COPENHAGUE – Discussion intercommunautaire avec les commissaires à la protection de données
Lundi 13 mars 2017 – 15h15 à 16h45 CET
ICANN58 | Copenhague, Danemark

NIGEL HICKSON: Messieurs dames, nous allons démarrer cette séance dans quelques instants. Je voudrais vous demander de vous approcher du podium.

Veuillez vous rapprocher pour nous accompagner de plus près merci.

JAMES BLADEL: Bonjour, nous vous demandons de prendre vos places comme Nigel l'a mentionné tout à l'heure. Rapprochez-vous. La salle est un peu grande pour notre audience, mais veuillez vous rapprocher de nous. Nous allons commencer dans environ 100 secondes.

Bonjour encore une fois, bon après-midi. Bienvenus à cette séance intercommunautaire. La question qui nous occupe, c'est la confidentialité des données. Et ceci a été réalisé par le comité gouvernemental. On a des experts du conseil de l'Europe, et la représentation de la communauté.

Nous accueillons nos collègues qui viennent d'arriver à Copenhague.

La question de la confidentialité des données affecte tous les acteurs, les gouvernements, les bureaux d'enregistrement, les opérateurs de registre et les titulaires de noms de domaine, on est des titulaires par million.

Alors, presque tous les aspects de la confidentialité ont des impacts, sont un défi pour l'activité de l'ICANN.

À la GNSO, nous travaillons dans les questions relatives aux politiques et nous analysons les systèmes de données, d'enregistrement de données. Nous espérons bien que cette séance vous informera de ce travail.

Nous allons donc commencer à partir d'aujourd'hui la collaboration continue et le dialogue avec toutes les organisations.

Ceci dit, nous allons commencer avec une séance j'espère intéressante.

Cette fois-ci, je souhaite la bienvenue à Johannes Kleijssen, directeur de la société de l'information contre le crime du conseil de l'Europe.

JOHANNES KLEIJSSEN: Merci monsieur le président, bonjour à tous. Je suis heureux et très reconnaissant à la GNSO, au GAc et au conseil d'administration de nous avoir accueillis aujourd'hui et d'avoir soutenu la proposition du conseil de l'Europe pour cette discussion intercommunautaire.

Nous allons vous raconter ce qu'est le Conseil de l'Europe et qui nous sommes.

On est constitué par 47 états, 5 observateurs dans plusieurs pays. On s'occupe du droit, de la loi, du respect de la loi. Et la société civile a travaillé avec nous pendant les 30 dernières années.

On a une plateforme pour la collaboration avec la société commerciale qui a d'ores et déjà un statut formel.

Le conseil de l'Europe travaille au niveau intergouvernemental et il devient de plus en plus un organisme multipartite. Pas comme celui que nous trouvons ici à l'ICANN.

J'ai entendu plusieurs parmi vous, vous m'avez sans doute entendu parler à Strasbourg lors de la convention sur les droits de l'homme. Nous avons défendu les droits de l'homme, mais nous voulons également assurer qu'il y ait des représentants de l'application de la loi. On a des conventions internationales qui s'occupent du droit pénal, et nous voulons travailler ensemble.

Nous avons un observateur au GAC depuis 2010, et jusqu'à présent, nous avons présenté 3 rapports pour discussions.

Un de ces rapports est en cours de débats pendant cette semaine.

Dans la séance d'aujourd'hui, on a donné beaucoup d'importance à la convention 108, la convention de protection des données qui réunit 50 états qui ont ratifié la convention. Et nous avons également 60 pays qui ont présenté la moitié des états mondiaux qui ont une protection de données.

Ceci va bien au-delà de l'Europe bien entendu.

La contrepartie de cette convention est la convention sur le cyber-délit, connue comme la convention de Budapest, Jusqu'à présent, le seul instrument international dans ce domaine qui a également 50 états participants, y compris les États-Unis et la France.

Nous travaillons avec 125 pays du monde entier sur le renforcement des capacités.

Pour l'événement d'aujourd'hui, nous espérons que cette discussion ne soit que le début d'un processus et pas un évènement unique.

Nous sommes persuadés qu'il s'agit de quelque chose qui est fait à temps, et il faut discuter de la question en ce moment. Et nous espérons bien que tous les sceptiques seront convaincus à la fin de cette séance, une fois que vous aurez entendu les speechs des commissaires de protection des droits.

Il y a de plus en plus de conflits légaux des parties contractantes par rapport à leurs obligations, et le droit international et l'ICANN. Ceci s'applique aussi à l'ICANN, et nous espérons que cette discussion ne sera que le début d'un processus qui pourra nous amener à des solutions multipartites.

Merci.

BECKY BURR: Bonjour. Vous savez que je suis divisée entre l'ICANN et la loi et la politique. Bien des fois, l'ICANN, ces choses entrent en collision, mais avant d'occuper mon poste au conseil, j'ai dû m'occuper de chacune des révisions du WHOIS.

Et me voilà maintenant ici.

Et je crois que vous, vous avez dit que nous avons besoin des autorités de protection de la loi. Des autorités de protection de données pour qu'elles nous accompagnent.

Je suis très reconnaissante du sponsoring du conseil de l'Europe et des autorités de la protection de données qui partagent ce dialogue avec nous.

Vous avez entendu qu'il ne va pas s'agir d'une conversation d'une seule voix, mais on a l'intention que cela devienne un dialogue ouvert, inclusif et continu.

Je vais présenter les membres du panel. J'ai d'abord des questions à poser, puis après un espace questions réponses dans la salle.

Tout d'abord, je vais mentionner quelqu'un qui est dans le panel, qui n'a pas de présentation, c'est un des sponsors : Monsieur Thomas Schneider, président du GAC et le vice président du service des affaires internationales et coordinateur de la société de l'information internationale en Suisse. J'ai dû lire tout cela parce que c'est franchement long.

Thomas nous accompagne aujourd'hui, et il va commencer avec les questions.

Il y a aussi Giovanni Buttarelli, superviseur de la protection des données qui a été désigné dans ce poste par parlement et le conseil de l'Europe pour une période de 5 ans en 2014. Il a travaillé auparavant dans ce bureau, et avant ça il a été secrétaire général de l'autorité de protection des données

italiennes depuis 97, c'est-à-dire presque dès le début de ce genre d'activité.

Willbert Tomesen, vice-président également du groupe de travail de l'article 29. Et il m'a fait rappeler aujourd'hui que l'article 29 c'est contacter avec l'ICANN en 2004, et à partir de là, on s'est communiqué régulièrement.

Joe Cannataci est le rapporteur spécial de l'ONU pour les questions relatives à la privacité. Il a étudié à l'université de Maltes et il appartient au groupe de la technologie de la faculté de droit à l'université de Birmingham. J'espère avoir bien prononcé ce mot anglais. Et il est professeur adjoint à une université en Australie.

Mais vous, les technologies [inaudible] qui attendent une discussion de politique continue, vous verrez qu'il est professeur à une université du Royaume-Uni et il travaille aussi à une société d'ordinateurs britannique.

Caroline Goemans-Dony, qui vient d'Interpol. Elle s'occupe du monitoring des processus, elle travaille avec 190 fonctionnaires qui travaillent dans la protection des données et qui sont désignés chacun des bureaux centraux de l'Interpol.

Puis Caroline et Gail qui sont à côté. Gail est le président des activités de règlementation de l'Internet Sociéty. Elle a

commencé sa carrière très près de mon cœur. Avant ça, elle a dédié plus d'une décennie à la commission fédérale du commerce des États-Unis et elle travaille avec adjoint. Il y a des experts de ce panel qui doivent se rappeler de Julie qui a travaillé avec l'autorité de la protection de données.

Je veux adresser quelques mots à [inaudible] qui vient de l'Irlande, qui a obtenu son master en droit européen.

Et finalement James Galvin, quelqu'un que tout le monde connait. Il appartient au comité consultatif sur la sécurité de l'ICANN depuis le début. Il a participé très activement dans l'IETF pendant plus de 20 ans. Il est le directeur des directions stratégiques et normes technologiques à Afilias.

Il y a un excellent panel qui nous accompagne. Nous savons qu'il y a beaucoup d'intérêts d'entendre parler de ce type de questions.

Je vais faire des questions d'introduction et je vais tout d'abord passer la parole à Giovanni Buttarelli.

Giovanni, pouvez-vous nous raconter les principes fondamentaux de la confidentialité qui sont à la base des lois de protection de données, y compris mais sans s'y limiter, les règlementations de protection de données qui vont apparaitre prochainement ?

GIOVANNI BUTTARELLI: Merci Becky de la présentation. Mon rôle est celui d'agir comme le premier orateur, et je voudrais vous dire que les principes que je vais mentionner n'appartiennent pas seulement à l'Union Européenne, ou des principes seulement contenus dans la convention du Conseil de l'Europe numéro 108. Parce que la protection des données devient de plus en plus globale.

Nous avons commencé à identifier 120 pays du monde qui ont des lois modernes de confidentialité des données. Et ils s'éloignent d'un système d'autoréglementation. Et malgré que certains principes sont mentionnés différemment, comme par exemple un principe spécifique. Il y a beaucoup de similitudes. Et on travaille dans le monde entier de manière de plus en plus poussée.

Je voudrais vous demander de ne pas penser que la protection des données est simplement une charge administrative en ce qui concernant la gouvernance de l'internet. Je veux dire, on fera une perspective générale, un aperçu général.

Et je dois dire qu'en 2014 on a publié le site web de mon institution et cela concerne le rôle européen de la gouvernance de l'internet en termes de valeurs démocratiques, en termes des relations avec les multiples parties prenantes pour la structure de la gouvernance, et aussi en ce lié aux besoins de publier ou

de promouvoir un réseau unique et non fragmenté dans le monde entier.

La confidentialité est considérée dans le monde entier comme un droit fondamental. Tandis que la protection des données a commencé à être considérée comme telle en Europe et dans certains autres pays.

Mais en fait, la protection concerne les données et la confidentialité. Ceci est considéré dans le monde entier comme un pré requis pour bénéficier d'autres droits fondamentaux, en faveur d'autres droits fondamentaux, y compris la liberté d'expression, le droit à l'identité personnelle et, plus récemment, à la dignité.

Alors mon institution va recevoir l'année prochaine la commission internationale sur la privacité et la protection des données pour se cibler sur l'éthique et sur les nouvelles technologies.

Il y a aussi les questions de la transparence qui concernent la clarté de qui fait quoi. Voilà donc pourquoi les nouvelles définitions adoptées récemment. Par exemple, en Europe, le rôle d'un contrôleur, d'une personne qui s'occupe de processus, ce sont des questions clefs pour identifier un cadre approprié en terme de responsabilité ou reddition de compte.

La légalité et la justice doivent être également mentionnées. La légalité veut dire non seulement avoir des fondements juridiques pour traiter les données, il doit y avoir une relation contractuelle, un intérêt légitime, une relation de collaboration, un intérêt vital du contrôleur pour une tierce partie. Mais il faut qu'il y ait aussi de la cohérence et du respect d'autres législations qui ne sont pas liées à la protection de données, comme les droits d'auteur, et le droit qui protège les consommateurs.

La privacité est incluse dans les nouveaux principes de l'Europe et ces principes doivent être respectés.

Le cadre régional récent de l'Union Européenne vise à renforcer les pouvoirs ou les facultés de supervision des autorités compétentes et vise à moderniser les cadres de protection de données avec une approche plus cohérente pour que les contrôleurs ne fragmentent pas leur politique en fonction du territoire.

Nous voulons avoir des contrôleurs plus responsables, c'est-à-dire que les autorités de protection de données soient plus sélectives, que les contrôleurs doivent mieux faire leur devoir. Et l'identification d'une politique durable. On parle aussi d'identifier les risques spécifiques vis-à-vis des responsabilités, démontrer que l'on respecte la politique.

Ce cadre est applicable aux individus, mais pas à toutes les personnes. Et les grandes données sont très importantes ici.

Il faut également voir quel est l'impact de ce cadre juridique dans toutes les données personnelles liées aux individus qui agissent en représentation, d'une société par exemple, ou d'une administration publique.

Je vais revenir sur les limitations, mais je veux dire que 13 ans après la réunion de l'ICANN à Rome, nous voudrions pouvoir revenir à la question que nous avons posée en 2003. À ce moment-là, on a posé trois questions à la communauté.

Premièrement, pourquoi un registre de noms de domaine sur internet doit être traité différemment à un référentiel de télécommunication lorsque l'on enregistre un nom de domaine. C'est-à-dire le droit à ne pas être inclus dans un registre.

Une deuxième question, c'est la suivante : comment ce principe se traduit dans la pratique ? Et la question est, existe-t-il une autre méthode moins intrusive, si on la compare à la publication obligatoire, qui ait le même objectif que le WHOIS, sans que toutes les données soient disponibles en ligne pour n'importe qui ?

La dernière et troisième question est liée à l'accès en masse au marketing direct.

Nous voulons donner une suggestion pour ce qui est de l'accès par des tiers. Et nous supposons il y a 13 ans, et la conclusion est toujours valide à mon avis, et je cite : « l'objectif du WHOIS ne peut pas être étendu à d'autres objectifs, parce qu'il est considéré souhaitable par des utilisateurs potentiels de ces référentiels. » Un exemple qui peut aider à l'identification de ces objectifs, et bien si nous voulions que ces principes soient vraiment effectifs dans la pratique.

Ce n'est pas l'Union européenne contre les États-Unis. On a une dimension globale pour renforcer la confiance sur l'internet. Nous, on est suffisamment flexibles pour faire en sorte que ce principe soit efficace dans la pratique.

Et nous prendrons des sauvegardes. Nous adopterons des sauvegardes parce qu'on est tous du même côté.

BECKY BURR: Je voulais vous demander de parler davantage sur la responsabilité, car c'est très important pour nous.

WILBERT TOMESEN: Je vais sans doute superposer certains points avec Giovanni, mais je veux avouer que j'ai été pendant pas mal d'années, pendant 25 ans, j'ai été superviseur de la protection des données. Et quand on fait ce travail on pense qu'on a tout vu,

qu'on connait tout. Mais bien des fois j'avoue que je suis étonné des dimensions et de l'atmosphère de cette réunion.

Et je tiens à vous remercier de m'avoir invité à y participer. Il s'agit d'une réunion très importante.

Pendant pas mal d'années, on a suivi de très près les débats liés à l'ICANN. Par exemple on a parlé de la disponibilité publique des données du WHOIS, j'ai participé de ces débats, savoir les conséquences, les implications du WHOIS.

Et ceci nous fait réunir en personnes et participer de débats après nos présentations.

Les Européens ont l'attente légitime que leurs données personnelles ne soient prêtées qu'à des propos légitimes. Et sans une autre finalité. Cela veut dire que toutes les données personnelles seront traitées dans un processus juste légal et transparent. Et ce sont les principes de base établis dans notre directive et dans la loi européenne.

Ce qui veut dire que nous devrions contrôler et demander aux contrôleurs de donner, des informations à des buts spécifiques, par la voie de processus et de modalités compatibles avec les processus et les principes établis, c'est-à-dire ce que l'on appelle la limitation de l'objectif.

Et deuxièmement, nous avons un principe qui dit que les données traitées doivent être appropriées pour l'objectif visé. Et c'est ce que l'on appelle la minimisation des données.

Le processus doit être prévisible, juste et transparent, comme mon collègue vient de le dire, dans un contexte qui nous permette de minimiser la minimisation.

On peut lire dans certains documents, comme par exemple les documents de Tim Berners-Lee que l'on perd le contrôle des données personnelles. Et à mon avis, nous sommes occupés de la supervision de ces données et d'être juste, transparent et prédictible dans le travail relatif aux données, selon ce que la loi a établi.

Ce sont des principes généraux, non négociables.

Je voudrais dire également que pour ce qui est de la disponibilité publique des données du WHOIS, il faudrait penser aux principes de la limitation des objectifs.

Vous savez que l'objectif du WHOIS c'est de mettre à disposition les données de contact. Alors le WHOIS a été repensé pour l'accès public, pour les agences de du respect de la loi ou ceux qui travaillent sur la sécurité.

C'est-à-dire, on utilise des données à des buts légitimes parce qu'il s'agit d'un objectif utile, comme on l'a mentionné. Et pour

que vous puissiez avoir ces données personnelles publiées, il est nécessaire qu'il existe un processus de publication qui protège la privacité et les intérêts de privacité et de confidentialité des utilisateurs.

Nous avons reçu différentes réclamations sur la disponibilité publique des données de contact et des données personnelles, qui s'expriment à travers le WHOIS. Ces données sont publiées dans de nombreux sites web et sont disponibles pour n'importe qui, pour n'importe quoi, que ce soit quelque chose de légal ou non.

Voilà mon premier commentaire, mais je voudrais ajouter quelque chose.

L'objectif principal des nouvelles règlementations, comme je viens de le dire, est d'avoir un processus transparent, juste et prévisible pour le traitement des données personnelles partout dans le monde.

Cela veut dire que pour être responsables face à vous, nous devons pouvoir démontrer notre respect des DPA à travers les exigences légales.

Une fois de plus, il faut faire le traitement de données et tenir compte de la limitation des données. Et sans aucun doute, nous allons être évalués par chacun des pays et par chaque DPA de

l'Union Européenne. Et les DPA ont exercé leur pouvoir dans ce sens, sans aucun doute.

En même temps, je voudrais dire que je suis convaincu qu'il y a des organisations qui tiennent compte de ces principes fondamentaux, de ces règles avec des principes fondamentaux. Et on essaie de mettre en œuvre ces règles, gagner la confiance et le respect des consommateurs.

BECKY BURR: Merci, je passe maintenant la parole à Joseph Cannataci. Pourriez-vous parler de l'accès des tiers aux données ? C'est une question très importante pour cette organisation, dans le contexte du WHOIS et aussi dans le contexte de certaines questions relatives aux données.

JOSEPH CANNATACI: Je veux remercier les organisateurs du fait d'avoir mis sur la table ce sujet.

Je crois que ce serait mieux de commencer en parlant de certaines questions mentionnées par Giovanni Buttarelli et d'autres collègues.

Lorsque nous parlons de l'accès de la part des tiers, il faut tenir compte de la manière dont les lois de confidentialité et de

protection de droits sont appliquées et d'où elles viennent. En réalité, elles sont issues des États-Unis vers les années 67 et 73, et plus tard en Europe.

Elles ont été créées de la manière suivante. Si on va donner des données pour un objectif en particulier, il faut s'assurer que ce soit pour cet objectif ou compatible avec cet objectif initial. Alors si quelqu'un utilise mes données dans un contexte bancaire pour avoir un prêt ou une hypothèque, on va utiliser ces données pour ces objectifs en particulier. Il peut y avoir aussi une politique d'assurance, mais il ne va pas y avoir d'objectifs au-delà.

Si l'on parle de l'accès par des tiers, il faut tenir compte que l'on est dans un contexte où il faut débattre de la question.

Deuxièmement, je crois que l'on peut voir la manière dont tout a changé. Alors si je reviens 30 ans en arrière, quand on a démarré tous ces débats pour protéger les données de la police – ici vous avez Caroline qui travaille aussi avec la protection de données à Interpol – et bien on applique les mêmes principes. Mais il faut tenir compte également des premières recommandations et règlementations émises par le conseil de l'Europe.

Tout cela a été construit sur la base que le contrôleur de données allait s'occuper de recueillir ces données et que les forces de la police allaient conserver ces données. Par exemple,

les fournisseurs de services de santé allaient aussi disposer de cette information.

Mais aujourd'hui, il y a une réalité. À savoir une distance considérable entre la police, ou un fournisseur de services de santé ou un fournisseur de produits pharmaceutiques. Pas nécessairement pour l'obtention de données, mais que cela dépend des données obtenues par d'autres personnes.

Il y a des données qui sont collectées par des sociétés privées. Et bien des fois, les citoyens ne sont pas au courant de tout cela. Cela est particulièrement important dans une série de contextes.

Pourquoi ? Parce que si l'on demande à une série de sociétés qui participent de l'internet, on doit leur dire qu'ils ont des centaines ou des milliers de demandes de données, des métadonnées ou des données de contenu. Et ceci ne doit pas forcement être dans un contexte de renseignement ou d'application de la loi.

Bien des fois, il y a une société qui peut recevoir 17 000 demandes. Il y a beaucoup de pressions, non seulement au niveau de la compagnie, mais aussi en relation avec les systèmes juridiques. Et on n'a pas le temps d'aborder toute cette problématique. S'il y avait un [inaudible] par exemple, on pourrait entamer une procédure légale et cela pourrait donner

lieu à des procédures de 11 à 13 mois pour pouvoir accéder aux données.

Alors l'accès des tierces parties est de plus en plus en plus complexe, c'est une question de plus en plus complexe du fait qu'il y a une série de gouvernements, y compris les gouvernements européens, les États-Unis, et le gouvernement de l'Australie, de la Nouvelle-Zélande, un grand nombre de gouvernements qui ont déclaré que quelque chose de sacré, comme par exemple la vierge, ou le principe des données ouvertes.

Il y a 30 ans, ce n'était pas le cas. Il fallait penser à une mesure de protection. Et on continue d'avancer.

Alors, lorsqu'on a demandé des analyses pour faire la triangulation, on arrive à des données ouvertes, et bien des fois, on arrive à un point et on dit : ha bon ? L'objectif des données, cet objectif d'avoir des données ouvertes de grandes données, implique que l'on donne à des tiers un accès qui va leur permettre, c'est-à-dire qui va découler dans une transformation de la politique publique. Ceci est très important pour les tiers, et c'est très important pour l'environnement de l'ICANN.

Parce que dans l'environnement de l'ICANN, bien que l'ICANN utilise ou aide à donner une meilleure infrastructure technologique, l'ICANN aide aux gens à se connecter entre eux et

doit également faciliter la manière de mettre en place certaines décisions en matière de politique.

Alors en ce sens, il faut tenir compte de ce que je viens de mentionner.

En ce qui concerne l'accès des tiers, il faut également se rappeler du contexte de l'infrastructure légale et des politiques que tous les états mettent en place et que Giovanni a mentionnées.

On a beaucoup d'états qui ont suivi le modèle européen et les principes européens. C'est-à-dire que lorsqu'ils abandonnent les principes et qu'ils fournissent l'accès à ces principes, l'accès des tiers ne peut être octroyé comme règle. Si c'est à un but spécifique, c'est-à-dire pour protéger la sécurité des états, pour la sécurité publique, pour les intérêts monétaires de l'état, pour la défense contre les offenses pénales.

Donc au moment de le faire, ça doit être fait dans un contexte juridique, où il y a une loi. C'est la loi qui doit soutenir ce type de décision et fournir des sauvegardes appropriées.

Donc quelles que soient les discussions qui surgissent de cette salle et du processus que j'espère que l'ICANN va tenir avec les personnes qui sont assises autour de la table et en dehors de la salle, ça va se faire suivant ce même esprit.

Sachant donc qu'il faut savoir ce à quoi les personnes s'attendent, quelles sont leurs attentes. Et les personnes s'attendent à avoir des remèdes. Les sociétés veulent pouvoir faire leurs affaires partout dans le monde, et les citoyens espèrent voir leurs données personnelles protégées partout dans le monde à travers des sauvegardes qui, comme j'aime bien répéter, leur permettent d'opérer et de servir sur un internet sans frontière.

C'est-à-dire que les sauvegardes ne doivent pas non plus connaitre de frontière.

Donc j'espère que l'ICANN pourra contribuer à l'identification de ces remèdes et à l'identification des sauvegardes qui pourraient être des sauvegardes techniques ou de politique, ou des sauvegardes juridiques, et quand il serait approprié d'avoir une combinaison de tout cela. Merci.

BECKY BURR: Merci, je pense qu'ici on a tendance à penser plutôt aux forces de l'ordre et à l'application de la loi comme une partie du débat, et d'autre part, les défenseurs des politiques comme l'autre part à ce débat.

Mais j'apprécie le fait que le titre de Johannes est directeur de la société de l'information et des actions contre les délits du conseil de l'Europe.

On a ici également avec nous Caroline Goemans-Dorny, qui est fonctionnaire de protection de données chez Interpol, et je voudrais savoir un peu plus comment elle travaille dans le cadre de l'application de la loi sur ces sujets.

CAROLINE GOEMANS-DORNY: Merci de cette question et merci de m'avoir invitée à ce panel qui est fort intéressant.

Vous saurez peut-être qu'Interpol est l'organisation de police internationale qui couvre 190 pays membres, et qui agit comme centre d'information internationale auprès des bases de données des polices. C'est-à-dire que l'on traite beaucoup d'informations.

À vrai dire, franchement, l'Interpol n'existerait peut-être plus si elle n'avait pas investi des efforts et des fonds pour mettre dans la pratique les principes confidentialité de données depuis 1982.

Donc ça me ramène à la base, parce qu'il faut que je vous explique les fondements pour lesquels nous avons mis en place ces principes. Et bien pour que la coopération policière soit efficace, il nous faut de la confiance, il nous faut une certaine

réputation, et il nous faut surtout combler les fossés, surtout lorsqu'on travaille dans un environnement mondial.

Lorsqu'on veut appliquer des principes dans le cadre des normes et des standards de protection de données, il nous faut de l'aide. L'Interpol a mis en place un cadre sous-jacent à travers lequel les forces de police peuvent coopérer de manière efficace du point de vue technique et opérationnel.

Ça prend du temps que de construire ces fondements solides. Et donc notre investissement a été à long terme et notre croissance à la protection de données au long terme a montré le fait que l'Interpol réfléchit à ces questions depuis très longtemps. Ce n'est pas par accident que les premières règles de l'Interpol sur la protection de données datent de 1982. Cette date suit de près l'adoption de la convention 108 du conseil de l'Europe.

Par la suite, au long des années, les principes ont été développés de plus en plus. Et ce de manière détaillée, à travers 136 dispositions. Et nous comptons 11 mises à jour depuis 1982. C'est-à-dire qu'on a vu des mises à jour des normes de protection de données, une tous les 3 ans à peu près.

Le processus de protection de données est dynamique, et l'aide, et les normes ne sont utiles qui s'ils sont dynamiques, s'ils sont souples. Donc je pense que pour Interpol c'est vraiment utile

d'avoir des règles souples qui nous permettent de les adapter à nos buts.

Bien sûr, c'est toujours un défi de le faire. Notre dernière mise à jour des règles était en 2016, en novembre. Et le rôle de l'organe de supervision du comité de pilotage a été renforcé à travers cette mise à jour. Et on pense déjà à la prochaine mise à niveau des règles, surtout en pensant aux sociétés privées.

Il y a beaucoup d'évolutions dans ce cadre, et notre cadre devrait être adapté à cette évolution que nous avons connue.

Cela m'amène au point de la réputation dont je parlais tout à l'heure. Ce n'est pas tout simplement une question de droits à la vie privée, mais plutôt tous les droits fondamentaux sont impliqués. Le droit de police efficace, le droit à la liberté d'expression et la constitution de l'Interpol évoquent exprès la Déclaration universelle des droits de l'homme, le principe de la neutralité comme principe organisationnel, c'est-à-dire que l'organisation ne peut pas interférer dans des questions religieuses, militaires, ou politiques, ou ethniques encore. Tout cela est reflété dans les normes de traitement de notre organisation.

Et dans ce sens, une valeur de l'Interpol est de pouvoir agir comme centre d'échanges. On a une équipe interdisciplinaire d'analystes, d'avocats, d'officiers de police, des personnes qui

travaillent 24 heures sur 24 pour traiter les plus de 3 000 demandes mensuelles que nous recevons des pays qui adhèrent à la corporation de l'Interpol pour chercher des personnes ou pour les faire arrêter.

Nos règles se fondent sur l'égalité, la légalité et la qualité et tout se fait manuellement. On utilise aussi des outils automatiques, bien sûr, pour déclencher des recherches de certains mots, et on a des critères spécifiques et des seuils spécifiques pour nous mettre au travail.

Notre centre d'échanges constitue donc un rôle important d'informations et nous permet d'avoir une coopération policière plus efficace.

Finalement, je parlais des principes de confidentialité et de vie privée mondiaux, et c'est ça la différence, je pense, qui nous permet de pouvoir combler les lacunes entre les législations, les processus commerciaux, et de créer une interopérabilité qui nous permet de fonctionner, non seulement au niveau technique.

Nos normes se fondent sur des normes de mise en œuvre. C'est très bien d'avoir des normes, mais elles ne servent à rien si on n'a pas de mise en œuvre efficace. Il faut les faire appliquer pour qu'elles soient utiles. Les normes de l'Interpol ont été adoptées par 190 pays membres, et tout le monde y est inclus.

La coopération à travers Interpol est volontaire, mais une fois que vous avez choisi de coopérer, les règles sont contraignantes, il y a des sanctions qui peuvent être imposées au cas où cela n'était pas le cas. Il y a des mesures de correction aussi. Et si on y réfléchi, les principes de confidentialité et les principes de protection de données qui en découlent sont des principes de bonne gouvernance.

Pourquoi intenter des procès contre une personne ? Il faut voir d'abord quel est le processus, quelle est la légitimité d'un procès, comment on peut se conformer à la loi. On a des principes de bonne gouvernance et les organisations commerciales qui respectent correctement les principes de gouvernance ont de bonnes sociétés, font de bonnes affaires.

Je pense que c'est ça l'essentiel.

Ces normes ne peuvent pas nous contraindre tout simplement selon les normes juridiques. Au moment d'appliquer des principes de vie privée et de confidentialité. Il s'agit de principes, de règlementations, de politique, des principes commerciaux, de technologies. Donc il faut apporter tous les défis que nous avons devant nous.

Finalement, il y a une autre composante qui est celle de l'éthique. La règlementation dit ce que l'on peut faire et ce que l'on ne peut pas faire, alors que l'éthique dicte ce que l'on

devrait ou ne devrait pas faire. C'est ça qui est important sur internet aussi. Merci.

BECKY BURR: Merci Caroline. Thomas, le GAC a participé à ces discussions et à ces dialogues. Et je voudrais savoir quel est votre avis concernant l'esprit du GAC devant cette nouvelle étape de dialogues.

THOMAS SCHNEIDER: Merci Becky et bienvenue à tous.

Avant tout, on devrait remercier le conseil de l'Europe d'avoir pris cette initiative que nous soutenons pleinement et que nous célébrons.

Il nous semble qu'il est opportun et pertinent de tenir cette discussion ici et maintenant à Copenhague. Parce que, comme tout le monde, nous savons de plus en plus que la protection de la confidentialité des données et la protection de la vie privée en général va au-delà des questions clefs de la loi. C'est important pour les citoyens, pour les sociétés, pour les gouvernements, pour les institutions, et les institutions internationales, comme l'ICANN, qui ont des fonctions qui ne sont pas nécessairement liées à la vie privée dans leur travail quotidien, mais qui doivent s'en occuper.

De nos jours tout le monde travaille avec des données. Donc on s'implique tous dans ce travail.

L'utilisation de données devient la ressource clef pour l'innovation économique et pour l'innovation en général. Il s'agit d'un outil qui nous permet de vivre de manière plus aisée, plus sécurisée et cela a beaucoup de potentiel pour l'innovation ;

En même temps, il y a beaucoup de risques d'abus et d'utilisation malveillante des données. Face à cette nouvelle continuité d'utilisation de données. Les personnes sentent qu'elles perdent le contrôle de leurs données.

Donc il y a des défis clefs auxquels il faut que l'on fasse face. L'un des défis qu'on se demande, non pas seulement en tant que gouvernement, mais en tant que personnes et en tant que société, c'est par rapport au fait qu'on a différentes juridictions, différentes législations, différentes règlementations. Et puis aussi au sein d'un même pays, on a différentes parties du gouvernement qui ont différentes fonctions. Il y en a qui sont censés protéger les droits de l'homme et du citoyen, alors que d'autres secteurs sont sensés faire la persécution des délinquants, et très souvent, les sociétés privées, et les compagnies en général se voient coincées entre ces différents secteurs d'administration au niveau global et au niveau national.

Très souvent on se trouve avec des attentes en conflit au sein des compagnies, par rapport à ceux qu'ils attendent des gouvernements et des demandes qu'ils ont au niveau de privacité et de service. Les consommateurs veulent voir leurs données protégées, leurs données confidentielles, mais ils veulent également des services pour pouvoir faire parvenir leurs données à l'autre bout du monde.

Donc on propose ces services sans savoir particulièrement comment faire face aux défis que nous avons devant nous.

Lorsque Johannes disait que le Conseil de l'Europe devient une institution multipartite, je dirais qu'on pourrait le confirmer après avoir représenté mon pays au sein du conseil de l'Europe pendant une décennie. On comprend des sociétés, la société civile, d'autres experts. Et moi par exemple, j'ai fait partie d'un groupe de travail d'experts qui a travaillé sur l'élaboration de lignes directrices sur les droits de l'homme pour les FSI, pour qu'ils les incorporent à leurs principes, et ce en coopération avec les FSI, avec la société civile et avec les experts en matière de droits de l'homme.

Au cours de nos travaux, on s'est rendu compte qu'au sein d'une même institution, le secteur qui travaillait sur le cyber-délit travaillait sur des lignes directrices pour faire appliquer la loi au sein des FSI. Et ça nous a pris un moment de nous rendre

compte que l'on travaillait de manière isolée. Une fois que l'on s'en est rendu compte, on a commencé à communiquer pour essayer de faire en sorte que ces lignes directrices pour les FSI en Europe soient conformes entre elles. Et il a fallu que l'on élimine certains des points qui posaient conflits avant de les publier.

Mais cela représente un exemple de l'importance de travailler en coopération et non pas de manière isolée.

Je pense qu'ici, c'est la première fois à laquelle les commissaires de protections de données communiquent avec d'autres industries, et avec l'industrie des noms de domaine.

Nous applaudissons donc le fait que ce dialogue ait été établi au sein de l'industrie des noms de domaine de partout dans le monde.

L'ICANN peut également apprendre beaucoup de la règlementation de la confidentialité et de la manière dont la confidentialité se développe partout dans le monde. Pour ceux qui élaborent des cadres pour les nouveaux gTLD, ou pour d'autres services au sein de l'ICANN, lorsque cela pose un problème, ils peuvent voir comment surpasser ces défis de conformité avec les règlementations à venir, de manière à ce que les acteurs commerciaux et les utilisateurs ne soient pas

forcés à décider s'ils veulent manquer aux règles de l'ICANN ou aux règles du pays.

C'était le cas dans le passé, on le sait. Et donc l'idée est de pouvoir avoir des règles qui soient cohérentes entre elles.

J'enlève maintenant ma casquette de représentant et je fais une remarque à titre personnel.

Dans mon pays, lorsqu'on discute de politiques de données et de l'avenir des politiques de données, de plus en plus de personnes se disent que l'idée de protection de données par rapport à l'interdiction de l'utilisation de données pourrait ne pas être une pensée qui nous permette de mettre en œuvre nos droits, de protéger nos droits en matière de vie privée et de confidentialité dans l'avenir comme un bénéfice.

Les données devraient être utilisées pour résoudre des problèmes de manière à améliorer nos vies, pour vivre de manière plus aisée.

Je pense que l'idée serait d'utiliser des données moins prohibitives et de contrôler et de protéger nos données, de voir qui peut utiliser quelles données et à quel but. Pour que l'on puisse considérer comment tirer profit du potentiel du partage de données, de tout ce que nous sommes en train d'élaborer de

manière à pouvoir élaborer des politiques qui soient plus utiles pour le 21e siècle.

Cette discussion fait partie d'une discussion annuelle, j'espère qu'on pourra interagir pour trouver quels sont les problèmes qui se posent aux personnes.

Je suis content de voir cette discussion ici. Bien que l'on continuera de discuter sur d'autres questions au sein du FGI, du forum de gouvernance internet, que nous allons accueillir cette année du 18 au 21décembre de cette année à Genève. Merci.

BECKY BURR: Merci. Nous allons passer aux questions interactives du public. Nous avons d'autres travaux de base qu'il faudrait que l'on installe ici, que l'on présente.

Concernant la disponibilité des données du WHOIS, Gail, il a des sociétés qui se voient impactées par les modifications et il faut que l'on travaille au niveau de la conformité. À votre avis, quelles sont les nécessités des sociétés dans ce secteur, dans ce cadre ?

ABIGAIL SLATER: Merci Becky. Je suis membre de l'association internet de Washington DC, nous représentons plus de 40 sociétés mondiales d'internet.

On n'était pas à l'ICANN depuis la transition des fonctions IANA, mais on était fiers de participer à cette initiative. On a surtout participé à un groupe de 14 organisations différentes qui comprenait la société civile qui ont lancé un [amicus brief] au Texas, au soutien de la NTIA, et cela au nom de l'intérêt public de la société internet.

Je pense que j'ai trois minutes à parler, parce que le principal aujourd'hui est de savoir ce que vous en pensez.

Je pense qu'il est important de savoir quels sont les besoins des sociétés. D'abord, je dirai la certitude juridique, la sécurité juridique.

Les fondements et la mission de l'ICANN, et je lis, est « de maintenir la stabilité, la fiabilité et la sécurité, l'interopérabilité mondiale, la résilience et l'ouverture du DSN au niveau opérationnel ». Et je pense que la base de données du WHOIS est un aspect clef pour cette mission.

Lorsqu'on parle de principes de confidentialité ici, il me semble que le plus important est d'en discuter dans le contexte du WHOIS et dans le contexte utilisé par le gouvernement Obama,

qui est celui des égalités en concurrence. Ces égalités concurrentes, en matière de WHOIS, comprennent les questions d'application et de défense des marques commerciales. On a également la confidentialité, l'égalité de protection des consommateurs, la protection au niveau de la fraude et du spam… Donc il y a différents aspects et il est important de savoir en tout cas que les égalités sont toujours concurrentes de toute façon.

À partir de ma recherche avec la communauté de l'ICANN, on a publié un rapport au sein de SSAC de 2012 qui était appelé « WHOIS : l'aveugle et l'éléphant ». Ça fait référence à une parabole hindoue, ou on a différentes personnes aveugles qui doivent comparer l'éléphant. Et chacun touche une partie du corps de l'éléphant et chacun est en désaccord sur comment l'éléphant est, ce qu'il fait, quel est son aspect. Parce que chacun a vu une petite partie du même animal. Et je pense que c'est une bonne analogie au moment de parler des égalités concurrentes.

Dans le droit européen, en matière de confidentialité et de vie privée, cela n'a pas été reconnu pourtant. Même si c'est un principe important. Dans le système de l'Union Européenne, le système judiciaire et les tribunaux doivent garantir qu'il y ait un équilibre entre le respect du droit fondamental à la vie privée, et d'autre part les intérêts de pouvoir demander des données

personnelles pour le libre mouvement des personnes, qui est important dans ce contexte. Mais c'est également important qu'il y ait un équilibre pour les sociétés.

Le droit européen a commencé à reconnaitre ces principes dans l'article 6, il y à peu près 18 mois.

Et puis, pour répondre à la question de Becky, les sociétés ont besoin d'une sécurité juridique. En ce moment le système a des égalités concurrentes et des principes qui ne sont pas clairement délimités. Mais les sociétés ont besoin de sécurité juridique. Et si nous allons suivre le régime de confidentialité ou de vie privée de l'UE, je voudrais savoir si ce régime semble être le mieux pour tout le monde, s'il faudrait que l'on applique ce principe à l'ICANN comme meilleure politique.

Mais je signale que cela n'a pas été discuté. Et par conséquent, aujourd'hui, on appliquerait cela à toute la base données du WHOIS, ou alors au RDS, qui ne fonctionnera plus.

À partir des recherches, on a vu que plus de 40 % des saisies dans la base de données du WHOIS ont été saisies par des personnes morales, et non pas des personnes physiques. Donc il faut faire la distinction.

Il est important que les sociétés comprennent si cela s'appliquerait ou pas au contexte de l'ICANN.

Une autre question de seuil serait : quels sont les types de données qui sont impliqués à travers les normes de confidentialité du régime européen dans le contexte du WHOIS ?

Dans le système européen, on a un standard qui s'applique aux informations d'identification personnelle, c'est-à-dire des informations qui peuvent vous ramener à une personne, vous permette d'identifier une personne. La base de données du WHOIS contient plutôt des informations techniques, ce n'est pas des informations personnelles ou sensibles confidentielles.

Donc il serait utile pour les sociétés de comprendre qu'est-ce qui est compris dans les normes de confidentialité dans le contexte du WHOIS, par rapport aux informations qui sont incluses, des informations qui ne sont pas comprises.

Donc ce sont des questions importantes et je vous remercie d'avoir lancé le dialogue aujourd'hui. La GNSO et la communauté des commerçants en général s'attendent à pouvoir continuer ce dialogue.

BECKY BURR: Merci Gail. Finalement, on a Jim Galvin qui va nous parler de l'industrie des noms de domaine. Cette industrie sera directement affectée par les changements de normes. Quelles

sont les questions techniques qu'il faudrait que l'on garde à l'esprit et que l'on considère lorsqu'on tiendra ce dialogue ?

JIM GALVIN: Merci Becky de me poser cette question.

Lorsque je pense aux principes et aux pratiques concernant la confidentialité et aux solutions que nous allons mettre en œuvre pour la communauté, et aux solutions qui sont disponibles pour pouvoir satisfaire à ces besoins de vie privée, je m'inquiète par rapport à deux questions.

D'une part on a la gestion de données. Dans l'industrie, on a chacun nos propres processus internes pour collecter des données dans un emplacement, de l'envoyer ailleurs pour le stocker, de l'envoyer ailleurs pour faire un backup ou une copie de sécurité et le copier ailleurs pour avoir des services en temps réel. Ou ailleurs pour fournir d'autres services alternatifs, à l'intérieur des services d'annuaire, comme le WHOIS par exemple. Apparemment il y aurait un remplacement du RDAP pour ce faire.

Mais on copiera quand même les données là-bas. Et la confidentialité aura sans doute un effet, un impact sur ce que nous faisons. Où les données sont ? Où elles sont envoyées ?

Tout cela est important. Cela pourrait nous faire changer nos propres architectures, nos propres processus internes.

Mais certaines des solutions sont plus efficaces que d'autres et elles ont un impact plus dramatique sur ce que nous pourrons faire ou pas, sur la capacité de le faire ou pas.

Lorsque nous pensons aux capacités que nous allons avoir pour pouvoir satisfaire à ces besoins, il faut penser à ce qu'il nous faudra faire pour pouvoir suivre la confidentialité des données sur tout l'écosystème. Donc ça fait partie de la gestion de données.

D'autre part, j'ai une autre inquiétude, comme je l'ai dit. Et c'est le fait de l'accès aux données.

Dans le système actuel, on a un système qui est relativement ouvert. Tout le monde peut accéder à toutes les données à tout moment. C'est ça le système du WHOIS qu'on a aujourd'hui, et c'est ça le service d'annuaire du WHOIS.

Mais l'autre extrême serait d'empêcher l'accès aux données en tout moment à tout le monde.

Mais on reconnait tous qu'on est en train de créer un système d'accès différencié. Et il va falloir que l'on crée des politiques qui définissent les rôles et qui décident qui va pouvoir accéder à quoi, et comment pouvoir décider qui accède.

Ça se fera à travers la création d'un système de gestion d'autorisations, il va falloir qu'il y ait des personnes qui reçoivent ces autorisations, il va falloir qu'il y ait un autre ensemble de personnes qui soient empêchées d'accéder. Et les personnes ayant cette autorisation, vont utiliser cette autorisation pour accéder à un certain ensemble de données.

Donc les systèmes de gestion d'autorisation vont avoir un coût associé, bien sûr.

Il y a différents types d'échecs qui pourraient avoir lieu dans ce type de système. Il pourrait y avoir des défaillances associées à ce système. Donc il y a beaucoup plus de charges associées à ce type de mesure d'atténuation.

Donc il faut que l'on considère à ce que nous avons aujourd'hui pour la gestion d'autorisation aujourd'hui, en tant que communauté. On opère des infrastructures assez grandes à l'heure actuelle, donc on a un système qui est assez solide, qui fournit un accès en temps réel, tout le temps, aux données. C'est-à-dire que c'est un système qui est à votre disposition tout le temps. Et on a un grand investissement à ce type d'infrastructure.

Dans un système qui gère les autorisations, si vous voulez pouvoir travailler, il va falloir que vous aillez l'accès aux données, et qu'il y ait un système qui fonctionne constamment

qui me permette de valider mon autorisation et de faire savoir au système que j'ai l'autorisation pour accéder à ces données.

Donc il faut comprendre quelle est la voie dans laquelle on avance, et autrement, si ça ne fonctionne pas, qui sera responsable.

En tant que communauté, il va falloir que l'on décide quelles sont les politiques que l'on va avoir pour pouvoir résoudre ce type de défaillances.

D'autre part, il y a des personnes qui connaissent déjà ça, mais pensez à l'infrastructure de l'autorité de certification, qui fonctionne et qui existe autour du monde. On a tous vu des échecs dans cette industrie.

Il faut que l'on pense aux politiques et à ce que cela implique lorsqu'on a ces types de problèmes. Comment va-t-on gérer ce type de problèmes, comment compte-t-on les traiter. Est-ce qu'on va les résoudre ou alors comment va-t-on appliquer des règles à nos autorisations qui nous permettent de voir si on a le droit d'accéder ou pas, et si on sera responsable des défaillances ou pas.

Donc mes deux inquiétudes sont les types de solutions que l'on cherche, quel est le type de performances et de capacité que

nous voulons fournir pour pouvoir remplir ces besoins, satisfaire à ces besoins de confidentialité.

BECKY BURR: On passe maintenant aux questions du public. Il y a un microphone au milieu, donc s'il y a des questions que vous voulez poser vous pouvez vous rapprocher du microphone.

En attendant, on a entendu parler de différentes questions. Indépendamment de l'approche que vous choisissez, on s'est dit que le traitement des données personnelles doit être légitime et que pour pouvoir atteindre les normes de transparence, il va falloir que l'on articule ce but de légitimité.

L'utilisation doit être en proportion avec le but de l'utilisation des données et ça ne peut pas bien sûr dépasser les droits de confidentialité individuelle.

Donc voyons un peu ces différents secteurs, ces différents aspects.

On a un commentaire de Joseph.

JOSEPH CANNATACI: Oui, en fait Gail parlait tout le temps de l'UE, c'est compréhensible, parce que c'était l'UE qui vient de conclure le GDPR.

Mais je pense qu'il faut se rappeler que le traité principal en matière de protection de données vient du conseil de l'Europe pas de l'UE. C'est la convention 108. Il s'agit d'une convention qui est ouverte, il y a des pays qui sont des signataires à cette convention, comme l'Uruguay ou la Tunisie ; et il y a des autres pays qui sont des observateurs.

Il y a beaucoup d'autres pays qui suivent cet exemple, et qui adoptent des normes.

Je ne veux pas que l'on parle de cette norme européenne plutôt que de parler des normes de l'UE, mais le GDPR aura un impact énorme pour la pratique au niveau mondial. Ce n'est pas une question de qui ça vient, mais il y a beaucoup de principes qui sont en conformité avec les normes européennes. Merci.

BECKY BURR: Merci. Dites votre nom au moment de parler.

LUTZ DONNERHACKE: Je m'appelle Lutz, j'ai participé de l'équipe du WHOIS une fois et j'ai participé à un débat sur le WHOIS détaillé et le WHOIS résumé.

Le WHOIS résumé implique que nous avons compris que nous avons une connaissance dans un système légal au niveau

mondial. On n'a pas de problème avec l'excès de données ou au fait d'incorporer des données. Le WHOIS résumé permet aux ordinateurs de prendre des données pour les identifier.

Étant donné que si on demande à un serveur ou à IANA, on peut faire une recherche spéciale d'un nom de domaine et on peut savoir où il est situé. Mais si on a un WHOIS résumé, on peut également obtenir certaines réponses des registres disant qu'ils ont vendu cela au bureau d'enregistrement suivant.

Si le bureau d'enregistrement a des données obtenues du client, vous pouvez fournir un serveur du WHOIS à l'échelle locale. Toute l'information obtenue ne doit pas abandonner le lieu où le droit est appliqué en principe.

Je vous encourage à penser à cette approche parce que c'est la meilleure manière d'aborder cette question ; merci.

BECKY BURR: Merci. Je voudrais ajouter quelques mots avant d'avancer.

Moi, je crois que l'ICANN cherche des noms de domaine. Par exemple des titulaires européens .COM par exemple, et il va chercher un WHOIS détaillé. Et en matière de protection de données, nous savons qu'il peut y avoir un transfert de ces données, par exemple en dehors de l'Europe.

On n'est pas très sûrs d'avoir éliminé le problème entre le WHOIS détaillé et le WHOIS résumé. C'est ce que je voulais dire.

D'autres commentaires ?

GIOVANNI BUTTARELLI: Pour continuer ce débat à propos des données détaillées et résumées, je veux dire qu'il n'est toujours pas très clair quelle est la voie à suivre.

En conséquences, avant d'aborder des questions relatives à la quantité de données, système centralisé contre système décentralisé, droit d'accès sur la base de la légitimité, je ne parle ici du respect de la loi. Je crois qu'il faudrait se mettre d'accord sur les objectifs. Parce que pour nous, pour le dire franchement, après avoir adopté notre point de vue en 2003, ce n'est toujours pas clair.

Pourquoi il est nécessaire de collecter ces données d'une manière déterminée, pourquoi il faut les publier autrement ? Et qu'est-ce que nous comprenons ou nous voudrions comprendre à partir de tout cela.

Je crois donc qu'il est nécessaire d'identifier une personne de contact, il faut avoir une personne de contact identifiée. Il faut faire une mise à jour permanente pour la publication de ces données.

C'est important pour mettre en place une politique robuste.

En premier lieu, je dois dire c'est la base, c'est le point de départ.

BECKY BURR: Je vais passer la parole à James et puis à Jim.

JAMES BLADEL: Compte tenu de votre suggestion, je crois que c'est l'un des objectifs primaires de l'élaboration de politique du RDS que nous avons débattu auparavant.

C'est bien de mener ce débat. Et il faut savoir que ce travail est le travail de base nécessaire pour aborder ce type de question.

JIM GALVIN: Merci. Je voulais également faire un commentaire et souligner que lorsqu'on parle des différentes solutions, il faut considérer le respect des exigences de confidentialité et faire des différences entre les solutions possibles.

Il y a des solutions qui ont trait au WHOIS détaillé et résumé, et il faut évaluer quelle est la solution la plus appropriée pour avoir d'avantages de solutions.

C'est une question qu'il faut réviser pour définir nos objectifs.

BECKY BURR: Vittorio.

VITTORIO BERTOLA: Merci. J'ai une série de questions, mais tout d'abord je veux partager avec vous ma frustration.

Parce que j'ai participé des réunions de l'ICANN pendant les 8 dernières années, et j'ai participé au conseil. Une série de questions qui sont constantes, parce que c'est pareil qu'il y a des années. [Applaudissements]

Monsieur Buturelli a été très gentil lorsqu'il nous a rappelé la réunion de l'ICANN à Rome il y a 14 ans. Et l'ICANN n'a pas pu, à ce jour, donner une raison pour laquelle il faut collecter ces données.

C'est difficile, c'est déprimant si vous voulez. Entendre des commentaires comme ceux que nous avons entendus par rapport à la confidentialité et au respect de la loi.

Moi j'aime pas les activités malveillantes bien entendu, mais n'a pas trait seulement à établir un équilibre entre les obligations contractuelles et la loi, parce que l'ICANN ne peut pas imposer des obligations aux gens.

La question est la suivante. Elle est adressée à monsieur Buturelli pour les autorités européennes et pour ceux qui

possèdent des lois similaires. La question est : il y a quelque chose qui sera changé, notamment la connaissance (informé) en Europe, parce que ces dernières années on n'a rien vu, on a été très patient avec les autorités, mais il faut faire des pas concrets pour pouvoir avancer.

Je me demande s'il y a quelque chose qui va changer par rapport à ce nouveau système au GDRP.

Je ne sais pas qui va répondre à ça. Mais les autorités de l'Europe et pour ce qui est de la protection des droits et la publication des données, la collecte de données… [Applaudissements]

Alors, que peut faire l'ICANN ? Parce qu'ils doivent s'adapter à la loi.

Merci.

GIOVANNI BUTTERELLI: Vittorio on n'est pas ici pour chercher des problèmes mais pour les résoudre. Parce que nous sommes une entité d'application de la loi.

En 14 mois ou 13 mois, nous allons commencer avec l'exigibilité. Il y a 20 ans ce concept était basé sur certaines choses et maintenant c'est différent.

La question est comment allons-nous nous préparer pour le 25 mai 2018, la journée numéro 1. C'est important. C'est applicable à tout le monde. Fournir des services au sein de l'UE, on ne va pas s'occuper des serveurs, de l'établissement de la localisation de certains services, et savoir où se trouvent ces services et où est-ce qu'ils sont offerts.

Je crois que lorsque l'on construit quelque chose, il faut adopter une stratégie. Et à mon avis, la stratégie ici c'est le principe de limitation. Ce n'est pas le seul au sein de l'UE. Il s'agit d'un principe qui se trouve à l'intérieur de la convention 108. Michèle a parlé aussi de la convention de l'OCDE, dans la jurisprudence du tribunal européen sur les droits de l'homme entre autres.

Il s'agit d'un élément stable, mondial, c'est un pilier qui exige de spécifier l'objectif. On ne va pas chercher un objectif trop détaillé.

Les gens qui donnent les informations pensent, lorsqu'ils donnent ces informations qu'il faut comprendre le contexte. Alors l'objectif doit être spécifique, explicite, et il ne doit pas être ambigu, il doit être clairement exprimé et clairement déterminé.

Moi, quand j'enregistre, je dois fournir des données, je dois fournir une personne de contact, et l'objectif est la légitimité.

Et nous devions garantir un certain niveau de transparence. Mais après, on a demandé d'essayer de comprendre avec vous l'importance des différentes modalités. Cela, on l'a fait il y a 13 ans et nous avons posé la question suivante : est-il vraiment nécessaire d'avoir des données détaillées, des données résumées qui soient publiées ? Y a-t-il une alternative pour pouvoir parvenir à cet objectif de manière plus équilibrée ?

Je crois que tout cela est très important. Et si le problème c'est la traduction des principes et bien là, on peut vous aider.

On a eu un cas important, mais je crois qu'après le mois de mai 2018, les autorités de protection de la loi seront responsables d'exiger tout cela dans différents domaines.

Cela pourrait arriver en juin, en septembre en décembre 2018. Mais le jour arrivera sans doute.

BECKY BURR: Gail, Joe et Willbert devront répondre à tout ça, parce qu'on n'a presque plus de temps.

ABIGAIL SLATER: Une raison pour laquelle ce débat nous a pris si longtemps, c'est qu'il faut revenir au point des équités en concurrence. Il y a des équités qui doivent être semblables, et la seule chose, le seul

principe de guide, à savoir les statuts constitutifs, et bien les statuts doivent défendre la résilience et la robustesse du DNS. Je ne crois pas qu'il y ait de l'équité là-dedans.

Pour ce qui est du WHOIS et le GDRP futur et les sanctions, et bien à l'UE c'est pareil et les entreprises ont besoin de guides. Il y a des obligations par rapport au commerce électronique, et cela a créé des obligations pour les sociétés membres.

Ces obligations ont trait à la divulgation d'éléments de données de manière publique. Nous allons voir si on va violer la directive du commerce électronique ou si l'on va violer les règlementations qui parlent du GDRP.

BECKY BURR: Willbert.

WILBERT TOMESEN: Je serai bref. Je trouve qu'il est important de voir la question de base.

Pourquoi a-t-on besoin du traitement de ces données ? Il est nécessaire de trouver une manière moins intrusive et plus inclusive. La responsabilité est importante.

Pour moi, cela veut dire qu'il faut se convaincre que l'on va aborder certaines questions et que l'on va assurer ces données. Alors, je dis au contrôleur : et bien, vous devez me convaincre que vous allez faire vos meilleurs efforts.

J'ai travaillé pendant ma vie pour exiger le respect de tout cela, et le respect veut dire être juste et être équitable.

On peut être forcé à exiger une chose déterminée, mais les contrôleurs doivent me convaincre de pourquoi il faut le faire et de comment il faut le faire.

Et de respecter les principes établis.

BECKY BURR: Merci Vittorio, je sais que vous attendez ma réponse. Et ma réponse est que finalement l'ICANN ne peut pas forcer les registres et les bureaux d'enregistrement à choisir quelle sera la loi applicable.

MARIA FREDENSLUND: Je suis la directrice d'une organisation non gouvernementale danoise. Nous travaillons au Danemark avec le crime en matière d'IP.

Et lorsque nous avons travaillé sur le respect de la loi, sur les activités criminelles liées à l'IP et à la protection de produits.

Nous voyons que les produits IP sont de plus en plus utilisés pour les utilisations malveillantes, pour le cinéma, la littérature, pour pouvoir faire d'autres délits.

Par exemple, un site web qui est toujours enregistré dans un pays étranger est utilisé pour attirer les consommateurs, les utilisateurs pour installer des programmes malveillants dans leurs ordinateurs dans le but de perpétrer d'autres crimes.

Alors les produits IP sont utilisés comme un moyen d'obtenir du trafic vers ces sites web.

Nous avons vu également l'an dernier, vous savez que la population danoise est d'environ 6 millions de personnes, et la dernière année, on a eu plus de 200 millions de visites à ce type de sites illégaux qui viennent d'adresses IP danoises.

Alors on peut voir que le problème est en pleine croissance.

Une des raisons, c'est qu'il est très facile d'accéder à l'internet de manière anonyme. Alors on peut établir un site web sur un nom de domaine étranger, avec une adresse d'un nom de domaine étranger et on peut faire n'importe quoi comme activité criminelle.

C'est un problème vraiment très sérieux.

Alors, mon point est le suivant. Je veux dire nous avons évidement besoin de faire respecter les lois sur l'internet. Cela veut dire respecter l'équilibre des droits fondamentaux, comme par exemple la confidentialité et la vie privée et d'autres principes. Mais pour l'instant, la question c'est que c'est très facile d'être un criminel, parce qu'il n'y a pas moyen d'interférer les activités illégales comme autorité policière, comme titulaire de droit. Et l'une des raisons, c'est que c'est vraiment très facile de conserver l'anonymat sur l'internet. Merci.

GIOVANNI : Moi, comme membre du pouvoir législatif, je vais parler à partir de ma connaissance en matière pénale.

Je dois dire que les autorités du respect de la loi accèdent légitiment et proportionné aux données. Mais aucune de ces dispositions n'évite… Pardon, je veux dire rien n'évite que le système du WHOIS soit accédé de manière simple.

Un des problèmes c'est l'exactitude des données. Des fois on voit cela comme une sauvegarde pour les données, mais cela implique aussi que l'on peut accéder à ce type de données.

Je tiens compte de vos commentaires, mais si le problème est la facilité de l'accès, c'est une question de coopération internationale.

Et encore une fois, les principes de protection des données ne sont pas le problème.

ELLIOT NOSS: Bonjour, je suis un bureau d'enregistrement. J'appartiens à l'organisation depuis longtemps.

Je voulais signaler que ce panel me surprend énormément. C'est le panel le plus positif et optimiste des 5 ou des 10 dernières années. [applaudissements]

Et cela est dû à l'ICANN on a un déséquilibre aujourd'hui. Et ce déséquilibre est tel que nous avons besoin de vous et de votre communauté pour devenir plus actifs.

Je vais revenir aux entreprises qui sont au milieu des intérêts et qui sont en concurrence. À l'ICANN, on est poussé par un de ces intérêts. La propriété intellectuelle et l'application de la loi. Nous voulons être entre ces deux.

J'ai deux demandes à vous faire. Premièrement, pour chacun de vous, et bien, commencez à être plus actifs. J'espère que ce panel ne sera que le début d'un site permanent au sein de la communauté de l'ICANN pour que des personnes comme vous qui travaillent dans les questions de confidentialité viennent ici. Et pour le bénéfice de chaque membre du GAC, soyez présents. Et le plus grand problème du GAC c'est l'application de la loi,

c'est-à-dire c'est pas l'application de la loi OU les membres du GAC.

Je pense que l'ICANN doit créer un bureau permanent pour la confidentialité et la vie privée. Quelqu'un ayant un véritable pouvoir. Et cela parce que cette communauté a des besoins mondiaux. Il faut prendre en compte les questions nationales, mais il y a des éléments internationaux, mondiaux, en termes des mécanismes particuliers et des approches spécifiques.

Et seulement si l'ICANN adopte cette position, nous verrons qu'il y a des sauvegardes qui traversent les frontières qui traversent les limites et qui peuvent être remédié. Merci.

[applaudissements]

BECKY BURR: Merci. Je crois que nous devons avoir un fonctionnaire chargé de la confidentialité.

MATHIEU WEIL: Merci à tous. Je suis Mathieu Weil. Je suis le PDG d'AFNIC, un ccTLD français, et je suis fournisseur de back-end de plusieurs gTLD en Europe.

C'est-à-dire que j'ai une perspective assez claire de l'industrie.

Je crois comme mon collègue que le futur est brillant. James, qui est un acteur de l'industrie, très respecté dans le monde entier, mais nous comme ccTLD, on est très préoccupé par cette règlementation. Nous la prenons très, très au sérieux. Et on l'a considéré très au sérieux pendant des années.

Ce que James nous dit, si vous regardez plus profondément la question, n'est pas bien exprimé. Il n'y a pas une lacune si grande entre être un acteur de l'industrie des noms de domaine et d'être de l'autre côté en adoptant les principes du GDRP. Nous sommes, nous appartenons à l'industrie au sein de la GNSO. Il faut discuter ceci au niveau européen, mais il faut comprendre quelles sont les préoccupations du point de vue des pratiquants. Il faut savoir quelles sont les données qu'il faut protéger. Il faut voir exactement ce que veut dire de suivre les principes de ces règlementations.

Et comme Elliot, nous sommes pour ces principes. Nous les soutenons fermement. Et nous voulons que l'internet unique puisse unir les personnes.

Je crois qu'il faut aller au-delà de la tendance de dire c'est une règlementation qui nous a été imposée. On est sur la mauvaise route. Et il y a des défis, notamment pour les acteurs mondiaux. Mais cela peut-être résolu si et seulement si nous essayons de

trouver la solution. Ces solutions sont présentes depuis longtemps et on peut les identifier.

Je crois que le problème le plus urgent c'est d'encourager l'ICANN a améliorer ses processus, d'aider les opérateurs de registre et les bureaux d'enregistrement à respecter les règlementations et qu'ils ne soient affectés par d'autres processus de l'ICANN pour pouvoir respecter tout ça.

Voilà, c'est ce que je considère l'enjeu le plus important pour les industries qui nous occupent.

JAMES BLADEL: Pardon, je crois qu'il veut répondre.

JIM GALVIN: Je crois que je suis d'accord avec vous. Ce n'est pas exagéré. Mon observation a trait plutôt à ce que nous créons un nouveau système de gestion d'identificateurs. On pourrait en parler plus tard pendant longtemps, mais ce système, à l'échelle globale, c'est-à-dire on n'a pas eu de succès dans aucune industrie. On n'a pas de système de gestion d'identificateurs mondiaux à échelle pouvant valider les données, avoir tous les renseignements en temps réel, etc. Mais je crois que si nous avançons dans cette direction, on va retrouver des problèmes à grande échelle que nous n'avons jamais trouvés auparavant.

BECKY BURR: Il y a maintenant le forum public qui commence à 5 h pile, je vais demander au reste des personnes qui sont dans la queue d'être bref, parce qu'on n'a pas de temps.

VICTORIA SHECKLER: J'ai une question divisée en deux parties. Pour ce qui est du respect du GDRP, il faut établir un système d'accès contrôlé, un RDS à accès contrôlés aux données d'enregistrement. Et il faut garantir l'utilisation légale, comme par exemple la suppression de données civiles ou criminelles.

De nombreuses parties prenantes doivent donner des données d'enregistrement et s'occuper des processus de PDP par consensus qui doit définit l'utilisation des données de la part des tiers ou bien utiliser le consensus comme un mécanisme pour légitimer la proportion.

BECKY BURR: Merci, très bonne question, mais on a très peu de temps, et on va y répondre à la fin.

KEITH DRAZEK: Bonjour. VeriSign. Je ne vais pas poser une question aujourd'hui ; mais les discussions précédentes m'ont convaincu de poser ces questions. Il y avait un WHOIS détaillé de 2014 pour

les registres .COM et .NET ; on devait passer du WHOIS résumé au WHOIS détaillé pour avoir les données de 142 millions de noms de domaine.

Il y en a un grand nombre qui sont aux États-Unis, mais il y en a d'autres non.

À la lumière des nouvelles règlementations et du paysage changeant depuis 2014, je suis curieux de savoir si vous avez une idée sur les implications pour que nos bureaux d'enregistrement doivent transférer 142 millions de noms de domaine dans un registre.

Et si l'on regarde 2018, avec les nouvelles règlementations et la possibilité d'un nouveau RDS, je voudrais savoir quelles sont les mesures à prendre.

BECKY BURR: Merci, mais c'est une longue conversation qu'il faudrait avoir à cet égard. Ce n'est que le début d'un dialogue. Je veux remercier le conseil de l'Europe d'avoir présenté et d'avoir oui présenté ces experts ici dans la salle et je vous remercie tous de votre participation. Merci.

NIGEL HICKSON: Merci Becky, il faut quitter la salle parce qu'il y a le forum public dans 9 minutes. Merci.

[FIN DE LA TRANSCRIPTION]