MONTREAL – Session de présentation du NextGen
Mardi 5 novembre 2019 – 13h30 à 15h00 EDT
ICANN66 | Montréal, Canada

DEBORAH ESCALERA : Nous allons commencer en temps et en heure.

Merci beaucoup d'être ici. Je m'appelle Deborah Escalera et je vous souhaite la bienvenue à cette présentation des NextGen. Nous allons commencer exactement à l'heure. Et j'aimerais tout d'abord vous souhaiter la bienvenue et remercier nos ambassadeurs NextGen qui sont venus me prêter main forte ici : Joao Pedro Martins d'ICANN63, nous avons également Jaewon Son d'ICANN64 et Stefan Filipovic d'ICANN63. Donc merci beaucoup d'être revenus nous prêter main forte ici à cette réunion à Montréal.

Sans plus attendre, nous allons commencer avec notre premier présentateur, Abdeali Saherwala. Abdeali, vous avez la parole. Allez-y.

ABDEALI SAHERWALA : Bonjour mesdames et messieurs. Je m'appelle Abdeali Saherwala et je suis une étudiante entre quatrième année à la faculté des sciences de l'environnement à l'université des York. Et malgré mes antécédents uniques, je suis ici pour parler d'un problème critique qui afflige notre société moderne, c'est la société post-vérité à travers les médias sociaux et ses implications politiques.

Avant de commencer, j'aimerais dire et reconnaître qu'ici même, nous sommes dans le Palais des congrès de Montréal et nous sommes situés sur des terres autochtones qui appartiennent à une nation autochtone. Nous avons des relations constantes avec les Premières Nations et les populations autochtones.

Les réseaux sociaux ont révolutionné la manière dont nous communiquons et ont beaucoup changé notre vie. Grâce aux réseaux sociaux, on peut savoir tout sur ce qui se passe dans la famille, chez les amis et en quelques secondes, je peux savoir ce qui se passe, si c'est important ou pas dans le reste du monde, que ce soit en Grèce, un problème économique ou bien l'approbation d'une mine en Australie.

Cela, c'est la puissance des réseaux sociaux et cela change beaucoup nos émotions, nos identités en temps réels. Nos opinions en sont modifiées et cela peut totalement changer et nous diviser également sans savoir tous les faits, tous les chiffres. Un adolescent au Canada, aux États-Unis ou en Europe peut devenir un terroriste en se réunissant avec un groupe de personnes peut-être islamophobes par exemple. Et cela peut créer des doutes dans notre esprit au niveau des faits, au niveau de la médecine, au niveau de la science. Des dizaines d'années d'améliorations, par exemple les vaccins, les améliorations médicales, les programmes médicaux peuvent maintenant poser problème à cause de ces réseaux sociaux.

Il y a un éléphant dans la salle. L'élection de Donald Trump aux États-Unis a totalement changé la société. On parle beaucoup de fausses

vérités ; il y a des personnes qui ne pensent pas qu'on a été sur la Lune par exemple. Mais avec la couverture de l'élection de Donald Trump, toutes ces théories du complot sont au grand jour. Vous voyez d'un côté René Descartes, ce philosophe français qui disait disait : « Je pense donc je suis. » et l'éducation, la recherche existaient et c'était la conscience de ce philosophe français que nous voyons. Et d'une autre côté, sur la droite, nous avons la post-vérité : « Je crois, donc j'ai raison. » Donc la post-vérité, c'est dénoter des circonstances où les faits objectifs ne sont plus réels, ne sont plus importants pour l'opinion publique. C'est maintenant plus du côté de l'émotion.

Ces dernières années, nous avons vu que dans les réseaux sociaux dans notre société, les personnes de plus en plus ne font plus confiance aux institutions établies, les universités, les gouvernements, les médias et les organisations internationales comme les Nations unies. On dit qu'ils ne répondent pas assez aux problèmes du monde. Il y a de plus en plus de post-vérité dans notre société. C'est causé par les réseaux sociaux et les entreprises de réseaux sociaux comme Facebook, WhatsApp, YouTube, Twitter, Instagram qui d'une manière ou d'une autre font des profits sur les fausses vérités.

Il y a des centaines de millions de personnes qui utilisent ces réseaux sociaux dans le monde avec plusieurs comptes, plusieurs plateformes, Facebook, Twitter, Instagram, LinkedIn dans mon cas et parfois même, plusieurs comptes sur la même plateforme. En 2018, Facebook a 2 600 000 000 de personnes, Instagram a plus d'un milliard de personnes. Ce sont des chiffres fous. En 2008, Facebook n'avait que 100 millions de personnes et cela a augmenté de 26 fois en 10 ans.

Donc Spiderman, vous savez qu'on peut le considérer maintenant comme un philosophe, a dit qu'avec beaucoup de pouvoirs, on a beaucoup de responsabilité. Mais Facebook n'est pas responsable par rapport à toutes les bêtises que l'on lit sur Facebook, aux fausses vérités que l'on obtient à partir de Facebook.

Facebook nous inonde et la plupart des gens maintenant prennent leurs informations de Facebook.

Dans le domaine anglo-saxon aux États-Unis, les adolescents s'informent avec Facebook. Dans le Moyen-Orient en fait, 28 % des personnes obtiennent de WhatsApp leurs informations. Au Royaume-Uni, Facebook vient au numéro deux et la consommation des nouvelles dans les réseaux sociaux en général entre 2018 et 2019, il y a eu de plus en plus de lecteurs de nouvelles sur Facebook. Comme conséquence, Facebook a dit qu'ils allaient retirer des informations fausses, notamment sur le génocide des Rohingya. Cela leur a pris plus de deux ans pour ce faire, pour qu'il n'y ait plus de fausses vérités sur le site Facebook. Et vous voyez Ashin Wirathu sur l'écran, dans toute sa vie, il a posté des posts islamophobes contre les Rohingya et dans des entretiens, il a dit des choses absolument horribles. Et malgré cela, Facebook a laissé tout cela sur l'internet, sur Facebook pendant plus d'un an même si les Nations unies avaient dit que Facebook était un facteur clé dans le génocide des Rohingya et dans ces atrocités qui ont été commises contre les Rohingya au Myanmar. La France et les pays d'Europe ont décidé de combattre les fausses nouvelles. Le gouvernement espagnol par exemple demande des actions de la part de Facebook. Au Royaume-Uni, il y a des enquêtes judiciaires qui

existent et des textes de loi sont en préparation. Emmanuel Macron, le président français, a décidé que Facebook, pendant les élections, ne pouvait plus présenter ces informations fausses.

Aux États-Unis, 50 % de la population soutien des enquêtes sur les réseaux sociaux qui ont interféré avec les résultats de l'élection de 2016 aux États-Unis. Il y a des groupes qui amplifient ces nouvelles, des groupes privés, semi-privés qui sont de plus en plus populaires parce que Facebook a promu des communautés. C'est devenu véritablement quelque chose de très toxique. YouTube a des algorithmes pour qu'on trouve moins de vidéos problématiques.

Et enfin, pour conclure, le département de la Défense a créé un programme dans le cadre de DARPA pour retirer parmi des échantillons les photos et vidéos qui posaient problème.

Mes recommandations sont les suivantes. Les consommateurs doivent plus s'informer, comprendre ce que sont les fausses, nouvelles. Les entreprises doivent engager des personnes capables de mieux comprendre ce qui se passe et traduire également. Enfin, les gouvernements doivent tenir comme responsables les réseaux sociaux, ils doivent limiter les fausses nouvelles, les trolls et les zombies qui existent sur l'internet. C'est une dynamique sociale qui est tout à fait négative, qui parfois est mortelle.

Merci beaucoup de votre attention.

DEBORAH ESCALERA : Merci Abdeali. Vous avez beaucoup travaillé sur votre présentation. Nous allons maintenant demander s'il y a des questions de l'auditoire dans la salle. Nous allons les gérer.

DAVID MARGLIN : Bonjour. Est-ce que Facebook essaie d'atteindre le pouvoir ?

ABDEALI SAHERWALA : Je ne sais pas comment répondre à cela. Mais je crois qu'ils peuvent faire beaucoup plus et faire en sorte que des personnes comme Ashin Wiradu n'aient pas la possibilité de s'exprimer autant sur la plateforme Facebook.

LUKAS BUNDONIS : Bonjour. Lukas Bundonis des États-Unis.

Ma question, c'est le concept de la post-vérité. Historiquement, il y a d'autres exemples, des moments historiques où les fausses vérités ont existé. L'église contrôlait la vérité, essayait de le faire, la propagande des Nazis. Qu'est-ce que l'on peut dire par rapport à l'exactitude des faits ? Est-ce que c'est quelque chose d'utile ? Qu'est-ce que l'on peut faire pour lutter contre ces fausses vérités ?

ABDEALI SAHERWALA : Ce qui s'est passé, c'est que plutôt que d'avoir une seule entité comme l'église catholique qui contrôlait totalement l'information, les gouvernements ou les groupes maintenant essaient de créer leur

propre réalité et voient les compagnies de réseaux sociaux comme étant une possibilité d'étudier et d'utiliser ces fausses vérités parce qu'il y a des milliards de personnes qui sont sur les réseaux sociaux qui peuvent être influencées de cette manière.

DEBORAH ESCALERA : Est-ce qu'il y a d'autres questions ? Très bien, merci beaucoup Abdeali. Nous vous applaudissons.

Notre prochain présentateur, Akshay Broota, vous avez la parole.

AKSHAY BROOTA : Merci Deborah.

Bonjour à tous. Je suis ici pour vous parler du RGPD. Je vais vous donner un aperçu de ce qu'est le RGPD et des conséquences que cela peut avoir sur l'Union européenne et sur le monde en général.

Je vais commencer par me présenter. Je suis Akshay Broota. Je suis en train de faire une maîtrise. Je fais une maîtrise en ingénierie à Université du Colorado à Boulder aux États-Unis. Et j'ai commencé à étudier le RGPD, son impact et je vais donc vous en parler.

Avant le RGPD, il y avait une loi qu'on appelait la directive sur la protection des données qui a été adoptée en 1995 et c'était avant l'explosion de l'internet, des téléphones intelligents, etc. Donc ce n'était pas vraiment efficace et on avait un problème au niveau de la protection des données.

Le principal objectif du RGPD a été de protéger les données personnelles. Le premier jet du RGPD a été publié en 2012. Il a été adopté au Parlement européen en 2016 et finalement, il y a été mis en vigueur en mai 2018.

Maintenant, on sait que le RGPD existe et nous voyons de quoi il s'agit. Il s'agit d'une loi qui régit la manière dont les entreprises protègent les données personnelles. Il est conçu pour harmoniser les lois sur la confidentialité des données à travers l'Union européenne. Le RGPD vise à offrir une transparence quant à la manière dont les entreprises traitent les données des consommateurs.

Les compagnies qui respectent le règlement du RGPD doivent justifier comment ils utilisent les données personnelles des clients et elles peuvent avoir des sanctions sévères et même des amendes de plusieurs millions d'euros.

Pourquoi le RGPD ? Nous avions des règles obsolètes dans la directive sur la protection des données. Ces règles ont été établies avant l'invention des téléphones intelligents, elles n'ont pas abordé les problèmes de confidentialité concernant les données personnelles et la façon dont les contrôleurs accédaient à ces données et les vendaient à des tierces parties et comment est-ce qu'ils visaient les consommateurs pour des produits spécifiques. Les personnes n'ont pas de contrôle de leurs données personnelles par conséquent ; il a fallut créer ce RGPD.

Ces objectifs sont d'assurer la transparence, d'éviter le blocage des fournisseurs, éviter l'utilisation abusive des données personnelles.

Cela garantit que ces objectifs sont atteints. Le RGPD accorde les droits suivants aux utilisateurs : droit d'être informé, droit d'accès, droit d'effacement, droit d'opposition, droit à la portabilité des données, droit à la limitation du traitement, droit à la rectification des données. Je vais me focaliser sur un de ces aspects qui est la portabilité des données.

Nous allons d'abord parler des problèmes concernant le RGPD. Le RGPD a été mis en œuvre avec un format électronique structuré et couramment utilisé qui permet d'autres utilisations. Donc le RGPD ne mentionne pas le format que les données doivent avoir entre le contrôleur et le consommateur. On ne mentionne que le fait que ce format doit être lisible par machine Il y a différents formats, PDF, Excel, etc. Donc il y a un manque de détails, d'explications concernant le format que ces données doivent avoir et qui est utilisé dans nos sociétés. Cela doit être lisible entre les contrôleurs.

Un autre concernant le RGPD, c'est qu'on ne mentionne pas la façon dont les tierces parties peuvent accéder aux différents sites. Quand on parle de transportabilité d'une compagnie à l'autre, les coûts qui existent concernant ce transfert de données sont des coûts inconnus, on ne sait pas. Le RGPD mentionne que les consommateurs ne sont pas responsables des coûts en ce qui concerne cette transition mais on ne sait pas si ces coûts seront entre la compagnie A et la compagnie B.

Voyons un petit peu la portabilité des données. La capacité pour les personnes de réutiliser leurs données sur des appareils et des services,

le RGPD article 20 le mentionne. La personne concernée a le droit de recevoir les données personnelles. Si je suis une personne qui veut passer d'une compagnie à l'autre, je veux invoquer mon droit à la portabilité pour transférer mes données d'une compagnie à l'autre et cela doit être fait de manière lisible pour la machine.

Lorsqu'on compare ces directives sur la protection des données, le RGPD au niveau de la portabilité des données, il y a une question de temps. Le RGPD dit que cela doit être fait dans 30 jours. Le coût, c'est le contrôleur qui est responsable mais on ne sait pas très bien quelle compagnie va assumer les coûts. Le format : lisible par l'utilisateur, format lisible par machine, format brut. Donc il faut que ce soit un format utilisé en général, on ne sait pas lequel. La sécurité, de nouveau, c'est très vague, on ne sait pas très bien quelle partie va assumer sa responsabilité face à la loi. Et la responsabilité : contrôleurs de données responsables de mauvaise gestion, on n'indique pas clairement qui est responsable.

Beaucoup pensent que cela a eu un certain succès jusqu'à maintenant mais une seule partie a été mise en œuvre. Il y a eu certaines préoccupations depuis la mise en œuvre du RGPD. Il y a eu une série de courriels qui concernaient les activités du RGPD, les personnes ont commencé à recevoir des courriels concernant le RGPD leur disant qu'ils devaient modifier leur système de confidentialité ou leur système de collecte de données. Il y a eu des problèmes de hameçonnage aussi. Je ne sais pas si vous connaissez Max Shem qui est un activiste autrichien. Lorsque le RGPD a été lancé, il a poursuivi

Google parce que Google forçait ses consommateurs à faire ce type de collecte de données.

L'impact du RGPD a été à l'extérieur de l'Union européenne a été très grand. Je viens d'Inde, je vis actuellement aux États-Unis et nous savons qu'en Californie par exemple, il y a eu une nouvelle loi de protection de la confidentialité de consommateurs qui va être appliquée à partir du 1er janvier 2020. Et cette loi en Californie oblige les résidents californiens d'assumer et d'être responsables de leurs données et des compagnies comme Google et Facebook vont devoir contrôler la vente des données des consommateurs aux tierces parties.

Le RGPD finalement est quelque chose qui est compliqué mais qui permet aux citoyens européens et aux citoyens qui sont à l'extérieur de l'Europe mais qui traitent avec des compagnies basées en Europe, ce RGPD permet une certaine flexibilité, permet aux utilisateurs de faire des changements et nous allons voir comment le RGPD va fonctionner et les résultats qu'il aura dans les années à venir.

Merci.

DEBORAH ESCALERA : Merci. Est-ce que nous avons des questions ? Pas de question ? Et bien, merci beaucoup.

Notre prochaine présentatrice, Ariane Nakpokou. Nous lui donnons la parole.

ARIANE NAKPOKOU : Merci beaucoup, merci Deborah de me donner la parole.

Bonjour à toutes et à tous. Je suis Ariane Nakpokou et je suis très heureuse d'être membre de NextGen. Je viens de terminer la licence en administration commerciale et je me spécialise dans la comptabilité. J'ai travaillé dans un programme sur l'intelligence artificielle et je vais parler de la gouvernance de l'internet et de l'intelligence artificielle. Je viens du monde commercial et il est intéressant pour moi d'en savoir plus sur les différentes suppositions concernant l'intelligence artificielle, donc de rentrer un petit peu plus dans les détails.

Nous allons parler de quelques généralités sur l'intelligence artificielle, essayer de mieux comprendre ce qu'il en ressort. Et nous allons parler du rapport avec le DNS, le système de noms de domaine, et ce que l'on peut faire pour qu'il n'y ait pas de problème entre les deux systèmes. Ensuite, nous allons parler de ce dont on parle beaucoup à l'ICANN66, le conflit entre le WHOIS et le RGPD. Je vais revoir ce que fait l'ICANN pour essayer de régler ces problèmes.

Nous sommes ici depuis samedi et j'en ai appris plus sur les différents points de vue des personnes. Ensuite, nous allons parler un petit peu plus d'intelligence artificielle et de la question de l'éthique et de l'intelligence artificielle.

Donc .ai, ou *artificial intelligence* en anglais, C'est un projet basé sur ce concept l'intelligence artificielle et vous savez peut-être que Montréal

investit beaucoup dans la recherche sur l'intelligence artificielle et c'est l'un des endroits du monde où l'intelligence artificielle est des plus avancée. C'est la capacité à raisonner, l'intelligence à percevoir des relations, des analogies, de calculer, d'apprendre à partir d'expériences et de répondre à des situations. Donc ce que nous attendons d'un système basé sur l'intelligence artificielle.

Il y a beaucoup de fantasmes au sujet de l'intelligence artificielle. Qu'est-ce qu'on peut attendre de l'intelligence artificielle, de ce concept ? Il y a beaucoup de points de vue à prendre en compte mais pour rester bref, il y a différents niveaux de recherche par rapport à l'intelligence artificielle, le traitement de la langue naturelle par exemple, il y a beaucoup d'experts également de la robotique qui travaillent dans le cadre de l'intelligence artificielle.

Ce qu'on utilise le plus, c'est les réseaux neuronaux, l'apprentissage de la machine également. On utilise l'expertise humaine dans les finances, dans la recherche médicale, les diagnostics. Il y a des réseaux neuronaux définissent et analysent les tendances et qui permettent d'apprendre.

Il y a différentes techniques qui sont utilisées. L'apprentissage des machines par exemple qui utilise les données et les algorithmes pour traiter et analyser les données et le système prend des décisions informées par rapport aux données qui ont déjà été analysées.

L'apprentissage en profondeur des machines existe également. Vous allez donc créer des réseaux neuronaux artificiels qui fonctionnent un

petit peu comme les neurones du cerveau et cela va permettre de prendre des décisions intelligentes.

Mais la différence entre les deux, c'est que l'apprentissage par la machine, on met une donnée et on a une seule réponse à la fois. Mais lorsqu'il y a un apprentissage plus en profondeur, c'est automatique, c'est un processus continu d'apprentissage. Et il faut fournir beaucoup de données à la machine dans ce cas de figure. Et la machine va se rendre compte qu'il y a des analogies qui peuvent être définies à partir de toutes ces données.

Quel est le rapport avec le DNS, avec le système de noms de domaine ? C'est tout à fait intéressant en ce qui concerne la sécurité parce que l'intelligence artificielle est importante pour les prestataires de services pour limiter les risques cybernétiques pour protéger les consommateurs. Pour reconnaître les tendances des attaques cybernétiques, on peut utiliser cette l'intelligence artificielle et améliorer les défenses du DNS et prendre des mesures intelligentes pour permettre aux bureaux d'enregistrement et aux consommateurs de ne plus être victimes de ces attaques cybernétiques.

Vous pouvez ainsi mieux protéger votre nom de domaine. Si vous avez quelqu'un qui tente d'enregistrer un nom de domaine similaire à votre nom de domaine, à ce moment, vous pouvez utiliser l'intelligence artificielle pour être informé du problème. Et c'est très utile parce que cela peut vous aidez à protéger votre entreprise et votre réputation enligne. Cela permet de limiter éventuellement les fraudes, les

attaques des sites web, les attaques à l'image personnelle que nous avons sur l'internet.

Vous pouvez améliorer également la performance de votre domaine parce que les prestataires de service internet vont se baser sur des analyses qui ont été effectuées par des machines et ils vont pouvoir définir une performance accrue du domaine et vous donner les meilleurs outils informatiques pour la gestion de votre contenu et pour l'optimisation du trafic internet qui va aller vers votre domaine.

Lorsque vous utilisez l'intelligence artificielle pour gérer votre DNS, vous avez un internet qui est beaucoup plus stable et intègre et vous avez en fait un WHOIS qui est beaucoup plus précis. Là, on peut se mettre à parler discussion RGPD, où est-ce que l'on met la limite dans ce droit de savoir et le respect de la vie privée. On peut à ce moment-là savoir qui est responsable des données ; cela, c'est absolument essentiel pour certains thèmes de traités. Mais on sait également que certaines informations peuvent être utilisées pour attaquer des personnes et maintenant avec l'intelligence artificielle, nous avons un processus et un contrôle qui sont effectués par des entreprises dans un espace avec assez de compétences technologiques. Nous pouvons avoir un outil utilisé par des régimes totalitaires qui vont manipuler l'internet et l'accès à l'internet.

L'approche de l'ICANN est de développer un modèle d'accès unifié et d'avoir un respect de la vie privée dans la conception même. Le système WHOIS, c'était le droit de savoir, le droit de savoir à qui appartenait le domaine. Maintenant avec le RGPD, après le EPDP que

nous avons eu depuis plus d'un an, nous avons eu une reconnaissance au niveau juridique, au niveau des lois européennes, au niveau des autorités de coordination visant à s'assurer que les différents bureaux d'enregistrement et registres fournissent quelque chose qui tient la route au niveau juridique.

En ce qui concerne les questions d'éthique qui se posent... Je crois que le temps imparti s'est écoulé et je pourrais maintenant répondre à vos questions. Merci.

Le RGPD, c'est donc le respect de la vie privée dans la conception-même du système et nous devons rester éthique lorsque nous définissons les systèmes. Il est extrêmement important d'être orienté vers l'humain et de ne pas transposer nos préjugés dans les algorithmes et de s'assurer que les possibilités de l'intelligence artificielle ne soient pas un repositionnement des inégalités que nous observons dans nos sociétés.

Merci beaucoup de votre attention. Je suis prête à répondre à vos questions.

DEBORAH ESCALERA : Merci beaucoup Ariane. Est-ce qu'il y a des questions ?

JOÃO PEDRO MARTINS : João Pedro du Portugal.

Est-ce que cela veut dire que l'ICANN est maintenant responsable, pourrait-on dire, de la création d'algorithmes éthiques ?

Parce que je sais que vous êtes du monde commercial. On pourrait dire et avancer que ceux qui forment et offrent le produit peuvent avoir beaucoup de pouvoir sur les algorithmes utilisés. Donc cela demande beaucoup de recherches, beaucoup de temps. Et j'y travaille également. Je crois que c'est un nouveau débat du point de vue de l'ICANN. Qu'en pensez-vous ?

ARIANE NAKPOKOU : À chaque fois que l'on pose ces questions, on pense toujours que l'ICANN parle de contenu et gère le contenu. Même si l'ICANN pourrait prendre en compte des termes qui sont utilisés dans les données, je pense que nous allons avoir plus de politiques à ce sujet et adopter des politiques plus éthiques et éthiques par rapport à l'intelligence artificielle. Et comme le RGPD que nous avons eu aujourd'hui, je crois que nous allons évoluer vers des politiques de l'ICANN. Je crois qu'il faut commencer maintenant dans nos politiques et nous devons réfléchir et avoir à l'esprit le bien-être de l'humanité et l'importance de politiques éthiques développées.

LUKAS BUNDONIS : Ariane, merci de votre présentation tout à fait fascinante.

Oui, l'intelligence artificielle, c'est beaucoup d'opportunités, de possibilités technologiques, c'est très enthousiasmant, il y a beaucoup de domaines. Mais cela cause beaucoup de problèmes parce qu'on a des produits, on met l'étiquette « intelligence artificielle » et en fait, ce n'est pas du tout de l'intelligence artificielle. Est-ce que vous ne

pensez pas que les clients vont donc acheter des produits parfois qui n'ont rien à voir avec l'intelligence artificielle alors qu'ils sont vendus comme étant ai ?

ARIANE NAKPOKOU : Oui, c'est absolument exact. Nous finançons l'intelligence artificielle parfois de certaines entreprises et c'est difficile de faire la différence entre ce qui est totalement de l'intelligence artificielle et ce qui est vendu comme étant de l'intelligence artificielle.

Au niveau commercial, je crois on met beaucoup d'efforts sur des solutions en place pour vendre des produits. Il y a des gens qui mentent sur l'aspect intelligence artificielle de certains produits. Et je crois que c'est un problème de concurrence qui va se poser.

LUKAS BUNDONIS : Est-ce que je peux vous rebondir sur cette question ? Est-ce que vous pensez qu'on peut mieux informer les consommateurs de ceci ? N'est-ce pas le travail des entreprises que de faire cela ?

ARIANE NAKPOKOU : La question de la confiance se pose. Définitivement, il faut se poser ces questions et s'assurer d'avoir plus la confiance des consommateurs.

DAVID MARGLIN : David Marglin est États-Unis.

Vous avez des points de vue positifs sur l'intelligence artificielle. Beaucoup de personnes pensent que l'intelligence artificielle et les technologies sont neutres. On dit aussi « Les armes ne tuent pas des gens, ce sont les gens qui tuent d'autre gens. » Est-ce que l'intelligence artificielle, c'est plutôt positif ou plutôt négatif selon vous ? Moi, je suis très inquiet de l'intelligence et l'utilisation de l'intelligence artificielle, ce sera de vendre plus de produits ou être plus néfastes pour les êtres humains comme on l'a peut-être entendu plus tôt dans une autre présentation.

ARIANE NAKPOKOU : C'est comme tout. C'est quelque chose de nouveau, donc on a des inquiétudes, on est anxieux parce qu'on ne connaît pas ce à quoi s'attendre. Mais cela existe déjà, c'est là, c'est présent. Il faut s'assurer tout comme notre internet qui existe également, il faut qu'il y ait beaucoup de directives, il faut que cela aille dans le bon chemin, dans la bonne voie. Et il faut absolument s'assurer – et c'est très difficile à exprimer – de contrôler la situation.

Lorsque j'ai commencé à travailler à Montréal à ces recherches, j'étais vraiment impressionnée par le bien que l'on peut réaliser grâce à cela. Des lunettes que je peux avoir pour toute ma vie. Il y a des solutions extraordinaires pour moi qui peuvent exister dans l'intelligence artificielle, des diagnostiques médicaux beaucoup plus précis. Donc il me semble que ce sont des choix de l'être humain.

Je crois qu'il faut qu'en tant que société, nous fassions des choix informés et que nous tirions profit de ces technologies. Et nous devons

absolument nous assurer que nous mettions des frontières également autour de tous ces concepts.

DEBORAH ESCALERA : Merci beaucoup Ariane. Une dernière question peut-être dans la salle ?

KUSHAGRA BHARGAVA : Bonjour, je m'appelle Kushagra de l'université de Californie du Sud à Los Angeles.

Excellente présentation. Une question très ouverte. Des chercheurs comme nous sommes dans les universités avancent dans leur travail. Lorsque vous nous parlez du droit de savoir, de l'éthique dans le concept même, qu'est-ce que vous pensez ? Est-ce que ces trois concepts vont ensemble, main dans la main ? Est-ce qu'on a toujours ces questions éthiques qui existent avec ce droit de savoir, avec ce respect de la vie privée ou est-ce que cela va dans plusieurs directions ?

ARIANE NAKPOKOU : Je pense le respect de la vie privée, c'est quelque chose de plus facile à réaliser. Je pense que c'est beaucoup plus clair que les questions d'éthique qui se posent. La question qui se pose, c'est que dans un algorithme, vous pouvez faire passer des préjugés. C'est une perception par exemple de ce qu'est une banane. On peut vous dire : « Une banane, c'est une banane. » mais en fait, c'est une question de perception, c'est une image. Je crois que le respect de la vie privée est

absolument essentiel. Vous pensez souvent en termes de consommateurs lorsque vous faites une conception d'algorithme. Sinon, il y a ces questions éthiques qui se posent également et que les entreprises doivent se poser.

KUSHAGRA BHARGAVA : Merci beaucoup, bonne réponse.

DEBORAH ESCALERA : Merci beaucoup Ariane pour votre présentation. Très bien.

Nous allons avoir deux présentateurs, un présentateur et une présentatrice maintenant, à qui nous allons donner la parole.

LILIA HERDEGEN : Est-ce que vous m'entendez ?

Bonjour à tous. Merci d'assister à cette présentation. Je vais vous présenter le monde merveilleux du DNSSEC. Je suis Lilia Herdegen et je vais faire cette présentation avec Austin Bollinger. Je suis à l'université, je fais une maîtrise sur la sécurité informatique.

AUSTIN BOLLINGER : Je suis Austin Bollinger. Nous venons du Michigan tous les deux. J'étudie et je travaille comme analyste de sécurité en ligne.

Nous allons vous présenter une brève histoire et les problèmes et les victoires du DNSSEC. Nous allons commencer par vous dire que tout le

contenu est présenté à des fins éducatives et informatives uniquement.

Il est important de souligner que tout protocole incluant DNSSEC comporte certains risques lorsqu'il est mal configuré.

LILIA HERDEGEN : Nous voulons nous assurer que tout le monde sait que le DNSSEC a été présenté par ICANN et sont utilisation encouragée par l'ICANN durant ces dernières années.

Pourquoi le DNSSEC ? En 1990, Steve Bolovin a parlé de quelque chose qui s'appelait l'empoisonnement du cache du DNS. Et ceux qui travaillent sur le DNS ont proposé une solution qui impliquait la signature cryptographique de requêtes de DNS. Nous avons ici des exemples sur la façon dont fonctionne cet empoisonnement du cache lorsqu'un utilisateur fait une demande et qu'il y a un résolveurs récursif qui est compromis. Donc on a ici deux possibilités : empoisonnement du cache ou un cache propre. L'utilisateur va s'inscrire avec son nom d'utilisateur. Si le site est empoisonné, il va avoir exactement le même aspect que ce qu'il devrait avoir mais cela peut être un site malhonnête qui va récolter les crédentiels. C'est l'empoisonnement du cache.

AUSTIN BOLLINGER : Ici, vous voyez quelques taux d'adoption du DNSSEC. Ce tableau est intéressant parce que nous nous sommes basés sur des informations. Et vous voyez qu'en 2015, il y avait 40 000 domaines signés et il y a une

augmentation importante en 2018, environ 200 000. Cela correspond donc à la signature de domaines avec le DNSSEC et cela est lié au travail de l'ICANN sur le DNSSEC pour résoudre le problème de l'empoisonnement du cache du DNS. Et il y a aussi des choses qui sont liées à cela et qui ont lieu en même temps et dont il faut tenir compte aussi.

LILIA HERDEGEN : Associés à ce taux d'adoption du DNSSEC, nous avons l'amplification du DNC. Cette amplification du DNS a commencé avant 2018 et c'était 66 % des activités de dénis de service. En 2018, il y a eu environ 1 040 % d'augmentation de ces attaques. Et en 2019, pendant le premier trimestre, il y a eu de nouveau une augmentation de 31 %.

Ici, vous voyez un exemple rapide. C'est une comparaison entre ces 66 % comparés à d'autres tendances, les différents flux, les différents types d'attaques.

AUSTIN BOLLINGER : Le DNS peut utiliser TCP ou UDP. Il est important de savoir qu'avec le protocole TCP, on a trois manières de faire la connexion. Avec UDP, on n'a pas vraiment ce qu'on appelle la poignée de main, la communication, la connexion. On ne peut pas savoir si l'adresse est vraiment ce qu'elle est et à ce moment-là, on peut attaquer l'adresse IP et donner lieu à une attaque. Et dans le cas spécifique de cette attaque de réflexion, on a une attaque du DNS. De nouveau, on a des usurpations d'adresses IP qui sont utilisées. Et dans le cas de

l'introduction du DNSSEC, cela permet d'avoir une attaque encore plus importante. Ici, vous le voyez.

LILIA HERDEGEN : Ici, nous avons une attaque d'amplification du DNS. À gauche, vous voyez la personne qui attaque qui va envoyer des milliers de zombies avec des demandes usurpées avec des adresses IP usurpées. Toutes ces adresses IP sont des adresses usurpées qui vont envoyer une requête à une victime qui va être la cible de ces attaques.

Ici, deux ou trois choses de plus concernant l'amplification du DNSSEC. En 2015, [inaudible] a constaté que certains trafics montraient un grand nombre d'attaques utilisant un domaine configuré par DNSSEC. On a demandé une mise en œuvre de la part de l'ICANN du DNSSEC.

AUSTIN BOLLINGER : Ici, avec le graphique que nous avons montré, vous voyez que depuis 2018, une augmentation de 1 000 % des attaques d'amplification du DNS a eu lieu ; 1 000 % des attaques par amplification du DNS ont eu lieu et je pense que cette information est très proche de ce que nous venons de dire. Et lorsqu'il est exploité, le DNS peut amplifier le trafic malveillant de 36 à 72 fois. Et apparemment ici, ces attaques peuvent être beaucoup plus importante. C'est un problème mais en même temps, lorsqu'on rajoute des informations supplémentaires dans ce protocole, cela engendre des attaques plus fortes. Donc c'est la sécurité qui ajoute des problèmes potentiels.

LILIA HERDEGEN : OWASP top dix, voici la liste de OWASP qui veut dire des projets de sécurité ouverts. Ce sont des personnes qui ont travaillé et qui ont fait une liste des dix principales vulnérabilités de risques. Depuis 2017 dans cette liste, pour ces risques, on a la mauvaise configuration de la sécurité et cela va avec le DNS. La configuration du DNS doit être faite et doit être mise entre les mains de sources de confiance et il faut être sûr qu'il n'y ait aucun défaut dans les processus.

AUSTIN BOLLINGER : Revenons à l'année 2013. l'époque, ICANN a recommandé d'atténuer l'amplification du DNS et cela voulait dire désactiver la récursivité sur les serveurs de noms faisant autorité, limiter la récursivité aux clients autorisés et le taux de réponse limite des serveurs de noms récursifs. ICANN a recommandé l'atténuation de l'amplification du DNSSEC déjà à l'époque. Et je pense que c'est important de dire aussi que lorsqu'on recommandait de déployer le DNSSEC, on recommandait ces systèmes pour atténuer les problèmes qui pourraient surgir en cas d'attaques.

Nous avons aussi parlé des pannes du DNSSEC. INX en 2019 est un site web qui répertorie les pannes DNSSEC et les échecs de validation. Educom.edu a contenu une délégation fictive de DNSSEC pendant plus de cinq ans. Il est intéressant. Je pense que les personnes qui ont testé tout cela l'ont dit, et qui ont publié ces enregistrements, c'est intéressant de voir le potentiel qui existe pour les pannes ou les défaillances du DNSSEC. Je serais curieux de voir maintenant

comment est-ce qu'on va maintenir cela et est-ce qu'on peut le maintenir puisqu'on va aouter maintenant quelque chose de nouveau à maintenir dans le futur.

Il est important aussi de souligner que si l'on veut continuer à corriger un site internet qui a des pannes ou des défaillances du DNSSEC, il va falloir avoir un serveur DNS qui va déshabiliter ce DNSSEC. Je crois que ce serait intéressant de voir comment les navigateurs vont maîtriser ou vont pouvoir travailler avec ce type de défaillances.

LILIA HERDEGEN : Les conclusions à tirer de tout cela. Nous avons constaté que si les serveurs DNS sont impliqués et ont des configurations appropriées, une menace minimale est posée, et si le DNSSEC atténue l'empoisonnement du cache du DNS.

AUSTIN BOLLINGER : DNSSEC n'est pas un chiffrement. Il signe des enregistrements DNS pour l'authenticité. Donc le DNSSEC est plus une question d'authenticité et il aide dans ce sens. Et c'est aussi important de savoir que nous avons mis l'accent ici sur le point qu'une configuration par défaut peut vous mettre en risque et peut aider les attaques à avoir lieu.

LILIA HERDEGEN : Voilà, si vous voulez nous contacter, vous avez ici nos coordonnées. Nous avons mis aussi le code QR. Nous sommes à votre disposition. Et

nous voulons saluer nos collègues du Michigan aussi, bonjour à tous. Voilà, nous avons terminé. Merci, merci beaucoup de nous avoir écoutés. Nous remercions aussi l'ICANN pour tout ce qu'ils font pour nous.

AUSTIN BOLLINGER : Nous sommes ravis d'être ici dans ce groupe de NextGen. C'est vraiment quelque chose de passionnant. Nous sommes ravis d'être ici.

Je voudrais aussi dire que le DNSSEC résout certains problèmes. Je ne suis pas contre le DNSSEC, c'est important de le dire. Mais il est aussi important de savoir que quand on dit à quelqu'un que le DNSSEC résout tout, ce n'est pas vraiment le cas. Merci.

DEBORAH ESCALERA : Bravo pour votre présentation. Est-ce qu'il y a des questions ? Nous allons commencer ici.

AKSHAY BROOTA : Je suis Akshay, je suis de l'université du Colorado aux États-Unis.

Bravo pour votre présentation. Le DNSSEC est relativement sûr. Sa sécurité augmente la complexité. Et il y a aussi davantage de problèmes. Que pensez-vous du DNSSEC ? Nous personnellement, nous pensons que le DNSSEC augmente les risques quant au trafic.

AUSTIN BOLLINGER : J'essaie de comprendre un petit peu votre question. Attendez une minute. Je pense que le plus important ici est de ne pas utiliser les configurations par défaut sur le serveur. Je pense qu'une largeur de bande croissante va être importante mais il savoir aussi que les mauvaises utilisations ont permis les abus du sus du DNS. Je pense qu'indirectement, cela risque de causer des préoccupations ou des problèmes parce que tout le monde n'a pas une configuration bloquée, la sécurité peut donc être un défi. Et il faut recommander aux gens d'avoir une certaine authenticité et pas par défaut de façon à ce que la configuration puisse fonctionner. Je crois que c'est le principal problème ici. Est-ce que j'ai répondu à votre question ?

AKSHAY BROOTA : Nous préférons ne pas rendre internet beaucoup plus sûr parce que cela prend davantage de largeur de bande. Est-ce que le DNSSEC sera la seule solution contre les problèmes de sécurité ? Parce que tout le monde n'a peut-être pas la flexibilité permettant de déployer le DNSSEC sur ces réseaux.

AUSTIN BOLLINGER : Je dirais que c'est une question très intéressante. Je pense que c'est un souci concernant le réseau et le fonctionnement du réseau.

Mais en ce qui concerne le DNSSEC, je dirais qu'il se focalise principalement sur la résolution du problème d'empoisonnement du cache par exemple. Le chiffrement du DNS accompagne aussi ce problème. Donc en termes d'augmentation de la largeur de bande

avec le DNSSEC, il y a un système d'expanseurs. Je sais que Firefox par exemple utilise un système avec les services de fournisseur en cloud qui offre une largeur de bande supérieure. Cela peut avoir un sens. Peut-être utiliser CDN pour ce type de trafic serait la solution. Et le DNSSEC avec le chiffrement du trafic du DNSSEC s'utilisent en même temps.

Je pense qu'il faut qu'il y ait davantage de travail là-dessus tous ensemble parce qu'il y a la partie du chiffrement, il y a la partie d'authenticité. Se focaliser tous ensemble de manière groupale serait beaucoup plus utile que de travailler séparément parce que le chiffrement et l'authenticité sont deux choses qui devraient être analysées en même temps.

DEBORAH ESCALERA : Est-ce qu'on peut voir les commentaires en ligne ? « Je vous remercie pour votre présentation. Je n'ai pas de question. Je voulais seulement les féliciter pour leur présentation. »

Est-ce qu'il y a d'autres questions dans la salle ? Oui, allez-y.

ABDEALI SAHERWALA : Est-ce que vous pourriez nous expliquer et expliquer à des personnes comme moi qui ne sont pas techniquement douées qu'est-ce que c'est que le cache et qu'est-ce que l'empoisonnement du cache ?

AUSTIN BOLLINGER : Bien, je dirais que lorsque vous avez un cache... Je vais vous donner un exemple du navigateur et du cache.

Lorsque vous allez sur un site internet, il y a des données qui sont téléchargées et il y a des images, etc. Vous pouvez permettre à votre cache de fonctionner et cela va conserver ces images sur votre navigateur dans votre machine de façon à ne pas être obligé de télécharger ces données à chaque fois.

Le DNS fait la même chose de façon à éviter de faire des requêtes au DNS en permanence sur le réseau. Lorsque vous avez un cache du DNS, ces données vont être conservées et dans le cas de l'empoisonnement du cache du DNS, un attaquant va être entre vous et il va vous offrir des informations incorrectes.

C'est comme une attaque avec l'homme du milieu. Lorsqu'un individu se trouve entre l'utilisateur et le cache, il injecte des adresses malhonnêtes et vous aurez des informations du cache qui seront des informations erronées et vous allez avoir une attaque comme l'attaque avec l'homme du milieu. Donc vous allez recevoir des informations incorrectes et le serveur va vous envoyer des informations incorrectes.

ABDEALI SAHERWALA : Tout cela se fait à travers le système ?

AUSTIN BOLLINGER : Oui.

JOAO PEDRE MARTINS : Pour revenir un petit peu sur ce que vous avez dit à propos de cette discussion, vous avez dit qu'il y a des exigences de sécurité importantes. Est-ce qu'à ce propos, vous pensez qu'il faut formuler un nouveau protocole qui implémenterait ces deux systèmes, ce qui va impliquer beaucoup de nouvelles conceptions, de nouvelles recherches ? Ou bien est-ce que vous proposez que le fait de combiner les outils existants ou les protocoles existants serait plus efficace pour être prêts en termes de continuité et en termes de lutte contre ce type de problèmes ? Merci.

AUSTIN BOLLINGER : Je pense que c'est la meilleure question qu'on m'a posée depuis le début ; merci beaucoup donc.

Ensuite, je dirais que lors de la réunion du SSAC, on a parlé des contraintes de sécurité au sein de l'ICANN et on doit introduire des chaînes de technologies de chaîne de blocs pour protéger le DNS.

Je pense que la décentralisation du système de domaines est quelque chose de très dangereux, surtout quand on parle de l'ICANN. L'ICANN est centralisée dans la façon dont les domaines sont gérés. À mon avis, ce qu'il faudrait faire pour introduire une certaine authenticité, ce serait d'aider les chaînes de bloc à gérer cela. On ne se focalise pas sur une zone racine spécifique. Parce que par exemple s'il y a une guerre, un pays va dire : « Je risque de mettre la main sur une série de

domaines. » Donc dans le futur, il faut faire attention parce que c'est quelque chose très puissant.

Et en termes de nouveaux protocoles, je pense qu'on a mis 20 ans pour arriver là où nous en sommes actuellement. Les changements du protocole internet demandent beaucoup de temps et c'est en même temps très lent mais en même temps, cela change en permanence. Donc je ne sais pas comment répondre à votre question mais je pense que les choses continuent de changer en permanence depuis 20 ans.

DEBORAH ESCALERA : Est-ce qu'il y a d'autres questions ? Bien. Merci beaucoup pour votre présentation.

Nous avons terminé pour aujourd'hui. Je vais remercier nos présentateurs qui étaient très bien préparés. Ils étaient un peu nerveux aussi mais bravo, c'était très bien, vous avez fait du bon travail. Je remercie les ambassadeurs qui sont venus nous soutenir.

Il va y avoir de nouveau demain des présentations. On va commencer à 15:15 dans la salle 512G. Donc on vous attend demain. Merci d'avoir assisté à ces présentations aujourd'hui.

**[FIN DE LA TRANSCRIPTION]**