ICANN77 | Forum de politiques – ccNSO : initiatives législatives affectant les ccTLD
Jeudi 15 juin 2023 – 10h45 à 12h15 DCA

CLAUDIA RUIZ : Bonjour et bienvenue à cette réunion concernant les initiatives législatives qui ont un impact sur les ccTLD de la ccNSO. Je suis Claudia. Je travaille avec Bart et Kim et nous sommes les responsables de la participation à distance pour cette séance.

Cette séance est enregistrée et suit les normes de comportement attendues de l'ICANN. Au cours de cette séance les questions et commentaires soumis dans le chat ne seront lus à voix haute que s'ils sont formulés dans la manière indiquée dans le chat. Je lirai les questions et commentaires à haute voix pendant la durée fixée par le président ou le modérateur de la séance.

L'interprétation pour la séance comprendra l'espagnol, le français et l'arabe. Cliquez sur le bouton d'interprétation dans Zoom et sélectionnez la langue que vous écouterez pendant la séance. Si vous souhaitez prendre la parole levez la main dans la salle Zoom et une fois que l'animateur de la séance aura appelé votre nom, activez votre micro. Avant de prendre la parole assurez-vous d'avoir sélectionné la langue dans laquelle vous vous exprimerez si ce n'est pas l'anglais. Mettez en muet tous les autres appareils et notifications. Veuillez indiquer votre nom et parlez clairement et à un rythme raisonnable pour permettre une bonne interprétation de vos propos.

Cette séance comprend une transcription automatisée en temps réel qui n'est pas officielle et ne fait pas autorité. Pour la visualiser, cliquez sur le bouton close caption dans la barre d'outils de Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN nous vous demandons de vous connecter aux séances en utilisant votre nom complet, un prénom et un nom de famille. Vous risquez d'être exclus de la séance à défaut.

Merci. Je passe la parole à Annaliese Williams.

ANNALIESE WILLIAMS: Merci. Bonjour à tous, merci de nous avoir rejoints pour cette nouvelle séance de la ccNSO organisée par le comité de liaison de gouvernance internet à la ccNSO. Je suis de l'administration du .AU et présidente de ce groupe.

Cette séance portera sur les initiatives législatives portant sur la cybersécurité et leur impact sur les ccTLD. Aujourd'hui nous aurons des intervenants du Canada, du Vanuatu, du Mozambique, du Costa Rica et d'ailleurs.

Nous allons voir quelles sont les initiatives législatives qui ont un impact sur les ccTLD et si les ccTLD ont la possibilité d'intervenir à l'élaboration de cette législation et, le cas échéant, ce qu'ils ont fait pour pouvoir modifier l'impact de ces initiatives. Chacun des présentateurs aura une quinzaine de minutes pour leur intervention, puis les questions et réponses. Nous allons essayer de respecter les délais pour que tout le monde puisse présenter et répondre aux questions. Si on a le temps, à

la fin de la séance, nous aurons un petit moment également consacré aux questions et réponses en général.

Pour rappel, nous aurons un service d'interprétation pour la séance, donc rappelez-vous de parler à un rythme raisonnable pour être correctement interprété.

Notre première intervenante, Sabrina, est directrice de programme au sein de CIRA, l'autorité canadienne, elle a travaillé sur différents projets de recherches liés au genre, au journalisme et à la sécurité. Sabrina, à vous.

SABRINA WILKINSON : Merci. C'est un plaisir d'être avec vous aujourd'hui, je suis là pour vous présenter la perspective de CIRA et l'implication de cette autorité avec la législation nationale qui s'occupe de la cybersécurité. Il s'agit d'un projet de loi qu'on appelle BILL C-26 qui avance en ce moment et je vais me consacrer surtout à la deuxième partie de ce projet.

Diapo suivante.

Pour cette présentation, j'aborderai trois questions principales. Tout d'abord je vous parlerai de ce que l'on propose exactement dans cette deuxième partie du projet de loi dans lequel est impliqué CIRA. Je voudrais vous expliquer quelle a été l'implication de CIRA dans ce dialogue par rapport au projet C-26 à ce jour pour ce qui est des positions de politique et leurs plaidoiries et finalement je vais parler des plans de CIRA pour continuer à participer.

Diapo suivante.

Ce projet de loi est composé de deux parties, je vais me concentrer sur cette deuxième partie à laquelle est impliquée CIRA. Ce que ferait cette loi proposée en cas d'être entérinée serait d'être une loi de protection des systèmes et ça s'appliquerait aux opérateurs règlementés au niveau fédéral sur quatre secteurs d'infrastructures essentielles : télécommunication, banque, énergie et transport. Ça permettrait au gouvernement d'impliquer des exigences aux opérateurs désignés des systèmes cybernétiques essentiels, donc plan de cybersécurité, rapports, etc. pour pouvoir développer des programmes consacrés à la cybersécurité, informer des évènements qui pourraient avoir lieu et pour garder des registres spécifiques dans le domaine de la cybersécurité.

Ce projet de loi prévoit d'établir des règlements de donner des ordres pour prendre certaines mesures pour aborder par exemple certaines instances de la cybersécurité, et ça leur donnerait également des pouvoirs d'application et ce qu'aurait le gouvernement dans les cas où ces mesures ne seraient pas prises ou si ces exigences ne seraient pas respectées.

Diapo suivante.

Alors, pourquoi ce projet de loi est d'importance pour CIRA ? Pourquoi nous appliquons-nous à ce dialogue de politique qui est en cours ?

Pour un nombre de raisons. Tout d'abord parce que le projet de loi C-26 a le potentiel, dans sa deuxième partie au moins, de comprendre beaucoup d'opérateurs qui sont au-delà de ceux qui sont déjà impliqués dans ce projet. Par ailleurs les objectifs de la deuxième partie sont en

ligne, les objectifs de la loi proposée, [inaudible], la ligne de l'infrastructure critique est un objectif qui est très en ligne avec la mission de CIRA de générer un domaine de confiance sur internet pour les canadiens. Et c'est également l'occasion d'améliorer ce projet de loi. Donc le projet de loi est pertinent pour nous en tant qu'opérateur de conformité, avec notre mission de générer un internet de confiance. Mais on le voit également comme la possibilité d'avoir un impact déterminant et intéressant et positif sur l'internet pour les Canadiens.

Et on est à Ottawa, donc géographiquement on est près également des espaces où sont prises ces décisions par rapport à la modification de la loi ou à l'adoption de ce projet de loi.

Finalement, notre participation au dialogue de politique concernant le projet de loi C-26 est conçue comme une opportunité de sensibilisation à propos du produit et également pour démontrer notre leadership. C'est-à-dire que CIRA peut contribuer comme un opérateur technique qui a l'expertise pertinente pour la cybersécurité et pour d'autres questions liées qui sont incluses dans le projet de loi. Et c'est également l'occasion de présenter le produit en tant que fournisseur de cybersécurité également.

Diapo suivante.

Dans ce projet de loi CIRA a trouvé différents aspects qui nous préoccupent. Et il y a cependant des domaines où on voit qu'on peut également apporter des améliorations, et c'est là où nous nous impliquons. Ce sont au moins les positions que nous avons au moment

d'essayer de nous mettre d'accord et au moment de décider de la deuxième partie du projet C-26.

En termes généraux, ces préoccupations sont en lien avec trois domaines thématiques clefs ou trois questions clefs.

Nous nous préoccupons à propos de la supervision. Comme je le disais, le projet de loi donnerait au gouvernement beaucoup de pouvoirs et, en particulier à propos de la possibilité que le gouvernement aurait de demander aux opérateurs impliqués par ce projet de loi de prendre des mesures applicables aux situations qui seraient jugées comme des urgences pour nous.

Il existe des dispositions de supervision existantes, mais dans une certaine mesure elles sont limitées.

CIRA se préoccupe également du partage d'information. Étant donné la quantité d'informations qui serait collectée dans le cadre de ce projet de loi si ce projet était entériné, et dans la mesure où ces informations seraient partagées entre beaucoup de parties.

Et, finalement, CIRA se soucie pour la transparence également. Donc nous reconnaissons qu'en matière de cybersécurité, dans une certaine mesure, il est nécessaire et important de garder la confidentialité, mais nous croyons qu'il est possible d'avoir plus de transparence de sorte que les Canadiens et les opérateurs aient plus d'informations sur la manière dont ces ordres envoyés aux opérateurs en particulier sont utilisés.

Diapo suivante.

Alors, pour répondre à ces trois préoccupations que nous avons soulevées, nous avons présenté trois recommandations. À haut niveau, dans notre implication concernant le projet de la C-26, nous demandons à ce qu'il y ait un mécanisme supplémentaire de supervision qui soit ajouté au processus d'envoi d'instruction pour la cybersécurité.

Nous demandons à ce que le partage d'informations dans le cadre de cette loi ne soit limité qu'à certains objectifs d'assurance d'informations pour la cybersécurité parce que nous croyons que les informations collectées dans le cadre de ce projet de loi ne devraient être partagées que dans certaines situations.

Finalement, nous demandons à ce qu'il y ait des rapports de transparence annuels qui soient publiés de sorte que les Canadiens et les opérateurs désignés puissent avoir davantage d'informations sur le fait de savoir comment les instructions sont utilisées par le gouvernement.

Diapo suivante.

Nous avons ces trois recommandations qui s'intègrent à différents amendements législatifs proposés pour répondre à nos différentes préoccupations. Mais, exactement, comment sommes-nous impliqués dans la prise de décision par rapport à la manière dont le projet de loi devrait être élaboré ou amendé dans le processus législatif, avec qui avons-nous échangé, dans quelle mesure avons-nous eu du succès ?

Nous nous sommes impliqués dans trois domaines. Tout d'abord nous nous sommes réunis avec les décideurs et d'autres parties prenantes, à savoir d'autres responsables qui sont impliqués dans ce dialogue à

propos du projet de loi C-26 et comment il devrait être amélioré. Nous avons rencontré les décideurs comme le personnel politique. Nous nous sommes également réunis avec différents fonctionnaires publics de haut niveau qui sont impliqués dans la rédaction de cette loi et qui travaillent dans le domaine de la cybersécurité et de l'infrastructure critique.

Au niveau public, nous avons participé à des espaces comme celui-ci. Nous avons fait partie d'un panel public dans une grande conférence de télécommunication du Canada où nous avons pu partager nos avis en tant que CIRA et discuter avec d'autres qui sont également impliqués dans ce débat et qui sont des experts en la matière.

Et nous avons publié des écrits où nous avons partagé nos avis de politique et la mesure dans laquelle nous croyons qu'elles devraient être intégrées à la loi.

Diapo suivante.

Comment prévoyons-nous de continuer à participer au processus à mesure que ce projet de loi continue à avancer dans le processus ?

Le projet en est à l'étape de comité. Il devrait être révisé par un groupe de parlementaires qui étudie des questions liées à la sécurité publique et à la sécurité nationale. Nous allons suivre de près les progrès du projet de loi à mesure qu'il avancera dans cette étape de comité et qu'il sera examiné par les parlementaires ainsi que par d'autres experts.

Nous allons continuer à nous réunir avec des décideurs et des parties prenantes qui font partie du débat pour pouvoir partager l'avis de CIRA et mieux comprendre ce que pensent les autres, ce qui les motive à agir.

Et nous allons également continuer à défendre publiquement l'opinion de CIRA en particulier en ce qui concerne la deuxième partie du projet de loi C-26 dans le cadre de divers forums publics, par exemple dans les espaces internationaux comme celui-ci mais également dans des réunions nationales.

J'espère vous avoir donné aujourd'hui un petit aperçu de ce qu'implique ce projet de loi dans les grandes lignes, quelle est l'implication de CIRA à ce jour et comment nous prévoyons de continuer à participer.

Je suis là pour répondre à vos questions.

ANNALIESE WILLIAMS: Merci beaucoup. Est-ce qu'il y a des questions ? Allez-y.

SEAN COPELAND: Oui. Je parle en ma qualité de citoyen canadien. Comment est-ce que votre rôle ou velléité de supervision a été reçu ?

SABRINA WILKINSON : Merci Seun. Je dirais que d'une manière générale nos recommandations ont été bien reçues de la part des décideurs politiques ainsi que les parties prenantes avec lesquelles nous nous sommes réunis.

S'agissant du mécanisme de supervision en particulier, on a essayé d'établir un équilibre entre fournir un niveau supplémentaire de supervision tout en maintenant un certain niveau de vitesse et de confidentialité. Parce qu'on sait que dans le domaine de questions nationales c'est essentiel et il est très important d'établir cet équilibre, ce juste équilibre. Et peut-être que si on ne procédait pas ainsi cet équilibre serait modifié.

ANNALIESE WILLIAMS: Merci. Y a-t-il d'autres questions à l'attention de Sabrina ? Ça ne semble pas être le cas. Passons à l'intervenant suivant, Norman Warputt. Norman est gestionnaire de l'organe de règlementation au .VU.

NORMAN WARPUTT: Bonjour à tous et bonsoir à nos participants en ligne. Je suis gestionnaire TIC pour l'organe de règlementation des télécommunications de Vanuatu. Également, ccTLD délégué.

La présentation que je vais vous faire ce matin, on va aborder un certain nombre d'initiatives sur lesquelles nous avons travaillé en coopération avec le gouvernement également avec les gestionnaires ccTLD.

S'agissant de l'organe chargé des télécommunications à Vanuatu, qui opère de manière indépendante du gouvernement d'après ses statuts, nous n'avons pas de conseil d'administration ni de commission. Nous avons un organe de règlementation et le personnel.

Nous avons des pouvoirs généraux et des fonctions générales qui s'occupent de règlementer la radio-télédiffusion à Vanuatu.

Diapo suivante.

Alors .VU est un espace de noms de premier niveau d'extension géographique qui est géré et administré par le bureau des télécommunications et radiodiffusion. Il s'agit d'une entreprise de télécommunication créée dans les années 80.

Lorsque l'organe chargé de la règlementation met en place une loi, elle stipule qu'il y a un administrateur pour gérer ces ressources. Donc nous avons une transition de télécom Vanuatu qui a commencé en 2017 et qui s'est finalisée avec succès il y a quelques années.

Donc, du point de vue de la sécurité de l'internet, lorsque nous étions en train de travailler sur la transition, TRBR a choisi GoDaddy comme opérateur de registre pour le ccTLD .VU en aout 2019. Donc ce nouvel opérateur de registre était chargé de fournir un service qui réponde aux meilleures pratiques de l'ICANN et au niveau international.

Nous avons développé une règlementation concernant les noms de domaine qui s'est finalisée en 2016. À l'heure actuelle, nous avons 34 bureaux d'enregistrement internationaux et 5 bureaux d'enregistrement locaux qui, jusqu'à présent, sont conformes aux normes attendues dans le domaine de la sécurité au niveau international.

L'organe chargé de la règlementation soutient et aide le gouvernement également pour l'élaboration de la loi sur la cybercriminalité qui nous aide également à informer les consommateurs par rapport aux risques de la sécurité sur internet.

Cette loi a été approuvée en 2021. L'une des initiatives sur lesquelles nous avons travaillé avec le gouvernement, en coopération avec le bureau du responsable de l'information du gouvernement, en vue de mettre en place une réponse d'urgence. Donc ce bureau a été créé en 2018 et est actuellement en fonctionnement.

Autre initiative, la mise en place de la gouvernance de l'internet national à Vanuatu qui aide également le gouvernement. Et nous avons accueilli le forum sur la gouvernance de l'internet en 2018. Il s'agit d'une plateforme multipartite qui facilite la discussion concernant les questions politiques relevant de l'internet.

Diapo suivante s'il vous plait.

Nous avons également mis en place une règlementation en termes d'enregistrement d'une carte SIM. Il s'agit d'une instruction du bureau de gestion des catastrophes naturelles qui nous a demandé d'avoir une règlementation en place. Cette règlementation a maintenant été finalisée et maintenant tous les fournisseurs de service internet et les deux principales entreprises de téléphones portables appliquent cette mesure concernant l'enregistrement des cartes SIM.

On a quelques initiatives au niveau national qui aident le gouvernement en coopération avec le responsable de l'information auprès du gouvernement. Pour l'instant nous sommes sur le point de présenter devant le parlement un certain nombre d'initiatives pour examen. Toutefois, ces initiatives nationales concernent la communication numérique dommageable, une initiative concernant la protection des

données à caractère personnel et la confidentialité et la protection des enfants en ligne.

Diapo suivante.

On a également beaucoup travaillé sur la sensibilisation, on a une règlementation pour la protection des consommateurs. Il est important de pouvoir informer les utilisateurs par rapport aux risques du hameçonnage sur internet et l'impact que cette règlementation aura sur les utilisateurs. Tout ça fait partie de notre programme de sensibilisation qui est mis en place chaque année.

Et on participe également auprès des écoles, des communautés rurales à Vanuatu et on le fait également dans d'autres forums comme le forum sur la gouvernance de l'internet et autres.

Voilà, merci à tous de votre attention.

ANNALIESE WILLIAMS: Merci, Norman. Y a-t-il des questions à l'intention de Norman ? Moi, j'ai une question si vous êtes d'accord. Je sais que vous n'avez pas directement participé en tant que chargé de la règlementation, mais récemment on a eu une cyberattaque très importante. Est-ce que vous pourriez nous offrir votre opinion sur la manière dont cela a eu un impact sur votre bureau ?

NORMAN WARPUTT: Merci de cette question. Oui, effectivement, ce qu'il s'est passé, bon je n'ai pas d'information détaillée sur le rançongiciel de l'année dernière

et toute l'affaire, mais ça a touché l'un de nos principaux serveurs. Donc le gouvernement a dû suspendre le serveur, bloquer le système, mais du point de vue de .VU on a dû déconnecter beaucoup de services en ligne pour s'assurer qu'on pouvait protéger le serveur et stocker les données en backup.

Donc on a fait les contrôles au niveau des sites web, des mails et le gouvernement a dû agir également pour régler ce problème. Voilà tout ce que je peux vous donner comme information.

ANNALIESE WILLIAMS: Merci. Y a-t-il d'autres questions ? Angela ?

ANGELA: Je voulais vous demander, est-ce qu'il y a une règlementation spécifique qui porte sur les radios en ligne ? Parce qu'en général vous avez tout cela prévu dans la législation sur la radiodiffusion, mais est-ce que vous traitez cela différemment parce que maintenant vous avez une radio qui fonctionne sur un nom de domaine. Est-ce que ça veut dire que les politiques du ccTLD qui traitent d'abus ou d'utilisation malveillante s'occupent également de ce qu'il se passe sur ces radios en ligne ?

NORMAN WARPUTT: Alors, le bureau de règlementation ne règlemente pas le contenu. On ne règlemente que les services télécom. On ne règlemente absolument rien au niveau du contenu, que ce soit sur un site web ou ce qui provient de télé ou radiodiffusion.

ANNALIESE WILLIAMS: Est-ce qu'il y a d'autres questions ? Ça ne semble pas être le cas ni en salle ni en ligne. Nous allons donc passer à l'intervenant suivant qui nous rejoint en ligne, à distance. Lourino Chemane qui est actuellement président de l'organe de règlementation au Mozambique. Auparavant il était conseillé auprès du ministère des Sciences et de la technologie et de l'enseignement supérieur. Et auparavant il était PDG du réseau de recherches et d'éducation du Mozambique. Je vous en prie, Lourino.

LOURINO CHEMANE: Merci de l'occasion de vous faire cette présentation. Je suis du Mozambique et je suis ravi de vous présenter ce que fait le Mozambique dans le domaine de la cybersécurité et des initiatives législatives liées aux ccTLD.

Nous représentons l'institut national des technologies de l'information et des communications qui règlemente les services numériques au Mozambique.

Je vais faire une petite introduction, je parlerai du mandat et des compétences de l'INTIC, de la gestion du ccTLD du Mozambique, de la législation approuvée, des politiques et stratégies en lien avec la cybersécurité, des actions de suivi par rapport à l'élaboration du cadre juridique et des conclusions.

Diapo suivante.

Alors l'INTIC a été créé par décret ministériel en 2011 et son exploitation et son organisation ont été redéfinies en 2020. Nous sommes l'autorité

de règlementation des TIC dans le pays et nous sommes supervisés par le ministère qui supervise le domaine les TIC actuellement il s'agit du ministère des sciences, technologies et de l'éducation supérieure.

Notre mandat inclut l'élaboration de politique afin de garantir la sécurité et l'intégration des systèmes de TIC et de lutte contre l'utilisation malveillante.

L'INTIC doit également veiller à ce que la gouvernance de l'internet au Mozambique soit comme elle doit être.

Notre mandat prévoit que nous devons garantir la mise en œuvre et le fonctionnement du système de certification numérique du Mozambique. Et nous travaillons également avec la législation des différents opérateurs et fournisseurs de service.

Dans le cadre des ccTLD, en particulier du domaine .MZ, je vais passer en revue notre histoire.

Notre TLD a été créé en 92 et a été exploité par l'université [inaudible] mais avec l'approbation de la loi de 2017 sur les transactions électroniques l'INTIC a été établi comme l'entité responsable de gérer le domaine .MZ. Donc en ce moment nous travaillons avec l'université qui avait enregistré ce ccTLD pour qu'elle nous cède les responsabilités et le rôle de gestion du domaine.

Cependant, étant donné l'histoire de ce domaine du Mozambique, nous allons laisser les fonctions techniques du côté de l'Université.

Il existe plusieurs compétences de l'INTIC de par la loi, mais entre autres nous devons donner des instructions pour les applications de la délégation et l'usage du domaine.

Le règlement actuel a été approuvé en 2020 et indique le processus et la procédure à suivre. Nous sommes des membres de SADC, de la communauté de développement d'Afrique méridionale, et notre ministre participe aux réunions de cette communauté et travaille pour recommander que tous les États membres mettent en œuvre le DNSSEC dans leur pays.

Diapo suivante.

Nous suivons également les développements législatifs autour du monde et je voulais partager avec vous la convention de Malabo, de l'Union Africaines en lien avec la protection des données.

Le Mozambique est l'un des pays signataires de cette convention. Nous suivons donc de près le travail des Nations Unies en amont de la préparation de cette proposition de la convention des Nations Unies contre l'usage des TIC à des fins de délinquance et nous travaillons pour accéder également à la convention de Budapest dans le cadre de l'exercice international que nous suivons.

Diapo suivante.

Pour ce qui est de l'action concernant la cybersécurité en particulier le gouvernement du Mozambique a approuvé notre politique et stratégie en 2021.

Ce document définit la coordination pour la cybersécurité et l'infrastructure ou la structure qui, comme vous le voyez, est présidée par le ministère qui supervise les TIC et un secrétariat technique.

Les membres de ce comité de cybersécurité impliquent les forces de l'ordre, les départements de justice, l'autorité de règlementation des TIC, l'autorité de règlementation des communications, le secteur académique, la société civile, le secteur privé et le CCIRT national.

L'approche est de superviser le processus de mise en œuvre de la cybersécurité dans le pays entre tous.

Diapo suivante.

La stratégie nationale pour la cybersécurité identifie 25 stratégies différentes organisées en 7 domaines thématiques. J'ai inclus ici ceux qui sont abordés dans notre discussion d'aujourd'hui avec des directives, des normes juridiques et des instruments pour la protection de notre infrastructure critique.

Nous avons établi un centre pour recherches et analyses du trafic internet, le CCIRT, le réseau national de CCIRT. Nous avons renforcé le cadre juridique sur la cybersécurité, nous avons répertorié les infrastructures d'information essentielles et tout cela renforce la sécurité étant donné le rôle d'internet comme partie de notre infrastructure fondamentale.

Diapo suivante.

Pour ce qui est du suivi nous voulions partager avec vous le travail qui est en cours dans la préparation des lois. Nous travaillons à la

préparation d'une loi sur la cybersécurité et une autre sur la protection des données à caractère personnel et la règlementation de l'enregistrement et l'octroi de licence pour les fournisseurs et opérateurs de plateformes numériques. C'est-à-dire d'autres règlements qui vont être développés dans les années futures qui vont être en lien avec le travail de notre ccTLD en matière de cybersécurité. Mais pour l'instant nous nous occupons de ces trois projets que je viens d'évoquer.

Dans l'élaboration du cadre juridique nous croyons que nous avons un rôle fondamental à jouer parce que nous sommes les responsables de la préparation des propositions de loi qui vont être présentées au gouvernement et poursuivre le processus législatif afin de pouvoir suivre la législation et d'autres instruments en lien avec les ccTLD.

Nous pouvons proposer des modifications pour la cybersécurité et le fonctionnement des ccTLD.

En tant que gestionnaire du ccTLD, INTIC est responsable de la gestion du domaine de .MZ mais également de fournir des services de résolution de nom, de maintenir l'infrastructure critique nécessaire pour compléter les requêtes DNS et fournir des services d'enregistrement aux bureaux d'enregistrement ce qui peut inclure la création ou l'annulation ou la suspension d'un nom de domaine et la mise à jour d'un serveur de nom. Nous croyons que dans ce sens INTIC a un rôle fondamental à jouer pour faire la diffusion des instruments nationaux liés à la cybersécurité et pour l'adoption de mécanismes qui ont un impact sur le fonctionnement correct de notre ccTLD.

Diapo suivante.

C'est ma dernière diapositive. Dans le ccTLD du Mozambique nous croyons qu'il y a des aspects de sécurité qui seront améliorés à travers la mise en œuvre de notre cadre juridique. Nous allons examiner les politiques d'enregistrement pour les nouveaux domaines sous le ccTLD du Mozambique, sous les aspects de sécurité, mettre en œuvre une infrastructure de sécurité du ccTLD centrée sur le DNSSEC, nous conformer aux recommandations des fournisseurs intermédiaires de services aussitôt que la loi sur la cybersécurité et le règlement pour l'enregistrement des fournisseurs intermédiaires de service aura été approuvée. Nous travaillons également pour nous conformer à la convention de Budapest, ce qui sera possible une fois que le processus d'accession aura été complété. Et nous travaillons pour nous conformer aux politiques de l'ICNNA pour les ccTLD, d'autres TLD et d'autres aspects liés avec la gestion de l'internet.

Et diapo suivante, finalement. Merci pour votre attention, désolé d'avoir parlé un peu trop vite. Merci.

ANNALIESE WILLIAMS: Merci Lourino. Y a-t-il des questions ? Oui, allez-y.

ANIL JAIN: Merci. Vous agissez en tant qu'autorité de règlementation et comme gestionnaire de ccTLD à INTIC, ne croyez-vous pas que ces deux rôles pourraient être en conflit entre eux ?

LOURINO CHEMANE: Merci pour cette question, Anil. En réalité, nous ne sommes pas seulement l'autorité de règlementation des TIC, nous sommes l'autorité qui règlemente la cybersécurité et nous travaillons également comme responsable du ccTLD. En général, nous avons la tâche de contrôler le développement de l'internet sur le pays. C'est-à-dire que le rôle que nous avons n'est pas exclusivement de gestionnaire ou d'autorité de règlementation. Vous demandez s'il n'y a pas de conflit d'intérêts entre tous ces rôles, nous croyons qu'il y a des mécanismes de gouvernance qui sont établis avec la participation de toutes les parties prenantes du pays qui peuvent nous aider à superviser les activités entreprises par INTIC.

Mais nous sommes un pays en développement et nous avons des limitations au niveau des ressources nationales. Nous ne sommes donc pas à même d'avoir plusieurs entités dans différents domaines liés aux technologies numériques. Mais nous avons deux autorités de règlementation, l'une pour les télécommunications et INTIC qui s'occupe des TIC, y compris ces autres domaines que je viens d'évoquer.

Je ne sais pas si j'ai répondu à la question.

ANNALIESE WILLIAMS: Merci. Y a-t-il d'autres questions ? Je ne vois pas de demande de prise de parole dans la salle et dans Zoom non plus.

Nous allons passer à l'intervenante suivante. Merci Lorino. La prochaine présentation sera celle de Rosalia, directrice exécutive du .CR, ccTLD du Costa Rica. Elle y travaille depuis 2012, elle a dirigé des projets en lien avec la gouvernance de l'internet, les FSI, la cybersécurité,

l'infrastructure de l'internet et des politiques internet. Et elle a été membre du conseil de LACNIC auparavant, a fait partie du groupe de travail LACTLD et du FGI local du Costa Rica.

ROSALIA MORALES: Bonjour, je viens présenter les initiatives de cybersécurité et comment la législation de cybersécurité a impacté notre ccTLD.

D'abord je vais vous présenter ce que veut dire la cybersécurité pour notre ccTLD, suivi de notre législation.

Pour le .CR la cybersécurité est un point central, nous travaillons intensément avec la cybersécurité et pour elle depuis 12 ans, ce qui veut dire que nous faisons partie du CSIRT national du Costa Rica, nous faisons partie du conseil d'administration et nous travaillons ensemble avec le gouvernement, les FSI et d'autres organisations clefs pour les infrastructures du Costa Rica à travers la fourniture d'ateliers et avec des agences internationales locales, mais également dans différents projets internationaux de coopération pour renforcer l'infrastructure de notre pays.

Nous faisons partie du CSIRT national et nous sommes l'organisation qui a fourni le premier matériel pour un CSIRT du gouvernement et national, donc nous travaillons avec les équipes sur les capacités techniques pour que le gouvernement puisse lancer les initiatives de cybersécurité locales.

Nous organisions des formations et des programmes de sensibilisation pour les écoles, les universités et la communauté technique du Costa Rica.

D'une manière générale, les politiques comme les personnes qui m'ont précédée dans leur présentation l'on dit, nous ne sommes pas responsables du contenu ni de quel que type que ce soit du changement qu'on pourrait apporter à un domaine. On aurait besoin d'une ordonnance d'un tribunal pour le faire. Il faudrait donc disposer de cela pour apporter un changement à un domaine.

Pour l'heure, le Costa Rica a ratifié la convention de Budapest en 2017. Toutefois, pour l'instant il y a un retard dans les autres législations complémentaires qui doivent être entérinées afin que cette convention puisse bien fonctionner ou puisse avoir une réponse rapide.

Pour nos agences locales l'un des principaux problèmes est celui des agents infiltrés virtuels. Ça, c'est simplement une idée qui est en cours de discussion au Costa Rica, mais ça n'a pas encore été ratifié. Et, deuxièmement les preuves numériques, comment traiter les preuves numériques au niveau local. Mais conformément à la convention de Budapest il y a un manque de son législatif pour pouvoir agir aussi vite et conformément à ce qui est stipulé dans cette convention.

Nous avons accepté le deuxième protocole supplémentaire de la convention de Budapest en 2022, il n'a pas encore été ratifié au Congrès, je crois qu'il y a un certain nombre de pays qui doivent encore adhérer et souscrire à ce protocole supplémentaire. Donc nous suivons les discussions et notamment par rapport à l'impact significatif que cet

amendement aurait sur le WHOIS. Et nous comptons sur nos homologues européens pour faire un excellent travail et nous aider à ce niveau-là.

Ensuite, il y a le texte de loi sur la cybercriminalité, une loi qui a été entérinée en 2016, et ça nous a aidés parce que cette loi permet aux clients locaux de savoir comment procéder en cas de litige et par le passé c'était une zone assez sombre, on ne savait pas quoi faire et il n'y avait pas de chemin clair à suivre pour savoir ce que devaient faire ou pouvaient faire les autorités locales en cas de délit cybernétique.

Enfin, traité sur la cybercriminalité qui est actuellement en cours de discussions au sein de l'ONU. Le Costa Rica a pour habitude d'être très neutre, d'observer et de voir ce qu'il se passe, donc nous attendons de voir ce qui ressort de cette discussion avant de prendre une décision.

Il y a d'autres initiatives qui ont affecté l'espace de la cybersécurité au niveau local et la manière dont nous opérons les ccTLD. Non pas forcément une loi adoptée par le Congrès mais ce qui a un impact sur les opérations.

Comme je vous le disais, le CSIRT national, nous y participons depuis sa création et depuis ces 3 derniers mois il y a un vif intérêt vis-à-vis du renforcement du CSIRT par rapport à ses équipements, sa formation, son personnel et offrir également une formation locale aux agences locales et à toutes les organisations telles que .CR qui offrent une stabilité à l'internet au Costa Rica.

Et le gouvernement des États-Unis a apporté un financement significatif à ce niveau-là et nous faisons partie des organisations qui aident le

gouvernement à renforcer les formations dans le domaine de la cybersécurité. Ces formations n'ont pas encore commencé mais on nous a demandé d'y participer et on attend de voir ce qu'il se passe. C'est un projet qui est censé durer 5 ans.

Donc l'intérêt vis-à-vis de la cybersécurité et le rôle qu'on joue auprès du gouvernement dépend du gouvernement en place. Ça n'est pas quelque chose de stable. Si certains gouvernements sont très impliqués, d'autres le sont beaucoup moins et dans ce cas-là le gouvernement en place est assez impliqué puisque nous avons été victimes de plusieurs attaques cybernétiques, aussi bien au niveau des hôpitaux qu'autres, administratif aussi. C'est pourquoi nous avons reçu l'aide internationale. Et depuis ces incidents cybernétiques, ça a été une priorité pour le gouvernement en place et nos organisations.

Il y a une stratégie dans le domaine de la cybersécurité qui a été mise en place et créée à la fin de l'année 2022 par le ministère des sciences de la technologie et des télécommunications en coopération avec l'OEA, organisation des États Américains. Cette stratégie dans le domaine de la cybersécurité n'a pas d'impact sur nos politiques ou nos activités quotidiennes. Nous participons simplement aux réunions de travail et de discussions dans le cadre de cette stratégie. Et c'est ce que l'OEA a mis en place dans différents pays, dans les régions. Ça ressemble à beaucoup d'autres stratégies mises en place par l'OEA. Ça ne s'applique pas forcément directement ou spécifiquement aux réalités de chacun des pays, c'est quelque chose d'assez large. Donc ça n'affecte pas la manière dont nous travaillons ou dont nous opérons.

À l'heure actuelle il y a un texte de loi qui est en cours d'approbation pour créer une agence de cybersécurité. Cette agence pourrait avoir un impact sur nos ccTLD et leur fonctionnement et sur la manière dont les données sont gérées dans le pays. Cette agence n'a pas été ratifiée au Congrès, il semblerait qu'il n'y ait pas d'accord pour le moment, mais les choses pourraient changer. Et en général lorsqu'il y a des discussions on peut facilement ajouter ou supprimer des amendements et voir ce qu'il se passe. Mais il faut nous assurer que ça ne va pas affecter de manière négative nos opérations et la manière dont on pourrait approuver cela ce serait de contribuer aux discussions vis-à-vis de cette loi parce que cette loi n'irait pas dans le sens de l'intention de ce gouvernement qui est en place d'améliorer la législation vis-à-vis de la cybersécurité. Peut-être qu'il y a eu trop de précipitation, c'est trop tôt encore, il n'y a pas eu suffisamment de débats avant de pouvoir approuver cette loi.

Donc conclusions générales.

Nous avons, après 12 ans de travail en coopération et travail avec les agences de cybersécurité, nous avons créé une relation étroite avec les forces de l'ordre et établi un dialogue ouvert s'agissant des différentes politiques, projets, tout ce qui, dans l'espace de la cybersécurité pourrait avoir une incidence sur les ccTLD. Donc nous avons une communication intense avec les agences chargées de l'application de loi. Et, finalement, c'est gagnant-gagnant pour toutes les parties prenantes.

La cybersécurité est actuellement un domaine d'intérêts prioritaire pour le gouvernement et pour les ccTLD en général ce qui, bien entendu, présente certains risques. Comme je vous le disais, il y a encore des

textes de loi qui sont en discussion, on ne connait pas encore le résultat final mais on va s'assurer que cela permet d'améliorer l'espace de la cybersécurité et que ça donne pas lieu à des risques ou un danger pour les utilisateurs finaux ou pour les ccTLD.

Donc il y a encore un long chemin à parcourir. Le Costa Rica vient tout juste de commencer à travailler dans le domaine de la cybersécurité et on commence à travailler avec les autres ccTLD pour voir comment nous aider à aborder ces nouvelles législations, comment ces législations peuvent nous aider à améliorer la situation et nous assurer que nos ccTLD se voient renforcés par cette législation et non pas affaiblis.

Et donc saisir toutes les opportunités pour travailler avec les autorités nationales comme étrangères dans la formation du personnel, vis-à-vis des technologies liées à la cybersécurité. Et donc qu'il y ait une formation des formateurs et qu'on puisse transférer ces connaissances et créer un internet plus sûr au Costa Rica.

Merci.

ANNALIESE WILLIAMS: Merci, y a-t-il des questions à l'attention de Rosalia ? Olga ?

OLGA CAVALLI : Merci. Merci à tous les présentateurs, présentations très intéressantes. Questions pour Rosalia, je sais que vous avez dit que c'est une toute nouvelle loi à laquelle vous êtes en train de songer, mais s'agissant de cette agence dont vous parliez, est-ce que vous avez une idée de comment cela va s'intégrer dans la structure bureaucratique du

gouvernement ? Est-ce cette agence dépendra directement de la présidence ? Comment va être l'interaction avec les autres ministères, de la Sécurité, de la Défense, etc. ? Je ne sais pas si vous avez une idée ?

ROSALIA MORALES: Merci, Olga. En fait cette loi vient du ministère des Technologies, des sciences et de la communication. Et le problème avec cette loi est que cela donne au ministère une certaine autorité qui relève du ministère de la Justice. Par exemple, ça donne au ministère la capacité de parler directement à interpole. Or, le ministère pour l'instant n'a pas l'expérience ni le personnel habilité pour le faire.

Donc ça porte un petit peu à confusion, on perd un peu de vue quel est le rôle de chacun des ministères. Mais cette loi est mise en avant et promue par le ministère des Sciences et de la Technologie.

ANNALIESE WILLIAMS: Y a-t-il d'autres questions ? Je n'en vois pas dans la salle ni sur Zoom.

Alors, il nous reste encore un petit de temps, j'allais poser une question à Rosalia mais je crois que je vais la poser à tous les intervenants à la fin. À quel point il est difficile de faire face à toutes ces initiatives législatives qui émergent. Donc lorsqu'on parviendra à la fin des présentations, je vais demander à tous de voir comment vous gérez cette situation.

Passons à la dernière intervenante, Barbara, directrice du ccTLD de la Slovénie et présidente du conseil. Elle a plus de 20 ans d'expérience dans la gestion des affaires européennes et une longue expérience dans les affaires de confidentialité et de cybersécurité.

BARBARA POVSE: Merci et bonjour à tous. Merci de ces mots aimables d'introduction. J'ai effectivement beaucoup d'expérience, vous vous en rendez compte. Et je me souviens même de l'époque où les législateurs et responsables de la règlementation ignoraient jusqu'à notre existence.

Bon, j'interviens en dernier, ça n'est pas simple. Mais je ne suis pas sûre si je dois m'excuser de ce que je vais vous présenter ou pas.

D'abord, j'aimerais vous remercier et remercier Martha Morera qui m'a aidée à préparer cette présentation. Et je vais vous expliquer comment .SI et en partie .PT sont confrontés à cet énorme volume de législation, notamment dans le domaine de la cybersécurité mais aussi dans d'autres domaines. Et merci également à Paulina du Centre Protect qui s'est assurée que tous les faits étaient corrects.

Mais veuillez m'excuser si je commets des erreurs, moi, elles sont à mettre sur mon compte.

Alors, vous connaitrez probablement le fait que tous les pays européens relèvent tous et sont tous tenus de respecter un cadre juridique européen, communautaire. Donc il y a une base juridique communautaire au sein de l'UE.

Diapo suivante s'il vous plait, parce que je ne vais pas vous faire une présentation trop détaillée par rapport à qui fait quoi dans l'UE est qui est responsable de quelle législation et comment les décisions sont prises.

Parce que, finalement, ce qui est intéressant c'est le résultat final, directives ou règlementation. Mais vous pouvez voir d'après tous ces cercles – et je dois vous avouer que je ne suis pas encore tout à fait à l'aise avec tous les processus en cours, et peu importe si je suis à l'aise ou pas car ce n'est pas ça l'important. C'est un excellent travail qu'on a grâce au travail d'une petite équipe du groupe CENTR. Et moi, du point de vue d'un tout petit registre tel que le mien on ne pourrait même pas suivre ce qui a lieu en ce moment sans même dire que nous aurions égale à zéro sans l'aide de ce centre.

Voici la liste des lois de l'UE liées à la cybersécurité qui sont pertinentes pour les cc et qui existent et sont déjà en vigueur.

Tout d'abord nous avons la directive NIS. La première directive NIS était un premier pas dans un énorme afflux de législations liées à la cyber sécurité qui a suivi et qui a eu une influence sur les enregistrements de ccTLD.

À l'époque, nous étions des fournisseurs de services essentiels, ce qui n'est pas la même chose que service critique. Mais nous avons beaucoup de responsabilités partagées cependant.

Maintenant nous avons NIS 2, avec d'autres exigences et nous en sommes maintenant à un moment auquel la directive NIS2 s'adopte dans la législation nationale.

NIS 1 n'était pas appliquée de la même manière dans tous les pays et voilà pourquoi maintenant les législateurs essayent d'avoir une coordination accrue.

Quant au fait de savoir quelle en sera l'influence dans notre secteur, nous discutons de l'art 21 beaucoup, de la vérification. Mais il y a beaucoup de points qui ne sont toujours pas clairs. Nous avons des obligations de rapport, il y a également des directives qui ont été divulguées par NIS 1 et nous avons des mesures de sécurité pour les opérateurs de TLD, mais nous avons également de nouvelles exigences pour la vérification des titulaires de nom de domaine, ce sont des recommandations et non pas des exigences.

Prochaine diapo.

Cela n'est pas concrétisé. Dans le domaine de la cybersécurité il y a toujours des travaux de législation en cours qui ne sont pas débouchés sur des lois concrètes mais nous voyons au quotidien des changements. Et, comme je l'ai dit, heureusement nous recevons des rapports du personnel de CENTR qui incluent la pertinence de chacune de ces législations pour les ccTLD. Et c'est extrêmement important pour nous.

Diapo suivante.

Comment gérons-nous toutes ces initiatives ?

Avec CENTR et en coordination avec un groupe de travail juridique et règlementaire nous coordonnons et nous sommes tenus au courant de ce qu'il se passe. Constamment nous essayons d'être au courant des législations qui sont sur le point d'être adoptées. Dès que les lois sont préparées au niveau de l'UE, dès qu'il y a des projets de loi nous essayons d'avoir une influence dans la mesure où cela a un impact sur nos travaux.

Vous allez pouvoir le voir sur CENTR et leurs documents disponibles sur leur site web, à travers les différentes réunions de l'UE avec les décideurs et législations. Donc nous intervenons à toutes les étapes du processus.

En tant que membres individuels nous essayons d'informer nos parlementaires nationaux afin qu'ils soient au courant des nouvelles lois qui sont préparées et de nos recommandations de changement.

J'ai inclus ici également un centre d'analyse et de partage d'information récemment établi par CENTR pour les ccTLD, également de grande importance pour la cybersécurité. Il y a beaucoup d'implications, de sensibilisation, beaucoup de formations au niveau de l'UE, comme vous l'imaginez.

Diapo suivante.

Alors, qu'en est-il par rapport à notre échelle nationale ? Les ccTLD devraient être aussi actifs que possible pour pouvoir avoir une influence sur le processus. Alors, comme je l'ai dit déjà, nous essayons d'avoir une influence au niveau européen à travers nos représentants nationaux. Nous adoptons également des lois nationales. Et nous essayons d'être en contact avec tous les niveaux, avec les ministères, avec les législateurs. Et on essaye de les former parce qu'il est nécessaire que toutes ces personnes comprennent les informations de base par rapport à ce que veulent dire certaines actions.

En Slovénie, tout est plus facile vous savez, on est un petit pays, on se connait tous, c'est beaucoup plus simple. On n'est qu'à deux degrés de séparation de la personne à laquelle il faut parler. Mais cela aide

également le fait qu'en tant qu'opérateur technique de plus en plus actif dans le domaine des politiques nous puissions réunir des experts techniques et non techniques à l'échelle nationale pour essayer de faire en sorte que ces personnes communiquent et parlent d'une langue commune.

Diapo suivante.

Quels sont les moyens que nous avons utilisés ? Toute sorte de canaux, nous avons participé à des débats publics, nous utilisons les connexions au ministère, nous avons rédigé des articles de blog, nous avons envoyé des emails, nous appelons des personnes par téléphone. Et bien sûr, lorsqu'il y a un processus de consultation public, une législation qui s'élabore nous essayons d'avoir une influence sur les délais. Parfois nous réussissons, parfois pas complètement.

La mise en œuvre du CPC qui est la protection des consommateurs transfrontalière, on a eu beaucoup de succès, on a communiqué avec le ministère responsable de la mise en œuvre et les résultats atteints étaient raisonnablement bons.

Par rapport à la mise en œuvre de NIS 2 on n'a pas connu tant de succès, l'autorité de règlementation nationale s'occupe de ses propres affaires en ce moment donc ils ne parlent avec personne. Espérons que cela changera bientôt.

Je considère qu'il est extrêmement important de parler, de communiquer. En tant que cc nous sommes aussi intéressés à la sécurité de l'internet que notre gouvernement. Nous n'avons qu'à nous

assurer que la législation qui est adoptée soit applicable et que l'on puisse faire ce qui nous est exigé et ce qui doit être fait.

Et, cependant, parfois on voit qu'on manque de compréhension à ce niveau-là.

Diapo suivante.

Quel est l'impact de cela sur notre travail ?

Nous essayons de penser à l'avenir, nous sommes penchés vers l'avant. On n'attend pas à ce que la législation soit adoptée pleinement, on essaye de se préparer à l'avance. Et on s'améliore. On n'a pas, bien sûr, la possibilité de savoir ce qui va venir mais on essaye de prévoir. Et nous suivons le processus depuis le début avec beaucoup d'aide de CENTR et nous avons beaucoup appris les uns des autres et nous partageons des ressources, surtout pour un petit opérateur de registre comme nous, c'est vraiment très important.

Ce que nous avons fait, même avant NIS, nous avons décidé d'appliquer le certificat ISO 27001 et ça a été une très bonne décision parce qu'on n'a pas eu autant de travail à faire avec ce certificat ISO 27001. Au début on a eu beaucoup de travail à faire au niveau de NIS et de son application, dans tous les domaines c'est difficile la conformité, mais dans celui-ci en particulier.

Donc, qu'est-ce que j'ai voulu dire avec ce que j'ai mis ici, l'effet Bruxelles ? Bruxelles est le chef de file dans le domaine de la cybersécurité et je pense que c'est important qu'on obtienne des lois mais qu'on ne soit pas isolés.

Donc la nouvelle exigence met sous pression – excusez-moi je bafouille. Non, plutôt on a beaucoup de nouvelles obligations qui sont onéreuses pour les opérateurs de registre. Il faut qu'on trouve de nouvelles personnes qui puissent gérer ces nouvelles exigences. Et donc on a besoin d'investir énormément dans nos infrastructures.

Donc cela devient très difficile, aussi avec cette nouvelle exigence, les procédures pour les enregistrements des ccTLD deviennent de plus en plus compliquées pour le titulaire de noms de domaine final. Ce qui veut dire que bientôt ils vont s'en lasser et ils vont s'adresser à un endroit où ce sera plus simple d'obtenir un nom de domaine. Et ça, ça va être problématique pour rester compétitifs vis-à-vis d'autres cc et d'autres gTLD.

Mais d'un autre côté, je pense qu'on veut tous recréer de la confiance en internet. Donc il faut trouver un juste équilibre entre une charge trop lourde et cela.

Donc on va continuer à travailler ensemble parce que finalement, nous les opérateurs de registre, nous sommes confrontés aux mêmes problèmes et au moins on peut se plaindre les uns auprès des autres puisqu'on est confrontés aux mêmes problèmes. Non je rigole, simplement on essaye de partager nos problèmes.

Voilà, j'ai fini.

ANNALIESE WILLIAMS: Oui, c'était la dernière diapo, effectivement. Merci, Barbara. Je crois que ce que vous avez dit est très important, être proactif. Y a-t-il des questions pour Barbara ? J'en vois beaucoup ici. Allez-y.

UGO AKIRI: Merci. Je faisais partie du .NG. Ma question est la suivante : lorsque vous dites que certains pays européens sont à la traine, est-ce que ça veut dire qu'une politique telle que le RGPD n'est pas appliquée dans tous les pays membres de l'UE ?

BARBARA POVSE: Non, je crois que je me suis mal fait comprendre. Non, je n'ai pas voulu dire que certains pays européens sont restés à la traine, je me suis peut-être mal exprimée. Je vous ai dit, s'il y a des erreurs ça vient de moi.

Non, ce que j'ai voulu dire c'est que le cadre juridique est le même, exactement le même pour tous les États membres de l'UE, on est tous logés à la même enseigne. Ce que j'ai voulu dire c'est qu'il y a beaucoup de charges mises sur les épaules des ccTLD européens. C'est ce que j'ai voulu dire, c'est que les ccTLD européens sont peut-être sous pression, mis sous pression davantage que d'autres.

ANNALIESE WILLIAMS: Alors il y a une question dans la salle et ensuite sur Zoom, mais on va d'abord aller dans la salle.

OMAR CONTREPAS : Bonjour, je suis de Digital Link. Ce que j'ai apprécié dans votre présentation c'est la collaboration. Vous avez pris en considération le fait qu'on a des ressources limitées et vous avez dit que vous avez travaillé avec le Portugal, avec CENTR et vous avez mobilisé toutes vos ressources. Je ne sais pas si vous avez des recommandations pour les ccTLD en dehors de l'Europe pour établir ce genre de collaboration, et je pense à l'Amérique centrale. Comment avez-vous ouvert ce canal de collaboration pour mobiliser tous ensemble vos ressources ? Je ne sais pas si vous avez des conseils, des astuces à nous transmettre ?

BARBARA POVSE: Oui, la situation est différente en Europe parce qu'on partage le même cadre juridique. Donc, même si l'application ou la mise en œuvre nationale peut varier, on a également des législations nationales qui varient d'un État à l'autre, il n'en demeure pas moins qu'on a tous un cadre juridique auquel se tenir.

Et lorsque j'écoutais toutes ces présentations, je me rendais compte que c'est la même chose au Costa Rica ou à Vanuatu, c'est à peu près la même législation qui est en place.

Donc je pense que les organisations nationales, en Europe c'est CENTR, mais ailleurs ce sera une autre organisation, peut offrir certainement un espace pour que les personnes qui s'intéressent à la politique puissent se rencontrer, parler et trouver un terrain d'entente.

ANNALIESE WILLIAMS: Merci, Barbara. Une question sur Zoom.

MICHELE NEYLON: Non, je suis dans la salle en fait. Barbara, la charge règlementaire, puisque là vous parlez du point de vue des opérateurs de registre, moi je parle plus du point de vue des bureaux d'enregistrement, vous, est-ce que vous avez une idée par rapport au fait de savoir si la Commission Européenne et leurs amis comprennent bien le niveau de situation ? C'est-à-dire qu'on est dans une situation très désavantagées et on nous regarde en rigolant, et c'est assez frustrant. Alors est-ce que vous pouvez me donner un peu d'espoir, est-ce que la Commission européenne est un peu consciente ou pas de cela ?

BARBARA POVSE: Barbara, je suis désolée, je n'ai pas de bonnes nouvelles. Mais c'est ce que je voulais dire et c'est pourquoi j'ai parlé des opérateurs de registre. Mais c'est vrai pour les opérateurs de registre, comme pour les bureaux d'enregistrement et les opérateurs en général. Rester concurrentiel dans cet espace hautement règlementé, c'est ça le problème. Mais, malheureusement je ne peux pas vous donner d'autres réponses, mais c'est frustrant, je suis d'accord avec vous.

MICHELE NEYLON: Oui, ce n'est pas bien encourageant.

ANNALIESE WILLIAMS: Y a-t-il d'autres questions pour Barbara ? Je vois que Bruce a la main levée.

BRUCE TONKIN: Merci. Alors, historiquement il semblerait que chaque cc, indépendamment en Europe, arrive à des règles qu'elle applique à sa communauté. Et maintenant vous parlez au niveau régional. Et lorsque je vois ces changements j'ai l'impression qu'ils sont dus à des changements plus larges au niveau économique et cela engendre des dommages collatéraux. Et je me demande si l'infrastructure en place est capable de gérer tout cela.

Est-ce qu'il y a des préoccupations par rapport à la confidentialité ou par rapport aux règles de « connaissez votre client ».

Donc est-ce que c'est un problème qui relève de l'industrie elle-même ou est-ce qu'il y a un problème un peu plus large ou profond ?

BARBARA POVSE: Vous voulez dire que c'est la Commission Européenne qui essaye de régler ça ou pas ?

Je crois que l'objectif principal est de reconstruire la confiance vis-à-vis de l'internet, c'est l'objectif principal. Maintenant comment procéder c'est une autre histoire.

BRUCE TONKIN: Donc c'est l'économie numérique, construire de la confiance vis-à-vis de l'économie numérique ?

BARBARA POVSE: Alors là vous avez fini par me perdre.

BRUCE TONKIN: En fait, je veux savoir ce qui sous-tend ce désir de règlementer tant en Europe.

BARBARA POVSE: Je ne suis pas bien sûre, peut-être que je ne suis pas la bonne personne à qui poser cette question.

BART BOSWINKEL: Annaliese, c'est là peut-être une bonne question pour l'IGLC, pour qu'il s'y penche.

ANNALIESE WILLIAMS: Nous avons beaucoup de membres de la zone Union européenne, donc on peut ajouter cette liste.

Nous avons une question de Chris.

CHRIS DISSPAIN: Alors, plusieurs choses. Pour répondre à la question de Michèle ou dire ce que j'en pense, je pense qu'ils s'en soucient peu. Ils ont simplement décidé de légiférer par rapport à ce qu'ils n'ont pas pu obtenir par l'intermédiaire du modèle multipartite. Et le fait que cela cible les ccTLD et bien ils n'ont pas le choix. Parce qu'il faut bien qu'ils légifèrent par rapport aux ccTLD.

J'ai organisé une séance l'année dernière à l'European Summer School, qui traitait de fragmentation et l'un des intervenants qui a travaillé très longtemps à la Commission disait : oui, on fragmente parce qu'on ne nous laisse pas faire ce qu'on veut. Donc voilà un peu la toile de fond de tout ça.

ANNALIESE WILLIAMS: Merci, Chris, de ce commentaire. J'ai la main levée de Jordan.

JORDAN CARTER: Moi c'est une question. Barbara, pensez-vous que la manière dont l'UE règlemente à un rythme si rapide est conforme à son soutien officiel au modèle multipartite ?

BARBARA POVSE: Alors là, vous me prenez de court un petit peu. J'en ris tellement vous me prenez de court.

ANNALIESE WILLIAMS: Écoutez, va pouvoir peut-être traiter cette question en groupe. Et, effectivement, comme vous l'avez suggéré, on pourrait ajouter cette question et la soumettre au comité dans son ensemble.

BARBARA : Merci, vous me sauvez.

ANNALIESE WILLIAMS : Y a-t-il une autre question pour Barbara ou les autres intervenants ? Michèle, c'est une nouvelle main ?

MICHELE NEYLON: Oui, je voulais vous remercier vous et CENTR parce que vous avez été extrêmement utiles depuis 1 an et vous avez essayé de nous aider à nous y retrouver dans tout ce mouvement un peu fou qui vient de la Commission européenne. Le fait est que la Commission européenne essaye de règlementer, et comme Chris l'a dit, elle essaye de règlementer parce qu'elle n'a pas pu obtenir ce qu'elle voulait. Et essayer de s'y retrouver c'est réellement difficile. Je sais qu'on a tous beaucoup consacré de temps ou on s'est beaucoup préoccupé par rapport à NIS2. Et on a eu peur que nos gouvernements commencent à dire : regardez ce que fait l'UE alors que les États-Unis font ça. Mais merci, parce que CENTR a été très utile.

BARBARA POVSE: Merci. Si un bureau d'enregistrement est heureux, alors moi aussi je suis heureuse.

ANNALIESE WILLIAMS: Bien, je pense qu'on va conclure là-dessus. Je crois qu'on a entendu de la part de tous nos intervenants que la cybersécurité est une source de préoccupation pour tous les gouvernements, il y a beaucoup de législations en place et d'autres projets de loi en cours. Donc ça a été une excellente occasion d'entendre nos expériences respectives.

Donc j'aimerais remercier tous nos intervenants, notamment Norman et Lourino qui ont fait leur première présentation devant la ccNSO.

Merci, la séance est levée.

[FIN DE LA TRANSCRIPTION]