DUBLIN – Sessão aberta do grupo de trabalho de segurança pública do GAC
Segunda-feira, 19 de outubro de 2015 – 15h00 às 16h30 IST
ICANN54 | Dublin, Irlanda

FALANTE DESCONHECIDO: Estamos falando, nessa sessão, vamos falar do tema da segurança pública, então eu acho que pelo tipo de tema que vamos tratar, seria bom que os senhores se aproximassem aqui nas primeiras fileiras e não fiquem tão longe.

ALICE MUNYUA: Boa tarde para todos. É uma sala tão grande, por favor pedimos que se aproximem para que esta seja uma reunião mais íntima. Sabemos que estamos concorrendo com outras sessões (CCWG), mas esta é muito importante. Então gostaríamos que sentassem mais perto de nós, obrigado. Boa tarde, eu sou a (Alice Munyua). Esta é uma reunião do (Comitê Assessor Governamental), especificamente do grupo de trabalho sobre segurança pública deste comitê. Que é um grupo de trabalho foi estabelecido segundo o princípio 27 do (GAC) e se centra nossas políticas e procedimentos da (ICANN), que tem a ver com a política pública.

Foi criado oficialmente em (Buenos Aires) os termos de referência foram oficialmente apoiados pelo (GAC) e os

principais membros são representantes de organismo de aplicação da lei, países e diferentes públicos de defesa de consumidores, de proteção dos consumidores, grupo de aplicação das leis, que combatem o delito, o crime e outros organismos dependendo da segurança pública. Se querem ter um detalhe maior em termos de referência, desse grupo de trabalho do (GAC), podem acessar o website do (GAC) aonde há um espaço de trabalho aonde estão esses termos.

É um tema bastante extenso mas vamos apresentar os palestrantes. Eu sou co-presidente desse grupo de trabalho em representação da (Comissão da União Africana), eu sou (Alice Munyua).

WANAWIT AHKUPUTRA: (Wanawit Ahkuputra) da (Tailândia), eu também sou vice-presidente do (GAC).

LAUREEN KAPIN: (Laureen Kapin), dos (Estados Unidos) da (Comissão Federal de Comercio), centrada na proteção dos consumidores.

BOBBY FLAIM: (Bobby Flaim), do (FBI).

JOHN CARR: (John Carr), representa a (Comissão das Entidades de Beneficência Britânica das Crianças) sobre a segurança infantil na internet.

CATHRIN BAUER-BULST: (Cathrin Bauer-Bulst), da (Comissão Européia) e líder da equipe que lidera luta contra o cyber crime, delito sexual.

GREGORY MOUNIER: Eu sou o (Gregory Mounier), da (Europa) da agência da aplicação da Lei Europeia, nos ocupando do (Centro de Cybercrime Europeu).

NICK SHOREY: Eu sou membro do (Reino Unido), do ministério de cultura, mídia e esportes.

JON FLAHERTY: Eu faço parte da unidade nacional de CyberDelito, sou (Jon Flaherty).

ALICE MUNYUA: Obrigado. Palestrantes muito distintos e esperamos ter um debate muito interessante. Vamos começar, um tema bastante completo, em primeiro lugar vamos receber um relatório

atualizado sobre o que o grupo de trabalho de segurança pública realizou desde (Buenos Aires), e depois, também, vamos falar do (WHOIS) e das leis de proteção dos dados da (Europa). Vamos ter também exemplo de (Alice Munyua) da (Europol) e vamos ver um guia de trabalho sobre o trabalho que vai realizar o grupo de segurança pública a nível nacional, em coordenação com o nível nacional e também especificação 11 do marco de segurança dos (gTLD) [00:04:17], e uma apresentação sobre a exploração infantil e as cadeias de (gTLD) novas. Então vamos passar a palavra a (Laureen Kapin) para que faça a atualização sobre o trabalho que a equipe realizou até agora.

LAUREEN KAPIN: Em primeiro lugar bem-vindo a todos, obrigado por estar aqui nessa enorme sala. Se quiserem se aproximar prometemos que não vamos ser agressivos nem ferozes, e agradeceríamos que se sentem mais próximo de nós. Se não me escutam ou tiverem alguma dificuldade em entender, eu vou tentar falar mais forte, mais devagar ou mais claro. Há várias apresentações e depois de cada uma vamos ter um período de perguntas e respostas. Mas se não tem a chance de fazer a pergunta, por favor, se sintam livres de nos perguntar de forma individual e nós vamos dar essa resposta. (Bobby Flaim), o meu colega, vai conduzir a discussão desse tema junto comigo e vamos estar controlando o tempo. Então vamos começar.

Mais uma vez, esse é o grupo de trabalho de segurança pública, queremos começar dando um pouco de contexto, de informação de contexto. Se bem, nosso grupo de trabalho de segurança é novo, as pessoas que estiveram pedindo, trabalhando pela segurança pública, participaram também nesse tipo de trabalho desde há bastante tempo, há mais de 10 anos. Durante esse tempo, estivemos promovendo diferentes questões, por exemplo, a criação de medidas de proteção para os consumidores no processo dos novos (gTLDS) e nesse sentido, temos uma expressão formal.

Foram propostas no assessoramento do (GAC) e no trabalho recente, também, nós entramos, em ter a certeza de que o (Board) aceite em implementar essas medidas de proteção. Então, tudo isso foi sendo desenvolvido durante algum tempo, e (Bobby) vai falar na melhora das disposições dos contratos.

ROBERT FLAIM: Quando entramos na criação do grupo de trabalho de segurança pública, os senhores devem lembrar que havia uma recomendação da aplicação da lei, pelo ano 2009 a 2013, continuamos trabalhando nessa direção com as especificações e com os grupo de trabalho.

Falamos da especificação do (WHOIS), o grupo de trabalho de serviços de privacidade e proxy, ou representação, e outros

temas que se vinculam com os nomes de domínio, com a segurança pública. Também, os senhores podem ver que há uma melhora no termo de (WHOIS), isso foi no começo. E nossos colegas vão dar uma explicação mais detalhada de porque é tão importante a exatidão do (WHOIS) para o trabalho que realizamos como funcionário da segurança pública, e como podemos conseguir um equilíbrio com as leis de proteção de dados europeias e também das políticas vinculadas com a segurança pública com relação a exatidão do (WHOIS).

Como os senhores sabem, isso está sendo feito há 10 anos já, e são temas constantes e que fazem parte de nosso trabalho.

LAUREEN KAPIN: Então, o que podemos extrair da primeira sessão é que sob o comitê assessor governamental, somos um grupo novo de trabalho. Já desempenhamos nossa função nesta área durante um longo tempo. Embora agora temos um papel mais formal para comunicar todo esse trabalho de incidência sob o guarda-chuva do (GAC).

O trabalho mais recente, eu quero que vocês saibam, como disse (Alice) no começo, que se ele se interessa ver o trabalho mais recente realizado, o website do (GAC) é onde essa informação está. Todos os grupos de trabalho do (GAC), de fato, tem um espaço público no website. Não é necessário ser

membro do (GAC) para acessar essa informação. Aqui está o link, como veem na tela, e o website também inclui informação sobre os representantes desse grupo, e os diferentes comentários que nós fomos apresentados. Esse foi o lugar a que têm que recorrer, se forem ler por conta própria, mais informações sobre nós. Vamos agora apresentar as partes mais destacadas do trabalho feito de forma recente. (Bobby), quero falar sobre o (RA) de 2013, porque sei que é um tema que você conhece muito bem.

ROBERT FLAIM: Sim, Quando se assinou o (RA) de 2013, houveram alguns elementos que surgiram daí, e estabeleceram as bases para o trabalho futuro. Uma delas era a especificação o (WHOIS), um dos trabalhos onde se faria a revisão. Então, agora em 2015, foi debatida a forma de como tratar a indicação do (WHOIS), que faz parte do (RA) (ICANN), como podia ser melhorada. Então, a (ICANN) e os registradores tinham algumas inquietações, porque receberam comentários.

Também se abriu de fato um período de comentário público, então o grupo de trabalho também fez suas contribuições através de comentários. Fizemos contribuições através do grupo de trabalho de serviço de proxy e privacidade, e também contribuímos do ponto de vista do (WHOIS) de próxima geração,

que também estava submetido a um período de comentário público. Então, este grupo de segurança pública agora faz parte do (GAC) e se centra nessas questões muito importantes. Se bem, nós temos muitos representantes da aplicação da lei, nosso grupo também estava aberto a outros funcionários do governo, como a agencia de (Laureen), que se ocupa da proteção dos consumidores, a aplicação também de medidas no âmbito civil e também a (FDA), por exemplo, dos (Estados Unidos) e suas equivalências em outras partes do mundo.

Esse tipo de organizações que podem ter um impacto na segurança pública. Por isso, vão ver que há comentários que foram elaborados através de todos os representantes no grupo de trabalho. Eu acho que o que temos aqui, em primeiro lugar, é a revisão da especificação da exatidão do (WHOIS). Antes a reunião de (Buenos Aires), os registradores fizeram comentários. De fato, fizemos uma sessão pública ali, e nosso interesse era tratar de ter mais especificidade sobre os comentários manifestados. Houveram alguns prazos utilizados pelos registradores e também uma linguagem qualificada, quando se falava de substanciar. Não estamos tentar ter uma definição mais exata do que estávamos falando, naquela especificação do (WHOIS), porque isto era uma coisa que sabíamos que íamos utilizar, e era bom ter certeza.

LAUREEN KAPIN: O (RAA) de 2013 marca algumas obrigações para os registradores, tem que verificar a exatidão de informação, e há um tempo, um período durante o qual tem que fazer essa verificação e atuar nesse sentido. E há alguma das perguntas no qual nos centramos, tem a ver com o que acontece se não temos uma resposta da pessoa que se supõe que tem que ter essa informação de contato. Em outra área, na qual apresentamos um comentário, tem a ver com o serviço de privacidade de proxy e representação. Isso foi feito com o grupo de trabalho que se ocupa desse problema.

Esse serviço, essencialmente, permite as entidades mascarar a sua informação. E podem existir motivos pelo qual devam fazer isso. E também, devem surgir inquietações, preocupações, quando isso acontece. Então, o grupo de trabalho em segurança pública apresentou um comentário a respeito de alguma das questões que apareciam no relatório que foi apresentado. Pensávamos que tinha que ser feita uma diferença entre disponibilidade desses serviços e, mais especificamente, se há um contato pelo qual se oferecem esses serviços comerciais, ou seja, se vocês, consumidores, pedem que deem sua informação financeira, número de cartão de crédito, informação bancária. Na verdade, têm direito, também, de saber com quem estão tratando. Em consequência, o serviço de proxy não deveriam estar presentes nessa situação.

Também, fazemos ênfase na necessidade da transparência e a responsabilidade para os provedores ou fornecedores de serviço de privacidade proxy, quando uma entidade de aplicação da lei está por trás do domínio que pode ser objeto de investigação. Essas solicitações têm que ser comandadas ou trabalhadas de forma confidencial, tal como, ou segundo o permitam as leis locais, porque os organismos de aplicação da lei estão interessados em que todos os fatos vinculados à investigação permaneçam sendo confidenciais, para que não se de a conhecer e desapareçam as provas e os diferentes bens. Desculpem, não estava apertando o botão certo.

Também fizemos comentários sobre o serviço do (WHOIS) de próxima geração. (Cathrin) vai se estender sobre este tema, que é uma questão muito complicada, na verdade, que tem a ver com o que funciona e o que não funciona com o (WHOIS). Se deveria existir um sistema subsequente, e no caso, surge todo uma série de perguntas sobre como deveria ser o sistema, quem deveria ter acesso à informação, e no nosso comentário, este relatório prelimitar, o que nós destacamos é que é uma parte complicada. E pela outra, tem que existir um equilíbrio que respeite o direito dos consumidores, mantenha a segurança do público, e também garanta a proteção dos dados pessoais dos usuários de internet. Portanto, aqui, queremos um equilíbrio de todos esses pontos de vista, e que as comunicações se

mantenham abertas, porque isto não é uma coisa irreconciliável. Nos (Estados Unidos), na comissão federal de governo, se ocupa tanto das questões dos consumidores, de proteção dos consumidores, como também de privacidade, tudo sob um mesmo organismo. Então não há inimizade ali. É importante ter um equilíbrio entre esses 2 aspectos. Esse é o recado principal que queremos transmitir, porque essa área é muito importante para nós.

ROBERT FLAIM: O representante da agencia nacional do crime vai falar sobre a especificação 11, que o quadro de segurança do acordo de registros, que se originou através do comunicado e assessoria do (GAC), em (Pequim), faz uns 2 anos e meio. Então (John) esteve trabalhando com os grupos de trabalho, junto com os registros, para estabelecer práticas voluntárias para ver como se podia trabalhar perante esses caso de phishing, de softwares maliciosos, de exploração infantil, para termos um acordo e poder trabalhar de maneira eficaz com esse tipo de abusos ou delitos. Isso é simplesmente o que eu comento como um resumo, depois vamos falar mais sobre o tema.

LAUREEN KAPIN: E, qual é o nosso trabalho para o futuro? Nós esperamos ter a representação do grupo de trabalho que se encarrega das

questões de competência, eleição do consumidor, confiança do consumidor, que vai ter um papel essencial para considerar todos os aspectos nessas áreas, além da exatidão do (WHOIS), em relação à informação dos domínios, algo também importante.

ROBERT FLAIM: Sim, há outra coisa que é muito importante, que quando vemos os abusos e atribuições, vemos também a outra cara do sistema, do (DNS), que é o sistema de endereços (IP), gerenciado pelo registro nacional de internet, e fora da (ICANN), a (ASO), organização, tem os recursos numéricos, e está tentando trabalhar nessas questões com os acordos de acreditação dos registradores, e está pedindo que façamos o mesmo. Os (RIR) são 5, então trabalhamos com eles, para poder desenvolver uma política global, para que todos tenham o mesmo tipo de práticas voluntárias, que garantam exatidão do (WHOIS), e também o processo de pesquisa de antecedentes de cada um.

LAUREEN KAPIN: Com relação ao trabalho do grupo sobre segurança pública, nos interessa ter maior participação e colaboração com outros grupos de trabalho dentro da (ICANN), queremos estender a nossa chegada a outros autores governamentais, a todos os países presentes, há muitíssimos organismos com pessoas que

são extremamente conhecedoras desses temas, pessoas que podem ser parceiros para nós, e servir-nos de guia. E também há outras partes interessadas dentro da (ICANN), que tem muitíssima informação que para nós é extremamente importante, e nós vamos tentar chegar a eles, aproximar-nos para beneficiar-nos também desse guia e dessa sabedoria que existe na comunidade da (ICANN). Essa é uma visão geral do tipo de trabalho que estivemos desenvolvendo no grupo de trabalho. Esperemos continuar avançando no futuro. Quero saber se há algum tipo de pergunta sobre os temas mencionados, porque seria um bom momento para utilizar os microfones disponíveis na sala. Há outras apresentações, mas achamos que seria mais organizado se tomássemos perguntas depois de cada apresentação.

ALICE MUNYUA: Muito obrigada aos 2. Há microfones aqui na frente, então quem quiser fazer perguntas, por favor, diga seu nome.

VOLKER GREIMANN: (Volker Greimann), sou do conselho da (GNSO) de partes interessadas, registradores, desde que existimos que estamos trabalhando sobre a exatidão do (WHOIS). Mas, é muito interessante, mas tem contrapontos esse tema da privacidade. Então, queria saber se esse grupo de trabalho, com seus

antecedentes, também pode lidar com as implicações de privacidade e matéria de (WHOIS), a respeito dos usuários de nome de domínio, e ver como se pode proteger a privacidade dos dados dos usuários. Realmente, o que vocês precisam é um dado de outro tipo de sistema, que possam chegar a necessitar.

ROBERT FLAIM: Acho que muitas das perguntas serão respondidas quando a (Cathrin) falar sobre a proteção de dados na (Europa), e outras questões, que geram desafios para as próximas gerações conseguirem um equilíbrio entre o que funciona e o que não funciona. Não quero roubar o momento de atenção à sua apresentação, mas vamos responder a pergunta para abordar esses problemas.

ARTHUR ZONNENBERG: Sou (Arthur Zonnenberg), trabalho para um registrador holandês creditado pela (ICANN) e também, além desse ponto da união europeia, quais seriam as questões a tratar pela comissão de comércio, em matéria de privacidade a respeito da união europeia, quero saber quais são os fundamentos, por exemplo, a respeito do que falaram quando alguém dá os dados de seu cartão. Bom, isso dá direito de saber quem está por trás do website, com quem estou tratando, e no caso de uma loja online, seria lógico, para receber o serviço. Mas, se for o ativista

que trabalha contra determinados interesses, talvez queira manter sua privacidade. Então, vamos ter que respeitar sua privacidade, para que possam apoiar as pessoas que trabalham em prol de determinados interesses. É claro que os (Estados Unidos) sempre foi objeto ou alvo de crítica, porque sempre está em consonância com esses interesses. Então, eu queria saber se o fato de eu dar os meus detalhes do cartão de crédito me dá direito de saber os meus direitos pessoais.

LAUREN KAPIN: Há diferentes opiniões acerca dessa questão. Do ponto de vista da proteção do consumidor, se alguém está passando dados sensíveis e, é claro que você tem o direito de estar em desacordo, consideramos que temos direitos a ver com quem estamos tratando, e entendo as questões que tem a ver com os grupos que defendem determinadas causas, podem defender seus próprios pontos de vista, mas se tratam com informação sensível. Então consideramos que o público tem direito a ver com quem estão tratando, e essa é uma perspectiva porque somos conscientes de que nem todos compartilham esse ponto de vista.

GLORIA: Oi, não tenho pergunta. Tenho 1 comentário. Isto decorre do (GAC), mas aqui temos integrantes dos organismos de

cumprimento da lei, e integrantes em outros países que não participaram nesses procedimentos, e eu queria que participassem mais. Sou (Gloria), da (Uganda).

LEE HIBBARD: Sou (Lee Hibbard), do conselho da (Europa) em (Strasburgo), (França). Estou em uma organização que emprega 47 países, temos a convenção de (Budapest), e também questões sobre venda de medicamentos online, acerca do cuidado da saúde, das farmácias na internet. Então, acho que o conselho da (Europa) também tem que estar nesse mapa. Somos membros observadores, e no (GAC), gostaríamos de colaborar com a experiência e conhecimento do conselho da (Europa). Temos muita coisa a compartilhar com vocês e o faremos na lista de e-mails, onde já enviamos comentários. Em junho desse ano, os 47 países concordaram com uma nova resolução à (ICANN) sobre direitos humanos e estado de direito. Isso é pra garantir que a (ICANN) respeite os procedimentos e os direitos humanos em suas políticas de segmento. (Peter) tem a palavra.

PETER KIMPIAN: Boa tarde, represento o (DPD) do conselho da (Europa). É um organismo assessor da convenção 108, estou muito contente de estar aqui. Também, como meu colega, quero oferecer cooperação, colaborar com nossas experiências, e outras

questões relativas. Como disse minha colega dos (Estados Unidos), a palavra certa seria equilíbrio, não há questões irreconciliáveis. O melhor, e digo, como funcionário que trabalha numa autoridade de proteção de dados na união europeia, o melhor é sentar e conversar abertamente, discutir perguntas, questões, e definir as melhores soluções possíveis. Estamos dispostos a fazê-lo, estamos muito contentes de fazê-lo, de estar aqui e o nosso trabalho é de experiência, de muito trabalho, etc.

ALICE MUNYUA: Obrigado, conselho da (Europa). Vamos continuar fazendo perguntas aos membros do (GAC).

DAVID CAKE: Quero fazer 2 comentários, um específico e outro geral. O específico é que recebemos suas contribuições do grupo de trabalho (PPSAI), e tenham presente que consideramos isso, mas tudo isso surgiu quando já tínhamos debatido os sistemas em profundidade, e tivemos 60 mil respostas do público em geral. Então, vocês, suas contribuições chegaram numa instancia tardia. Tem que se esforçar mais um pouco e participar numa instancia mais precoce. Entendo que é um grupo novo, mas queria informar-lhes que talvez seja mais necessária a participação de vocês.

Tenho um comentário mais geral. Os organismos encarregados da proteção de dados e leis, temos esse organismo que se dedicam à segurança pública, e à proteção de dados. Então, mas eles não estão aqui no grupo. Consideramos então que eles têm uma voz muito contundente para ser ouvida aqui, uma parte do cumprimento da lei. Então é tão importante que vocês sejam percebidos como um grupo que representa a segurança pública e cumprimento da lei. Então, os encorajo que sejam mais inclusivos, de forma mais ativa, principalmente para incluir os organismos que tem a ver com segurança pública e proteção de dados.

ALICE MUNYUA: Obrigado, (David). Nós não somos um grupo que faz lobby.

DAVID CAKE: Sim, entendo, mas vocês têm que garantir, incluir todas as vozes, e tem que procurar essas outras vozes.

ALICE MUNYUA: Levamos muito a sérios esses comentários. Ontem, falamos acerca disto quando esteve presente nos debates da (GNSO), surgiu o tema de que o (GAC) deve participar com mais antecedência, principalmente no (PDP). Para esse efeito, estamos trabalhando para conseguir esse objetivo, mas temos

que entender como que funciona a nossa vida. Temos que pedir, procurar as partes interessadas, peço desculpas se algumas coisas chegam mais tarde, vamos trabalhar mais de perto nos processos, temos membros que vão se unir nos diferentes grupos de trabalho para fazer contribuições como grupo de trabalho do (GAC). Obrigada pelos seus comentários.

DAVID CAKE: Eu entendo que esse grupo é novo, e alguns grupos de trabalho são anteriores, não tenho a máquina do tempo para poder trabalhar desde o início. Parabenizo a todos do grupo de coordenação (GAC)-(GNSO). A (GNSO) quer receber suas contribuições, e quanto mais precoce, melhor será para todos. Em especial, aqueles que tem que ver com um sistema X, se chega rapidamente , isso ajudaria a marcar o rumo que pode chegar até um grupo de trabalho. Seria mais fácil para todos que isso acontecesse com a devida antecedência para ajudar-nos a ter a resposta certa para nossas conclusões.

ALICE MUNYUA: Obrigado, (David).

AMADOU LY: Bom dia, sou (Amadou Ly), sou membro do colégio de regulamentação de telecomunicações da república de

(Senegal). Parabenizo e agradeço a todos os membros do grupo de trabalho e tenho muitas perguntas a respeito da segurança e confidencialidade. A segurança das informações, exemplo de países como o meu, (Senegal), país africano, que até agora, há pessoas que trabalham dentro das administrações e governos, que ainda utilizam endereços de e-mail genéricos, (Yahoo, Gmail), e o nível de internet não é suficiente, como para ter (.gov) no nosso país. Há executivos que trabalham em todas as administrações, e são correios eletrônicos que têm desde que eram estudantes, desde que começaram a trabalhar. Esse tema é fundamental. A internet hoje chegou a um nível insuspeitado para que pessoas trabalhem com dados confidenciais nas presidências, nas repúblicas, nas administrações de alto nível e não percebem que estão utilizando (Yahoo e Gmail). Podemos proteger essas pessoas sem deixar de trabalhar com as bases de dados?

As pessoas que tem ou que manejam base de dados muito importantes, com dados muito confidenciais, e não percebem que estão trabalhando com dados muito importantes para os estados, informação alojada em outros países, porque não há políticas de gestão de mensagens, e isso é mais evidente ainda quando vemos no cartão do convite de pessoas que o endereço é (Yahoo) ou (Hotmail). O tema é saber com quem trabalham os senhores. Temos que trabalhar com essas pessoas que

manejam dados importantes e que não estão num nível suficiente.

Esta é a responsabilidade, onde está o limite, o trabalho que os senhores podem fazer de forma conjunta para poder dar segurança, porque podemos criar firewalls, qualquer coisa, mais a nível da base de dados, não temos certeza das transações, não sabemos qual é o caminho que cumpre a informação, então aí eu acho que temos um problema muito grave. Acho que devemos dar reflexão e trabalho de forma conjunta com as diferentes pessoas, setores, que interagem para que os dados possam continuar seu caminho, obrigado.

LAUREEN KAPIN: Eu acho que o senhor mencionou questões muito importantes, e definitivamente a que devemos fazer material de educação e informação para que o público saiba como ter segurança na internet, e como considerar correios eletrônicos (Gmail, Yahoo), inclusive, se falam que são do governo, e não vou poder responder todas as perguntas que o senhor fez, porque são muito complexas, mas sei sim que há uma necessidade real de educar o público para que seja cauteloso quando utiliza a internet, seja porque estão comprando um produto, num lugar de encontros na internet, ou porque receberam um correio eletrônico que ganharam em concurso porque alguém está

apaixonado por eles e precisam de dinheiro à vista com muita urgência, todas essas são questões muito importantes que temos que levar em conta, sobre as quais temos que trabalhar, porque a vida das pessoas podem ser afetadas de forma negativa por aqueles que querem se aproveitar deles através da internet.

AMADOU LY: Muito obrigado pela resposta. O que me pergunto aqui é, como nós, na (ICANN), trabalhamos com os grandes autores, (Google), e as grandes empresas que manejam nas bases de dados o que fazemos com eles de forma geral, para tratar de fazer com que o manejo dessas base de dados seja mais seguro. Eu concordo com a senhora de que as pessoas são responsáveis pelos seus atos, mas também é uma responsabilidade de parte de todas as grandes empresas que manejam a base de dados e que também juntam todas as transações. Estou de acordo com vocês que temos que estar alerta, mas quero saber quais são as medidas que poderíamos chegar a tomar para tentar assegurar essas transações. Esta era a intenção de minha pergunta, obrigado.

ALICE MUNYUA: Muito bem, temos que passar à seguinte sessão, então muito obrigado pelos comentários. A colega da comissão europeia, (Cathrin), vai falar justamente de alguns desses assuntos, vai

falar de (WHOIS), das leis de proteção de dados, e com certeza, vamos ter vários exemplos que nos apresentem como tratar esse tipo de temas, assuntos, em alguns países africanos e em outros lugares. (Cathrin) tem a palavra.

CATHRIN BAUER-BULST: Eu não sei como posso solucionar os problemas de todo mundo, mas gosto de ver que há interesse sobre esse tema. Como já disse (Laureen), é necessário chegar a um equilíbrio, e na minha experiência nesse tipo de debates, sempre houve um benefício quando se começa por uma base de evidências sólidas, então, quero fazer uma introdução muito breve sobre as normas da união europeia que regem a proteção de dados, e as consequências que elas têm para processos como, por exemplo o redesenho do (WHOIS). Quando eu me preparava para armar essa apresentação, comecei a olhar para trás, a história de longa data do (WHOIS), toda a discussão em termos gerais, e agora falamos muito de prestação de contas e responsabilidade, e essa responsabilidade que é necessária também é um assunto que falamos há muito tempo. Há 2 mil anos, na república de (Platão), se falava na responsabilidade, e ali estava a história de um pastor que estava junto ao rebanho na colina, e chega a uma cova, onde encontra um anel.

E quando coloca esse anel no dedo, se torna invisível. Por essa invisibilidade, vai até a corte, mata o rei, tem relações com a rainha, e toma a posse do governo. Nesta obra de (Platão), a parábola é que aqui é uma questão de prestação de contas e responsabilidade. (Platão) e seus amigos chegaram à conclusão de que a responsabilidade é uma sensação de uma construção moral, então quando a pessoa sente que tiram a habilidade dos outros de ver, não é incentivo para trabalhar de forma responsável. Então, falemos deste assunto à partir dessa parábola e da história do anel deste pastor.

Então, eu acho que não necessariamente temos que fazer uma concessão reciproca. Eu trabalho no cyber-delito e estou, de fato, na vanguarda da defesa da proteção dos dados, porque eu quero evitar que roubem essa identidade dos dados, as credenciais, as imagem de crianças que utilizam para o abuso sexual. Estamos trabalhando para permitir os organismos de aplicação da lei, prever este tipo de delito, se proteger aqueles que sofrem, que são vítimas dele. Eu quero representar ambas as visões, então vou fazer um resumo breve como os mecanismos de aplicação da lei trabalham aqui, e o interesse central que tem. Na afirmação de compromissos da (ICANN), reassumida a obrigação de manter um acesso público, irrestrito e oportuno à informação do (WHOIS) completa e exata, e que é necessário revisar a eficácia da política do (WHOIS) a cada 3

anos. O (GAC), no comunicado de 2007, estabeleceu alguns princípios com respeito o que devia fazer o (WHOIS) para ajudar a aplicação da lei, as investigações, e também para ajudar a aplicar as leis nacionais e internacionais, e também para combater os usos abusivos, e também para ajudar as empresas e outras entidades a combater a fraude e salvaguardar os interesses do público.

Então, voltemos aos aspectos fundamentais da perspectiva europeia. A proteção e segurança dos dados são um direito fundamental que estão na carta orgânica da união europeia, artigos 6 , 7 e 8, que basicamente garante que todos tem o direito à liberdade, segurança, e que todas as pessoas têm o direito a serem respeitadas nas suas vidas privadas e familiares, nos seus lares e comunicações. Essa carta da união europeia é moderna no sentido de que contém direitos pertinentes à sociedade digital, e garante também a bioética e a transparência, mas também é mais específica com a proteção dos dados. No artigo 8, faz referência à proteção dos dados pessoais. Diz que devem ser processados de forma equitativa, e que todos tem direito a acessar informações reunidas sobre sua pessoa, e para ter a certeza de que essa informação seja certa.

Esses são direitos-chave numa sociedade democrática e não são absolutos, então, cada um desses direitos, o direito à segurança, privacidade e proteção dos dados têm que se equilibrar entre si,

e também com outros direitos fundamentais. Agora, quero, de forma breve, destacar as disposições mais importantes da nossa diretriz ou diretiva, que é o texto jurídico mais importante, com respeito aos dados na união europeia. A diretiva normativa faz referência à proteção dos indivíduos, com respeito ao processamento dos dados pessoais.

Escutamos muitas preocupações no passado, sob o fato de que não existia uma voz unificada na (Europa), nesse assunto. Os requerimentos de proteção de dados. E o tema principal aqui é que a base de tudo era uma diretiva que um tipo de instrumento legislativo específico que é vinculante quanto a suas metas ou alvos, mas que deixa que os diferentes estados membros decidam como implementar com a sua própria legislação nacional, para atingir essas metas, esses alvos. Então não quer dizer que temos um único conjunto de normas idênticas mas 28 sistemas diferentes, com o objetivo de permitir que todos procurem o mesmo objetivo, embora não tenham a mesma relação, e esse é todo um desafio. Estamos trabalhando para aprovar uma nova legislação de segurança de dados, esperamos aprovar no final desse ano como regulamentação para que já não seja necessário implementar a lei de forma diferente conforme os diferentes estados-membro, mas que se possa aplicar em si pelo próprio direito. Então, de alguma forma, podemos ter respostas mais coerentes de países europeus sobre

alguma dessas questões, uma vez que se tenha implementado esse instrumento. Eu quero explicar de forma breve também, a definição de dados pessoais que utilizamos na união europeia. É toda informação relacionada com uma pessoa natural, física, identificável ou não identificável, não se fala da sensibilidade da informação aqui. O único fator fundamental aqui é se a pessoa pode identificar ou não a uma pessoa, nome, dados pessoais ou endereço de (IP), podem ser considerado um dado pessoal.

No exemplo da união europeia, um cidadão que trabalha para a comissão europeia, ou em um determinado lugar, também pode ser considerado como um dado pessoal, porque é uma coisa que permite identificar a essa pessoa. Quando tem um número para agir nesse organismo dentro da comissão europeia. Então, não há interesse se a informação é sensível. O conceito de uma pessoa não identifica ou diferencia o conteúdo ou os dados que são transmitidos, para a informação do subscritor, apenas dados pessoais. Há outro conceito chave que já foi mencionado, que tudo que se faz com os dados é processá-los, seja que olhem, que armazenem, traduzem, divulguem, tudo corresponde o que consideramos processamento de dados. Então, quando se reúnem dados para processá-los, tem que ter motivo específico. A quantidade de dados tem que ser pertinente para seus fins que se buscam, e não ser excessiva, a informação tem que ser exata e atualizada, não se pode guardar

por mais tempo que o necessário, todo o exercício tem que estar legitimado por um fundamento legal, ou seja, a pessoa que é proprietária desses dados prestou seu consentimento ou porque eram necessários para celebrar um contrato, e alguns outros motivos.

Quem são os fatores para proteção desses dados? Eu estava falando da aprovação da regulação, isso será aprovado pelo parlamento europeu e o conselho da união europeia, que são os atores legislativos, a comissão europeia que está a cargo de propor legislação e monitorar, supervisionar a implementação, depois temos a autoridade de proteção de dados a nível nacional, que está a cargo de supervisionar a implementação da proteção dos dados a nível nacional, e depois grupos de trabalho do artigo 29, com certeza que os senhores já devem ter escutado, porque fez comentários em diferentes trabalhos, que um grupo que reúne, basicamente, a todas as autoridades, vinculadas com a proteção de dados a nível nacional, e a comissão numa função de assessoria, então, basicamente dá um assessoramento à comissão e a outros, sobre como devem ser implementadas as leis de proteção. E também está a corte de justiça, que é a única entidade autorizada a interpretar as leis em matéria da proteção de dados, e são quem dão as respostas quanto a implementação da regulamentação em matéria de proteção de dados.

O que significa isso do ponto de vista do (WHOIS)? Estamos redesenhando o (WHOIS), então há aspectos centrais que temos que considerar. Do ponto de vista da proteção do uso dos dados, e da aplicação da lei de um lado, a disponibilidade. Como acabamos de saber, esses dados tem que estar coletados para um fim legitimo, com fundamento legitimo, por exemplo, consentimento da pessoa que sujeita os dados, e qualquer serviço futuro de diretoria de registro também tem que garantir o objetivo, para que fim vai usar esses dados, porque também há um componente de prestação de contas, de responsabilidade. Não deve coletar mais dados que o necessário, e não deve guardar por mais tempo que o necessário.

O acesso, o fato de que seja um sistema público que a (ICANN), na sua firmação de compromisso, se comprometeu a conservar desse jeito, é um tema central de proteção de dados, a diretriz não diz nada sobre limitar o acesso aos dados. Mas, obviamente, pensando no espirito da lei, seria muito útil se os dados não fossem divulgados de maneira desnecessária, e com relação ao componente de exatidão, isso é simples, porque quando falamos dos componentes de aplicação da lei, e os que entendem de proteção dos dados, todos estamos alinhados, queremos que os dados sejam certos. Isso é o que posso compartilhar com vocês, e vou responder perguntas.

ALICE MUNYUA: Obrigado, (Cathrin). Há alguma pergunta ou comentário pra fazer? Então, talvez possamos avançar para a seguinte apresentação, onde veremos exemplos do (WHOIS), será (Greg) que vai apresentar, do centro de cyber-delitos europeu.

GREGORY MOUNIER: Peço, por favor, que coloquemos a apresentação.

ALICE MUNYUA: Parece que há uma pergunta. Apresente-se, por favor.

VOLKER GREIMANN: Sou do grupo de registradores do conselho da (GNSO). Quero agradecer por essa apresentação interessante, concisa, sobre a posição da união europeia sobre a proteção dos dados. Para muitos de nós, desde o início, ficou claro que o (WHOIS), tal como está agora, tem muitos dados privados, de milhares de cidadãos, que são publicados diariamente, e isso é problemático. Do ponto de vista da proteção de dados da (Europa), e também de outros países, então, precisamos de uma revisão clara e bem definida do (WHOIS) tal como está agora, para estarmos certos de que esses dados não estejam mais disponíveis livremente, tal como estão agora. Estariam de

acordo com isso? da perspectiva do grupo de trabalho da segurança pública, como se deveria implementar esse tipo de regime?

CATHRIN BAUER-BULST: Concordo com você, que o ideal seria que não houvesse um acesso total aos dados que estão agora disponível, mas como equilibrar isso na prática, com a função que tem que cumprir o (WHOIS)? A união europeia também tem legislação que exige que se publique essa informação nos websites, para todo, tudo que não está atuando, que não está publicando suas próprias fotografias mais, mas coloca da sua família, amigos, nesse caso, tem que cumprir com a obrigação do (WHOIS) e colocar informação detalhada de contato para poder assumir qualquer responsabilidade, caso se considere que cometeu algo ilegal. Então, é difícil achar o equilíbrio. Nessas circunstancias, não estou certa de que exista um sistema perfeito, acho que não podemos chegar a esse ponto, mas devemos ver as preocupações das partes. Lamento não ter uma solução perfeita.

VOLKER GREIMANN: Eu entendo que não exista solução perfeita, e continuando nesse mesmo caminho, quando vocês apresentam esse tema, é importante que diferenciem o conteúdo que aparece no

website, onde é necessário requisitos de abertura, e podem ser benéficos para que não vá para os endereços privados dos particulares, por exemplo, e o registro dos nomes de domínio, que se utilizem para enviar e-mails onde não há publicação alguma para o mundo externo, mas estão ali obrigado registradores a publicar seus detalhes privados. Também, então, gostaria de que vissem como alguns registros europeus estão gerenciando, publicando os dados do (WHOIS), é o que está fazendo (Nominet) no espaço europeu, a quantidade de dados visíveis ao público, e talvez se possa limitar a um nome ou endereço. Então, é importante que vocês vejam isso para tomar um modelo para a apresentação de dados privados, quando são apresentados no contexto da (ICANN).

DAVID CAKE: (David Cake), da (Austrália), emembro do conselho da (GNSO). Mais uma vez, tenho um comentário geral e outro específico. Foi muito boa sua apresentação, muito obrigado, acho que enfatiza a necessidade de pensar nas diferentes peças que constituem o (WHOIS), os princípios a que devemos aderir ao longo prazo, e também requisitos transitórios que talvez possam mudar, porque considero que seria, assim, eu vi no website essa semana que começaram a falar que iriam sair, porque não cobriam esses requerimentos. Acho que devemos ser flexíveis e

encontrar o equilíbrio entre as coisas que não mudam e as que vão mudar.

Vamos falar das que vão ser mudadas, temos o serviço de diretórios de registro, (PDP), que vão se desenvolver no próximo ano, na (GNSO), então, vai haver um esforço muito grande para responder todas as perguntas sobre quem tem acesso a esses dados, que dados se coletam, quem os vê. E é importante que haja a participação através do pedido de comentários públicos respondendo a nossas questões em forma de comentário, mas se trabalhassem com o grupo de trabalho, artigo 29, ou com entidade similar que tenham conhecimento profundo sobre proteção dos dados, isso realmente seria de grande valor, porque nos daria uma boa orientação, seria possível responder perguntas bem específicas, então sugiro que tenham a participação de pessoa com esse tipo de perfil. A partir do interesse de alguém que poderia participar em nome da (GNSO). Acho que na (ICANN) precisamos encontrar pessoas que tenham conhecimentos especializados sobre privacidade de dados, o que está no artigo 29, pessoas desse estilo.

ALICE MUNYUA: É por isso que o (GAC) desenvolveu esse grupo de trabalho, certamente vamos participar, especificamente de algum desses processos, e nas etapas precoces. Muito obrigada.

KIRAN MALANCHARUVIL: (Kiran Malancharuvil), da (MarkMonitor). Com relação ao grupo de partes interessadas dos registros, acho que aqui, apresentaram algumas posições que se contrapõem com o que foi dito nos comentários do grupo de trabalho de privacidade e proxy. Acho que tem a ver com a especificação da exatidão e do (WHOIS), onde se encoraja o acesso aberto à informação do (WHOIS) nesses vários campos de dados. Então, queria um esclarecimento, porque acho que há algumas coisas que disse que são contraditórias com o que esses grupos estão propondo.

CATHRIN BAUER-BULST: Se refere a mim? Não tinha reparado nisso. Não estou certa de onde está a contradição, o que estou tentando apresentar são 2 perspectivas diferentes. De um lado, a situação ideal da perspectiva da proteção dos dados, e do outro, a situação ideal do ponto de vista dos órgãos da lei. Como já disse no início da minha exposição, há direito a segurança e direito a privacidade, que são considerados direitos fundamentais do ponto de vista da união europeia, e também em outras regiões do mundo. E, nenhum desses direitos são outorgados de maneira absoluta, então, na prática, o que se tenta fazer é alcançar um equilíbrio e isso é o que temos de fazer nesse processo de desenvolvimento político. Muito obrigado novamente pelo convite ao

representante do grupo de trabalho, artigo 29, para que participemos, vou ficar certa de transmitir essa informação em (Bruxelas) e que meus colegas entrem em contato com vocês, e que saiba que vocês querem contar com a participação nesse processo. Esperamos alcançar o equilíbrio adequado entre esses 2 direitos fundamentais. Nenhum tem prevalência sobre o outro, então acho que não há uma contradição aqui.

KIRAN MALANCHARUVIL: Acho que seria útil a participação desse grupo de trabalho, e talvez a redação de comentários públicos através do grupo de segurança pública. Se podemos ter um exemplo do que a senhora está indicando como necessidade de achar um equilíbrio entre esses direitos, porque obviamente temos abertura na informação do (WHOIS) e temos de estar certos de que há um equilíbrio adequado e interesses legítimos de privacidade também. Acho que não se devem fazer declarações absolutas sobre a abertura do (WHOIS), e sobre isso. Agradeço o esclarecimento.

CATHRIN BAUER-BULST: Entendo sua preocupação, e estou mostrando a política atual, como está agora, da perspectiva dos organismos de aplicação da lei. Se não tratássemos dessa abertura do acesso, seria muito difícil fazer alguma outra coisa, então temos que nos concentrar

nesse processo de desenvolvimento de políticas com muito cuidado.

GREGORY MOUNIER: Obrigado, vou dar alguns exemplos da utilidade do (WHOIS), e de pesquisas feitas por alguns pesquisadores. Eu conto à respeito da agencia de cumprimento da lei, na (Europa), nós trabalhamos apoiando 28 estados membros e também forças policiais e organismos de cumprimento da lei. Nós criamos esse centro de cyber-delito europeu em 2013, e nos baseamos em informação que obtemos por parte dos estados membros.

Os nosso sócio, no cyber-delito, trabalhamos com o (Reino Unido), trabalhamos com o (FBI), por exemplo, dos (Estados Unidos), quanto ao cyber-delito, temos 3 grupos operacionais, dentre eles, um que se encarrega da fraude online, temos aquele que se encarrega da exploração sexual infantil, também online, e depois o terceiro, que se encarrega dos cyber ataques, que atacam sistemas de informação, e tem a ver com malware, onde há ataques voluntários. Me pediram que falassem sobre exemplos para que tenham ideia da utilidade do (WHOIS) para os pesquisadores na internet. Nós todos sabemos que há muitos serviços e produtos online que estão muito facilmente disponíveis, que podem ser comprados, ocultando sua verdadeira identidade. Não faz sentido que agora eu faça uma

enumeração dos mesmos, mas nesse contexto, o papel do (WHOIS) é crítico.

Os pesquisadores de cyber-delito têm essa ferramenta para saber quem é o culpado de um crime ou delito. Os delinquentes se protegem pelo anonimato, mas se temos um (WHOIS) com dados de usuários que sejam validados e exatos, podemos diminuir as possibilidades de que os cyber-delinquentes possam ocultar a sua identidade. Então, temos que conseguir isto de maneira tal que os cyber-delinquentes tenham que recorrer a técnicas mais complexas para ocultar sua identidade ou suas marcas.

Suponho que todos vocês estão, de alguma forma, familiarizados com botnet, que é uma rede de computadores infectados por software maliciosos, que permite que um criminoso controle essa rede de computadores e utilize um comando de forma a tal que os computadores façam várias atividades ilícitas ou diretivas. Então, vemos qual foi o último dos servidores que teve comunicação nessa botnet, o que tem a ver com os usos abusivos ou indevidos com (DNS).

Vemos que se alguém consegue manter uma cadeia de novos registros e domínios, então consegue ter uma botnet, uma rede se software maliciosa, muito efetiva. Estando em nomes de domínio, registradores, de todo o mundo, com rapidez. Um

sócio pode sustentar a solicitação de baixa de serviço, mas também outras tentativas para afetar a rede ou tomar a rede por parte de outras pessoas. Então, temos esta técnica de (DNS), que é de muita utilidade para o tema das botnet.

Quando pediram que eu viesse falar com os senhores, consultei uma equipe de investigadores, porque sou apenas um assessor de políticas, e trabalhei com eles, vimos algumas situações do ponto de vista do (WHOIS) e (DNS), e houve uma situação operativa muito recente, no qual a equipe encarregada desses temas teve que controlar um botnet que se dedicava a software malicioso que atacava sistemas bancários online. Houve uma comunicação com um dos suspeitos, no qual se compartilharam detalhes do domínio em questão. Então, fizeram uma busca de (WHOIS) sobre esse domínio, e obtiveram um e-mail usado para registrar domínio.

Depois fizeram uma busca reversa de (WHOIS) desse e-mail e encontraram outro domínio registrado com o mesmo e-mail. Entre esses nomes de domínio, havia um domínio criado por esse indivíduo em questão, há alguns anos, e tinha utilizado para criar um perfil profissional com seu currículo, sua foto, etc. Antes de ser um cyber-criminoso, quando utilizou esses detalhes pessoais, conseguimos encontrar uma base de dados num pais onde morava, e vimos sua verdadeira identidade. Então, demonstramos que essa pessoa era, de fato, um cyber-

criminoso e assim conseguimos fazer ou começar ações judiciais. Se temos dados exatos, podemos encontrar um culpado de um crime com muito mais rapidez. Dou outro exemplo de botnet, que é um exemplo negativo. Um de meus colegas dedicou 3 meses a estudar um cyber-criminoso que se dedicava a desenvolver web-inject para atacar clientes de um sistema bancário.

Uma vez que a vítima estava infectada por esse software malicioso, iniciava-se a sessão no seu portal de banco online, e chegava a um domínio, que mandava um website do cyber-criminoso, que era muito semelhante ao website verdadeiro. Então, quando a vítima ingressava seus dados, eram captadas pelo criminoso. Meus colegas, nos últimos 3 meses, viram que o suspeito tinha registrado 18 domínios diferentes com web-inject, todos eles, apontando para pessoas no (Reino Unido), (Países Baixos), e (Alemanha), e que tinha 4 conjuntos de identificadores para identificar tudo isso e registrar essa informação. Tanto correios eletrônicos, nomes e números de telefone. Então, se trabalhou em cada um desses identificadores, e como resultado, chegou a muitos outros identificadores, e nenhum deles conseguimos ter uma identidade real. Mas, se é um cyber-criminoso que trabalha corretamente, entre aspas, então a pessoa dedica um tempo muito valioso de investigação a perseguir, em vão. Meus colegas

dedicaram 3 meses e não conseguiram encontrar essa identificação, porque os identificadores não eram legítimos, mas tinham sido obtidos de uma botnet. Então, se naquele momento, o registrador tivesse validado esses dados, talvez meus colegas não teriam desperdiçado seu tempo, e teriam dedicado seu valioso tempo a investigar esse caso. Este é um exemplo de quando não temos os dados exatos ou precisos, e como perdemos nosso tempo.

Não vou falar sobre este caso, é uma botnet muito famosa, que surgiu em fevereiro. Dedicamos muito tempo, gastamos muito tempo, porque não tínhamos dados exatos de (WHOIS) da pessoa que estávamos procurando. Mas, eu quero contar uma coisa positiva. É uma caso de exploração sexual infantil, esses são os websites que estão na mão de criminosos na web, aberta, não na web escura ou (Darkweb), ou oculta, e o que fazer é vender material de pornografia infantil, online, então, por 99 dólares por mês, os clientes têm acesso ilimitado a material de pornografia infantil. O que fizeram os meus colegas é ver esses websites e reunir os nomes de domínio desses websites utilizando diferentes técnicas. Depois, reuniram informação do (DNS) associadas a esses nomes de domínio, associado a endereços de (IP), ferramentas disponíveis para os registradores e para qualquer investigador, e depois tiveram um conjunto de dado de (WHOIS) associados a esses nomes de domínio. Então,

na teoria, o que temos é o domínio A, que a informação específica do (DNS), que indica que está relacionado a um endereço de (IP) A. O domínio B tem informação de que está vinculado ao (IP) B, mas não tem vinculação de diferentes domínios. Quando se faz uma referência cruzada entre os 3 conjuntos de dados, formação de (DNS), nomes de domínio e dados de (WHOIS), é possível encontrar um endereço de correio eletrônico válido em comum em todos esses domínios, que foi utilizado pelo registratário para registrar os domínios.

Então, utiliza um só correio eletrônico para comunicar-se com o registrador para pagamento. Como conclusão, conseguimos deter um grupo de criminosos e dar baixa a esses websites. Infelizmente, esse é um negócio tão bom que continua surgindo. Então, como conclusão, quero reiterar o que falei antes, os dados confiáveis e precisos do (WHOIS) são muito importantes para que os organismos de cumprimento da lei possam combater o cyber-delito, mas se alguém é um cyber-criminoso muito bom, por assim chamar, pode ter sucesso, mas poupa um tempo valioso de investigação, que faz com que a vida do cyber-criminoso seja mais difícil, e para isso estamos no cumprimento da lei.

ALICE MUNYUA: Obrigado, (Greg). Há participantes remotos, (Olof), da secretaria do (GAC), vai ler para o pessoal da (ICANN).

OLOF NORDLING: (Olof Nordling), pessoal de apoio para o (GAC), para os registros. Há uma pergunta de um participante remoto, que se chama (Mike Illishebo). É um colega da reunião (ICANN-52), e trabalha para a polícia da (Zâmbia). Ele diz, "(Whois) é uma ferramenta poderosa para pesquisa de cyber-delito, mas há falhas por parte de registratários, que muitas vezes não dão nomes e endereços exatos ao registrar um site, portanto, é difícil fazer uma investigação. Há alguma forma no qual os registratários possam garantir a veracidade da informação verdadeira durante o processo de registração? Além disso, quanto avançou a (Europol) para garantir que os programas de criação de capacidade sobre cyber-crime sejam introduzidos para organismos de cumprimento da lei na (África)."

ALICE MUNYUA: Obrigado. Alguém do painel quer responder?

GREGORY MOUNIER: Com respeito ao programa de capacidade da (Europol), infelizmente, não estamos participando nesses programas. Apoiamos a investigação dos países membros, acho que há um

portfolio muito amplo, a (Interpol) tem um portfolio muito mais amplo para apoiar as comunidades na (África), mas acho que meus colegas tem algo para acrescentar.

CATHRIN BAUER-BULST: Nós temos esse tipo de programa de criação de capacidade de países africanos, e temos novas oportunidades de fundo de recursos para os países africanos, e estamos vendo isso dentro da área de criação de capacidades e matéria de cyber-crime.

ALICE MUNYUA: Infelizmente, está acabando o tempo, há 5 pessoas que querem realizar perguntas, peço que sejam breves, para que os outros palestrantes possam fazer comentários.

ELLIOT NOSS: Muito obrigado. Tive respondido 2 de minhas perguntas, os senhores fizeram um bom trabalho quando detectaram a maior força para as investigações. Todos sabemos que os criminosos, às vezes, cometem um erro tolo, e isso acontece nos negócios também, quando alguém comete um erro, é substituído por pessoas mais inteligentes. Então, quando tratamos com a comunidade que se dedica à segurança, devemos falar com eles sobre sua experiência com registradores, e com esse intercambio, para obter informação. Fizeram isso?

GREGORY MOUNIER: Uma resposta rápida. Eu não falei especificamente sobre a relação com os registradores, mas os investigadores dizem que, em termos gerais, se tem uma boa relação com o registrador, e geralmente obtém uma cooperação muito melhor, do que quando essa relação não é boa. Então, estamos educando os investigadores a nível interno para ter uma relação positiva com os registradores, e com o setor privado, que muitas vezes tem as ferramentas para resolver uma investigação de um cyber-delito, então, o setor privado tem que saber quais são as limitações, o que queremos, e prestem as informações certas.

ELLIOT NOSS: Eu acho que isso é muito positivo, não tem que ser apenas uma relação pessoal, há muitos dados que são muito valiosos para uma investigação.

ALICE MUNYUA: Lamento interromper, mas temos 10 minutos. Vou pedir às outras pessoas que enviem as perguntas depois da sessão, porque estamos ficando sem tempo. Faça sua pergunta, mas responderemos depois.

ARTHUR ZONNENBERG: Obrigado por sua apresentação. Estou tentando entender o que os senhores descreveram quanto aos erros tolos dos cyber-criminosos, tendo também o que se disse a respeito do endereço de e-mail e a importância que tem, mas, por exemplo, se alguém rouba a identidade da (Cathrin), e tem uma cópia de seu passaporte, eu como registrador, como que eu sei que não se trata de (Cathrin), que não é ela que está fazendo? A única coisa que eu posso fazer é perguntar se ela registrou tal nome de domínio, e geralmente, contatamos as pessoas por telefone, mas pode ter alguém que responda o telefone e que diga ser (Cathrin), mas eu não sei quem é. Então, como que eu posso validar o que estou fazendo para verificar a identidade, através de vários métodos, que não vou divulgar, e, por outra parte, não tenho qualquer problema com que vocês tenham meus dados, mas sim que oponentes políticos obtenham meus dados, sou ativista a respeito de uma causa política.

ALICE MUNYUA: Não vamos responder as perguntas agora. Podem continuar realizando suas perguntas, vamos responder depois, porque temos 2 apresentações pendentes.

ASHWIN SASONGKO: Obrigado, (Ashwin) da (Indonésia).

Um banco deve saber exatamente quem é seu cliente, e ver seu documento de identidade europeu, exemplo. É a mesma coisa quando uma pessoa quer um e-mail, devemos saber quem está por trás, e se uma companhia quer ter um website, tem que saber quem é a pessoa de contato técnico, e onde estão os escritores. Obrigado.

PETER KIMPIAN: Tenho uma pergunta. Talvez, seja importante destacar que a (Europol) está trabalhando junto com um regime exaustivo de proteção de dados de muito alto nível, (S3), e há um grupo da (Europol) que está investigando o tema de proteção de dados, todo o processamento de dados dentro da (Europol), ou seja, que tem muito conhecimento e experiência. Volto ao que disse antes, muito conhecimento da (Europol) e a nível europeu pode ser valioso nos organismo de cumprimento da lei, e em toda estrutura do nosso setor, para o futuro.

WANAWIT AHKUPUTRA: Eu acho que temos que continuar avançando. Vou passar a palavra ao representante do (Reino Unido). (PSWG) começaram a trabalhar e vão compartilhar com todos nós a tarefa que estão fazendo e fizeram no seu país.

NICK SHOREY: Em primeiro lugar, sou parte da equipe do (GAC) em nome do (Reino Unido), e estou num subgrupo que foca nas atividades de grupo de trabalho de segurança pública. Antes de me dedicar à governança de internet, era investigador de cyber-delitos, e também um consumidor de serviços de domínio e proxy, então, vi esse tema de vários ângulos. No (Reino Unido), como em outros países, temos amplas variedades de organismos governamentais, os responsáveis e interessados na segurança pública que se estende pela internet.

O grupo de trabalho de segurança pública reúne todos os departamentos para que pudéssemos fazer uma consulta sobre esses temas. Parte de tributos fiscais, alfandegas, o escritório de propriedade da informação, o órgão regulador de produtos medicinais, outro órgão nacional dedicado à luta contra o delito, a polícia do (Reino Unido), e também os que integram a coalisão de sociedades benéfica das crianças pela segurança da internet. (John Carr), está à minha direita, e é representante dessa coalisão, e esperamos responder a essa pergunta de (David) sobre a ampla abrangência do grupo de trabalho de segurança pública quando pensamos nos que participam. Acho que nessa área os governos colocam suas preocupações e problemas de maneira clara, então, há muita gente trabalhando com esse problema e tentando estabelecer interação com a

comunidade de internet, e às vezes essas pessoas não acham uma solução prática para esse problema.

Aqui está (John Flaherty), que é um pesquisador técnico e especialista, e vai contar o que estão fazendo no grupo da especificação 11, realizamos também reuniões mensais em (Londres) falando do trabalho, desenvolvendo opiniões, algumas recomendações de consenso, que são parte da responsabilidade do (PSWG), e a melhor maneira de discutir as melhores práticas da nossa parte, como governos, para ver como podemos trabalhar de maneira mais eficaz com a comunidade de internet, para tentar dar solução a esses temas. Como (Fadi) disse hoje de manhã, a (ICANN) é uma parte do ecossistema de internet, e no nosso trabalho sobre governança de internet, vemos que se um elemento de estratégia mais ampla, no fórum de governança da internet, esse é muito bom exemplo, da mesma forma que no conselho da (Europa).

WANAWIT AHKUPUTRA: Temos 2 minutos, (Nick).

NICK SHOREY: Vou me apressar. Vemos isso como parte de uma estratégia mais ampla, e estamos tentando desenvolver workshops de toda uma jornada, e queremos registradores, as companhias que se

encarregam de analisar as ameaças que também contribuam a isso, esperamos que esse grupo possa facilitar a colaboração e participação ativa entre o governo da comunidade que conforma a (ICANN) para desenvolver soluções mutuamente benéficas e práticas. Como podem participar, e são membros de um órgão de segurança pública do governo, podem trabalhar com seus representantes governamentais que estão aqui presentes na (ICANN).

O grupo do (Reino Unido) pode também facilitar a participação e o contato com outros membros do (GAC) para chegar às organizações de segurança pública que correspondam. Às vezes, é difícil que encontrem essa pessoa adequada. Aproximem-se de nós, e talvez a gente possa aproximá-los com alguém da (Europa), e se vocês querem pertencer a uma comunidade mais ampla, podem trabalhar de maneira direta dos processos da (ICANN), e podem colaborar para chegar a essas soluções práticas. Acho que abrangi tudo.

WANAWIT AHKUPUTRA: (John), peço desculpas, temos 1 ou 2 minutos para sua intervenção.

JOHN FLAHERTY: Posso falar rápido da especificação 11, já foi mencionada aqui, se encarrega das questões de uso indevido, abuso, em torno ao uso dos nomes de domínio, surgiu em resposta a assessoria do (GAC), do (NGPC), à partir da reunião em (Pequim), posso dar uma atualização rápida, explicar o avanço atingido no grupo de trabalho, vamos discutir nessa semana também, na reunião 54 da (ICANN). quanto a uma relação entre o grupo de trabalho de segurança pública e os registros, me pediram pra ser copresidentes desse grupo de trabalho do marco de segurança e eu disse, “Bom, estive trabalhando na pesquisa de cyber-delitos no (Reino Unido) e nunca me pediram essa informação, e nunca conseguimos uma solução.” Às vezes, um registro tem uma inovação técnica também mostra o maravilhoso, e então, essa relação que temos com todos os registros, não esperamos que possam dar todas as respostas, mas que nos ajudem. Ainda não armamos por escrito o marco sobre o qual trabalhamos, mas simplesmente o colocamos em prática. Qual resenha geral posso dar?

Nos focamos no uso e na salvaguarda dos novos (gTLDs) e da proteção deles, também responder às ameaças de segurança, os botlines, o phishing, a substituição da identidade, o grupo também está vendo como um registro escolhe responder as ameaças de segurança, porque queremos na sessão que teremos com o registrador, oferecer estudos de caso para ver o

que está se fazendo, como podemos continuar desenvolvendo uma solução produtiva no grupo de trabalho, está conformado por profissionais, pessoas do âmbito do cumprimento, de órgãos de polícia, de registros e registradores, do grupo de trabalho do (GAC), agora temos uma voz e um lugar na mesa, e tentamos incidir nesse marco o benefício mutuo, e que todas as partes possam aprofundar seus conhecimentos das ameaças e reduzir os tempos para poder chegar àqueles que utilizam botnets, software malicioso, phishing, e ocasionam prejuízos. Estamos desenvolvendo o marco de segurança central, que queremos inibir a forma, estamos trabalhando nos princípios, diretrizes, e não queremos ser refletivos, queremos ser mais flexíveis do ponto de vista técnico, principalmente quando dizemos que há alguns registros que já estão trabalhando, dando esse tipo de informação com relação a como responde em relação aos abusos, também desenvolvemos princípios, diretrizes para a (ICANN), e temos uma carta orgânica, não é uma política que funcione para todos os registros, pode funcionar para um, para outro, não, para proteger os clientes. Também queremos colaborar para poder aplicar as melhores práticas que existem atualmente, entre os diferentes autores, e queremos redigir um documento quadro, estabelecendo as diretrizes básicas. Esperamos que para o final de janeiro de 2016 possamos ter um rascunho para ser submetido a comentário público.

WANAWIT AHKUPUTRA: Realmente, ficamos sem tempo, mas posso passar a palavra à (John Carr), para que faça sua apresentação.

JOHN CARR: Posso fazer em 3 orações. A nossa coalisão em favor do bem estar infantil está muito interessada nesses temas, mas estamos trabalhando com a (ICANN), a partir da nova rodada de (gTLDs), e quando se fez a solicitação de (.kids) e outros nomes similares, é óbvio que se vamos criar um espaço que vai levar à criação de websites que tem a intenção de atrair grandes quantidades de crianças e jovens, então achamos que isso coloca preocupação do ponto de vista da segurança, e temos que considerar isso desde o início do processo, quando se fez a última rodada, isso não foi assim, e não queremos que isso se repita no futuro, por isso estou tão grato de fazer parte desse grupo.

WANAWIT AHKUPUTRA: Muito obrigado a todos, peço desculpa, porque realmente não ficamos com tempo, e vamos rever as perguntas colocadas, nas transcrições, e publicar as respostas no nosso website.

ALICE MUNYUA: Não vamos responder uma pergunta online, mas vamos pedir que a apresente, obrigado.

WENDY SELTZER: Queria me referir ao tema da segurança pública como signatária de um desses projetos de registro, um comentário elaborado por várias mulheres que defendem a inclusão das mulheres vítimas e sobreviventes de abuso. Signatária desse tipo de comentário nos quais se fala da informação privada que é publicada online. Pedimos a proteção da informação privada quando redigíamos esses comentários e tivemos que entrar em contato com organismos da informação para que soubessem que tínhamos publicado essa informação. É um processo circular, muitos de nós nos faz lembrar como a publicação forçada de informação, muito similar ao que solicita o (WHOIS), e, na verdade, isso constitui uma invasão de privacidade. Também uma preocupação do ponto de vista da segurança pública e privada.

ALICE MUNYUA: Quero aproveitar para agradecer a todos os integrantes do painel e todo o público que participou. Da próxima precisaremos de 3 horas, e não 1 hora e meia. Vamos preparar uma sessão para a próxima reunião da (ICANN).