ICANN74 | Forum de politiques – Présentations de NextGen (1 sur 2)
Mardi 14 juin 2022 – 13h15 à 14h30 AMS

DÉBORAH ESCALERA: Bonjour à tous, nous allons commencer. Bonjour et bienvenue à la prochaine session de l'ICANN. Je suis Déborah Escalera et je suis la responsable de la participation à distance pour cette séance.

Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendues de l'ICANN. Durant cette séance, les questions et les commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre adéquate et de la bonne manière.

Nous lirons les questions durant la séance. L'interprétation pour cette séance aura lieu en anglais, espagnol, français et russe. Cliquez sur l'ICANN dans le Zoom et sélectionnez la langue que vous allez écouter dans la séance. Pour parler, veuillez la main dans la salle Zoom, une fois que le facilitateur de la séance dira votre nom, il ouvrira votre micro et vous pourrez prendre la parole. Avant de parler, sélectionnez la langue que vous allez parler. Veuillez indiquer votre nom pour les enregistrements et parler à un rythme raisonnable. Mettez en sourdine tous les autres dispositifs et notifications.

Donc, encore une fois, parlez à un rythme raisonnable pour que l'interprétation soit adéquate.

Je vous souhaite la bienvenue à cette séance et je remercie tous les participants pour le travail acharné qu'ils ont fait pour préparer leur présentation.

Je voudrais remercier tout le monde, tous les mentors qui ont travaillé avec les étudiants durant les semaines passées et pour les avoir aidés dans les processus de l'ICANN.

Avec cela, je voudrais passer la parole à Joël Christoph.

JOËL CHRISTOPH: Merci beaucoup. Bonjour à tous, merci à toutes les personnes qui sont là. Je vais faire ma présentation sur la cartographie de la croissance de l'internet en 2022. C'est un document sur les connaissances démographiques et économiques que nous avons reçues de différentes sources afin de pouvoir les étudier.

Prochaine diapo.

Avant de commencer, j'aimerais que tout le monde considère quelle est la proportion de la population dans les pays à revenus faibles et quelles sont les personnes qui utilisent l'internet. Quel est donc le pourcentage de cette population.

Dans ces pays à faible salaire, combien de souscriptions, d'abonnements de téléphone portable, y a-t-il ? Vous pensez qu'il s'agit de 25, 75 ou peut-être quelque chose de différent ? Combien de serveurs sécurisés y a-t-il parmi les personnes en Amérique du Nord ? Peut-être qu'il s'agit d'une chose plus difficile à exprimer.

Voilà donc certaines des questions auxquelles nous allons essayer de répondre à la fin de cette présentation.

Prochaine diapo.

Donc, dans la décennie passée, nous avons vu des changements lorsqu'il s'agit des recherches de beaucoup de personnes et de ce qui a été publié. Nous voyons une croissance énorme lorsqu'il s'agit de l'internet depuis les années 90, surtout avec les réseaux sociaux et Facebook dernièrement, alors qu'au niveau de la base on va parler de la censure.

Donc le but de cette diapo est de montrer que nous avons une croissance dans l'intérêt de beaucoup de ces sujets, de ces thématiques car il s'agit d'une tendance persistante. Cela indique donc que les bourses sur ces sujets vont devenir très importantes, et tout ça va faire partie de tous les documents qui vont être écrits dans l'avenir.

Nous allons passer maintenant au centre du sujet. Voilà donc la proportion de personnes par région qui utilisent l'internet.

Malheureusement, la légende sur la gauche, comme vous le voyez, n'est pas tout à fait claire. Mais vous voyez qu'il y a une augmentation dans différentes régions par rapport au nombre de personnes qui utilisent l'internet. Il y a aussi une accélération qui est nette par rapport aux années, on voit dernièrement surtout en Asie, une croissance plus rapide. Et puis, dans ce sens-là il y a une convergence vers 90 % dans les pays ou régions à fort revenus. Comme vous le voyez, en Amérique du Nord.

Comme vous voyez, en marron, le groupe a faible salaire, cela correspond aux pays qui ont les salaires moindres, des catégories de faible salaire, et cela est identifié par la banque mondiale. Ce sont des gens qui vivent en moyenne avec 2,7 € par jour. Vous voyez que malgré tout, qu'une personne sur 5 a accès à l'internet. C'est donc un signe, parce que là il s'agit de technologie qui est un petit peu différente, cela correspond à l'accès par ces personnes dans les parties du monde qui sont à plus faible salaire.

Nous allons comparer cela avec les chiffres absolus. Nous voyons qu'alors qu'il y a un démarrage assez rapide d'utilisation aux États-Unis, comme vous le voyez en vert, sur la décennie passée, nous avons tout de même vu une croissance énorme, par exemple en Chine et en Inde/

Il y a quand même une population assez élevée, donc on sait que cette tendance va continuer pour ce qui est de l'utilisation de

l'internet et, bien sûr, que cela va aussi être démontré dans d'autres parties du monde.

La partie inférieure de ce diagramme représente les autres 10 pays par rapport aux 10 pays principaux, ce sont les pays avec le plus grand nombre d'utilisateurs. Il s'agit de l'Inde, de la Fédération Russe et du Brésil. Quand on va comparer les utilisateurs par rapport aux abonnements de téléphone mobile, cela nous donne une idée de la manière avec laquelle les gens vont avoir accès à l'internet. Voilà les données qui nous ont été fournies par la Banque Mondiale.

Et vous voyez ici que dans beaucoup de régions, Amérique du Nord, Europe, Asie Centrale, nous avons beaucoup d'abonnements, beaucoup plus d'abonnements de téléphones portables. Voilà des groupes qui appartiennent à salaire faible. Il y a tout de même des abonnements de téléphone mobile, une personne sur deux. Donc il y a quand même une tendance à ce que l'accès à l'internet à travers les téléphones portable va s'accroitre à travers le monde.

Si on considère cela avec les abonnements fixes, c'est une manière différente d'accéder à l'internet et de communiquer, nous voyons qu'il y a une augmentation qui n'est pas aussi marquée, surtout durant la dernière décennie. On voit des conversions un petit peu plus rapides dans certaines régions,

surtout en Asie Centrale, et dans d'autres régions. L'intérêt de tout cela c'est qu'à travers toutes les régions, comme l'Amérique du Nord, il y a tout de même des cas où on est au-dessous du seuil des 50 %.

Quand nous passons au nombre de serveurs sécurisés de l'internet, pour 1 million de personnes, vous voyez les certificats qui utilisent la technologie de cryptage, et vous voyez ici, il y a une grosse différence entre les diapos et entre les régions. Parce qu'en Amérique du Nord, surtout aux États-Unis et au Canada, il y a un plus grand nombre de serveurs par rapport à la population et aussi par rapport à l'Europe où ces certificats ne sont pas aussi fréquents.

Prochaine diapo.

Si nous considérons de prendre un peu de recul et que l'on considère encore une fois l'utilisation de l'internet par rapport au partage de la population et le revenu par personne, il y a donc un changement dépendant des pays, plus d'utilisateurs vont utiliser l'internet. Sur le graphique vous voyez qu'il y a un point de saturation, cela correspond à un niveau de revenus, par exemple pour les États-Unis, Bahreïn, Norvège, la Suisse où les niveaux de revenus sont plus élevés. Et là on sature puisqu'il n'y a pas autant de problèmes.

Prochaine diapo s'il vous plait.

Dans la dernière diapo, je voulais prendre du recul et considérer comment nous allions pouvoir représenter cela à travers le temps. Cela aussi représente l'intensité de l'utilisation. Donc cela est basé sur des recherches faites aux États-Unis, on a demandé combien d'heures s'engagent-ils sur les réseaux sociaux. En 2018 vous voyez qu'il y a des nouvelles technologies qui ont été développées. Et aussi il y a eu l'introduction de nouveaux outils portables, ce n'est pas une substitution mais plutôt une augmentation du temps d'engagement des utilisateurs. Et cela suggère que de nouvelles technologies seront développées et donc un accès différent sera développé. Ce sera donc un rajout de lignes qui seront connectées numériquement.

Et, avec cela, je voudrais en terminer avec ma présentation. Je vous remercie et je passe la parole à Déborah.

DÉBORAH ESCALERA: Merci. Y a-t-il des questions pour Joël ? Nous allons voir s'il y a des questions des participants en ligne. Merci, Joël, pour votre présentation. Très bien.

Nous allons passer à notre prochaine présentatrice, Mirabella Knoben. Mirabella, vous pouvez prendre la parole.

MIRABELLA KNOBEN: Merci, merci à tous, merci de participer à cette séance. Aujourd'hui je voudrais faire une présentation, c'est un document que j'ai créé l'année dernière, c'est similaire à ce qu'on appelle une thèse. J'ai participé à un séminaire sur la loi des services numériques et donc je vais expliquer cela et mon sujet c'était la règlementation du contenu et les algorithmes et quels sont les principes qui sont nécessaires pour respecter les droits de l'homme dans la sphère numérique.

Passons à la prochaine diapo.

Très bien, quand il s'agit de la loi sur les services numériques, comme vous le savez Face Book, Whatsapp, etc. sont devenus des plateformes que l'on doit utiliser tous les jours. Vous savez qu'elles ont un rôle important dans l'influence des opinions et aussi dans la fourniture d'informations. Et de façon à mettre à jour la règlementation du E-Commerce, depuis décembre 2020 l'Europe a publié cette loi sur les services numériques. Il s'agit de définir une règlementation plus stricte pour les plateformes de média-sociaux. Et donc récemment, à la fin avril, il y a eu un accord politique sur le DSA, donc par rapport au Parlement et au Conseil de l'Europe, c'est une règlementation et ce n'est pas une directive.

Donc voilà, le système va s'appliquer à partir du 1ier janvier 2024. Merci, prochaine diapo.

Alors, quels sont les algorithmes ou les systèmes de recommandation au sens du DSA ? Alors ils sont définis dans l'article 2, Lettre O du DSA : ils sont des systèmes entièrement ou partiellement automatisés qui suggèrent à l'utilisateur un contenu spécifique sur l'interface utilisateur. Cela peut être vu comme des systèmes de recommandations, les utilisations de telles plateformes, on leur démontre des contenus customisés de façon journalière.

Prochaine diapo s'il vous plait.

Nous allons passer maintenant à la partie centrale de mon travail, quelles sont les interférences qui peuvent avoir lieu avec les droits de l'homme. Je me suis centrée sur la liberté d'information et la liberté d'expression. Dans les deux cas, cela est mentionné dans la charte des droits fondamentaux.

Je parlerai d'abord de la liberté d'information. Les plateformes de réseaux sociaux sont conçues pour satisfaire les utilisateurs et pour que nous, en tant que personnes, nous revenions pour chercher des contenus avec lesquels nous sommes d'accord, que nous connaissons. Cela peut donner lieu à une limitation concernant les contenus, une espèce de bulle, de filtre, parce que nous voyons des contenus qui nous plaisent, avec lesquels nous sommes d'accord et cela devient très subjectif et tendancieux. Par rapport à cela, la liberté d'expression peut être en danger parce

que les personnes vont développer leur opinion en fonction des données, des éléments reçus. Et tout cela est basé sur les algorithmes, sans contrôle humain.

Par conséquent, cela va avoir un impact sur le développement des opinions. La liberté d'expression est donc aussi en danger lorsque l'on ne travaille qu'avec certaines informations.

Donc la question serait : quels sont les principes dont nous aurions besoin pour éviter cette interférence ?

Personnellement, je me suis concentrée sur deux principes possibles dans mon travail de thèse. D'abord les systèmes qui sont basés sur ce que j'appelle la conception participative qui signifie que les systèmes qui sont basés sur cette conception participative vont inclure davantage de participation humaine et représentent, par conséquent, davantage de valeur de différentes personnes. L'objectif ici est de créer un algorithme qui va incorporer les valeurs de chaque société.

Et, vous avez entendu dire cela, on en parle beaucoup ici à l'ICANN, on parle du modèle multipartite qui est un modèle interne à l'ICANN, mais je dirais qu'ici, à la base, ce modèle pourrait aussi être mis en œuvre dans les plateformes de réseaux sociaux. Et l'objectif de ce modèle c'est que l'on puisse entendre la voix de toutes les parties prenantes et que ces voix soient entendues de la même manière, qu'elles aient la même force.

Donc on a un processus participatif et inclusif en fonction de la taille de ces plateformes en ligne. On peut donner l'exemple de Face Book, dans ce cas-là c'est difficile de mettre en œuvre ce modèle, mais l'idée de base c'est que toutes les parties prenantes puissent faire entendre leur voix. C'est une manière de garantir la transparence et de garantir aussi une participation en ligne.

Et, pour repartir sur cette idée de transparence, dans la loi des services numériques l'article 29 inclut une exigence de transparence, ce qui veut dire que les plateformes en ligne sont obligées à communiquer et à divulguer les paramètres les plus importants pour que les utilisateurs sachent quels sont les paramètres qu'ils utilisent. Et le deuxième aspect c'est la possibilité d'exclusion. Cela signifie que quand ouvre une application, Instagram, Face Book, on va avoir d'abord la possibilité d'utiliser la plateforme avec et sans système de recommandation. On ne sait pas encore comment cela va être mis en œuvre, mais cela va être plus ou moins comme ce que nous voyons lorsque nous ouvrons un site internet et que nous acceptons que l'on utilise les cookies. C'est un peu le même système. L'objectif ici serait d'éviter les interférences concernant la liberté d'expression et autres droits fondamentaux. Les utilisateurs pourront, suite à cela, avoir davantage confiance dans les plateformes, ce qui sera positif pour elles ;

Pour conclure à propos de ces fonctions principales, je dirais qu'il faut tenir compte des trois fondamentaux, et comme internet n'a pas de frontière, bien que cette loi de services numériques soit une loi européenne, je dirai qu'il faut trouver une solution au niveau international parce qu'internet ne termine pas dans l'Union Européenne. Il faut créer un monde en ligne attirant et sûr, à long terme, et pour ce faire on doit travailler de manière mondiale.

DÉBORAH ESCALERA: Y a-t-il des questions pour Mirabella ? Des questions de participants à distance ?

En tout cas merci pour votre présentation. Nous allons maintenant donner la parole au prochain intervenant, il s'agit de Jan Batzner.

JAN BATZNER : Bonjour à tous, merci de m'avoir donné la parole ici. La sécurité internet est un objectif qui nous concerne tous. Nous allons parler des incidents liés à la sécurité dans le cyberespace.

Donc un exemple pourrait être par exemple un déni de service qui va faire que les utilisateurs ne pourront pas accéder à un site ou un Spouffing, ou Instagram écrit avec une faute d'orthographe commise exprès, le hameçonnage, etc.

Est-ce qu'on peut revenir en arrière ? Merci.

Je voudrais évaluer les conceptions prévalentes des sources de données publiques sur les cyber-incidents. Les sources de données publiques qui distribuent des informations sur ces incidents. Ici, vous voyez un graphique d'un réseau que j'ai créé, et vous voyez ces incidents regroupés par pays affectés. Chaque point représente un pays et vous avez la couleur qui correspond à l'intensité du conflit.

Donc il y a des différences au niveau de ces sources de données. Donc le registre de cyber-incidents de l'ICANN va enregistrer tous les incidents de cyber-sécurité qui ont lieu dans l'espace de l'ICANN et dans les produits de l'ICANN. Pour définir ce qu'est une vulnérabilité ou un incident de cyber-sécurité, c'est quelque chose qui met en danger l'internet, tout ce qui met en danger l'ICANN et ses données, et tout ce qui est ici en dessous, vient de l'espace public dans lequel on partage des informations sur ces incidents de cybersécurité.

Je vais vous parler de ces informations et nous verrons si nous pouvons parvenir à une conclusion.

Prochaine diapositive.

Ici, vous voyez le registre de cybersécurité avec la date, le problème et des tas d'informations. Donc cela apparait dans le

paragraphe qui figure à droite. L'état de tous ces incidents qui figurent sur cette liste est fermé, clos.

Nous allons voir l'avantage et l'approche des politiques publiques. Ce que nous voulons voir ici dans cet ensemble de données. Donc on voit qu'il y a plusieurs lignes superposées, ici l'objectif serait que cela mesure la même chose, mais ce n'est pas le cas. En vert, on voit les informations qui viennent de l'université de Heidelberg, en jaune les informations du Conseil de relation étrangère et en bleu un ensemble de données provenant d'une autre organisation et on voit que tout est différent. Par conséquent on peut conclure qu'il y a des méthodologies différentes qui sont utilisées pour collecter ces informations. Les informations qui correspondent à l'université de Heidelberg, la ligne verte, sont les plus – peut-être – inclusives.

Voyons si on peut regrouper ces informations par pays. Si c'est le cas, on va voir qu'on a la quantité d'incidents venant vers ce pays ou sortant de ce pays, ensuite nous verrons le niveau de réciprocité. Par conséquent, si un pays est victime d'une cyber-attaque et si ce pays rend la pareille, c'est la réciprocité. Donc ici, la réciprocité n'est pas complète, donc la réciprocité complète serait 1, le manque de réciprocité serait 0, donc on arrive au maximum à 0,5 comme niveau de réciprocité.

Et ici vous voyez la façon de quantifier ces informations, cela est mesuré par la [Freedom House] et vous voyez les caractéristiques des conflits qui ont eu lieu sur la cybersécurité. À gauche, vous voyez la relation entre – sur le graphique 3 et 4 – les attaques qui sortent et sur la droite vous voyez la réciprocité. Mais rien n'est très clair sur ces diagrammes. Et, une des raisons pour cela est qu'il y a une série d'États dans lesquels on assiste à de nombreux conflits. Il y a différentes approches qui tentent de quantifier tout cela.

Mais en tout cas, ce que l'on peut dire, c'est que cela peut donner lieu à des erreurs.

Ici, vous voyez en rouge les pays qui sont les plus importants ici dans notre analyse.

Je conclurais en disant qu'il y a 3 aspects dont on peut tenir compte ici puisque l'objectif de cette approche est la transparence, et on y parvient grâce à l'analyse des parties prenantes, la prise de conscience. On a vu que la méthodologie a un grand impact sur les réponses que l'on trouve ensuite. Donc pour la même question on a différentes questions. Voilà, merci.

DÉBORAH ESCALERA: Est-ce qu'il y a des questions pour Jan ? Des questions de participants en ligne ? Non ? Parfait, nous allons passer à la prochaine présentation. Nadeshda Arteeva.

NADESHDA ARTEEVA: Merci. Je vais parler de l'utilisation malveillante du DNS dans l'Union Européenne et la façon dont on peut le traiter.

La principale manière de définir l'utilisation malveillante du DNS c'est à travers la fréquence et la variation dans le temps. Comme cela a été vu en 2021, il y a une définition qui a été adoptée par l'ICANN concernant les parties contractantes et, selon l'ICANN ça peut être des réseaux zombies, des hameçonnages, des autres systèmes. Et pourquoi avons-nous besoin d'une définition ? Parce que la plupart des parties prenantes veulent une définition des dommages qui peuvent avoir lieu de manière à pouvoir évaluer les effets de quelque chose qui est très souvent imprécis.

Récemment il y a eu un rapport de l'Europe qui a suggéré de nouvelles études sur l'utilisation malveillante du DNS et qui a mis en place des stratégies. Je reviendrai à cela plus tard dans ma présentation. Il s'agit là d'un document très important pour toute la stratégie de l'utilisation malveillante du DNS en Europe.

Donc si on se base sur ce qu'a dit la Commission Européenne, l'utilisation malveillante du DNS, et cette étude, doit évaluer

l'impact de cet abus et doit mettre en place des mesures et politiques pour identifier les écarts. Et cela définit cet abus, c'est l'inactivité de l'utilisation des noms de domaine et de toutes les activités illégales.

Prochaine diapo.

Nous allons parler de l'évolution de cette question de l'utilisation malveillante, pas seulement dans l'UE, mais aussi dans la communauté en général.

Donc il y a des dispositions contractuelles qui régissent les abus de DNS qui, à l'origine, proviennent du travail lié aux politiques effectuées par la communauté ICANN en 2009/2010 sur la prévention des abus d'enregistrement, RAPWG. Donc cela souligne les points les plus importants de la stratégie ICANN.

Sur ce sujet, il y a plus de 6 ans, dans le document SAC077, le SSAC a écrit sur l'indice de santé du marché proposé par l'ICANN. C'était une première tentative d'aborder cette question de l'utilisation malveillante du DNS.

Vous voyez ici la façon dont ils en ont parlé. Ils ont offert de développer et de maintenir des mesures efficaces pour souligner la protection des consommateurs plutôt que les normes de l'industrie. Et si l'on se réfère à certaines parties, on sait qu'il n'y a pas beaucoup de travail qui a été fait pour l'instant et ce problème

est devenu critique surtout durant la Covid, parce que le volume de nouveaux enregistrements de domaines qui a donc inclus le coronavirus a augmenté le travail.

Donc, à l'époque, il y avait un forum de coalition sur les effets qui incluait les experts, ils ont publié les données qui ont démontré qu'il y avait une augmentation durant la dernière semaine de février. Et, en même temps, le CDC a commencé à envoyer des avertissements d'une pandémie mondiale. Donc, initialement, l'ICANN a encouragé les bureaux d'enregistrement d'être plus proactifs en ce sens et à mettre en place des mécanismes plus spécifiques. Les abus liés à la Covid ont été importants, il y a eu beaucoup de problèmes en général, et le gouvernement a donc été mis en garde car il y a eu des conséquences au niveau de la pandémie. Cela impliquait des nouvelles directives. En 2020, l'ICANN a donc mentionné la question et cela est devenu une priorité. Il y a eu une stratégie qui a été mise en place pour les bureaux d'enregistrement et les opérateurs de registre afin de pouvoir définir ces noms de domaine malveillants.

Prochaine diapo.

Cependant, on voit maintenant ce qui permet aux abus de noms de domaine de se produire ? Donc il y a eu une étude en 2021 qui a été citée et confirmée dans le rapport de l'Union Européenne, et cette étude a confirmé qu'une des raisons principales de cet abus

du DNS était le manque de données parce qu'il y a eu la règlementation du RGPD.

Comme vous le savez, le RGPD a été adopté et a donc restreint la publication des données personnelles dans le WHOIS.

Donc, en réponse, l'ICANN a établi de nouvelles politiques qui ont permis aux bureaux d'enregistrement et aux opérateurs de registre de rediriger ou d'éviter de mettre ces informations dans le WHOIS. Et, ensuite, il y a eu des conséquences, 85 % des titulaires de nom de domaine gTLD ne peuvent plus être identifiés.

Un autre problème qui est en rapport avec l'utilisation malveillante du DNS, les rapports prennent beaucoup de temps et la longue durée de vie d'un rapport. Et, bien sûr, jusqu'à aujourd'hui, beaucoup de personnes peuvent dire que cela prend 10 jours, même 20 jours, donc durant cette période de temps qui peut varier, pour certaines personnes cela peut être assez long tout de même.

Il y a donc un manque de connaissances sur cette thématique et donc on ne sait pas forcément quelles sont les actions requises.

Prochaine diapo s'il vous plait.

Donc, comment pouvons-nous aborder ce problème de l'utilisation malveillante dans l'UE ?

Il y a des mesures qui peuvent être entreprises d'après l'UE pour aborder cette question. Tout d'abord il faut choisir des fournisseurs avec plus de validations, du moins des standards pour les enregistrements de domaine. Donc il faut des standards plus importants, il faut prendre une approche différente, vérifier quel est le client pour vérifier qu'il n'y a pas d'utilisation malveillante du DNS.

Un autre point c'est de mettre en place des solutions de prévention et de remédiation, actions proactives, des noms suspects contenant des mots clefs de marques ciblées. Donc il faut encore une fois que les compagnies aient un système de détections proactives. Il faut aussi augmenter l'adoption de contrôles de sécurité. Alors, souvent il y a notifications entre les serveurs de DNS, il faut donc éviter que les hackers prennent le contrôle des séances sur l'internet.

Donc, l'auteur suggère dans cette recherche que les protocoles soient mis en place et adoptés comme une première ligne de défense.

Et, le dernier point, c'est qu'il faut qu'il y ait de meilleures normes dans les domaines de premier niveau. Donc pour les TLD, malheureusement, les TLD génériques sont les domaines les plus utilisés de façon malveillante. Pour les ccTLD il y a une grande concentration de fraude parce que de nos jours il est très facile

d'obtenir un TLD pour moins de 1 USD. Donc dans le rapport il est suggéré que des mesures soient prises par rapport à cette question.

Merci. Je serais heureuse de répondre à vos questions si vous en avez.

DÉBORAH ESCALERA: Merci. Y a-t-il des questions ? Il y a une question dans l'audience, vous voulez venir au micro ? Merci.

[DAVID] : Merci de votre présentation, merci à tous. Je suis curieux : est-ce que vous demandez à l'ICANN de faire plus que ce qu'elle fait déjà ? Parce que c'est quand même contentieux cette question, la vie privée, etc. Donc cela inclut le DNS2, je pense que ça s'appelait, donc il y a toutes ces exigences. Donc en fait, que voulez-vous que l'ICANN face à ce moment ? Si vous pouviez vous assoir avec Goran, que lui diriez-vous ? Vous pourriez lui dire : voilà c'est ce que j'aimerais que vous fassiez. Donc, encore une fois, qu'aimeriez-vous qu'il soit fait dans ce sens ?

NADEZHDA ARTEEVA: Merci pour votre question. Pour moi, je voulais adresser la situation avec la Covid surtout, en disant que lorsqu'il y a des

crises, d'ailleurs dans cette situation, on devrait avoir une réaction plus rapide. Surtout quand il s'agit d'utilisation malveillante du DNS durant la pandémie, il faut voir que les conséquences étaient importantes, avec des impacts sur les vies. Par exemple cela a amené des personnes à avoir accès à de fausses informations.

Pour moi, il y a des points critiques. Il y a eu des critiques vis-à-vis de l'ICANN et moi je voulais surtout adresser la manière avec laquelle ICANN a fait face ou abordé la crise.

DÉBORAH ESCALERA: Je pense que nous avons une question en ligne de David, ha c'était vous, d'accord, merci. Pardon. Très bien. Vous voulez venir au micro, Monsieur ? Merci.

NON IDENTIFIÉ : Merci. Alors, les informations sur la plupart des abus au niveau des extensions de gTLD, mais en fait, il y a d'autres plus anciens pour les ccTLD… Vous pouvez répondre à cette question ?

DÉBORAH ESCALERA: Vous expliquez s'il vous plait ?

NON IDENTIFIÉ : Oui, vous avez les données de ces gTLD qui sont les plus impliqués dans les processus d'utilisation malveillante du DNS ?

NADEZHDA ARTEEVA: Oui, dans le rapport, cela avait été présenté dans un brief, il n'y avait pas d'exemples. Oui, je pense que nous pourrions faire cette recherche.

NON IDENTIFIÉ : Vous avez mentionné certaines choses spécifiquement, vous avez dit que cela était un problème surtout pour les nouveaux gTLD. Mais pourquoi ne pas donner des noms ? Vous avez pourtant basé votre rapport sur ces données, donc vous pourriez partager un peu plus de ces données. Si vous ne pouvez pas, ce n'est pas grave.

NADEZHDA ARTEEVA: Oui, le rapport que j'ai cité c'est le rapport de l'UE sur l'utilisation malveillante du DNS, oui, si vous voulez, je peux absolument partager les données utilisées pour faire ce rapport.

DÉBORAH ESCALERA: Merci. Sachez que toutes ces présentations seront publiées sur le site ICANN à la fin de cette journée. Oui, nous avons notre prochaine présentation qui va nous venir de Liubomir Nikiforov.

LIUBOMIR NIKIFOROV: Oui, je n'ai pas l'habitude de ces présentations. Prochaine diapo. Je m'appelle Liubomir Nikiforov, je suis en doctorat à l'Université de Barcelone, avec un focus sur le consentement, la transparence et la gouvernance de l'internet.

Aujourd'hui cette présentation va souligner le manque de directive, l'absence de définition du consentement. Donc la situation mène à des problèmes de transparence et de risque de décrédibilité pour l'ICANN et ses parties prenantes. À la fin de ma présentation je parlerais de solutions possibles.

Prochaine diapo.

Nous parlons de la procédure contractuelle pour l'enregistrement d'un nom de domaine générique de premier niveau. Il y a trois parties, les bureaux d'enregistrement, il y a les titulaires de nom de domaine, la personne qui veut enregistrer, et vous avez l'opérateur de registre. Voilà les trois parties incluses.

Donc cet accord a un article, plus d'un mais il y en a un qui est très intéressant pour moi, l'article 2 paragraphe 18 qui établit les exigences concernant la protection des données. On parle aussi des données personnelles, des besoins de notification et de l'identification du réceptionnaire des données et de son consentement.

Prochaine diapositive.

Donc ici, vous voyez cet article dont je parlais. Et, comme vous le voyez c'est le seul article consacré aux données personnelles, il comprend toutes les informations et tout ce qui est fait avec les données personnelles. Il est difficile à lire et à comprendre.

Quel est son objectif et son utilité ? On peut se le demander.

Alors, quels sont les enjeux et défis qui existent ? Je vais me focaliser sur les enjeux concernant l'article 2 paragraphe 18, les opérateurs de registre doivent demander aux bureaux d'enregistrement d'obtenir le consentement de chaque titulaire de nom de domaine de premier niveau, et cet article 2 ne définit pas ce que sont les exigences pour la validité de ce consentement et n'explique pas non plus la forme qui existe pour cela.

Donc afin d'identifier cette problématique je vais utiliser le RGPD pour montrer ce qui n'est pas correct ici. En fonction de cette règlementation européenne pour que cela soit valable, pour qu'un consentement soit valable, il doit être informé, spécifique, libre et sans ambiguïté.

À partir de l'article 2 paragraphe 18 de cet accord de registre, on ne comprend pas quand et comment ce consentement peut être obtenu, s'il doit être obtenu dans cet objectif ou pour le traitement des données, quel moyen peut être utilisé, est-ce que

cela peut être fait par la violence ou l'intimidation ? Et, concernant les informations données par le titulaire de nom de domaine, on ne sait pas s'il peut refuser de donner son consentement et s'il a d'autres alternatives lorsqu'il refuse de donner son consentement.

Prochaine diapositive.

Alors, pourquoi est-ce que c'est important ? Et bien nous vivons dans une société dans laquelle les données jouent des rôles très importants. Ces données et ces informations peuvent être vendues, c'est pour ça que c'est important qu'il y ait une confiance dans les parties prenantes de l'ICANN, une crédibilité et une fiabilité envers l'institution, une confiance pour un internet ouvert et transparent.

Au niveau de l'UE on a des protections concernant le traitement de données, il y a des accords qui peuvent donner lieu à des utilisations malveillantes pour les titulaires de noms de domaine dans différents pays du monde, un processus dans lequel le titulaire de nom de domaine comprend le résultat du traitement de ses données, des accords qui seraient dans le bénéfice de ce titulaire de nom de domaine pour qu'il puisse, en cas de difficultés ou de désaccords, mettre en place des poursuites judiciaires.

Prochaine diapositive.

Comme je l'ai dit, je vais vous présenter des solutions. D'abord, réviser cet article, cette clause, de façon à la rendre plus facile à lire et plus claire.

Je ne suis pas tout à fait d'accord avec la clause des données personnelles, les accords de base registre et bureaux d'enregistrement, il faut savoir quand le consentement doit être donné, quelles sont les exigences. Par exemple, on pourrait appliquer le RGPD, ses règlementations, lorsque le consentement est demandé, qui doit être un consentement libre, informé et non ambigu. Si l'on voit que notre empreinte numérique existe, nous devons pouvoir donner notre opinion la concernant.

Ensuite, il y a des garanties démocratiques concernant notre dignité numérique qui doivent être prises en compte et respectées.

J'en ai terminé, merci.

DÉBORAH ESCALERA: Est-ce qu'il y a des questions ? Merci beaucoup, nous allons regarder s'il y a des questions en ligne.

Bien, je vous rappelle que toutes ces présentations seront diffusées sur le site internet de l'ICANN. Si vous avez des questions vous pouvez me les envoyer par email, à mon adresse, ENGAGEMENT@ICANN.ORG.

Je vous remercie d'avoir participé à cette réunion aujourd'hui, et je vous rappelle que demain une autre réunion du même type aura lieu, avec d'autres présentations du même type qui seront faites. Je vous remercie.

[FIN DE LA TRANSCRIPTION]