On va passer en revue les parties les plus importantes de notre travail. Donc, on va vous parler de contrat d'accréditation de bureaux d'enregistrement 2013.

ROBERT FLAIM : Le RAA 2013. Cela a jeté les bases d'un travail futur, notamment en ce qui concerne la spécification concernant le WHOIS.

En 2015, il y a eu des discussions par rapport à la façon dont la spécification, concernant le WHOIS, qui fait partie du RAA, serait traitée. L'ICANN et les bureaux d'enregistrement avaient rencontré des difficultés, il y a eu des commentaires, il y a eu une période de consultations publiques à laquelle a contribué le Groupe de travail sur la sécurité. Nous avons fait cela. Nous avons également fait des commentaires au Groupe de travail qui travaille sur les services d'anonymisation et d'enregistrement fiduciaire ainsi que le Groupe qui s'occupe du RDS concernant le WHOIS. Même si, au départ, nous n'avons pas eu suffisamment de représentants des agences d'application de la loi. Ce groupe a été ouvert à d'autres agences de protection des consommateurs et d'autres groupes ou organisations qui s'occupent de la sécurité publique des organisations aux États-Unis et d'autres agences qui travaillent dans le domaine de la sécurité publique. Ces commentaires ont été reçus par le Groupe de travail et nous les avons analysés.

Nous avons ensuite l'exactitude du WHOIS. Avant la réunion de Buenos Aires, l'ICANN et les bureaux d'enregistrement avaient fait des commentaires par rapport à cette question de

l'exactitude du WHOIS. Et nous voulions mieux comprendre les spécificités de ces commentaires qui avaient été formulés. Nous voulions obtenir davantage d'informations et de spécifications par rapport à ces commentaires.

Comme vous allez l'entendre par la suite, nous avons travaillé là-dessus et nous sommes intéressés à obtenir davantage de spécifications par rapport à cela.

LAUREEN KAPIN : Le RAA 2013 a des implications en matière de vérification de l'exactitude des informations de WHOIS par les bureaux d'enregistrement. Si ces vérifications ne sont pas faites ou s'il y a des réclamations, il y a des actions qui s'ensuivent. Et certains commentaires visaient justement à ce type de réponse qui devrait être obtenu au cas où un bureau d'enregistrement ou la personne – ou au cas où la personne qui doit fournir ces informations ne le ferait pas.

Nous avons également travaillé dans le domaine des services d'anonymisation et d'enregistrement fiduciaire. Ce service permet aux entités de cacher des informations. Il y a des raisons pour lesquelles ils font cela. Et il y a des inquiétudes par rapport à cela. Le Groupe de travail sur la sécurité publique a commenté certains cas et nous avons dit qu'il fallait établir une différence

entre la disponibilité de ces services. S'il y a, par exemple, des services commerciaux qui sont utilisés, dans ce cas-là, le consommateur doit fournir des informations de carte de crédit, etc. Et à ce moment-là, on a le droit de savoir à qui on a affaire. Et donc, les services d'anonymisation et d'enregistrement fiduciaire ne devraient pas être disponibles dans ce type de situation. Ensuite, il devrait y avoir une certaine transparence et réduction de comptes de la part des fournisseurs de ce type de services. Une agence d'application de la loi doit pouvoir demander les informations par rapport à qui est derrière un certain service, si cela est prévu dans les lois locales, car les agences d'application de la loi doivent pouvoir mener à bien des enquêtes et accéder à certaines informations.

Ensuite – pardon, ce n'était pas le bon micro.

Nous avons également présenté des commentaires sur les services WHOIS de nouvelle génération, dont Catherine va vous parler plus en détail. Il s'agit d'une question très compliquée. Il faut voir ce qui fonctionne et ce qui ne fonctionne pas aujourd'hui au niveau du WHOIS pour voir s'il devrait y avoir un nouveau système qui le remplace. À ce moment-là, il faudrait savoir à quoi devrait ressembler ce nouveau système. Et nous avons mis l'accent dans nos commentaires - par rapport au rapport préliminaire, nous avons mis l'accent, donc, sur le fait

de savoir que ce nouveau système doit trouver un équilibre, car il doit respecter les droits les consommateurs, préserver la sécurité publique et assurer la protection des données personnelles des internautes.

Nous travaillons pour que les canaux de communication soient ouverts, car les intérêts doivent pouvoir être réconciliés. Il faut pouvoir préserver la confidentialité et en même temps les droits des consommateurs. Les agences peuvent être en contact et un certain équilibre peut être retrouvé. La question du WHOIS reste un domaine très important pour nous.

ROBERT FLAIM : Le représentant de l'Agence nationale du crime va vous parler de la spécification 11, à savoir le cadre de sécurité du contrat de registre, quelque chose qui est né après l'avis du GAC de Beijing il y a deux et demi.

John a travaillé depuis le Groupe de travail, avec les registres pour établir des pratiques volontaires, essayer de voir comment travailler dans les cas d'abus botnet, hameçonnage, logiciel malveillant, exploit5ation des enfants afin de trouver – d'arriver à un accord coopératif arc le registres et travailler de manière efficace avec ce type d'abus.

C'est un petit résumé que je vous fais maintenant. Après, on va parler davantage.

LAUREEN KAPIN : Quel est notre travail à l'avenir? Nous espérons avoir la représentation du groupe de travail qui s'occupe des questions liées à la concurrence, le choix et la confiance du consommateur, qui aura un rôle central pour considérer tous les aspects dans ces domaines. En plus de l'Exactitude du WHOIS par rapport aux informations des domaines, il y a aussi quelque chose d'important.

ROBERT FLAIM : Oui. Il y a quelque chose aussi d'important lorsqu'on voit les abus, etc., nous voyons l'autre partie du système du DNS, les adresses IP, qui sont gérées par les RIRS, les Registres Internet régionaux. Et en dehors de l'ICANN, nous avons les organisations des ressources numéros qui essaient également de travailler sur ces questions avec les contrats d'accréditation des bureaux d'enregistrement, et on nous demande de faire la même chose. Les RIRs sont cinq. Alors, nous travaillons avec ces cinq RIRs pour pouvoir développer et coordonner une politique globale pour qu'ils aient tous le même genre de pratique volontaire

garantissant l'exactitude du WHOIS et aussi le processus de recherche d'antécédents.

LAUREEN KAPIN : Pour ce qui est du travail du Groupe sur la sécurité publique, nous voulons avoir davantage de participation et de collaboration avec d'autres groupes de travail au sein de l'ICANN. Nous voulons pouvoir arriver à d'autres acteurs gouvernementaux. Il y a un grand nombre d'organismes avec des personnes qui connaissent très bien certaines questions des gens qui pourraient nous aider dans notre travail et nous servir de guide. Il y a, bien entendu, d'autres parties intéressées au sein de l'ICANN qui ont beaucoup d'informations très importantes pour nous, et nous essaieront donc d'y rapprocher et bénéficier de toutes leurs connaissances au sein de la communauté de l'ICANN.

Voilà donc un panorama général du type de travail que nous avons fait jusqu'ici dans notre groupe de travail. Nous espérons continuer de progresser à l'avenir.

Je voudrais savoir si vous avez des questions à poser sur ces questions parce que ce serait le bon moment pour vous d'utiliser les micros disponibles dans la salle.

Il y a d'autres présentations, mais nous trouvons que c'est plus organisé de faire la séance de Q & R après chaque présentation.

ALICE MUNYUA : Merci, Bobby et Laureen. Il y a deux micros ici dans la salle. Si vous voulez vous rapprocher vous pour poser vos questions.

Dites votre nom, s'il vous plaît.

VOLKER GREIMANN : J'appartiens au Conseil de la GNSO pour le Groupe des parties prenantes des bureaux d'enregistrement. Depuis le début, nous travaillons sur l'exactitude du WHOIS. C'est une question importante. Cependant, il y a aussi la question de l'anonymisation, de la privacité. Je voudrais savoir si ce groupe de travail, avec les antécédents qu'il a, il peut aussi travailler sur les conséquences de la privacité en matière de WHOIS, sur l'exactitude aussi par rapport aux utilisateurs de noms de domaine et voir comment on peut protéger les données privées des titulaires des noms de domaine. C'est un WHOIS dont vous avez besoin ou quelque chose de différent?

ROBERT FLAIM : Je crois que ces questions seront répondues lorsque Catherin va vous parler de la protection des données en Europe et d'autres

questions qui créent des défis dans les prochaines générations et trouver un équilibre entre ce qui fonctionne ou pas. Je pense que nous allons pouvoir répondre à vos questions pour pouvoir aborder vos inquiétudes.

VOLKER GREIMMAN : Parfait. Merci.

ARTHUR ZONNENBERG : Bonjour. Je m'appelle Arthur Zonnenberg, je travaille pour un bureau d'enregistrement hollandais, Hostnet, accrédité par l'ICANN. En plus de ce point de l'Union européenne, quelles seraient les questions à traiter par la Commission fédérale du commerce en matière de vie privée et par rapport à l'Union européenne? Je voudrais savoir quels sont les fondements, par exemple, sur ce que vous avez parlé lorsque l'on donne les données de la carte de crédit. Cela vous donne le droit de savoir qui est derrière le site Web, à savoir qui on a affaire. Et dans le cas d'une affaire en ligne, ce serait logique pour recevoir un service. Mais s'il s'agit d'un activiste qui travaille contre certains intérêts, voilà donc pourquoi il veut maintenir la vie privée, le respect des données de la vie privée. Alors, il faudra respecter la confidentialité pour donner du soutien aux personnes qui travaillent en faveur de certains intérêts. Les États-Unis ont fait

l'objet de critique normalement parce qu'il répond à ces intérêts. Je voudrais savoir si le fait que je vous donne le détail de ma carte de crédit vous habilite à connaître mes données personnelles.

LAUREEN KAPIN : Je veux dire qu'il y a différentes opinions par rapport à cette question. Du point de vue de la protection du consommateur, s'il y a quelqu'un qui donne – qui fournit ces données sensibles, vous pouvez être en désaccord, bien entendu. Nous considérons que nous avons le droit de savoir à qui nous avons affaire. Et je comprends bien les questions sensibles ayant trait aux groupes qui défendent certaines positions. Ils peuvent défendre leur propre point de vue, mais si on a affaire à des informations sensibles, nous considérons que les consommateurs et que le public a le droit de savoir avec qui il a affaire, avec qui il est en contact. Et voilà un point de vue. Nous savons bien que ce n'est pas tout le monde partage notre point de vue.

ALICE MUNYUA : Allez-y.

GLORIA : Bonjour. Je n'ai pas une question, mais j'ai un commentaire. Ceci vient du GAC, mais ici, il y a des membres des organismes de l'application de la loi et il y a des membres d'autres pays qui n'ont pas participé à ces procédures. Je m'appelle Gloria et je viens de l'Ouganda.

LAUREEN KAPIN : Merci.

ALICE MUNYUA : Lee.

LEE HIBBARD : Bonjour. Je suis Lee Hibbard de Strasbourg, du Conseil de l'Europe. J'appartiens à une organisation formée de 47 pays. On a assigné la Convention de Budapest, la Convention de cybercriminalité et nous travaillons aussi sur la vente de médicaments en ligne, les soins de santé et la question des pharmacies sur Internet. Je veux que le Conseil de l'Europe participe aussi. Nous sommes membres observateurs du GAC et nous aimerions bien participer et collaborer avec la connaissance et l'expérience des différents groupes du Conseil de l'Europe. Nous avons beaucoup à partager avec vous et nous

le ferons dans votre liste de diffusion où nous avons envoyé des commentaires.

En juin de cette année, ces 47 pays ont accordé une déclaration sur l'ICANN, les droits de l'homme et l'état de droit. Cela pour garantir que l'ICANN respecte les procédures et les droits de l'homme dans ces politiques et ces procédures. Je vais donc vous passer cette information à travers mon collègue Peter, qui va prendre la parole.

PETER KIMPIAN : Bonjour. Je m'appelle Peter. Je représente le T-PD du Conseil de l'Europe qui est un organe consultatif qui s'occupe de la Convention 108. Je suis heureux d'être ici.

Comme mon collègue, je veux coopérer et collaborer avec notre connaissance et notre expérience sur la protection de données dans la mesure du possible. Je crois que comme notre collègue des États-Unis l'a bien dit, le mot correct serait « équilibre ». On peut toujours trouver une solution. Et le mieux - et je le dis comme fonctionnaire qui travaille comme autorité de protection des données - le mieux, c'est de s'assoir, de débattre des questions et de définir les meilleures solutions possibles. Nous sommes heureux d'être ici, je le répète, et nous offrons notre

collaboration, notre énergie, nos connaissances et notre expérience. Merci beaucoup.

ALICE MUNYUA : Merci au Conseil de l'Europe. Nous aurons une réunion avec vous au GAC.

David.

DAVID CAKE : Je veux faire deux commentaires. Un commentaire spécifique et un commentaire général. Le premier, c'est que nous avons reçu vos commentaires au Groupe de travail PPSAI et – gardez à l'esprit que nous considérons tout cela. Mais nous avions déjà débattu de ces questions en profondeur. Nous avons reçu 60 000 réponses du public en général. Vous êtes arrivés un peu tard avec votre collaboration, alors, je crois que vous devez participer de manière plus précoce. Je sais bien qu'il s'agit d'un nouveau groupe, mais je voulais vous informer qu'il faudrait peut-être davantage de participations de votre part.

Et l'autre commentaire, plus général, les organes chargés de la protection des données et les lois de protection, eh bien, sont consacrés à la sécurité publique et à la protection des données. Mais dans votre groupe, ils sont absents.

Alors, nous pensons qu'ils ont leur mot à dire ici et ils veulent faire entendre leur voix. Ils sont une partie très importante de l'application de la loi, alors il est important que vous soyez un groupe qui représente tous les points de vue des organes de la sécurité publique et de l'application de la loi.

Je vous suggère donc d'être plus inclusif, notamment pour les organismes qui ont trait à la sécurité publique et à la protection de données.

ALICE MUNYUA : Merci, David. Nous, nous ne nous sommes pas un groupe qui fait du lobbying.

DAVID CAKE : Je comprends bien, mais vous devez vous assurer d'être suffisamment inclusif et justement, inclure toutes les voix. Et vous devez aller les chercher.

ALICE MUNYUA : Nous prenons très au sérieux ces commentaires. Hier, nous avons parlé de la question lorsque vous avez participé à des débats à la GNSO, et la question est apparue du fait que le GAC doit participer de manière plus précoce, normalement dans le PDP.

On travaille pour y parvenir, mais il faut comprendre aussi comment nos gouvernements fonctionnent. Il faut consulter avec nos parties prenantes, il faut consulter nos villes capitales. Et je m'excuse si nos commentaires arrivent un peu en retard. On va faire tout notre possible pour travailler dans les processus de plus près.

Il y a des membres qui vont participer de différents groupes de travail pour pouvoir faire leurs apports de manière directe comme groupe de travail du GAC. Merci de vos commentaires.

DAVID CAKE : Je comprends bien que ce groupe est relativement nouveau, et certains groupes de travail vous précèdent, alors vous ne pouvez pas participer dès le début, bien entendu. Je vous félicite du travail du Groupe de coordination du GAC et de la GNSO pour que le GAC puisse participer de manière plus précoce dans le PDP de la GNSO. La GNSO veut recevoir votre contribution, et nous voulons les recevoir le plus tôt possible parce que ce sera mieux pour tous, notamment la contribution du GAC et si toutes ces contributions arrivent rapidement, eh bien, l'idéal serait de les recevoir après le rapport initial. Et cela pourrait servir à indiquer la route à suivre par un groupe de travail. Ce serait plus facile et mieux pour tous, et cela pourrait nous aider à donner une réponse pour faire nos conclusions.

ALICE MUNYUA : Merci, David.

AMADAOU LY : Je suis membre du Collège de régulation des télécommunications et des postes de la République du Sénégal. Donc, je vous félicite et je remercie l'ensemble du Groupe de travail. Je m'interroge beaucoup sur la question de la sécurité, la sécurité et la confidentialité, la sécurité des informations surtout pour les pays comme les nôtres, Sénégal et les pays africains, où, aujourd'hui, jusqu'à maintenant, il y a des personnes qui travaillent au sein des administrations et des gouvernements qui utilisent encore des adresses mail génériques, comme Yahoo, Gmail, etc. Et le niveau de l'Internet n'est pas arrivé à un niveau où on a des .GOUV dans nos pays. On a des hauts cadres qui travaillent partout partout dans les administrations et qui travaillent, avec une adresse mail à la volée, qu'ils ont construite depuis qu'ils étaient étudiants ou depuis qu'ils ont commencé à travailler. Donc, cette question est fondamentale. Et donc, l'Internet aujourd'hui est utilisé à un niveau où on ne peut pas le soupçonner. Où des gens travaillent avec des données confidentielles, dans des présidences, des républiques, dans des primatures, dans des administrations de haut niveau et qui ne se rendent pas compte qu'ils utilisent

Yahoo, Gmail, etc., etc. Et donc, est-ce qu'on peut protéger ces personnes-là sans pour autant travailler avec les *data bases*, les sites qui ont les *data bases*, les bases de données importantes? Où les gens vont loger leurs informations confidentielles aux États-Unis, au Singapour, partout! Sans se rendre compte qu'ils ont des données puissantes des états qui sont hébergés ailleurs parce que simplement dans les administrations, il n'y a pas de politiques de DSI, il n'y a pas de politiques de gestion de messages, etc., etc., et c'est plus flagrant quand, à l'international, on voit certaines cartes de visite des gens qui ont Yahoo, Gmail, etc.

Et donc, au-delà de ces aspects-là purement techniques et technologues, est-ce que vous travaillez avec les personnes qui ont des données importantes et qui hébergent des données importantes? Quelles sont les articulations entre ce que vous faites et leur responsabilité à eux, votre responsabilité? Où est-ce que se limite la - où est-ce que se trouve la limite? Ou, en tous cas, le travail que vous pouvez faire les uns et les autres pour pouvoir sécuriser les gens pour ne pas travailler qu'en amont? Parce qu'on peut faire des *firewalls*, mais tout ce qu'on peut mettre en amont, si, au niveau des bases de données, on n'est pas sûr de la transaction, on n'est pas sûr de la transition, on n'est pas sûr du cheminement des informations sur lesquelles on travaille, je pense qu'il y a un gros problème, en tous cas, de

mon point de vue, qui nécessite beaucoup plus de réflexion et de travail ensemble avec les différentes parties prenantes, les différentes personnes qui interagissent pour qu'un mail soit acheminé pour qu'une donnée soit transitée.

Je vous remercie.

LAUREEN KAPIN : Je crois que vous avez présenté des questions très importantes. Il faut bien évidemment faire une tâche de formation, d'éducation pour que le public connaisse comment être sûr lors des transactions Internet et savoir comment gérer les courriers, comme Gmail ou Yahoo, même si l'on dit qu'ils appartiennent au gouvernement. Je ne pourrai pas répondre à toutes vos questions, qui sont très complexes, mais ce que je sais, c'est que l'on a un besoin réel d'éduquer le public pour qu'il soit très prudent lors de l'utilisation de l'Internet, lorsqu'ils achètent un produit, lorsqu'ils accèdent à un site de réunion parce qu'ils ont reçu un courrier qui leur dit qu'ils ont gagné un concours ou parce que quelqu'un est amoureux et a besoin d'argent immédiatement. Ce sont des questions très importantes qu'il faut garder à l'esprit et sur lesquelles il faut travailler parce que vraiment l'avis des gens peut être affecté de manière très négative parce qu'on veut profiter d'eux si Internet.

ALICE MUNYUA : Avez-vous un autre commentaire ou une autre question?

AMADOU LY : Le fond de ma question la plus profonde, c'est quelle – comment nous, ICANN, on travaille avec les parties prenantes, telles que Google, les grosses entreprises qui gèrent les *data bases*? Qu'est-ce qu'on fait avec eux, de manière générale, pour essayer de subtiliser encore davantage les données qui transitent? Même si en amont, je suis d'accord avec vous, chacun doit être vigilant, chacun est responsable de ses actes sur la toile, mais je pense qu'il y a une responsabilité assez profonde de l'ensemble des grandes entreprises des grosses bases de données et qui hébergent nos transactions. Donc, c'est un peu ça. Mais je suis tout à fait d'accord avec vous qu'il faut être vigilant. Mais c'est surtout : quelles sont les mesures qu'on peut prendre ou, en tous cas, qu'on est amené à prendre pour aller au-delà et essayer de sécuriser davantage? C'était un peu le sens de mon propos.

ALICE MUNYUA : Merci beaucoup de vos commentaires. Mais il faut passer maintenant à la prochaine section. Ma collègue de la Commission européenne, Catherin, va vous parler de certaines

questions liées à ce que l'on vient de parler, le WHOIS, la loi de protection de données, et là, nous aurons peut-être plusieurs exemples qui nous montre la manière d'aborder ce genre de questions dans certains pays africains et ailleurs.

CATHERIN BAUER-BULST : Merci, Alice.

Je ne sais pas comment je peux donner des solutions pour tout le monde, mais j'aime voir qu'il y a beaucoup d'intérêt sur la question. Comme Laureen l'a déjà mentionné, il est nécessaire d'arriver à un équilibre. Et d'après mon expérience dans ce genre de débat, il y a eu toujours un bénéfice lorsque l'on commence avec des évidences solides.

Je voudrais faire une brève introduction sur les normes de l'Union européenne qui gèrent la protection de données et les conséquences de ces normes pour des processus comme la reconception du WHOIS.

Quand je préparais ma présentation, je voyais l'histoire par rapport à WHOIS, et je me suis rendu compte que l'histoire de cette discussion sur la responsabilité et le fait de savoir si on a besoin d'une réduction de comptes se rapporte également à cette discussion sur le WHOIS. J'ai trouvé la première mention, la première fois que cela a été mentionné, c'était dans la

République de Platon il y a 2 000 ans, où il y avait l'histoire de la personne qui gardait ses moutons et qui voulait, donc, les rendre invisibles pour ne pas qu'ils puissent être attaqués. Donc, il est allé voir le roi et a renversé le gouvernement. Et ce que l'on voit dans ce livre de Platon, on voit qu'il y a un problème de réduction de comptes, de responsabilité. Et la responsabilité a été vue comme une construction morale. Donc, lorsque les autres ne peuvent pas nous voir, il n'y a pas d'encouragements pour agir de manière responsable. Ce serait la morale de l'histoire.

Et je pense que nous ne devons pas forcément ici trouver un compromis. Je travaille en matière de cyberdélit et je me trouve à l'avant-garde de la protection de données pour éviter que des données confidentielles soient volées pour que les images des enfants ne soient pas utilisées pour des délits sexuels. Et nous travaillons pour permettre aux organismes d'application de la loi de prévenir ce type de délit et protéger les gens qui en sont victimes.

J'aimerais représenter les deux visions ici. Je vais faire un récapitulatif par rapport à ce que les organisations de protection d'application de la loi considèrent leur mission. Dans l'affirmation d'engagement de l'ICANN, on parle de l'obligation de garder un accès public, opportun et ouvert à des

informations WHOIS publiques et exactes. Et ici, il faut donc analyser l'efficacité de la politique WHOIS tous les trois ans.

Dans son communiqué de 2007, le GAC a établi des principes par rapport à ce que devrait être le WHOIS. Le WHOIS devrait contribuer à l'application de la loi ou à la mise ne place d'enquêtes et à l'application des lois internationales. Il devrait contribuer également à lutter contre les utilisations frauduleuses et devrait également aider les entreprises et autres entités à lutter contre la fraude et sauvegarder les intérêts du public.

Voyons maintenant les droits fondamentaux du point de vue de l'Europe. La confidentialité des données figure comme un droit dans la charte de l'Union européenne où l'on dit que tout le monde a droit à la sécurité et à la liberté. Tout le monde doit pouvoir être respecté dans sa vie privée, dans sa famille, dans sa maison. Cette charte de l'Union européenne est moderne, en ce sens qu'elle contient des droits qui ont trait à la société informatique. Elle assure la bioéthique et la transparence. Mais la charte est encore plus spécifique en ce qui concerne la protection des données. Dans son article 8, elle fait référence aux droits – à la protection des données à caractère personnel. Ces données doivent être traitées de manière équitable, et tout

le monde peut avoir accès pour s'assurer que ces données soient exactes.

Très bien. Il s'agit des droits clés dans une société démocratique, mais il ne s'agit pas de droits absolus. Chacun de ces droits, le droit à la sécurité, à la confidentialité des données à caractère personnel doit retrouver un équilibre par rapport à d'autres droits fondamentaux.

Je vais brièvement vous montrer quelles sont les dispositions les plus importantes de notre directive, la directive 95-46 CE concernant la protection des données à caractère personnel. À l'Union européenne, cette directive concerne la protection des individus en ce qui concerne le traitement de leurs données à caractère personnel. Nous avons écouté beaucoup d'inquiétudes par rapport au fait qu'il n'y avait pas une directive unifiée en ce sens en Europe pour la protection des données. Et le problème principal, c'est que la base de tout était une directive, à savoir un instrument législatif spécial contraignant au niveau des objectifs, mais qui laisse aux états membres la liberté de décider comment ils veulent la mettre en œuvre au niveau de leurs lois nationales.

Cela veut dire que nous n'avons pas un ensemble unique de lois, mais plutôt 28 lois différentes qui visent le même objectif, à savoir un même objectif, mais différentes lois. C'est un vrai défi

et nous travaillons sur la rédaction nouvelle d'une nouvelle loi sur la protection des droits pour qu'il n'y ait pas besoin de mettre en place la loi ou appliquer la loi différemment dans les différents états.

Nous pouvons donc avoir des réponses plus cohérentes de la part des pays européens une fois qu'on aura appliqué cet instrument.

Je voudrais vous expliquer très brièvement la définition de « données à caractère personnel » que l'on utilise dans l'Union européenne. Il s'agit de toute information liée à une personne identifiée ou identifiable. On ne parle pas de la sensibilité de l'information ici. Le seul facteur fondamental ici est le fait de savoir si l'on peut identifier ou pas une personne. Un nom, une adresse IP peut être considéré une donnée à caractère personnel. Dans l'exemple de l'Union européenne, un citoyen qui travaille pour la Commission européenne et qui a plusieurs citoyennetés peut être considéré comme ayant des données personnelles. Ces différentes citoyennetés peuvent être considérées comme des données personnelles. Peu importe si l'information est sensible ou pas, il s'agit de données à caractère personnel.

Il y a un autre concept clé qui a été déjà mentionné. Tout ce que l'on fait avec les données, c'est les traiter. On peut les stocker,

les éliminer, les divulguer, mais tout cela rentre dans ce que l'on appelle le « traitement ». Quand on collecte des données pour les traiter, il faut qu'il y ait un objectif spécifique. Le nombre de données doit être pertinent par rapport à l'objectif poursuivi, l'information doit être mise à jour. On ne peut pas garder l'information plus longtemps que nécessaire et tout exercice doit avoir une raison légitime. C'est-à-dire que la personne, le propriétaire de ces données doit avoir donné son consentement ou parce que ces informations sont nécessaires pour signer un contrat, etc.

Qui sont les acteurs pour la protection des données? Je vous ai parlé de l'adoption des réglementations par le Parlement européen et le Conseil de l'Union européenne, ces acteurs, ce sont - la Commission européenne qui doit proposer les lois et surveiller leur mise en œuvre. Ensuite, on a les autorités de données au niveau national qui doivent surveiller la mise en œuvre de la protection des données au niveau national et ensuite, le Groupe de travail sur les articles 29, dont vous avez entendu parlé probablement parce que ce groupe a fait des commentaires dans différentes consultations, il s'agit d'un groupe de travail qui regroupe les autorités liées à la protection de données au niveau national et la Commission dans une fonction consultative. Ce groupe conseille par rapport à la mise en place des lois de protection.

Et puis, on a la cour de justice de l'Union européenne, le seul organe autorisé pour interpréter les lois en matière de protection de données. C'est eux qui nous donnent les réponses en ce qui concerne la mise en œuvre des réglementations en matière de protection de données.

Qu'est-ce que cela veut dire du point de vue du WHOIS? On est en train de modifier le WHOIS. Et il y a trois éléments clés dont il faut tenir compte du point de vue de la protection des données dans l'application de la loi. D'un côté, la disponibilité. Comme on vient de l'apprendre, ces données doivent être collectées à des fins légitimes, pour des raisons légitimes, avec le consentement de la personne faisant l'objet de ces données. Et tous les services de répertoire doivent s'assurer qu'ils soient très clairs, l'objectif ou la finalité pour laquelle on utilisera ces données. Il y a une composante de responsabilité ici. La collecte de données doit correspondre à l'objectif souhaité. Et le fait qu'il s'agisse d'un système public et que l'ICANN, dans son affirmation d'engagement, ce soit engagé à le préserver ainsi, c'est un élément clé du point de vue de la protection des données. La directive ne dit rien par rapport à la limitation de l'accès aux données. Mais si l'on pense à l'esprit de la loi, ce serait très utile de ne pas divulguer les données de manière non nécessaire.

En ce qui concerne l'exactitude, c'est assez simple, parce que quand on parle des organisations d'application de la loi et de la protection des données, nous voulons tous que les données soient exactes.

Voilà tout ce que je voulais vous dire. Et avec grand plaisir je répondrai à vos questions.

ALICE MUNYUA : Merci, Catherin.

Est-ce qu'il y a des questions ou des commentaires? Je vous prie de vous rapprocher du micro pour faire vos commentaires.

Nous pourrions donc avancer et passer à la présentation suivante où nous allons voir des exemples de WHOIS. Greg va faire cette présentation. Il appartient au Centre de cyberdélit européen.

GREGORY MOUNIER : Merci.

ALICE MUNYUA : Ah, pardon, il y a une question.

VOLKER GREIMANN : J'appartiens au Groupe de bureau d'enregistrement du Conseil de la GNSO.

Je tiens à vous remercier de cette présentation tellement intéressante sur la position européenne en matière de protection de données. Pour beaucoup d'entre nous, dès le départ, il était très clair que le WHOIS, tel qu'il existe aujourd'hui, a beaucoup de données à caractères privé, de millions de citoyens qui sont publiés de manière quotidienne, et cela pose problème du point de vue de la protection des données au niveau de l'Europe ainsi qu'au niveau d'autres pays.

Nous avons besoin de mettre en place une révision claire, comme celle qui a lieu maintenant pour nous assurer que ces données ne soient pas librement disponibles comme c'est le cas aujourd'hui. Et du point de vue du groupe de travail sur la sécurité publique, comment ce type de régime devrait être mis en œuvre?

CATHERIN BAUER-BULST : Je suis d'accord avec vous pour dire que l'idéal, ce serait qu'il n'y ait pas un accès ouvert et complet à toutes les données qui sont disponibles. Mais comment peut-on trouver un compromis entre cela et la fonction que doit assurer le WHOIS dans la pratique? Dans l'Union européenne, il existe des lois qui exigent

que certaines informations soient publiées sur les sites Web, par exemple pour tout acteur qui n'agit pas à titre personnel, c'est-à-dire qui ne publie pas ses propres photos, mais plutôt les photos de sa famille, de ses amis, etc. Dans ce cas, la personne doit inclure dans son site Web des informations détaillées de contact pour pouvoir assumer la responsabilité, au cas où un délit serait commis.

Il est très difficile, donc, de retrouver un équilibre. À ce stade, je ne suis pas sûr qu'il existe un système parfait, mais il faut essayer d'écouter les avis des uns et des autres et trouver une solution de compromis. Malheureusement, on n'a pas de solution parfaite.

VOLKER GREIMANN : Je comprends très bien qu'il n'y a pas de solution parfaite, mais lorsque vous présentez ce sujet, il est important d'établir une différence par rapport au contenu, par exemple, qui peut apparaître sur un site Web où des informations sont exigées pour, par exemple, ne pas mettre les adresses privées des individus. Et une différence entre cela et l'enregistrement des noms de domaine qui peuvent être utilisés pour envoyer des courriers électroniques parce que les titulaires sont obligés de publier des données privées. J'aimerais donc savoir comment des registres européens gèrent et publient les données WHOIS,

ce que Nominet, ce que fait d'autres registres de l'Espace européen. Il y a beaucoup de données qui sont visibles au public. Il y a des données qui se limitent à un nom ou à une adresse parfois. Mais il est important que l'on puisse voir cela pour établir un modèle pour la présentation des données à caractère privé lorsqu'on analyse cela dans le contexte de l'ICANN.

ALICE MUNYUA : S' il vous plaît, vous pouvez vous présenter.

DAVID CAKE : David Cake, membre du Conseil de la GNSO.

Encore une fois, j'ai un commentaire général et un commentaire spécifique. De manière générale, je crois que c'était une présentation très intéressante - merci beaucoup -, car elle met l'accent sur le besoin de penser aux différents éléments du WHOIS et aux principes auxquelles nous devons adhérer à long terme.

On parle aussi des critères qui pourraient changer ou des prérequis qui pourraient changer. J'ai vu cela dans les différents sites Web que l'on envisageait de fermer parce qu'il ne respectait pas certains critères. Je pense que l'on doit être

flexible quand même et trouver un équilibre entre les éléments qui peuvent changer, les éléments qui ne peuvent pas changer.

Et puisque l'on parle des éléments qui peuvent changer, nous avons les services d'annuaire de données d'enregistrement de nouvelles générations, RDS, il y a un PDP concernant ces services sur lequel travaille la GNSO.

Et il y aura un grand effort pour essayer de répondre aux questions en ce qui concerne l'accès à certaines données, quelles sont les données collectées, etc., qui peut voir les données…

Il est important qu'il y ait une participation dans la période de consultations publiques. Mais il serait important aussi que l'on puisse travaillera avec le Groupe de travail sur l'article 29 ou des entités qui puissent avoir une expertise profonde en matière de protection de données. Je pense que cela serait vraiment très utile parce que cela nous permettrait de répondre à des questions spécifiques.

Je vous suggère donc d'essayer de faire en sorte que des gens ayant ce type d'expertise puissent participer à votre travail.

Je pense qu'à l'ICANN, il nous faut trouver ces gens qui ont des expertises par rapport à leur confidentialité des données,

comme c'est le cas des gens qui travaillent dans ce groupe de travail sur l'article 29.

ALICE MUNYUA : Très bien. C'est pour cela que le Groupe de travail a créé ce groupe de travail. Nous allons nous assurer – nous allons faire en sorte que les gens ayant cette expertise puissent participer à ce processus de manière précoce. Merci.

KIRAN MALANCHARUVIL : Kiran Malancharuvil de MarkMonitor. En ce qui concerne le Groupe de parties prenantes de registres, je pense qu'il y a des positions divergentes par rapport à ce qui a été dit dans les commentaires sur le Groupe de travail qui travaille, en ce qui concerne les services d'anonymisation et d'enregistrement fiduciaire. On encourage un accès ouvert aux informations de WHOIS pour ce type de données.

J'aimerais que l'on m'explique ou que l'on me clarifie cela, car je pense qu'il y a certains éléments que vous avez présentés qui sont – qui vont à l'encontre de ce qui a été proposé.

CATHERIN BAUER-BULST : Vous parlez de moi?

KIRAN MALANCHARUVIL : Oui.

CATHERIN BAUER-BULST : Très bien. Je ne m'en étais pas rendu compte. Je ne suis pas très sûre de savoir où est la contradiction. Ce que je voulais vous présenter, ce sont deux perspectives différentes. D'un côté, la situation idéale du point de vue de la protection des données et d'autre part, la situation idéale du point de vue des organismes d'application de la loi.

Comme je vous ai dit au début de ma présentation, il y a le droit à la sécurité et le droit à la vie privée. Et ce sont des droits fondamentaux du point de vue de l'Union européenne et dans d'autres régions du monde. Aucun de ces droits ne peut être exercé de manière absolue. Dans la pratique, ce que l'on essaie de faire, c'est de parvenir à un équilibre. C'est ce que l'on doit faire dans ce processus d'élaboration de politiques.

Merci encore de m'avoir invitée à – merci d'avoir suggéré que des gens représentant le Groupe de travail sur l'article 29 puissent participer. Je vais me charger de contacter ces personnes et je vais m'assurer qu'ils sachent que vous voulez qu'ils participent.

Nous espérons pouvoir retrouver un équilibre dans ce processus entre ces deux droits fondamentaux. Aucun de ces deux droits ne peut prévaloir et donc, je ne pense pas qu'il y ait une contradiction ici.

KIRAN MALANCHARUVIL : Je pense que ce serait utile que ce groupe de travail tienne compte des commentaires qui ont été faits. Et ce serait intéressant d'avoir un exemple de ce que vous nous dites par rapport à l'équilibre recherché entre ces deux droits. Nous voulons, bien sûr, une certaine ouverture dans les informations du WHOIS, et que cela soit équilibré par rapport au besoin de protection des données à caractère privé. Il ne faut donc pas faire de déclaration absolue en ce qui concerne les informations du WHOIS.

CATHERIN BAUER-BULST : Je comprends très bien ce que vous dites. Et du point de vue de l'application de la loi, si nous n'essayons pas de faire en sorte que l'accès aux informations soit ouvert, ce serait difficile de faire autre chose. Donc, il faut se concentrer sur le PDP de manière très prudente.

ALICE MUNYUA : Je donne la parole à Greg.

GREGORY MOUNIER : [*Presentation not interpreted*]

ALICE MUNYUA : [*Speech not interpreted*]

OLOF NORDLING : [*Question not interpreted*]

ALICE MUNYUA : [*Answer not interpreted*]

GREGORY MOUNIER : [*English Spoken*]

… je crois qu'il y a un portfolio de l'Interpol bien plus vaste pour donner le soutien aux informations en Afrique. Je crois que mes collègues ont quelque chose à dire.

CATHERIN BAURR-BULST : Nous avons ce type de programme de création de capacités pour les pays africains et nous avons de nouvelles opportunités de disposer des fonds pour les pays africains. Et nous analysons

cela dans le domaine de la création de capacité en matière de cyberdélit.

ALICE MUNYUA : Malheureusement, nous n'avons plus de temps. Il y a cinq personnes qui veulent poser des questions. Je vous demande d'être brefs pour que le reste, les membres du panel puissent faire leur présentation.

Merci beaucoup.

Elliot.

ELLIOT NOSS : Elliot Noss de Tucows.

Merci d'avoir répondu à deux de mes cinq questions. Tout d'abord, vous avez fait un très bon travail du fait d'avoir décelé la robustesse pour les recherches. Nous savons bien que les délinquants ou les criminels font des erreurs bêtes, et cela se passe aussi dans les affaires. Ceux qui font des erreurs bêtes ne restent pas le marché : ils ont été remplacés par des gens plus intelligents. Mais quand on a affaire à la communauté qui se consacre à la sécurité, il faut parler avec eux de leur expérience avec les bureaux d'enregistrement et de leurs échanges avec les bureaux d'enregistrement pour obtenir des informations.

GREGORY MOUNIER : Vous l'avez fait. Je n'ai pas parlé des rapports avec les bureaux d'enregistrement, mais les chercheurs me disent qu'en général, s'ils ont une bonne relation avec un bureau d'enregistrement, ils reçoivent une bien meilleure coopération que lorsque cette relation n'existe pas. Alors, on est en train d'éduquer les éducateurs pour créer une relation positive avec les bureaux d'enregistrement et avec le secteur privé qui, pas mal de fois, a les outils pour résoudre une recherche d'un cyberdélit, de sorte que le secteur privé sache quelles sont nos limitations, ce que nous faisons et qu'il nous donne les informations dont nous avons besoin.

ELLIOT NOSS : Je crois que cela est encourageant. Ce n'est pas seulement une relation personnelle : il y a beaucoup de données qui sont très importantes pour une enquête ou une recherche.

En deuxième lieu…

ALICE MUNYUA : Elliot, je regrette de vous interrompre, mais nous n'avons que dix minutes. Je regrette de vous interrompre. Je demande au reste des personnes de nous envoyer les questions après la

séance parce que nous n'avons plus de temps pour les présentations.

Merci. Vous pouvez poser votre question qui sera répondue plus tard.

ARTHUR ZONNENBERG : Merci de votre présentation. J'essaie de comprendre ce que vous avez décrit par rapport aux erreurs bêtes des cyberdélinquants. Je comprends aussi ce que vous avez dit par rapport à l'adresse de courrier électronique et de son importance. Par exemple, s'il y a quelqu'un qui vole l'identité de Catherin et a une copie de son passeport, moi, comme bureau d'enregistrement, comment puis-je savoir que ce n'est pas Catherin qui le fait? La seule chose que je peux faire, c'est lui demander si elle a enregistré un nom de domaine quelconque.

Alors, en général, nous contactons les gens par téléphone, mais il peut y avoir quelqu'un qui réponde par téléphone et qui me dise : « Oui, je suis Catherin », mais je ne sais pas qui c'est, Catherin.

Alors, comment trouvez-vous que moi, je puisse valider ce que je fais pour valider l'identité avec des méthodes que je ne vais pas divulguer. Et d'autre part, je n'ai aucun problème du fait que vous, vous ayez mes données. Mais j'ai des problèmes sur le fait

que mes opposants politiques possèdent mes données si je suis activiste d'une cause politique.

ALICE MUNYUA : Nous n'allons pas répondre aux questions maintenant. Vous pouvez continuer à les poser. Nous allons y répondre plus tard parce qu'il y a encore deux présentations qui nous restent.

ASHWIN SASONGKO : Bonjour. Je m'appelle Ashwin de l'Indonésie.

En Europe, nous avons un concept qui dit « connaissez votre client ». C'est-à-dire qu'une banque doit savoir exactement qui est son client et voir le document d'identité. Et la même chose si vous voulez un courrier électronique, il faut savoir de qui il s'agit. Si une société veut avoir un site Web, il faut savoir quelle est la personne de contact technique et où sont situés les bureaux de la société. Merci.

ALICE MUNYUA : Merci.

Allez-y.

PETER KIMPIAN : J'ai une question. Il est peut-être important de signaler qu'Europol travaille conjointement avec un régime de protection de données de très haut niveau, notamment sur EC3. Et il y a un groupe d'Europol qui mène des enquêtes sur la protection des données, le traitement de données au sein d'Europol et qui connaît très bien, qui a beaucoup d'expériences sur la question. Et je reviens à ce que j'ai déjà dit à Europol, il y a beaucoup d'expertises qui peuvent être importantes dans les organismes d'application de la loi et dans toute la structure de notre secteur dans l'avenir.

WANAWIT AHKUPUTRA : Je crois qu'il faut continuer. Je passe la parole maintenant au représentant du Royaume-Uni, du PSWG, qui a commencé à innover, à travailler. Ils vont partager avec nous le travail effectué dans leur pays.

Nous passons la parole à Nick Shorey en premier lieu.

NICK SHOREY : Merci beaucoup. Je travaille à l'Équipe du GAC, et donc je travaille dans ce sous-groupe du GAC qui travaille sur les activités de sécurité publique.

Avant de m'occuper de la gouvernance de l'Internet, j'étais enquêteur en matière de cybercriminalité et des problèmes de protection du consommateur. Donc, je peux voir cette question à partir de différentes optiques. Au Royaume-Uni, nous avons un grand nombre d'organisations gouvernementales qui sont responsables et qui s'intéressent à la sécurité publique, y compris la sécurité sur Internet.

Pour répondre au lancement du PSWG, c'est-à-dire le Groupe de travail sur la sécurité publique, nous avons réuni tous les départements afin de mener à bien une consultation par rapport à ces sujets. Nous avons donc parlé avec le Bureau des douanes, le bureau qui se charge de la propriété intellectuelle, le bureau régulateur des médicaments, d'autres organes qui se chargent de la lutte contre la criminalité ainsi que la Coalition de lutte contre l'exploitation des enfants. J'ai ici John Carr qui appartient à cette coalition.

Donc, nous espérons pouvoir répondre à cette question qui a été posée par David par rapport à la portée de notre travail au sein du Groupe de travail sur la sécurité publique.

Dans ce domaine, les gouvernements manifestent des préoccupations de manière très claire. Il y a beaucoup de personnes qui travaillent à ce sujet et qui essaient, donc, d'interagir avec la communauté de l'Internet. Il y a des solutions

pratiques qui ont été trouvées. Ici, à ma gauche, nous avons John Flaherty qui est enquêteur et expert en la matière. Il va nous raconter un petit peu ce qu'il a fait quand il a travaillé dans le Groupe sur la spécification 11. Nous avons eu des réunions mensuelles à Londres pour élaborer des recommandations de consensus qui feront partie de la réponse du Royaume-Uni, au PSWG. Mais c'est une façon excellente de partager des expériences et d'échanger par rapport à la question des meilleures pratiques en tant que gouvernement, pour voir comment nous pouvons travailler de manière efficace avec la communauté Internet et essayer d'apporter une solution à ces problèmes.

Comme Fadi l'a dit ce matin, l'ICANN fait partie de l'écosystème de l'Internet. Il n'est qu'une partie de cet écosystème. Et dans notre travail sur la gouvernance de l'Internet, nous voyons qu'il s'agit d'un élément dans une stratégie plus ample. Nous participons au forum sur la gouvernance de l'Internet, ça en est un bon exemple, ainsi que dans le Conseil de l'Europe.

WANAWIT AHKUPUTRA : Nous n'avons que deux minutes.

NICK SHOREY : D'accord. Excusez-moi, alors.

Nous voyons cela comme faisant partie d'une stratégie plus globale. Nous essayons de développer des ateliers d'une journée. Nous aimerions bien que les bureaux d'enregistrement ainsi que les sociétés qui s'occupent d'analyser les cybermenaces puissent contribuer au travail de ce groupe. Nous voulons encourager la participation et l'échange entre le gouvernement et la communauté de l'ICANN pour développer des solutions qui puissent être pratiques pour les uns et pour les autres.

Comment participer si vous êtes membres d'un organe de la sécurité publique du gouvernement? Vous pouvez travailler avec les représentants gouvernementaux qui soient présents à l'ICANN. Le Groupe du Royaume-Uni peut également faciliter la participation d'autres membres ou peut faciliter le contact avec d'autres membres du GAC pour que vous puissiez prendre contact avec les organisations concernées. Parfois, on ne sait pas à qui s'adresser, donc vous pouvez vous adresser à nous et nous pouvons vous donner le point de contact au G7 ou quelqu'un qui travaille à la réservation de données au Conseil de l'Europe. Si vous appartenez à une communauté, vous pouvez travailler de manière directe au processus de l'ICANN et vous pouvez ainsi collaborer pour trouver des solutions pratiques qui soient bénéfiques pour les uns et les autres. Merci.

WANAWIT AHKUPUTRA : Nous n'avons plus de temps. Je suis désolé. Je m'excuse. Nous n'avons que deux minutes pour votre intervention.

JOHN FLAHERTY : Très bien.

Est-ce que je pourrais parler plus vite que ça?

La Spécification 11, on en a parlé déjà, elle concerne l'utilisation frauduleuse par rapport à l'utilisation des noms de domaine. Cette spécification a été créée à partir de l'avis du GAC à Pékin. Je peux vous en parler rapidement. Je peux vous expliquer quels sont les progrès que l'on a accomplis au niveau du Groupe de travail. On va en reparler cette semaine dans la réunion de l'ICANN.

En ce qui concerne la relation entre le Groupe de travail sur la sécurité publique et les bureaux d'enregistrement, moi, j'ai été – moi, je suis coprésident de ce groupe. J'ai travaillé dans l'enquête des cyberdélits au Royaume-Uni et on n'a pas eu de demandes d'informations. Et jamais on n'a trouvé de solutions. Parfois, un registre met en place des innovations très intéressantes, mais voilà la relation qui existe avec les registres. Et nous n'espérons pas que tous les registres pourraient nous

donner une réponse, mais nous attendons d'eux qu'ils puissent nous aider. C'est pour cela que nous avons créé un cadre qui permet de mettre en œuvre ce type de relations. Nous nous sommes focalisés sur l'utilisation et la sauvegarde des nouveaux gTLDs, la protection des nouveaux gTLDs. Nous avons essayé de répondre aux menaces en matière de cybersécurité qui arrivent à partir des réseaux zombis, de l'hameçonnage, etc. Le Groupe essaie de voir comment les registres répondent aux menaces en matière de sécurité. Nous allons apporter des études de cas dans les séances que nous aurons avec les bureaux d'enregistrement et les registres pour leur montrer ce que l'on fait.

Le Groupe de travail est composé de professionnels, des gens qui travaillent dans l'application de la loi, la police, les registres, les bureaux d'enregistrement. Et maintenant, nous avons une voix, nous pouvons donc essayer d'avoir une influence sur ce cadre.

Tout le monde peut donc approfondir ces connaissances par rapport à ce type de menaces afin de pouvoir identifier les délinquants.

Nous développons donc un cadre de sécurité central que nous – sur lequel nous travaillons pour essayer d'établir les principes qui vont régir ce cadre. Nous voulons être assez souples du point

de vue technique. Nous savons qu'il y a des registres qui travaillent déjà avec ce type d'information. Nous avons développé des principes au niveau de l'ICANN et nous avons rendu disponible une charte. Il n'y a pas encore de politique qui puisse fonctionner pour tous les registres. Ce qui peut fonctionner pour un registre peut ne pas fonctionner pour un autre.

Nous voulons travailler en collaboration pour pouvoir échanger les meilleures pratiques qui existent entre les meilleurs acteurs. Finalement, nous voulons rédiger un document-cadre pour établir les critères de base. Nous espérons que pour la fin janvier 2016, ce document — une version préliminaire de ce document pourrait être publiée pour consultation publique. Merci.

WANAWIT AHKUPUTRA : Nous n'avons vraiment plus de temps. Je vais donner la parole à John Carr pour qu'il fasse sa présentation.

JOHN CARR : Je vais être très bref. Bien évidemment, notre coalition en faveur du bien-être des enfants est très intéressée à ces sujets dont on discute. Nous travaillons de manière très active avec l'ICANN depuis la création de la dernière série de nouveaux gTLDs, et je pense qu'il est évident que si l'on veut créer un espace qui va

nous amener à la création de sites Web, qui ont pour intention d'attirer de grandes quantités de jeunes et d'enfants, à ce moment-là, eh bien, cela peut poser des problèmes au niveau de la sécurité. C'est pour cela qu'il faut agir dès le départ, bien en amont. Nous voulons nous assurer que les erreurs qui ont été faites dans la première série de nouveaux gTLDs ne se répètent pas dans un deuxième processus.

WANAWIT AHKUPUTRA : Merci beaucoup à tous les orateurs. Je m'excuse vraiment parce qu'on n'a plus de temps. Nous allons donc passer en revue les questions qui ont été posées et nous allons publier les réponses sur notre site Web.

ALICE MUNYUA : Nous n'allons pas répondre aux questions en ligne, mais nous vous demandons de poser votre question.

WENDY SELTZER : Merci. Je voulais faire référence à la question de la sécurité publique. En tant qu'auteure d'un des commentaires de ce processus d'enregistrement — des services d'enregistrement fiduciaire et d'anonymisation, je travaille avec les victimes

d'abus, les femmes victimes d'abus, et des cas où des informations privées sont publiées en ligne.

Nous demandons – quand nous avons rédigé ces commentaires, il a fallu se mettre en contact avec les organisations d'application de la loi pour qu'elles sachent que ces informations avaient été publiées sur Internet.

Donc, il s'agit d'un processus circulaire. Beaucoup d'entre nous pensent à la publication parfois obligatoire d'informations. Et c'est un petit peu ce qui se passe avec le WHOIS, cela porte atteinte à la vie privée, et cela pose problème du point de vue de la sécurité publique et privée.

ALICE MUNYUA : Je tiens à remercier tous les membres de ce panel ainsi que le public qui a participé.

La prochaine fois, nous allons avoir besoin de trois heures et non pas une heure et demie. Nous allons essayer de prévoir cela pour la prochaine réunion de l'ICANN.

Merci beaucoup.

[**FIN DE LA TRANSCRIPTION**]