KOBE – 2e atelier des dirigeants d'At-Large portant sur les politiques : trouver le juste équilibre entre le respect de la vie privée et la stabilité et la sécurité de l'utilisateur final de l'Internet
Dimanche 10 mars 2019 – 10h30 à 12h00 JST
ICANN64 | Kobe, Japon

YESIM NAZLAR: Hello. Bienvenue à tous pour cette deuxième partie de notre journée, deuxième séance.

Avance de commencer, je vais faire un petit rappel.

Comme vous le savez nous avons un service d'interprétation en espagnol et en français pour la séance d'aujourd'hui. Donc n'oubliez pas de donner votre nom avant de prendre la parole. N'oubliez pas non plus de parler à une vitesse raisonnable pour permettre à nos interprètes de faire un travail correct.

Ensuite, si vous voulez prendre la parole, vous pouvez utiliser et ces petits panneaux avec votre nom dessus et vous le mettez ici verticalement devant vous.

Et pour le moment c'est tout ce que j'ai à vous dire. Je donne maintenant la parole à Jonathan Zuck.

JONATHAN ZUCK: Merci à tous de revenir ici. Ces conversations sont très productives.

En ce qui concerne la dernière séance, nous avons Glenn McKnight qui a réalisé un document Google et qui a écrit un petit peu tout ce qui a été dit. Donc il va envoyer au groupe le lien de ce document pour que vous puissiez envoyer vos notes de cette dernière séance et votre opinion concernant ce qui a été dit. Donc voilà, je vous remercie à l'avance.

Cette séance est destinée à donner lieu à une discussion interne d'At-Large, des membres d'At-Large concernant ce que nous essayons d'accomplir dans le contexte du RGPD. Et nous avons ici quelques invités qui sont des experts dans ce domaine et qui vont nous fournir des informations.

Nous allons en parler, nous allons continuer à parler de cela après cette séance, mais je voudrais d'abord partir d'une base qui soit la même pour tout le monde.

Et donc, on a aussi dit cela lors de la dernière séance, nous devons essayer de finir cette phase 1 du EPDP.

Donc le défi d'At-Large, un des défis d'At-Large, est que nous voulons encourager les intérêts des utilisateurs finaux. Et ce sont en général des titulaires de noms de domaine et des personnes qui ne sont pas des titulaires de noms de domaine. Ce sont ces

utilisateurs finaux, et leurs intérêts ne sont pas quelque chose qui peut être défini de façon très simple.

Nous pensons aussi que les utilisateurs finaux qui ne sont pas des titulaires de noms de domaine ont été sous-représentés dans ces discussions. Donc on essaye de faire entendre la voix de ces utilisateurs qui ne sont pas des titulaires de nom de domaine. Nous ne disons pas que les utilisateurs finaux qui sont titulaires de ces noms de domaine sont les seules personnes ici concernées.

Nous allons essayer de discuter du problème de la perspective, du point de vue des utilisateurs finaux qui ne sont pas des titulaires de nom de domaine.

Nous allons prendre des décisions pour soutenir ces personnes-là. Voilà ce que nous allons essayer de faire.

Et puis, le problème des utilisateurs finaux qui ne sont pas titulaires de noms de domaine concerne tout le monde, même ceux qui sont titulaires de noms de domaines. Lorsque je prends un ticket en ligne par exemple, je suis un utilisateur qui n'est pas titulaire de nom de domaine.

Donc il y a des catégories de tâches que tout le monde réalise sur internet, nous tous, que nous soyons les personnes qui ont fondé internet ou pas, nous faisons tous des activités, comme par

exemple envoyer un email, faire des achats en lignes, etc. Donc nous voulons faciliter ces activités, tenir compte des intérêts liés à ces activités, plutôt que nous limiter à une approche selon le type d'utilisateur, voilà.

Donc c'est ce que je voulais préciser ici.

Prochaine diapo.

Donc le chemin à suivre, le chemin qu'il nous reste à suivre. La phase 1 est terminée, donc nous devons maintenant passer à la phase 2.

Dans la phase 1 nous avons décidé quelles étaient les raisons de collecter les données, quelles données devaient publiques et quelles données devaient être conservées comme étant privées, dans quels cas le RGPD s'applique - c'est quelque chose qui a été beaucoup discuté - et à qui s'applique ce RGPD, quand est-ce qu'on parle de questions géographiques, etc.

Bien, en ce qui concerne la phase deux maintenant. Qui aura accès à ces données privées, ces données qui seront considérées comme privées, dans quelles circonstances ces gens auront accès à ces données, en utilisant quels mécanismes cela sera fait.

Donc si quelqu'un veut faire des changements dans ces catégories, je vous demande de prendre la parole tout de suite.

Si vous avez des commentaires à faire, c'est le moment. Il n'y en a pas ? Bien, prochaine diapo.

Qui pourra accéder à ces données ? Donc les forces de l'ordre, pour la protection des consommateurs, les chercheurs de cyber-sécurité pour la sécurité et la stabilité des systèmes de réputation, comme systèmes de spam, de malware, etc., les propriétaires de PI. Et hier, nous en avons parlé, il n'est pas nécessaire d'être un candidat pour une propriété intellectuelle pour être concerné par tout ce qui concerne le malware, la fraude et la contrefaçon, cela intéresse tout le monde.

Prochaine diapo.

Donc la première discussion que je voudrais avoir concerne les forces de l'ordre. Certaines des questions qui ont été posées étaient : comment est-ce que les forces de l'ordre vont utiliser les données du titulaire de nom de domaine, comment elles les ont utilisées jusqu'à maintenant ? Comment obtenir des données ? Est-ce que les forces de l'ordre ouvrent automatiquement tout ce qui concerne le RGPD et donc ils n'ont pas besoin de s'inquiéter. Comment est-ce que le blackout du WHOIS a-t-il affecté les forces de l'ordre dans le passé ? Nous avons déjà quelques exemples, certaines anecdotes de choses qui se sont passées, et si vous voulez vous pouvez ici prendre la parole et nous en parler.

Je vais commencer par Laureen qui va nous donner sa perspective sur ces questions, puis je donnerai la parole au reste de la salle.

Il s'agit d'une discussion, il ne s'agit pas ici… Il n'y a pas de concurrence, de rivalité, on essaye d'obtenir des informations, de mettre ces informations sur la table, c'est pour cela que cette discussion a lieu, on veut savoir comment on va aborder la prochaine phase. C'est comme cela que nous allons travailler.

Donc Laureen je vous donne la parole.

LAUREEN KAPIN: Merci de m'avoir donné la possibilité ici de vous parler de ces questions importantes.

Je suis un avocat de la Commission de Commerce Fédéral qui s'occupe des forces de l'ordre et des agences de forces de l'ordre aux Etats-Unis, qui travaillent sur la protection des consommateurs et sur la protection de la vie privée. C'est le mandat que nous avons ici, au niveau de notre Commission.

Nous avons aussi une approche concernant la concurrence, mais je ne vais pas vous en parler.

Donc je ne suis pas ici pour rivaliser, je voudrais seulement partager des perspectives concernant le WHOIS, l'importance du

WHOIS pour les forces de l'ordre, pour la protection des consommateurs et les autorités qui travaillent dans ces domaines.

Et j'apprécie vraiment l'accent qui a été mis par la communauté At-Large, et l'approche prise par la communauté At-Large concernant les utilisateurs qui ne sont pas titulaires de nom de domaine, parce que c'est un petit peu… On se demande toujours qui va parler au nom des utilisateurs finaux, c'est-à-dire en notre nom à tous. Et je suis heureuse de voir que Jonathan a défini ces utilisateurs finaux, ces utilisateurs finaux qui sont très importants, qui jouent un rôle très important pour notre commission, nous devons protéger le public contre les pratiques malhonnêtes, nous ne voulons pas que les gens soient victimes d'actions malhonnêtes, nous essayons de les protéger.

Cela dit, je vais maintenant passer à la façon dont les forces de l'ordre comptaient sur le système du WHOIS et je parlerai ensuite de certaines choses que vous connaissez déjà, donc je n'approfondirai pas trop.

Mais je dirai que notre organisation utilisait WHOIS comme outil de recherches. Et en tant qu'outil de recherches, il nous était utile pour des systèmes de financement en cas d'hypothèques pour les personnes qui essayaient de tirer profit de personnes qui n'avaient pas de crédit, qui leur offraient des opportunités pour

obtenir un taux d'intérêt plutôt bas, qui essayaient de monter des escroqueries de ce type à travers des sites internet, en envoyant des emails, et la façon dont le WHOIS était utilisé pour voir qui était derrière certains sites internet qui essayaient d'escroquer les personnes.

Nous avons aussi compté sur le WHOIS lorsque nous faisions des recherches sur la violation de la vie privée. Par exemple lorsqu'une organisation essaye d'installer des systèmes d'espionnage sur les sites internet des utilisateurs, nous allons utiliser le WHOIS pour voir qui est derrière cette attaque d'hameçonnage et cet espionnage qui enfreint les voies de protection de la vie privée.

Donc voilà, c'est comme cela que nous travaillons pour protéger le public.

Et je veux aussi dire que ce n'est pas seulement pour lutter contre les activités malhonnêtes et de fraude, c'est aussi contre les violations de la vie privée.

Nous ne sommes la seule organisation qui travaille aux États-Unis et dans le monde avec le WHOIS dans ce sens-là.

Et avec un autre collègue à moi, qui travaille dans le groupe de travail sur la sécurité du public, il s'agit du co-président de ce groupe, j'ai aussi entendu un ami qui travaille dans les services

secrets des États-Unis qui m'a dit que ce service secret a un mandat très large, et au-delà de la protection du président et de faire l'objet de nombreux films, de romans, ils doivent aussi sécuriser des évènements auxquels nous participons tous, comme par exemple des évènements publics dans lesquels des personnes politiques vont prendre la parole. Il y a des menaces qu'ils peuvent détecter lors de ces évènements, qui sont connectés à des sites internet. Ils vont utiliser le WHOIS pour faire ce type d'enquêtes. Ils vont utiliser le WHOIS pour identifier les modèles d'activités qu'ils vont découvrir. S'il y a des domaines qui les intéressent, ils peuvent utiliser cet outil de tierce partie pour voir à qui appartient ce domaine, qui est donc la personne qui est derrière ce domaine.

Ça va être une composante clef de certaines enquêtes lorsqu'il y a des menaces, dans le cas d'évènements, dans le cas de personnalités, aussi dans le cas de contrefaçons, ils font des enquêtes pour les activités de contrefaçons, ils vont utiliser cela comme outil dans leurs enquêtes.

Et je peux passer ici différents domaines d'escroqueries. Escroqueries à travers les emails, escroqueries de différents types. Il y a des personnes qui perdent beaucoup d'argent aujourd'hui à cause de ce type de fraudes qui existent et des

histoires aussi de tromperies, et que les services des États-Unis sur lesquels ils doivent enquêter.

Il y a des organisations de sécurité pour la protection des enfants aussi qui utilisent le WHOIS pour détecter les domaines qui sont associés avec des menaces.

Tout cela pour dire qu'il y a une large gamme d'activités dans lesquelles les forces de l'ordre et les autorités de protection des consommateurs, tout cela est utilisé pour éviter que nous ayons des problèmes. Donc c'est un outil très, très important. Voilà.

Je vais maintenant passer à deux autres questions importantes, puisque Jonathan m'a dit que… N'a pas donné de restriction au niveau du temps, mais je ne vais pas exagérer.

Donc il y a aussi d'autres façons de trouver des personnes, des utilisateurs. Il y a des autorités, en cas de procès, il y a différents outils, mais qui sont très longs à utiliser, qui peuvent demander beaucoup de temps. Le fait de se présenter devant le tribunal pour demander une approbation, pour faire des enquêtes, sont des systèmes qui demandent beaucoup plus de temps, qui coûtent beaucoup plus cher que le fait de chercher un nom dans une base de données, et cela peut être fait en quelques secondes. Donc on peut aussi faire appel aux tribunaux, mais cela demande beaucoup plus de ressources, c'est beaucoup plus long. Et cela

veut dire que le travail va être plus long. Et lorsqu'il y a une urgence qui surgit, cela n'est pas possible de travailler. On ne peut pas attendre, les choses sont urgentes, et donc on ne peut pas présenter cela devant un tribunal, attendre sa réponse, etc.

Bien, je vais maintenant passer au dernier point, parce que je pense que Greg va vous donner beaucoup d'informations sur cela.

Je voulais aborder la troisième question, parce que c'est très important, c'est un problème important. Les forces de l'ordre sont-elles couvertes par le RGPD, de façon à ce qu'il n'y ait pas de souci à avoir dans ce domaine ? Non, ce n'est pas le cas, surtout pour les forces de l'ordre étrangères.

Le RGPD reconnait l'équilibre qui doit exister au niveau de la protection, de la confidentialité. Mais il y a ici une préoccupation, parce que les autorités publiques, dans le cadre du RGPD, n'ont pas été interprétées – à mon avis - comme incluant les autorités des forces de l'ordre qui ne viennent pas de l'Union Européennes.

Si vous venez de l'Union Européenne, il y a une voie qui existe, qui a été rédigée, qui est contenue dans ce RGPD et qui permet d'avoir une justification pour obtenir ces informations, mais ce n'est pas clair. On ne sait pas si les forces de l'ordre étrangères ont aussi ces mêmes voies de recours.

Donc le RGPD est très long, très compliqué, et il y a encore des points à interpréter par les organisations juridiques de l'Union Européenne et de l'extérieur de l'Union Européenne.

À mon avis, il n'y a pas encore une voie très claire pour les forces de l'ordre étrangères, pour qu'elles puissent obtenir des informations dans le cadre du RGPD, et je pense que c'est un grand problème, particulièrement pour quelqu'un qui vient des États-Unis par exemple et qui appartient aux services des forces de l'ordre comme c'est mon cas.

Donc voilà, c'était un petit peu ce que je voulais vous dire concernant les forces de l'ordre et leurs utilisations du WHOIS, l'importance du WHOIS pour les forces de l'ordre, la façon dont nous travaillons, le temps nécessaire pour ce type d'actions. Il y a parfois des domaines, des obstacles, qui existent au niveau du RGPD pour les forces de l'ordre du monde entier pour obtenir les informations dont ils ont besoin pour nous protéger, pour protéger les utilisateurs finaux.

JONATHAN ZUCK: Merci Maureen, je vais donner la parole à Kathy, et ensuite nous verrons les thèmes qui vont être abordés.

Kathy, je vous ai entendu dire que beaucoup de gens, qui sont des acteurs malhonnêtes, sont un petit nombre de personnes. Et vous

avez aussi dit que les intérêts sont très importants dans ce domaine, et que les conséquences du fait de révéler des données, ces conséquences ont un grand impact aussi. Donc je voudrais savoir un petit peu quelle est votre approche, et quelle est votre opinion concernant les problèmes des forces de l'ordre.

Je vous donne la parole.

KATHY KLEIMAN: Merci Jonathan. Je vais vous donner un peu de contexte, et peut-être que Laureen vous pourrez répondre aux questions pour qu'on travaille ensemble, d'accord ?

Je suis Kathy Kleiman, co-fondatrice de l'unité constitutive des utilisateurs non-commerciaux. Ça fait trop longtemps que je participe à ces réunions.

C'est bon comme ça ? C'est pas trop fort ? D'accord, je me rapproche du micro alors. D'accord. Donc je parlerai doucement.

Parlons un peu du contexte. L'internet, en fait, serait différent si on n'avait pas de commerce en ligne. Mais l'internet est la plus grande source de communication des hommes, c'est l'ONU qui l'a dit, ce n'est pas moi qui le dis.

Donc il y avait une règle, que pour avoir une imprimerie au Royaume-Uni autrefois, il fallait avoir une adresse et une licence

du gouvernement britannique. C'est parce que si vous disiez quelque chose qui les critiquait, ou si vous imprimiez quelque chose qui les critiquait, ils seraient venus détruire votre imprimerie. Cela a été supprimé dans la constitution américaine lorsque qu'on s'est [émancipé] du Royaume-Uni. Et c'était pour protéger les personnes qui recevaient les communications, non pas pour protéger les imprimeries, mais pour que les consommateurs puissent avoir des informations qui leur disaient vraiment ce qu'il se passait. Parce qu'il y avait énormément de journaux dans beaucoup de pays qui étaient contrôlés par les gouvernements et les citoyens. Et il y a beaucoup de personnes qui critiquent ce que font leurs gouvernements.

Avant, je partageais un groupe de droits de consommateurs qui critiquait des personnes qui n'étaient pas dans le pays. Et eux, ils n'étaient pas dans le pays, mais leur famille était là. Et donc ils parlaient de la vente de ressources publiques à des personnes privées qui faisaient partie de la famille du président. Ils critiquaient cela, il y avait beaucoup de corruption, il y avait une élection à venir qui serait contrôlée par des moniteurs internationaux. Donc, ils allaient obtenir des informations à travers les noms de domaine, leurs sites web étaient parmi les principaux traitres du pays, mais c'était le seul endroit où on pouvait obtenir de bonnes informations. Parce que ce média

n'était pas contrôlé par le président. Et on m'a dit que s'il était su qui contrôlait ce site web, la famille serait tuée. Donc on a tout fait pour protéger leurs données WHOIS, et c'était avant l'existence des services d'anonymisation et d'enregistrements fiduciaires.

À l'époque, je me suis présentée auprès des forces de l'ordre et j'ai dit : j'ai un problème. Moi je peux travailler avec les forces de l'ordre de mon pays, des États-Unis, pour essayer d'avoir un processus. Moi, je sais quel est le processus aux États-Unis, je peux travailler avec eux. Mais lorsqu'en Chine on me dit : donnez-moi les informations, je veux avoir les informations parce que cela enfreint le droit pénal, je dois dire : attendez, attendez un instant, c'est une violation en fait des lois de la Chine, donc il faut que je supprime ce qui est dit.

Mais en fait, on n'a pas de norme internationale. Et les forces de l'ordre n'opèrent pas tous de la même manière. Aux États-Unis, ou dans d'autres pays, on ne peut pas donner d'accès illimité à n'importe quelle information. Il y a toujours un processus, parce qu'on a des protections qui protègent les orateurs, les utilisateurs finaux, et toutes les personnes en fait.

Je pourrais continuer à parler, je serais contente et prête à répondre à vos questions s'il y en avait.

C'est difficile de travailler, tout cela a été créé avant nous, avant l'existence de réseaux de scientifiques nationaux, c'était une question de confiance entre utilisateurs, il n'y avait pas de données, c'était des départements d'informatique de différentes universités.

Donc moi, ma question pour vous c'est si les forces de l'ordre ont déjà tué des journalistes.

JONATHAN ZUCK: Merci Kathy. Pour avoir un peu de contexte, je pense qu'on n'aura plus de WHOIS public dans l'avenir.

Donc en fait la question serait d'avoir l'accès aux données, de voir si cet accès pourrait être public ou pas. Parce que l'idée d'avoir un accès public serait un peu difficile à respecter. Donc en fait, c'est ça qu'il faut qu'on discute.

KATHY KLEIMAN: Oui, pardon, moi ma question c'était si les forces de l'ordre ne voulaient pas d'accès illimité aux données parce que, en fait, ils veulent faire ce qu'ils veulent.

Donc l'idée que le WHOIS…. Oui, non, non, ce n'est pas que je suis passionnée par rapport à ce sujet, c'est pour ça que je parle vite.

Si c'était public… Oui, ils voudraient bien avoir ce type d'accès illimité aux données, c'est ça que j'entends de vous…

Comment trouvez-vous un équilibre ? Même en tant que force de l'ordre, comment devons-nous présenter ces questions, comment formuler ces questions lorsqu'on parle aux forces de l'ordre, lorsqu'on a des organisations qui posent des questions à certaines des organisations gouvernementales les plus puissantes au monde ?

JONATHAN ZUCK: Laureen, vous voulez rebondir là-dessus ?

FARSANEH BADII: Farzaneh Baddi, NCSG. Je voulais que ce soit clair que la mission importante de notre unité constitutive et des forces de l'ordre est de ne pas empêcher le travail des autres. Pourtant les forces de l'ordre autour du monde sont redevables. Nous savons qu'elles ont cette obligation traditionnelle. Donc il devrait y avoir des mesures pour qu'elles soient redevables en cas d'accès aux données. Et cela est très important pour nous.

Pourtant, ce que nous entendons également est que le WHOIS est utilisé constamment à des buts qui ne sont pas véritablement

dans le respect de la mission de l'ICANN. C'est très controversé. Je sais qu'on a un conflit dans ce sens, mais c'est ça mon idée.

D'autre part, je voulais dire : pourquoi croit-on que la vie privée et la sécurité sont toujours l'une contre l'autre ? Ce ne sont pas deux concepts opposés. En fait il devrait y avoir des mesures de divulgation de données aux personnes qui ont un intérêt légitime pour les avoir, et pour que les données ne soient pas publiées directement.

Et moi, ce qui m'inquiète, et depuis une vingtaine d'années, c'est le fait qu'il y a toujours eu cette pousse, cette lutte pour que les données soient publiques. Donc on n'avait pas d'équilibre à atteindre, et les acteurs qui voulaient que les données WHOIS soient publiques, ce sont les informations personnelles des titulaires de nom de domaine. Ce sont des informations qui contiennent leur nom, leur prénom, leur adresse email, l'adresse de leur maison, leur numéro de téléphone. Donc pour les autres acteurs, je pense que ce serait bien s'ils pouvaient reconnaitre également que la vie privée des titulaires de nom était quand même importante pour les utilisateurs finaux, non seulement pour les titulaires.

Et finalement je vais dire, lorsque nous parlons par exemple de la capture de nom de domaine, qui est de plus en plus importante, c'est qu'on ne peut pas le mettre en terme de noir et blanc. Cette

question de l'usurpation de nom de domaine en fait doit être vue du point de vue un peu plus équilibré. On aura une vie privée qui doit être protégée, mais il y a des aspects positifs de le faire.

J'avais un autre commentaire à faire.

JONATHAN ZUCK: Est-il lié aux forces de l'ordre ?

FARZANEH BADII: Oui. Pour l'accès des forces de l'ordre aux données, John vous avez dit que les données WHOIS étaient rédactées partout, qu'elles étaient expurgées et qu'il ne fallait pas revenir à chaque fois à la même discussion, mais il y a eu des essais pour avoir une différentiation géographique et dire que le RGPD ne s'applique pas à toutes les régions et que donc les titulaires de nom de domaine ne devraient pas avoir des données protégées et donc avoir des données publiques. C'est un problème qui n'a toujours pas été résolu.

JONATHAN ZUCK: Merci. Merci Farzi. Moi, je voulais attendre la partie des questions, mais Greg, est-ce que vous avez un commentaire à faire tout de suite ? Ou Vous pouvez attendre. Vous attendez ? D'accord.

Donc est-ce qu'il y a des questions ? Vous avez déjà entendu parler du contexte des forces de l'ordre, on a entendu Laureen, Kathy et Farzaneh, mais avez-vous des questions qui sont liées aux acteurs des forces de l'ordre ?

Olivier.

OLIVIER CREPIN-LEBLOND: Merci Jonathan. J'ai une question pour Kathy, et vous m'en voudrez hein, je le sais, je m'excuse d'emblée.

En 2015, les laboratoires de Kasperky avaient enregistré 758 000 000 d'instances de cyber-attaques. Combien de personnes ont été emprisonnées en raison de la publication, divulgation de registre WHOIS dans ces années ? Parce que j'imagine que ce n'est pas tellement de gens… Pas autant que ça.

FARZANEH BADII: J'ai une question : qu'entendez-vous par cyber-attaque ? Parce que les cyber-attaques ne sont pas toutes gérées par les données WHOIS. Si vous voulez des données sur la quantité de personnes qui ont été emprisonnées et/ou des groupes minoritaires qui ont été emprisonnés dans certains pays, par exemple, en raison de ces attaques, je pourrais vous donner ces données. Il y a également des questions de harcèlement.

Ces données ne peuvent pas être publiées. Donc on n'a pas toutes les données. Ce n'est pas que les pays vous disent : bon regardez, il y a eu des attaques, il y a des personnes qui ont divulgué des informations, voilà qui a été emprisonné, untel ou untel. Ce n'est pas comme ça que ça se passe.

Il n'y a pas un jour spécifique auquel ces données auront été mises à disposition, mais ça arrive…

OLIVIER CREPIN-LEBLOND: En termes généraux, je voudrais savoir quel était le suivi que l'on fait de cela.

FARZANEH BADII: Si une personne est emprisonnée en raison d'un enregistrement de données WHOIS, il faudrait que l'on s'inquiète.

OLIVIER CREPIN-LEBLOND: Donc on devrait faire la même chose pour les cyber-attaques, le spam, le malware etc.

JONATHAN ZUCK: Tout à fait, je pense qu'on a ces discussions par rapport aux enjeux. Dans ce cas-là, les discussions [se penchent] sur ce qu'on est en train de faire…

[Coupure micro]

… Non je pensais qu'il rigolait, que c'était une vanne.

ANDREI KOLESNIKOV: Je voulais vous demander à tous de participer à cette réunion, pensant à ce sujet qui nous occupe, aux forces de l'ordre, pas de passer aux emprisonnements, aux majorités, minorités. On a un sujet, je voudrais vous demander de vous limiter à ce sujet. Merci.

KATHY KLEIMAN: Oui, les forces de l'ordre sont toujours une question qui est en rapport avec les droits des citoyens, donc je ne comprends pas pourquoi on n'est pas passé à cet autre sujet.

On pourrait le faire, si vous voulez on peut discuter ce seul sujet, mais on est là et tant qu'on est là on pourrait discuter de l'équilibre entre les deux, entre les forces de l'ordre et les droits des citoyens.

ANDREI KOLESNIKOV: Je n'étais peut-être pas clair. On a des données, concrètes, sur les changements, suivant l'implication du RGPD et son application. Cela est très lié aux activités de l'ICANN. Et je voudrais plutôt qu'on se borne à cette question.

On n'a pas tellement de temps. Donc je voudrais que l'on discute de données.

KATHY KLEIMAN: On n'a pas, nous, ces données-là.

JONATHAN ZUCK: Oui, en fait je vais intervenir ici. On est une communauté At-Large qui est très grande, on n'est pas tous d'accord sur ces questions, l'idée est de se concentrer sur ces aspects pour pouvoir avoir des discussions enrichissantes, pour essayer d'atteindre un consensus. Donc essayons de le faire.

On a qui dans la liste ? Ricardo ? D'accord.

RICARDO HOLMQUIST: Je parlerai en espagnol.

NON IDENTIFIE [SEBASTIEN]: Non, non, il ne faut pas s'excuser, c'est votre droit de parler en espagnol, hein.

ALAN GREENBERG: Est-ce qu'on peut avancer ?

RICARDO HOLMQUIST: Ma question était pour le premier intervenant, je m'excuse je ne vois pas son nom, c'est Laureen. Laureen, très bien. Ma question est s'il y a des statistiques par rapport aux données dont vous parlez. Parce que, comme pour ce qui est des droits de l'homme, on a un gros problème lorsque les pays et surtout lorsqu'on parle… Pas des pays qui ne sont pas complètement démocratiques, et vous avez les données du WHOIS dans ce type de pays vis-à-vis des données dans un pays peu démocratique, comme le votre, mais quelle est la fréquence avec laquelle vous accédez au WHOIS pour vérifier des informations ?

Combien de fois par semaine, par mois, par an ?

Est-ce que vous avez ce type de données et leur impact ? Si c'est une fois par jour, bon, ce n'est pas un problème d'aller demander à un juge de vous donner un permis pour accéder à ces données.

Dans un pays comme le mien, vous pourriez avoir des problèmes et être emprisonné si vous accédiez directement à ces informations sans avoir de permis. Donc il faut en fait avoir une stratégie.

Je voudrais savoir si vous avez des statistiques.

LAUREEN KAPIN: Merci de cette question. Je suis sûre qu'il y a des statistiques. Je ne pourrais pas vous les donner tout de suite, mais à partir de mes discussions avec mes collègues des forces de l'ordre, je dirais qu'aux États-Unis, comme autour du monde, il y a beaucoup d'organismes qui utilisent les données WHOIS des centaines de fois par jour, et peut-être même plus, parce qu'ils ont beaucoup d'enquêtes. Et c'est ça le volume de leur travail.

D'autres dépendances, comme la mienne par exemple, pourraient les utiliser avec une fréquence un peu moins importante, mais il y a une grande variabilité dans l'utilisation de tout cela.

J'observe qu'il y a beaucoup d'agences et de forces de l'ordre qui les utilisent une fois par jour peut-être s'ils ont un cas actif entre leurs mains.

Ce sont des généralisations bien sûr, mais certaines dépendances ont des statistiques que je n'ai pas immédiatement pour les partager avec vous.

Mais je suis contente que vous posiez cette question parce que je voulais également connaitre ce qu'ont dit mes collègues de l'autre côté de la table, Farzaneh et Kathy, parce que ce sont des sujets très importants par rapport à la mauvaise utilisation du

WHOIS et à la manière dont les personnes peuvent être en danger. C'est une réalité.

J'apprécie beaucoup votre point de vue par rapport à notre pays, c'est un exemple qui est dramatique sur notre crise disons. Mais je ne suis pas sûre, et je dirais conflit.

Je pense qu'il n'y a pas de gens dans cette salle qui soutienne le WHOIS et qui soit contre la liberté d'expression. Mais c'est un risque, et c'est un risque qu'il faut que l'on aborde.

Donc je voudrais être sûre que dans ma déclaration, qui se concentre sur ces risques financiers, physiques et toutes ces différentes instances, et sur la lettre qui se concentrait sur les statistiques par rapport aux malwares, à l'hameçonnage, au farming par exemple, tous ces différents risques, à l'exploitation et au dévoiement et aux différents risques que cela pose, il devrait y avoir un équilibre entre les risques et le travail de la communauté. Du point de vue des forces de l'ordre en tout cas.

Moi, qui viens des États-Unis, je dirais qu'on se concentre sur la protection du public. Mais il faut toutefois, reconnaitre la valeur de ce qu'ont dit mes collègues. Et c'est vrai qu'on n'a pas tous les mêmes priorités. Et c'est la réalité.

JONATHAN ZUCK: Merci Laureen. On a une longue liste d'intervenants qui commence à s'accumuler. Je voulais essayer d'avoir des paramètres.

Puisque nous avons ces membres du panel, essayons de traiter cette séance comme si c'était une séance de faits. On ne va pas en profiter ici pour exprimer ses opinions, l'idée est de leur demander des informations.

On aura d'autres occasions pour nous exprimer, mais l'intérêt d'avoir ces gens-là est de leur demander des informations. Je pense que c'est ça ce qu'il y a de plus intéressant pour nous ici ce matin.

Suivant ce que les membres du panel ont dit, je dirais que c'est à vous d'essayer d'aller davantage en profondeur dans les renseignements.

HUMBERTO CARRASCO: Je vais m'exprimer en espagnol.

Donc je vais attendre un instant parce que ma question est pour Farzaneh, pour Kathy. Donc je veux qu'elles m'écoutent.

Donc je crois que c'est Farzaneh qui a dit qu'à un moment ou à un autre il y avait des débats sur l'utilisation du RGPD selon les régions. Ça c'était la norme. Il y avait plusieurs régions où ce n'est

pas applicable tout simplement. C'est un concept d'extra-territorialité de la loi.

Moi, je suis Chili. Beaucoup de juristes du Chili vont dire que le RGPD n'est pas applicable à nous, ne s'applique pas. Mais il y a des cas, comme Riccardo Holmquist qui a deux nationalités, il est italien et vénézuélien. Donc même quand il est au Venezuela, il est sujet au RGDP.

Donc nous devons respecter les lois du RGPD pour des personnes comme Riccardo qui ont deux nationalités. Mais comment est-ce que, lorsque vous gérez les datas, vous allez distinguer qui est binational ?

Donc quelle est la solution à un cas de ce type ?

JONATHAN ZUCK: Je ne sais pas si on pourra vous trouver une réponse aujourd'hui, je ne sais pas qui pourra répondre…

FARZANEH BADII: Oui, le RGPD, on n'est pas concerné par les nationalités avec le RGPD, donc ce n'est pas le problème qu'il soit binational.

Le RGPD s'intéresse à l'existence physique des sujets de données dans l'Union Économique Européenne. Si vous n'êtes pas citoyen

européen et que vous résidez en Europe, là le RGPD s'applique à vous. Mais pour un citoyen européen qui ne réside pas en Europe, et bien là le RGPD ne s'applique pas à vous.

Donc ce n'est pas un problème de citoyenneté. Vous avez besoin de collecter… Il y aura besoin de collecter les passeports des personnes, ce serait absolument impossible.

JONATHAN ZUCK: Marita vous avez le micro.

MARITA MOLL: Merci. Ma question est pour Laureen.

Vous avez suggéré tout à l'heure, lorsque vous vous êtes exprimée, qu'une des barrières du WHOIS, obstacle du WHOIS, que ça va prendre plus de temps pour obtenir les informations dont vous avez besoin quand il y a des violations.

Dans la plupart des sociétés démocratiques, je crois qu'on perd en effet d'un côté, mais c'est un choix. Donc nous voulons qu'un juge, par exemple, autorise des écoutes téléphoniques. Mais étant donné que c'est l'internet et que tout va si vite, maintenant vous donnez l'impression que vous voulez l'avoir tout de suite.

Je crois qu'il faut prendre le temps d'effectuer ce travail d'analyse qui, en effet, lorsqu'on a un respect de la vie privée, doit être mené.

Est-ce que vraiment ce sera un problème négatif selon vous ? Est-ce que vous pourriez élaborer là-dessus ?

LAUREEN KAPIN: Oui, quelques points pour vous répondre. Tout d'abord, nous ne voulons pas revenir en arrière à un WHOIS public. LE RGPD est une réalité, nous en sommes bien conscients.

Et vous sembliez supposer qu'on devrait repartir un petit peu en arrière, ça ce n'est pas du tout ce que nous voulons faire, ce n'est pas du tout le cas.

En effet, parfois, cela prend beaucoup de temps, je sais que Greg va revenir là-dessus.

Au niveau philosophique vous savez – moi j'aime beaucoup les questions de ce type – nous vivons dans un monde où vous et moi allons donner des informations sensibles sur l'internet. Et nous avons le droit de savoir ce qui arrive à ces informations.

Nous avons des annuaires téléphoniques, nous avons beaucoup de situations où les informations dont on parle, je ne parle pas d'écoutes téléphoniques – ça c'est un problème de contenu les

écoutes téléphoniques – moi je parle de contacts, pas de contenus. Et bien on s'attend à pouvoir contacter les gens, et je crois que c'est assez raisonnable cela.

Je crois que le public devrait pouvoir accéder aux informations pour, en toute sécurité, savoir à qui on parle, à qui on a accès, qui on contacte. La société doit en effet décider quelle carte de crédit on utilise pour acheter de la musique sur internet et ainsi de suite.

JONATHAN ZUCK: Merci beaucoup. Nous avons Alan.

ALAN GREENBERG: Merci beaucoup. Deux points.

Hadia a répondu à Humberto, et c'est très complexe, c'est encore plus complexe que cela. Il y a des personnes au Chili pour qui le RGPD va s'appliquer. Pas parce qu'ils sont citoyen d'un pays ou un autre, mais en raison d'entreprises par exemple.

Le RDS et l'équipe d'analyse de cela va faire un rapport dans les 24 heures qui va être publié. Il y a eu une analyse dans le monde entier des forces de maintien de l'ordre et nous allons en savoir beaucoup plus lorsqu'on va pouvoir lire ce rapport avec beaucoup de statistiques. Combien de fois on utilise le WHOIS, quel est l'impact de ne pas avoir de WHOIS, éventuellement.

Nous avons donc plus d'informations à ce sujet, nous allons avoir des chiffres également, c'est une première enquête qui a été effectuée, mais qui va être très intéressante pour nous.

JONATHAN ZUCK: Merci ; je donne la parole à Holly.

HOLLY RAICHE: Moi ce que j'aimerais savoir des deux côtés des présentateurs, je crois qu'aux États-Unis et dans les pays occidentaux, il y a un équilibre, il y a un respect des lois, c'est extrêmement important pour le droit que les personnes ont sur la protection de leurs informations. Il y a des systèmes de contrôles et d'équilibrages.

Mais ce que j'aimerais savoir, c'est qu'est-ce que vous feriez comme tests dans les spécifications temporaires en tant que forces de l'ordre, dans le respect de la vie privée, donc comment pourriez-vous avoir accès à ces données.

C'est une question très difficile, mais je crois que vous voudriez que tout le monde ait l'accès, nous, nous ne sommes pas d'accord avec vous, nous aimerions en savoir plus, comment on peut protéger les personnes lorsque les lois de leur pays ne les protègent pas.

Vous, vous semblez dire que vous voulez avoir un accès pratiquement complet.

LAUREEN KAPIN: Oui, et bien je ne sais pas si mes collègues veulent répondre à cela, donc je vais essayer.

C'est une question très, très difficile. Je comprends bien. Et je n'ai pas une réponse facile pour vous. Je ne sais pas s'il y a de réponses faciles.

Ce que je sais, c'est que dans la phase numéro 2 le travail va se concentrer sur, comme l'a dit Jonathan, qui a besoin d'accès et pourquoi, et quelles procédures vont être utilisées pour obtenir l'accès aux données. C'est comme cela qu'on va travailler et gérer la situation. Mais c'est très difficile.

KATHY KLEIMAN: Donc je parlais à Farzi, au niveau de l'EPDP, qu'est-ce que l'on dit à ce niveau ? Moi, je crois qu'il y aura une double juridiction qui serait appropriée, même si le résultat ne me satisfera pas véritablement.

Moi je suis juriste aux États Unis pour principalement le premier amendement, et cette idée des registres et des bureaux d'enregistrement et des titulaires de noms de domaine qui

existent dans certains pays, avec beaucoup de liberté d'expression, il existe ces données qui peuvent être requises par les forces de l'ordre dans différentes régions du monde. Si ce sont des expatriés peut-être…

Donc ça c'est un peu inquiétant. Donc moi je crois que le rapport avec les forces de l'ordre, avec les juridictions, avec les différentes juridictions des registres, bureaux d'enregistrement et titulaires de noms de domaine.

LAUREEN KAPIN: Une nouvelle fois, ce qui m'inquiète un petit peu à ce niveau, avec cette approche, c'est qu'avec toutes les fraudes qui existent, toute l'exploitation qui existe dans l'internet, dans le monde entier, d'une manière regrettable, ce n'est pas dans une seule juridiction que ça se passe. Les forces de l'ordre doivent pouvoir faire des enquêtes.

Et très souvent, de nos jours, on travaille sur plusieurs juridictions en tant que forces de l'ordre. Par exemple, les Américains pourraient obtenir uniquement des informations de personnes dans leur juridiction. Je crois avoir compris ce que vous avez dit. Je crois donc que cela poserait des problèmes, parce que l'on travaille par exemple, si par exemple on est limité à la Chine, ce que vont faire les autorités chinoises.

Pour moi, cela ne correspond pas à la réalité des fraudes et malversations qui existent, et les enquêtes doivent être internationales maintenant. C'est au niveau global que ça se joue.

KATHY KLEIMAN: Et bien la réponse… Moi j'étais à une conférence il y a une dizaine d'années, et j'ai posé cette question, et moi je crois qu'en effet on travaille au niveau mondial, c'est très clair pour l'ICANN. Mais pour l'équilibre par rapport aux lois de chaque pays, les lois qui limitent par exemple l'étendue des forces de l'ordre, du travail des forces de l'ordre, vous avez en effet des fraudes qui existent, vous avez aussi des dissidents d'un autre côté, des personnes qui s'échappent d'un pays, vous avez des génocides, nous avons des pays qui veulent éliminer d'autres pays ou groupes religieux. Alors, ces institutions religieuses par exemple, doivent être protégées, on ne peut pas les trouver comme cela si facilement.

Il faut protéger des données sensibles, religieuses, sur l'identité sexuelle par exemple, sur les orientations politiques.

Donc beaucoup d'organisations non commerciales veulent qu'il y ait une forte protection du niveau du RGPD. Et il y a beaucoup d'autres pays par contre qui aimeraient beaucoup avoir la possibilité d'avoir des informations sur tout le monde.

JONATHAN ZUCK: Hadia ?

HADIA ELMINIAWI: Moi, j'avais une question. Je crois qu'on n'a pas répondu à la question qui est : comment le blackout du WHOIS a eu un impact sur les forces de l'ordre.

Moi, ce que j'aimerais dire c'est que les communautés vulnérables, c'est très important ça de les protéger. Elles existent, il y a des mécanismes qui existent déjà, par l'intermédiaire desquels vous pouvez protéger les communautés vulnérables dans par exemple le respect de la vie privée, l'entiercement des données. Il y a des moyens par lesquels les communautés vulnérables peuvent être protégées.

D'un autre côté, il faut prendre en compte les droits des citoyens. Par exemple le trafic, l'exploitation des enfants, le trafic d'êtres humains. Donc ce n'est pas seulement les problèmes techniques qui se posent.

Et, dernier point, on est tous d'accord pour dire que le WHOIS est mort et ne va pas revenir. Mais on parle maintenant de l'accès des forces de l'ordre et des mécanismes pour protéger les données, avec des mécanismes dont on n'a pas encore parlé, mais il est très

clair que par ce type de mécanismes, vous serez en mesure de savoir qui a accès aux données, quelles forces de l'ordre ont accès aux données.

Et dans des cas où il y a une violation des droits des citoyens, et bien vous devriez être en mesure de pouvoir tenir pour responsable les personnes qui l'effectuent.

Donc on parle de systèmes tout à fait différents. On parle de communautés vulnérables qui pourront être protégées, et il existe déjà des mécanismes pour ce faire.

En ce qui concerne la question de la juridiction, je dois dire que moi je suis quelqu'un qui est spécialiste des questions techniques, je suis ingénieure, je ne suis pas juriste, mais dans certains cas, vous ne connaissez pas la juridiction du site web, où le site web se trouve. Vous avez besoin d'avoir plus d'informations pour retrouver le site web, pour le situer et le géolocaliser.

Donc il me semble que ce n'est pas très réaliste cette première étape dont vous parliez tout à l'heure.

JONATHAN ZUCK: Merci beaucoup Hadia. Et bien nous allons clore la liste. Moi je veux vraiment qu'on soit disponible.

On n'est pas là pour changer vos idées, on est simplement là pour vous informer et s'informer tous ensemble de la situation. Donc gardez cette distinction à l'esprit. Je ne veux pas que ce soit un débat.

Bon, je crois que je vais avancer. Vous voulez répondre, c'est ça ?

KATHY KLEIMAN: Oui. Donc Hadia, vous êtes au EPDP, vous suivez ça de très près. J'ai été co-présidente des problèmes qui existaient il y a quelque temps. C'est Farzi qui s'occupe de l'EPDP, donc je suis tout à fait d'accord, je ne suis pas au courant de tout. Mais la transparence ne suffit pas. Il y a déjà des familles qui sont arrêtées. La transparence ne suffit pas.

Aux États-Unis, on avait un problème avec les Chat-Room, vous savez les personnes qui utilisaient des identités dans des chat-room, des salles de discussion. Et il y avait des choses qui étaient dites, des insultes par exemple, et on voulait savoir qui se cachaient derrière ces identités. Donc les ISP avaient ces identités. Et donc, il y a eu des procès, on a été en justice. Il y avait des droits de se défendre, des à se défendre, des droits à utiliser un statut protégé. Pourquoi j'ai le droit de ne pas donner mon identité lorsque je suis sur une chat room. Cela pose des questions importantes. Est-ce que vous voulez révéler mon

identité ce qui va être peut-être un problème de sécurité pour moi. Et les droits ont été protégés aux États-Unis de cette manière, lors de ces actions en justice.

Donc je crois qu'il faut encore améliorer ces points, il faut vraiment que ce soit très solide comme mécanisme de protection.

ABDULARIM OLOYEDE: Oui, merci beaucoup.

Moi, je suis d'une partie du monde où nous avons beaucoup d'abus, d'utilisations malveillantes, notamment gouvernementales, et je comprends bien que l'internet c'est la voix de l'homme ordinaire. Les forces de l'ordre jouent un autre rôle.

Parce que les activistes pour les droits de l'homme de la société civile sont des personnes qui prennent des risques. Dans chaque action, on s'engage, on prend des risques pour les droits de l'homme en tant qu'activistes. Nous nous exprimons et nous avons l'anonymat de l'internet qui est très important pour cela qui parfois nous permet de nous exprimer uniquement de cette manière.

Donc est-ce que vous pensez que les activités de plaidoyer doivent être faites dans l'anonymat ? Moi, je ne le pense pas, mais qu'en pensez-vous ?

JONATHAN ZUCK: Et bien écoutez, on ne va répondre à cette question, c'est une question très philosophique, on va en parler un petit peu plus tard, on va en parler en groupe, parce que ça, ce n'est pas une question qui se pose aujourd'hui dans notre sujet.

Donc merci à toutes et à tous de votre participation. On va passer au transparent suivant.

Je ne sais pas, on l'a perdu peut-être ? Je ne le vois pas à l'écran. Ha bah c'est peut-être celui-là.

Alors catégorie suivante. Les ressources et les recherches et les questions de réputation également. Donc il y a deux catégories.

Donc plutôt que d'attendre le transparent, Greg pourquoi est-ce que vous ne partagez pas avec nous les données que vous avez dans ce contexte ?

GREG AARON: Oui, merci beaucoup. Je m'appelle Greg Aaron, je suis membre de ICANN SSAC, et j'ai travaillé également à l'EPDP. De jour, je suis

un professionnel de la cyber-sécurité, qui fait de la détection de la limite des risques de l'internet dans l'espace de DNS. Donc je fais de la recherche également au groupe anti-hameçonnage.

Il existe des données sur l'impact qui existe dans ce nouveau monde sur les données. Et je crois que la plupart du travail qui est fait pour protéger les utilisateurs sur l'internet est effectué par le secteur industriel. Recherches au sens large. Des personnes qui veulent savoir ce qui se passe sur l'internet, qui essaient de définir les problèmes, les abus, les cyber-crimes, de diverses manières.

Donc on utilise différentes données et les forces de l'ordre s'engagent dans beaucoup de cas d'abus au quotidien et se concentrent sur les personnes qui perpètrent ces crimes. Mais il y a des ressources qui sont contrôlées dans l'internet.

L'internet, c'est le réseau de réseaux. Ce sont des entreprises, des universités, des gouvernements, d'autres entités qui gèrent ces services et qui véritablement gèrent la cyber-criminalité dans la plupart des cas.

Alors qu'est-ce qui doit être bloqué ? Qu'est-ce que vous ne voulez pas dans votre réseau ? Et vous avez des utilisateurs que vous ne voulez pas voir hameçonnés par exemple. Donc il faut définir les problèmes, bloquer parfois. Les chercheurs en sécurité bloquent certains points d'entrée de l'internet, au quotidien.

Ce qu'on essaye de faire, c'est de trouver les noms de domaine qui ont été inscrits par des criminels et les suspendre. Ne pas permettre l'utilisation de ces noms de domaine criminels. Combien de criminels ont-ils enregistré ou enregistrent-ils chaque année ? Des noms de domaine, des millions… Des millions de noms de domaine sont inscrits de manière criminelle. Environ 5 millions de noms de domaine.

C'est pour ça qu'on a des listes de blocage, comme Spamhaus. On est protégé par ces listes d'une manière ou d'une autre, pour ne pas être hameçonné, pour que nos navigateurs ne reçoivent pas de pourriels.

Donc ça, vous voyez, c'est une limite ces 5 millions de domaines frauduleux et criminels.

La manière dont on a compris cela, c'est grâce aux informations de WHOIS. Bon, ce sont des fausses données, ils ne donnent pas leur vrai nom les malfrats, les criminels. Mais vous savez on peut obtenir des informations et identifier beaucoup de noms de domaine suspects en voyant un petit peu comment le WHOIS, à quoi ressemble le WHOIS. Beaucoup de mauvaise foi dans le WHOIS, on réussit à s'en rendre compte avec les informations de contact par exemple.

Donc vous pouvez essayer de trouver des noms de domaine malfaisants d'autres manières, mais vous savez, ils changent les noms des serveurs très rapidement. Donc on a des outils qui sont très utiles, qui existent depuis de nombreuses années, et on utilisait – je le disais – le WHOIS pour cela, pour voir qui est derrière telle ou telle activité.

J'aimerais vous montrer quelques transparents.

Voilà ce qu'il se passait avant et après. Ça, ce sont des données de SPAMHAUS, qui est une liste de blocage pour noms de domaine. Ce que ça nous montre, c'est que le nombre de noms de domaine qui ont été identifiés et qui ont été listés par leurs services, avant et après la spécification temporaire. Ça nous montre bien qu'on a perdu la capacité avec les spécifications temporaires d'identifier les noms de domaine malfaisants à hauteur de moins 70 %.

Donc il y a des personnes qui sont impactées par cela. Il y a moins de noms de domaine frauduleux qui sont bloqués depuis les spécifications temporaires.

Donc ici, on voit des listes pour deux noms de domaine de premier niveau US et GDN, où les opérateurs de registre n'expurgent pas les données de contact. C'est-à-dire qu'on peut toujours les voir. Ici, comme vous voyez, dans le serveur, on peut

toujours trouver et énumérer les serveurs qui ont toujours ce problème d'hameçonnage et de malware. Et les données montreront le succès général des serveurs si on passe au dernier graphique.

Le serveur avait le même problème que SPAMHAUS, mais encore pire. Avant le temp spec était bleu, le rouge suivait. Et après le temp spec, ils ont perdu la capacité de trouver beaucoup de noms de domaine. Et en termes généraux, la quantité de noms de domaine qui sont toujours dans la liste noire a diminué. Ce qui se traduira en plus de dommages pour les utilisateurs.

Maintenant que nous avons plus de perspectives qu'en mai dernier, nous pourrions commencer à voir les effets de tout cela.

Encore une fois, lorsqu'on travaille sur ce type de problèmes sur internet, il est essentiel d'agir rapidement. On essaie de trouver autant que possible en aussi peu de temps que possible parce qu'on veut le bloquer et le fermer. Si on ne le fait pas suffisamment vite, les criminels, les délinquants, peuvent faire ce qu'ils veulent. Et ça, c'est un problème.

Il faut également savoir que les délinquants en général enregistrent plus qu'un nom de domaine à la fois. Et j'ai eu des cas de recherches dans lesquels les délinquants avaient enregistré des centaines de milliers de noms de domaine en

même temps. S'il est possible de les trouver et de les mettre en suspension en même temps, ce serait le mieux, ça augmenterait les coûts pour eux et ça empêcherait qu'ils puissent endommager les autres à travers leur méthodologie.

En général, les recherches sont la meilleure manière de le faire, mais il n'est pas facile de réagir suffisamment vite. Donc la vitesse et le dépistage de tous ces noms de domaine frauduleux sont l'essentiel.

Comment pourrions-nous avoir tous les outils nécessaires et nous conformer à la loi en même temps. Et c'est ça la grande question. C'est une question qui va devoir être considérée dans la deuxième étape de l'EPDP.

Le RGPD, par défaut, dit que les données doivent être protégées, que le sujet des données a le droit de recevoir cette protection pour ses données, de contrôler les données qui sont partagées. Mais le RGPD dit explicitement qu'il y a des utilisateurs légitimes pour les données et que cela devrait être équilibré vis-à-vis des droits à la vie privée.

Le RGPD lui-même énumère certaines de ces caractéristiques d'équilibre. C'est-à-dire qu'il vise spécifiquement que les utilisateurs, comme par exemple la protection des réseaux qui identifie et qui empêche une fraude et que le signalement du

problème aux forces de l'ordre sont donc les objectifs ou les usages légitimes, et que ce sont les personnes qui font cela qui devraient pouvoir accéder à ces données. La vraie question est comment trouver un équilibre et comment le faire.

Donc l'idée d'avoir un accès accrédité serait d'avoir une espèce de réseau que peuvent utiliser les personnes privées pour vérifier ces données. L'idée générale est qu'il faut qu'il y ait un cadre juridique où les parties sont obligées à respecter certaines exigences, à savoir de respecter le RGPD.

Par exemple dans ce type de cadre, il faudra que vous disiez pourquoi vous demandez d'accéder à un registre. Et cela devrait être enregistré. Donc on devrait prendre note de cela, il devrait y avoir l'intention pour laquelle vous demandez d'accéder à ces données.

Et puis, on dit également qu'il faut que vous ayez des données exclusivement pour la durée dans laquelle vous pourriez vous en servir, autrement qu'il faudrait supprimer les données, que vous ne pourriez pas conserver.

À travers tout cela il y aurait un cadre qui obligerait les parties à respecter toutes les lois.

Il faudrait également que cela soit audible. C'est-à-dire qu'on ne peut pas tout simplement dire la personne X peut maintenant

voir les données tout simplement. Il faudrait également que l'on puisse vérifier comment ils font leur travail, susceptible de passer par un audit. En fait qu'on devrait pouvoir contrôler ce que les personnes font avec ces données.

Les cadres d'accréditation devraient pouvoir être discutés. Mais le problème est que personne n'a établi ces cadres, parce que c'est quelque chose de tout neuf et il n'y a pas beaucoup d'expérience.

Une partie de la discussion pourrait donc porter sur cela pour la deuxième étape de notre travail. Ça prendrait un conseil juridique, ça prendrait quelques jours pour voir comment le flux de données pourrait se faire, il devrait y avoir un organisme d'accréditation qui révise les demandes d'accréditation des différents utilisateurs, qui octroie les accréditations, etc.

Il semblerait que le RGPD nous autorise à faire tout cela. Mais la grande question est : quel est l'équilibre, comment nous pourrions le faire pratiquement, comment satisfaire à toutes les exigences juridiques.

Mais s'il était possible de nous remettre à toutes ces exigences, de surmonter toutes ces exigences, il semblerait que l'on puisse voir, que l'on puisse trouver un moyen pour le faire.

Merci.

JONATHAN ZUCK: Merci. Yesim, est-ce que vous pouvez avancer dans mes diapositives. On passe à la suivante rapidement. Très bien.

Tout cela sera publié, mais il y a deux liens ici. J'ai utilisé mon propre Wiki cpwg pour préparer cette diapositive. On a quelques informations de Milton Mueller dans un article qui aborde ce qui a été dit. Il y a également un lien qui évalue l'impact du blocage de ces listes de blocage et de l'impact qui est associé. Donc cpwg.wiki/mueller et l'autre c'est cpwg.wiki/blacklisting. Vous pouvez consulter cela.

Oui, oui, bien sûr, c'est votre copain Milton Mueller. Il a publié cet article de blog très récemment, il a publié les données dont parlait Kathy. Et donc je voulais que tout le monde puisse y accéder.

Est-ce que vous voulez aborder cette question ? On vient d'avoir énormément d'information de la part de Greg.

Oui, c'est tout neuf, effectivement.

ALAN GREENBERG: Jonathan, votre micro est allumé.

FARZANEH BADII: Moi, je n'aime pas cette guerre de données. Ça peut être factuel, mais il se pourrait qu'il y ait une compagnie qui ait des registres en 2018, après trois mois de l'entrée en vigueur du RGPD et qui a dit qu'il avait beaucoup de problèmes de spam.

Et puis, il y avait une autre compagnie qui a dit que parce que le WHOIS avait été expurgé, en fait ce spam n'avait pas eu d'impact ou qu'il n'avait pas eu l'impact prévu, la quantité de cas n'avait pas augmenté tellement.

Et puis les données qui ont été divulguées par d'autres compagnies disant qu'en fait le hameçonnage s'était réduit.

Mais je ne pense pas qu'on doive mettre l'accent sur les sondages, sur les données, parce qu'alors on aurait d'autres sources de chiffres. Il faudrait que l'on revienne dessus d'ici un an ou deux pour voir lorsque les organisations neutres et indépendantes, qui n'ont pas d'enjeu ici, comment elles peuvent le résoudre.

Je ne suis pas sûre si les statistiques nous permettront de résoudre le problème. Je ne veux pas miner le travail que font les chercheurs de sécurité et dire : oui, c'est vrai que les cas de spam se sont réduits ou n'ont pas changé en raison de la réduction de WHOIS.

Et puis, sur Paul Vixie, on disait également qu'il y avait le WHOIS qui ne serait probablement pas nécessaire pour les attaques de cyber-sécurité.

Ca c'est mon avis personnel.

Lorsqu'on voit ces statistiques, il faut qu'on les voie plus objectivement, sans trop supprimer. Donc de notre côté dire en fait, ne pas dire leur travail n'est pas important et de votre côté de ne pas dire : c'est notre travail qui est le plus important, le WHOIS c'est une partie intégrale de la cyber-sécurité.

GREG AARON: Je pense qu'en fait, à l'ICANN, lorsqu'on travaille sur l'élaboration de politique, il faut que l'on se base sur des données, sur des faits. Parce que souvent on n'en a pas.

Donc en ce moment, on commence à consolider les données qui montrent par exemple la situation avant et après l'entrée en vigueur du RGPD. Ce n'est pas une bonne idée de tuer le facteur nécessairement, parce que dans ce cas-là, le facteur est la personne qui a les données.

D'une part, on voit que le dépistage s'est réduit, dans certains cas. Mais si vous voyez la quantité de messages de spam qui sont envoyés sur internet, on voit qu'il s'agit d'un chiffre constant. Et

on voit donc une activité qui a lieu, mais qui n'est pas toujours visible.

Donc les données sont importantes, je pense qu'on ne peut pas toujours juger les raisons pour lesquelles les personnes collectent et analysent les données.

[Coupure micro]

KATHY KLEIMAN: Oui, j'avais déjà demandé à Jonathan avant de venir s'il y avait des données à réaliser.

Je pense qu'on devrait peut-être prendre le temps, pas maintenant mais à un autre moment, de regarder les diapositives tous ensemble pour les évaluer.

Je voulais ajouter ici le nom d'Elliot Noss, c'est le président et co-fondateur d'une société dans la ville de Panama. Et deux mois après l'entrée en vigueur du RGPD, il nous a dit que la quantité de messages spam qui était envoyée s'était réduite, parce que le WHOIS était en train d'envoyer les noms de domaine, le WHOIS, les dates et échéances de tout cela, et qu'il y avait des millions de messages spam qui avaient été envoyés aux titulaires de noms de domaine.

Il a dit, Paul Vixie, qui était l'un des créateurs du DNS, de la recherche et de la cyber-sécurité, il nous a dit qu'en fait le WHOIS était désuet, qu'il n'était plus nécessaire pour de grandes quantités de recherches et de données de sécurité.

J'ai ici une question pour Laureen et pour Greg et pour vous tous. Et je vous demanderais qu'est-ce que c'est qu'un chercheur de cyber-sécurité. Parce que je pense que c'est ça le problème, c'est qu'on n'a pas de [référentiel] pour l'accréditation. Et c'est ça la question qu'il faut que l'on se pose pour les chercheurs de cyber-sécurité.

On a eu ce problème dans le passé. On devrait voir ce que font des groupes comme le groupe de travail anti-hameçonnage par exemple. Donc c'est eux qui vont faire de sorte que leurs personnes, leurs équipes soient tenues pour responsables, c'est à eux de le vérifier.

GREG AARON: Merci pour cette question Kathy. Nous nous sommes nous-mêmes penchés sur cette question. Nous avons essayé d'y répondre. On essayait de voir ce qu'étaient les responsables de la cyber-sécurité.

Pour nous, les personnes qui ont une responsabilité professionnelle de s'occuper de ce problème seraient en fait celles qui devraient être tenues pour responsables.

Mais ça pourrait ne pas être suffisamment restrictif lorsqu'on pense à l'accès aux données. Parce que l'accès aux données implique certaines responsabilités qui doivent être définies. Et certaines personnes, ou certaines entités, pourraient ne pas être à la hauteur du niveau des responsabilités et l'audit et la gestion de données pourraient être nécessaire pour cela.

Dans notre groupe de travail, on se demandait si on ne pourrait pas avoir un organisme d'accréditation pour l'examen des membres, sachant que les membres ont souvent des rapports avec eux.

Mais à un moment donné, on se dit il y aura des personnes qui n'auront pas la possibilité de gérer des données, de voir comment le faire. Et il faudrait que l'on définisse un processus de candidature et d'évaluation assez long pour pouvoir définir qui pourrait faire cela correctement et puis pour évaluer le travail de manière périodique et pour avoir la possibilité, bien sûr, de faire des audits par exemple.

Donc c'est un groupe assez grand, mais les personnes qui pourraient bien le faire ne sont pas tellement nombreuses.

COLLIN KURRE: Bonjour, je voulais faire une intervention toute courte. J'entends ce que vous dites par rapport au besoin d'avoir des données et au sein de la communauté on essaie de développer de nouveaux modèles d'impacts qui pourraient être utiles pour la sécurité, pour l'anonymisation, pour la vie privée, la confidentialité.

J'essaierai de partager ces informations, je les partagerai sur le chat puisqu'elles pourraient être utiles pour vous tous et pour cette discussion.

JONATHAN ZUCK: Oui, en fait, une partie de ce qui nous intéresse c'est la question de l'urgence pour cette question.

On a Olivier, Hadia, Holly, Humberto et Andrei. Et je vais devoir fermer la liste d'intervenants après ça.

OLIVIER CREPIN-LEBLOND: Merci Jonathan. Ma question en fait est : quelle est la fréquence avec laquelle on utilise ces données d'enregistrement pour pouvoir qualifier un nom de domaine comme étant une source de spam ou de malware.

J'aurai cru qu'il y ait d'autres moyens pour le faire. Donc peut-être qu'on devrait repenser à la manière de dépister les spams, qu'on pourrait avoir des mécanismes d'intelligence artificielle. Je sais… Mais peut-être que ce serait une possibilité, non ?

GREG AARON: Oui, merci de nous poser cette question. C'est vrai que le WHOIS est l'un des outils que l'on utilise, mais ce n'est pas le seul.

Il y a d'autres mécanismes comme le système pot de miel, il y a d'autres mécanismes qui vous permettent de trouver en fait le spam utilisant trois pots de miels par exemple. Parce qu'en fait, c'est ce que veulent les personnes qui envoient du spam, c'est là qu'on aura le crime, le délit.

Et souvent, cela indique qu'il y a un problème et quels sont les noms de domaine qui sont utilisés pour ce même but. Parce que leur but est de provoquer un dommage et de le faire rapidement.

Les personnes qui le font utilisent différents outils, ils appliquent différentes corrélations, ils appliquent l'intelligence artificielle, ils n'utilisent pas la chaine de block, le block chain.

OLIVIER CREPIN-LEBLOND: On ne pourra plus rebondir après, donc j'en profite maintenant. S'ils ont les données pour les serveurs de noms, de DNS et les

registres, avec ces deux là ne pourraient-ils pas établir une corrélation, un paradoxe ?

GREG AARON: Non. Parce que les délinquants vont enregistrer les noms de domaine dans des serveurs de noms qui ont l'air assez innocents, comme celui qui est fourni par défaut par le bureau d'enregistrement lorsque vous enregistrez un nom de domaine.

L'idée n'est pas de bloquer énormément de gens. Et puis ils utilisent des serveurs de noms lorsqu'ils sont prêts à commencer à agir. Et on le sait parce que les personnes regardent les fichiers de zone et ils envoient des requêtes aussi.

C'est un mécanisme d'escroquerie. Et c'est pour cela que l'on est conscient. On a commencé à le regarder parce que peut-être si l'on perdait des outils, les personnes commenceraient à le compenser autrement et cela pourrait ne pas être une bonne idée.

Il y a des opérateurs de réseau en ce moment qui commencent à bloquer des TLD entiers. Et les noms des TLD qui passent par leurs réseaux sont bloqués. Ce n'est pas une bonne idée.

L'idée est d'avoir l'acceptation universelle, etc., de garder tout ce que nous avons conquis. Mais on commence à voir s'il y a des

obligations qui pourraient être un peu plus précises et qui pourraient avoir des effets prévus qui soient uniques dans leur genre.

JONATHAN ZUCK: Merci, on va se limiter aux questions, parce qu'on aura nos propres débats à l'interne là-dessus à un autre moment. L'idée est de profiter des membres du panel, comme je l'ai dit tout à l'heure. Hadia ?

HADIA ELMINIAWI: J'ai une question à poser à Greg. À quel point avez-vous besoin de donner l'historique de vos recherches. Ou alors, avez-vous besoin de donner l'historique en tout cas ?

Je voulais également réitérer la question du RGPD et de l'intérêt légitime. Tout ce que j'allais dire était que l'article 48 du RGPD dit que pour empêcher la fraude, cela représente un intérêt légitime, et qu'un autre article établit des sécurités internet et des sécurités des réseaux. Merci. Donc par rapport aux données historiques, qu'en direz-vous ?

GREG AARON: Ces données historiques sont utiles dans certaines enquêtes profondes, surtout lorsqu'on doit savoir qui est responsable. Les

forces de l'ordre le font aussi. Dans certains cas, on voudrait savoir qui est le responsable, c'est ça qui est important. La majorité de ce qui se fait est en temps réel, et donc on dépend véritablement de données concrètes.

JONATHAN ZUCK: Merci beaucoup. Holly ?

HOLLY RAICHE: Donc quelques questions. Tout d'abord la manière dont vous avez décrit ce que vous faites, c'est potentiellement criminel, mais pas obligatoirement criminel, donc là je pense au RGPD, aux relations avec les forces de l'ordre.

Et en ce qui concerne les exceptions, de qui peut avoir accès aux données, et là on parlait des agences de maintien de l'ordre, quelle définition est assez large pour vous donner assez de protection, de latitudes, dans l'obtention des données pour pouvoir faire votre travail ?

Donc est-ce que vous pourriez rentrer dans l'exception de qui n'est pas supposé recevoir des données ? Donc est-ce que ça peut vous limiter dans votre travail ?

Les agences de forces de l'ordre s'attaquent donc aux criminels, mais est-ce qu'elles travaillent également dans le domaine de la protection des consommateurs par exemple ?

Ça dépend un petit peu de l'interprétation du RGPD. Donc c'est une question d'interprétation, de définition des exceptions. Ça, ça me parait très important. Je vois que Kathy sourit…

JONATHAN ZUCK: Oui, si vous le permettez, je vais poser plusieurs questions à la suite de la vôtre.

Les exceptions dont vous parlez, est-ce que vous pensez que le RGPD doit prendre en compte la participation ?

GREG AARON: Oui, comme je l'ai mentionné, la plupart de ces fonctions ne sont pas des fonctions de forces de l'ordre. Ce sont des fonctions des personnes qui opèrent les réseaux.

Donc les forces de l'ordre peuvent poursuivre les criminels, mais par exemple, une banque doit bien comprendre qui sont ses clients, protéger ses clients, gérer les paiements et ainsi de suite.

JONATHAN ZUCK: Donc est-ce que le RGPD comprend cette distinction, prend en compte cette distinction ?

GREG AARON: Il me semble que c'est assez explicite et clair, ça a été conçu, le RGPD, pour permettre l'accès aux forces de l'ordre. Le RGPD, vous savez, il y a des lois parallèles et séparées pour les forces de l'ordre, pour gérer le respect de la vie privée par exemple, le rôle de l'industrie je crois et du secteur industriel est assez clair.

LAUREEN KAPLIN: Ce n'est pas seulement les forces de l'ordre qui peuvent demander l'accès dans le cadre du RGPD.

HOLLY RAICHE: Je vais demander à Jonathan d'interpréter ce que j'ai dit, parce que je ne crois pas que vous ayez compris ma question.

JONATHAN ZUCK: Il pense que le RGPD prend en compte les forces de l'ordre, voilà sa réponse.

Je voulais donner la parole à Humberto.

HUMBERTO CARRASCO: Merci beaucoup. Je serais très bref. Question et commentaire. Il me semble que nous avons un contraste entre ces deux positions, au niveau de la droite et de la gauche, côté droit et côté gauche.

En ce qui concerne les données, je crois qu'il y a une erreur dans le point de vue. Parce que Kathy mentionnait des informations au sujet de l'amoindrissement d'un nombre plus limité d'hameçonnages par exemple.

Mais d'un autre côté, il y a des plaintes de Greg, parce que parfois il est impossible d'obtenir les données. Donc c'est un aspect préventif qui existe actuellement.

On n'est pas en mesure d'accéder aux données. En ce moment il y a des crimes qui sont supposés être commis, ça c'est une réaction.

C'est pour cela que je pense qu'il y a un problème ici. On parle de deux différents aspects et ça peut être une erreur.

JONATHAN ZUCK: Merci beaucoup. Je vais donner le dernier mot à Andrei.

ANDREI KOLESNIKOV: Bon, moi j'ai travaillé pour des entreprises privées qui travaillent sur l'hameçonnage, sur les utilisations malfaisantes, et au

quotidien, on travaille avec un bureau d'enregistrement. L'entreprise en moyenne a 25 ans, ce sont des jeunes employés qui ont 25 ans à peu près et qui essaient de protéger tout le monde sur l'internet. Mais les clients sont des banques, des compagnies aériennes, des grosses sociétés. Et ils doivent gérer donc le WHOIS, et grâce au bureau d'enregistrement, qui est américain, la plupart des demandes… C'est une entreprise russe, mais 8 % des demandes passent par GoDaddy, les gros bureaux d'enregistrement américains. Et les noms de domaine malfaisants sont retirés.

Mais ils voient déjà l'impact des changements avec le RGPD, parce que les réactions sont plus lentes, le temps de réaction est plus long.

Donc je ne dis pas que tout pose problème, mais il y a une différence qui existe, c'est tout ce que je voulais dire au niveau des faits.

KATHY KLEIMAN: Oui, c'est une observation tout à fait juste. Le temps de réaction est plus bas parce qu'avec le RGPD, le bureau d'enregistrement doit évaluer les besoins de la demande et les droits qui existent également. Donc une intervention humaine qui est effectuée.

Olivier, il n'y a pas encore d'intelligence artificielle, on y travaille, mais ce sont des personnes, des employés qui travaillent à cela. Ce n'est pas automatisé. Et donc c'est plus lent.

Je pense que ça va s'accélérer avec l'accélération des compétences des employés.

FARZANEH BADII: Et la personne faisant la demande doit être responsable, c'est pour cela…

ANDREI KOLESNIKOV: Même s'il y a des lettres officielles, qui sont envoyées, qui sont signées ? C'est ça ?

FARZANEH BADII: Ca peut être urgent en effet, ça peut être expédié, et il y a une possibilité d'avoir une procédure plus urgente, plus rapide.

JONATHAN ZUCK: Je crois que nous avons conclu tout le temps… Ça fait des années qu'on parle de cela, ça prend beaucoup de temps de présenter la situation d'aujourd'hui.

Mais j'aimerais remercier les participants à cette table ronde, les participantes. Je crois qu'on a beaucoup appris ce matin.

On va continuer le débat et envisager les prochaines étapes de l'EPDP. Donc j'apprécie beaucoup cela.

FARZANEH BADII: Oui, merci. J'apprécie beaucoup cette invitation, c'était très intéressant de présenter pour nous et de travailler avec At-Large. On a été heureux de présenter notre perspective, c'est très important que vous soyez bien au courant.

JONATHAN ZUCK: Merci beaucoup aux interprètes, aux personnels techniques, on apprécie tout cela, merci. Et c'est l'heure du déjeuner.

Et la prochaine séance commence dans quelques minutes, dans 5 minutes, donc on n'a pas de pause de 15 minutes. On va avoir un déjeuner de travail à partir de 12 h 15. Donc restez dans la salle.

**[FIN DE LA TRANSCRIPTION]**