
BARCELONA – Sessão Entre Comunidades: GDPR
Quarta-feira, 24 de outubro de 2018 – 09:45 às 12:00 CEST
ICANN63 | Barcelona, Espanha

BRUCE TONKIN: Certo. Vamos começar para que possamos aproveitar ao máximo o tempo que temos esta manhã.

Meu nome é Bruce Tonkin e fui convidado a presidir esta sessão entre comunidades sobre o GDPR. A ideia por trás das sessões entre comunidades é realmente reunir a comunidade para vermos como a comunidades como um todo é capaz de se concentrar em problemas importantes e resolvê-los. Nesta sessão entre comunidades temos representantes de várias partes da Organização ICANN. Temos representantes da GNSO, que é responsável pelas políticas relacionadas aos nomes de domínio de gTLDs.

Para a câmara de partes contratadas, temos Nick Wenban-Smith da Nominet. Nick é o conselho geral da Nominet e também um agente de proteção de dados. A Nominet está envolvida com os dois nomes com código de país, no caso deles o .UK, e também nomes genéricos de primeiro nível, como .BLOG.

Para o Grupo de Partes Interessadas Comerciais, temos Flip Petillion. Acho que é assim que se diz. E Flip é de uma firma na Bélgica que

Observação: O conteúdo deste documento é produto resultante da transcrição de um arquivo de áudio para um arquivo de texto. Ainda levando em conta que a transcrição é fiel ao áudio na sua maior proporção, em alguns casos pode estar incompleta ou inexata por falta de fidelidade do áudio, bem como pode ter sido corrigida gramaticalmente para melhorar a qualidade e compreensão do texto. Esta transcrição é proporcionada como material adicional ao arquivo de áudio, mas não deve ser considerada como registro oficial.

fornece serviços de resolução de disputas e costuma participar de disputas relacionadas a nomes de domínio.

Para o Grupo de Partes Interessadas Não Comerciais, temos o Professor Milton Mueller da Georgia Tech, de Atlanta, Geórgia, nos EUA.

Do Comitê Consultivo de Segurança e Estabilidade, temos Greg Aaron. Greg é o vice-presidente do iThreat Cyber Group e trabalha com informações sobre ameaças e investigando o uso de nomes de domínio para abusos on-line.

Do Comitê Consultivo At-Large, temos Hadia El Miniawi. Hadia é diretora do Centro de Empreendedorismo do DNS no Egito.

Do Comitê Consultivo para Assuntos Governamentais, temos Ashley Heineman. Ashley é responsável pelas políticas da Internet na NTIA nos Estados Unidos. E eu acho que o GAC tem o difícil desafio de, quando analisar questões como privacidade, ele precisa ver como isso é tratado por TODOS os diferentes governos que fazem parte do Comitê Consultivo para Assuntos Governamentais e encontrar soluções que sejam relevantes globalmente.

Também temos um representante das partes interessadas de agências legais fiscalizadoras, que é Chris Lewis-Evans. Ele trabalha na Agência Nacional de Crimes do Reino Unido e é responsável por gerenciar as investigações na Internet.

E representando a proteção de dados, temos Cristina Monti. Cristina trabalha na unidade de Proteção e Fluxos de Dados Internacional no departamento do Diretor Geral de Justiça da Comissão Europeia.

Então, temos um painel com participantes de renome. Todos eles trabalham há anos, quero dizer, lidam com os desafios relacionados à proteção das informações pessoais.

Achei que seria importante dar a vocês um pouco de contexto. E provavelmente seja relevante retomarmos a RFC-1591, que foi escrita por Jon Postel em 1994. Na verdade, em outubro faz 20 anos da morte de Jon. Ele morreu no dia 16 de outubro de 1998. É interessante lermos estas palavras escritas há mais de 20 anos, mas que ainda merecem ser consideradas e servem de reflexão.

Na RFC, Jon disse que os gerentes de nomes de nível superior são os administradores do nome delegado que eles receberam, mas têm o dever de servir à comunidade.

Ele também disse que as preocupações com os direitos e a propriedade dos domínios não são apropriadas. O apropriado é preocupar-se com as responsabilidades e o serviço à comunidade.

Então, os titulares de nomes registrados que detêm nomes de domínio com nomes no nível superior têm a responsabilidade de obedecer a lei em sua própria jurisdição. Alguns desses titulares de nomes registrados são pessoas físicas, e o contexto dos titulares de nomes registrados é geralmente o de pessoas físicas.

Então, também precisamos considerar que os dados pessoais dessas pessoas físicas estão protegidos por diversas leis de privacidade no mundo todo.

Se pensarmos em como a ICANN se encaixa nisso, podemos entender que a missão da ICANN é limitada, que é coordenar a alocação de nomes na zona raiz... estou me referindo à parte da missão que é relevante para este assunto. Mas é a atribuição de nomes na zona raiz do DNS, ou seja, quem será responsável por operar esses nomes no nível superior. E ela coordena o desenvolvimento e a implementação de políticas relacionadas ao registro de nomes de domínio em gTLDs.

Mas existe uma exceção muito clara que também diz que a ICANN não deverá regular serviços que utilizam os identificadores da Internet nem o conteúdo que esses serviços transmitem ou oferecem. Então, a ICANN não faz isso.

Sendo assim, depende de outras partes, geralmente depende das autoridades de fiscalização legal e de outras autoridades fiscalizadoras públicas agirem e controlarem se os titulares usam os nomes para violar a lei.

Por sua vez, essas autoridades normalmente dependem de organizações do setor privado, como organizações de segurança cibernética, que coletam informações sobre um incidente para realizar uma investigação adequada.

Também é interessante refletirmos sobre a derivação do WHOIS, que é o motivo pelo qual estamos reunidos hoje, eu acho, para falarmos

sobre como devemos olhar para a próxima geração de informações que fornecemos em um registro. Eu li a RFC... a RFC original do WHOIS, que é a 1982.

Na verdade, ele era um serviço de diretório para as pessoas que usavam a ARPANET naquela época. E ele exigia o nome, o endereço, o número de telefone e o endereço de correspondência, endereço de e-mail delas. Interessante, ele não era não chamado de e-mail naquela época. Era chamado de caixa de correio em rede.

Depois, à medida que foi evoluindo, ele se transformou em uma fonte de contatos dos administradores e do pessoal técnico dos nomes de domínio de algumas poucas instituições grandes e famosas. E, nesse caso, era muito claro quem era a entidade legal responsável. Apenas era difícil encontrar a pessoa relevante entre as centenas de funcionários que trabalhavam nessas organizações.

O mundo de hoje é muito diferente. Temos centenas de milhões de registros de domínios. Além disso, em vez de grandes instituições, esses nomes são geralmente registrados por pessoas e muitas delas atual apenas como comerciantes independentes. Ainda assim, precisamos identificar a identidade legal que é responsável pelo uso do nome. E ainda precisamos conseguir entrar em contato com o titular do nome registrado para resolver possíveis problemas.

Uma questão que geralmente é esquecida é que, muitas vezes, o titular do nome registrado é a vítima, não o criminoso, das atividades que usam o nome de domínio. É muito comum as pessoas terem o site delas hackeado. E-mails são hackeados. E quando estamos

investigando um problema, geralmente o titular do nome registrado não sabe nada sobre o caso e, na verdade, precisa de ajuda para solucionar o problema. Então, nem sempre o titular do nome registrado foi o responsável pelo problema que resultou no uso do nome.

Acho que vale a pena refletirmos sobre alguns registros públicos semelhantes, e existem vários que provavelmente são semelhantes... têm características semelhantes a registros de nomes de domínio da Internet.

Um deles são os registros de informações de empresas. Então, vários países têm leis que exigem que qualquer parte que queira negociar seja registrada como um negócio, que seja registrada como uma empresa; e as informações coletadas como parte desse processo geralmente são dados pessoais, como o nome, o endereço e o número de telefone da pessoa física... pessoas físicas que são os diretores da empresa.

Outro exemplo são os registros de carros. É aqui que o registro conterá informações sobre o veículo, como a cor dele, o tipo, o modelo, mas também terá dados pessoais sobre o proprietário do veículo, que pode ser uma empresa ou uma pessoa, uma pessoa física.

Acho que os registros de veículos são uma analogia semelhante à ICANN, porque se pensarmos em uma agência de registros de veículos que gerencia os identificadores, os identificadores exclusivos que estão aparafusados na parte traseira de um carro, às vezes podemos... eles podem ser identificadores pessoais. Então, algumas pessoas

escolhem ter placas com números personalizados em alguns países. Mas se alguém quiser ser contatado, essa pessoa geralmente pintará o número na lateral do veículo, se for uma empresa. Mas geralmente não vemos pessoas colocando o nome delas na lateral de um veículo.

Além disso, se analisarmos quem é responsável pelo que é feito com o veículo, geralmente a licença para usar o veículo, você pode dirigir para onde quiser. Você praticamente pode fazer o que quiser dentro desse veículo. Você pode colocar qualquer coisa dentro do veículo. Você pode colocar qualquer pessoa dentro do veículo. Mas as agências responsáveis por emitir o número da placa não se importam com isso. A única coisa que importa para eles é conseguirem identificar o proprietário do veículo.

E são outras agências reguladoras, então, se o seu carro estiver em um estacionamento e alguém repara que parece que... parece que está cheio de drogas, a polícia investigará e entrará em contato com a autoridade de registro para ter mais informações sobre esse carro.

Se você se envolver em um acidente de trânsito, a primeira coisa... digamos que alguém bate no seu carro e foge, a única coisa que você sabe sobre essa pessoa é o número da placa. Com esse número de placa você pode... como cidadão de alguns países, certamente sei que na Austrália e no Reino Unido isso é possível, você pode pesquisar informações sobre o carro no registro usando o número da placa. Com essas informações você saberá o tipo, o modelo e a cor do carro, mas não quem é o proprietário.

Mas isso permitiria que você tivesse certeza de que é o carro certo, porque talvez você se lembre vagamente do número da placa e não lembra bem quais são os últimos dígitos. Você pode verificar para ver se é o carro certo, como cidadão público.

Depois que tivesse certeza de que é o carro certo, você levaria essas informações para a polícia e diria que essa pessoa bateu no seu carro e fugiu. Depois disso, a polícia poderia pegar essas informações sobre a pessoa física que possivelmente é proprietária do carro.

Então, temos muitas analogias com a nossa situação, de que a ICANN não se importa com o conteúdo dos sites. A ICANN não se importa com o conteúdo dos e-mails que você envia. Outras pessoas se importam com isso. A única coisa com a qual nos importamos é coletar informações sobre as partes que sejam proprietárias dos nomes de domínio, que possamos entrar em contato com essas partes, e outras pessoas são responsáveis por fiscalizar o uso desses nomes de domínio.

Os registros de números de telefone também são semelhantes, porque eles geralmente têm nomes e endereços de pessoas físicas, e a maioria dos países permite que pessoas físicas não tenham os nomes e endereços delas disponíveis publicamente.

Os registros de domínios com códigos de país têm... são parecidos com o cenário de gTLDs. A diferença, no entanto, é que eles são operados em uma única jurisdição. E a maioria dos registros de códigos de país na Europa obviamente tem atualizado a implementação dos serviços de diretório deles para estar em

conformidade com as normas do GDPR. Então, podemos aprender com eles e ver o que fizeram. Mas ainda precisamos encontrar uma solução que funcione no mundo todo, e não apenas em um país.

Se analisarmos o exemplo da Nominet, apenas para dar um exemplo de como eles gerenciaram isso, eles mostram uma quantidade mínima de informações no WHOIS público. Eles têm acesso autenticado para as agências legais fiscalizadoras no Reino Unido, mas nenhuma agência fora do Reino Unido tem acesso ao registro de maneira automatizada.

Além disso, eles também têm um formulário no site deles onde um usuário legítimo pode se inscrever para solicitar acesso às informações, e é necessário declarar para que fins elas serão usadas. E a Nominet avalia cada caso individualmente. E com base em quem está pedindo as informações e para que finalidade, eles avaliam se o propósito é legal. Depois disso, eles enviam as informações para a parte solicitante.

Então, eles criaram uma solução que aparentemente respeita as leis, tanto no Reino Unido quanto na Europa em geral.

Os Registros Regionais da Internet também... em geral os Registros Regionais da Internet têm informações sobre a organização que provavelmente é uma empresa de telecomunicações ou um Provedor de Serviços de Internet ou, em alguns casos, grandes organizações que têm intervalos de endereços IP. Então, a maioria dos dados naturais estão relacionados aos contatos dessas organizações.

Mas, novamente, o RIPE, por exemplo, que está sediado na Europa, precisaria ter uma solução em conformidade com o GDPR.

Então, no que diz respeito à IETF, temos muitos códigos em funcionamento. São sistemas em operação que existem hoje e atendem às leis dos países em que operam e precisam atender aos requisitos das leis de privacidade.

Se analisarmos como as leis de privacidade evoluíram, veremos que muitos países têm leis que protegem os dados pessoais. E, na verdade, elas foram atualizadas com o advento de sistemas de informação escaláveis e altamente acessáveis. Antes, se você quisesse informações sobre uma empresa, precisaria ir pessoalmente ao escritório da empresa e provavelmente olhar o fichário. Além disso, você ainda levaria várias horas para encontrar um registro. Bem, na verdade, podemos acessar esse registro daqui. Estou em Barcelona. Posso acessar o registro da empresa no Reino Unido. Então, o acesso a eles está muito melhor do que antigamente.

Além disso, a quantidade de informações nesses registros é muito maior do que há duzentos anos, considerando, por exemplo, certidões de nascimento, atestados de óbito e casamentos... essas informações eram geralmente guardadas nas igrejas. Não havia uma centralização. Você precisaria ir à igreja onde a pessoa nasceu ou morreu e lá estaria o registro. Agora os registros são muito mais centralizados e temos milhões deles.

Então, a tendência global tem sido atualizar progressivamente as leis de privacidade. Na Europa, observei que, na década de 50, acho que

após a Segunda Guerra Mundial, havia uma preocupação e muito mau uso, me parece, das informações de identificação pessoal durante a guerra. Então, esses conceitos começaram a ser considerados como parte de um direito humano básico.

Depois, na década de 80, a Europa adotou a convenção de proteger o processamento automático de dados. Acho que foi quando a computação em grande escala começou a ter um destaque maior na década de 80.

Na década de 90 já tínhamos uma derivativa... perdão, diretiva para a proteção de dados. Mas isso foi implementado de maneiras diferentes em cada país. E o desafio para as empresas era analisar como a lei era aplicada em cada país da Europa individualmente. As empresas tinham um custo alto para fazer isso.

Então, o GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) em 2016 foi criado para oferecer uma abordagem uniforme para todos os países para que as empresas pudessem criar uma implementação uma vez que pudesse ser aplicada em todos os países da Europa.

Ele é uma padronização da lei de privacidade. Não era algo realmente novo. Às vezes escuto as pessoas dizendo: “Nossa, agora temos essa lei de privacidade em 2016”. Na verdade, já tínhamos leis de privacidade na Europa desde a década de 80, mas o GDPR é uma padronização dessas leis.

O desafio para a ICANN é que precisamos... isso novamente se aplica a maioria das leis de privacidade... de uma definição clara da finalidade para... a coleta de dados. Acho que é importante discutirmos aqui a distinção entre a finalidade da coleta de dados para o registro público que, como vimos no 1591 de Jon Postel... é basicamente um serviço para a comunidade... e entre a coleta de dados para fins corporativos, como, por exemplo, para o registrador. Os registradores oferecem muitos serviços. Eles oferecem hospedagem na web, design, serviços de marketing. Eles coletam vários tipos de informações para seu próprio uso corporativo.

Mas a ICANN está preocupada é com a coleta de informações que se tornarão parte do registro público, então, na verdade, parte das informações públicas.

Precisamos decidir o que pode ser coletado. Precisamos decidir os campos que estarão disponíveis para o público em geral, se isso não precisará de autenticação; em outras palavras, não sabemos que tem acesso às informações. Quais campos devem ser disponibilizados para usuários legítimos com finalidades legais? Como poderíamos autenticar esses usuários legítimos ou legais? E o nosso desafio é criar uma solução que funcione no mundo todo.

Temos dados de pessoas físicas em praticamente todos os países do mundo agora. E muitos usuários geralmente estão localizados fora dos países onde os dados estão armazenados.

Além disso, temos diferentes leis aplicadas a pessoas físicas, mas também temos diferentes leis aplicadas às organizações que

armazenam esses dados. Então, isso é muito mais complicado do que desenvolver uma solução para um determinado país ou até mesmo para uma determinada região de países.

É importante apenas lembrarmos os princípios de privacidade incluídos no GDPR. Novamente, esses princípios são comuns a muitas normas de privacidade, mas o conceito de transparência, que o usuário deve dizer por que os dados estão sendo coletados, como eles serão armazenados, como serão processados, como serão liberados para terceiros.

O conceito de uma limitação para a finalidade. Só devemos coletar dados por motivos legítimos e especificados.

A minimização de dados é apenas um limite para o que é necessário. Então, se... e é nesse caso que ouvimos diferentes discussões. Para um registrador, um registrador que queira coletar informações para que possam prestar um serviço de e-mail não precisa de um serviço de correspondência postal. Porque o registrador nunca envia a correspondência pelo correio postal. Ele envia pelo correio eletrônico. Então, se você perguntar a um registrador que não tem nenhum outro requisito da ICANN, ele diria: “Bem, nós... precisamos coletar o cartão de crédito”. Isso basta para nós. Mas para uma finalidade pública, talvez você queira coletar mais informações, e cabe à comunidade decidir quais informações deverão ser coletadas.

Precisão, os dados devem ser atualizados constantemente. Na GNSO tem uma norma que diz que, todos os anos, os registradores devem lembrar os registrantes ou os titulares do e-mail registrado sobre os

dados armazenados no registro público, no WHOIS, e esse consumidor tem a oportunidade de atualizar os dados. Então, é uma tentativa de manter os dados atualizados. Obviamente, os registradores disponibilizam serviços para que os consumidores possam atualizar os dados a qualquer momento. Acho que, no que diz respeito à precisão, basicamente estamos em conformidade com o GDPR porque damos às pessoas a capacidade de atualizar os dados.

Os limites de armazenamento são, em uma situação normal do consumidor, assim que o consumidor parar de pagar com um cartão de crédito, você não precisará mais armazenar nenhum dos dados dele porque ele não será mais um cliente. Mas um registro público geralmente tem um prazo de armazenamento maior porque, no caso de litígios, talvez um problema fiscal, a maioria das empresas... países exigem que certas informações sejam armazenadas por alguns anos para a aplicação de impostos, por exemplo. Então, os limites de armazenamento são identificar do que precisamos enquanto comunidade da ICANN e por quanto tempo as informações devem ser armazenadas. Talvez as duas coisas durante a inscrição, mas após isso, que informações devem ser armazenadas.

Integridade e confidencialidade são basicamente segurança, de que os dados devem estar seguros.

Então, acho que uma das coisas que ouvi com frequência nesses painéis foi as pessoas dizerem o que consideram requisitos, e acho que isso já foi feito várias vezes. Em vez de vocês, sabe, pedirem para que cada membro do painel repita isso, eu resumi os principais aqui.

Certamente uma das suposições que tenho ouvido esta semana é que precisamos apoiar nosso processo de desenvolvimento de políticas. Existe a tentação de descobrirmos que ele é lento demais para tirarmos os recursos desse processo e colocá-los em outro lugar. Mas, para a ICANN funcionar, precisamos garantir esses recursos, nossa contribuição e ajudar as pessoas nesse processo de desenvolvimento de políticas. Então, minha suposição inicial é que ele será concluído e produzirá uma política.

Qualquer solução produzida deverá respeitar as leis de privacidade dos dados. O GDPR é apenas uma delas, na verdade. Existem várias.

Qualquer solução deverá permitir que as agências legais fiscalizadoras e agências públicas investiguem e responsabilizem os titulares de nomes pelo uso do nome de domínio.

Qualquer solução deverá proteger as pessoas que estão correndo risco. Eu costumo ouvir anedotas relacionando quando as pessoas... se separam, e há algum tipo de violência na relação que uma das partes... que precisou se mudar para outro local geográfico quer proteger o local dela, basicamente para se proteger contra a violência. Então, precisamos pensar nessas situações, que esses dados podem ser usados para causar dano real se forem liberados para a pessoa errada.

RDAP, ouvimos falar muito sobre isso. Novamente, acho que não é uma questão difícil. A comunidade técnica basicamente acredita que o RDPA é suficiente para as finalidades mencionadas na maioria das discussões. Mas o RDPA é apenas uma linguagem. É apenas uma

forma de trocar informações. O RDPA não é uma solução. É apenas uma linguagem que escolhemos para usar na troca de informações. Mas ela tem alguns recursos eficientes. Alguns desses recursos eficientes são que ela aceita o conceito de distribuímos as informações, em vez de centralizá-las. E ela tem fluxos padronizados de informações, que solucionam alguns problemas com o antigo modelo de WHOIS thin, onde tínhamos muitas implementações diferentes.

É muito parecida com o EPP, que é um padrão desenvolvido para permitir a comunicação entre os registros e registradores. Mas isso não substitui uma política. Precisamos ter uma política, para o RDPA possa implementar essa política.

A outra suposição aqui é que os registros e registradores sejam responsáveis pelos dados que armazenam. Eles coletam informações para uma série de finalidades, sendo que nem todas elas estão relacionadas ao nome de domínio, e eles são responsáveis pelo processamento e pela divulgação delas. Então, eles também precisam assumir essa responsabilidade.

Acho que a pergunta de abertura para o painel pode ser, considerando o histórico, considerando outros registros públicos, como os problemas para proteger dados pessoais têm sido gerenciados nesses registros, como é o conceito de termos usuários legítimos acessando informações que não estão disponíveis para o público em geral, que proteções precisam ser implementadas, etc. Compreendendo o contexto de que as leis de privacidade estão sendo

desenvolvidas no mundo todo, acho que nosso desafio é criar uma solução em tempo hábil. Na verdade, a primeira pergunta para o painel é: quais são os impedimentos que eles veem na ICANN após uma semana de discussão sobre esse assunto, o que eles percebem como barreiras ou impedimentos para encontrar uma solução, e o que eles acham que pode ser feito para superarmos esses impedimentos? O que cada um de vocês pode fazer? E temos uma sala cheia de pessoas. Temos centenas de pessoas nesta sala. Como vocês podem ajudar... ajudar as equipes de política, ajudar as pessoas que estão participando dos diferentes grupos de partes interessadas a criar uma solução eficiente?

Então, vou abrir para o painel para que possamos ouvir as opiniões deles sobre como encontrar a melhor solução e superar quaisquer impedimentos. Ashley, pode falar.

ASHLEY HEINEMAN:

Vou começar logo. Sim, vou começar em termos gerais e não tocar muito nos detalhes sobre o que estamos falando. Acho que muitos dos impedimentos, pelo menos os que eu enfrentei no último ano, mais ou menos, são as pessoas chegarem com noções preconcebidas sobre o que o outro lado está pensando e fazendo e quais são as motivações dele. E também descobri que, depois que realmente começamos a falar com as pessoas, particularmente as pessoas que representam opiniões, perspectivas e interesses diferentes, quando começamos a realmente falar sobre o assunto, vemos que não pensamos tão diferentemente assim. Mas acho que precisamos ter

mais oportunidades para realmente conversarmos e sermos construtivos e trabalharmos em direção a um objetivo comum e evitarmos as situações que tendemos a repetir quando expomos as nossas posições. Não estamos trabalhando realmente para encontrarmos um ponto em comum. E tenho esperança de que podemos superar isso. Eu já vi isso acontecer. Mas acho que esse assunto já está na mesa há tanto tempo, tem tanta bagagem, é difícil verificar essa bagagem na entrada e apenas trabalharmos juntos de maneira construtiva. Obrigada.

BRUCE TONKIN:

Sim. Acho que o desafio que temos é que as pessoas questionam as motivações e dizem: “Bem, você só está nessa posição porque tem esta determinada opinião”, e a realidade é que as opiniões da maioria das pessoas são mais ou menos equilibradas quando falam em privacidade, mas, às vezes, elas vêm a estes fóruns públicos e apenas falam sobre uma parte extrema disso. Talvez uma forma de lidarmos com isso seja fazermos várias perguntas. Então, as pessoas precisam parar de se meter em conversas com alguém de outro grupo de partes interessadas apenas para dizer: “Esta é minha posição, e estou certo”. Em vez disso, gostaria de pedir que vocês façam mais perguntas sobre por que as pessoas têm uma determinada opinião; assim, talvez consigamos encontrar um meio termo. Mas, sim, certamente, acho que uma facilitação mais eficiente e talvez cursos para as pessoas sobre como fazer perguntas, em vez de declarar suas opiniões, seria muito útil. Milton.

MILTON MUELLER:

Acho que o principal impedimento está muito claro para mim enquanto membro do EPDP, que é uma esperança muito grande em certas partes da comunidade de que possamos, de alguma forma, recriar o antigo WHOIS ou, de alguma forma, ter acesso aos dados com a facilidade e a liberdade que havia antes. E, é claro, nos 20 anos de existência do WHOIS, houve um acúmulo muito forte do interesse em igualdade no acesso a esses dados. Empresas inteiras se basearam nisso. O que acontece frequentemente é que, no EPDP, acabamos tendo um debate sobre o acesso e tudo se torna subordinado a esse interesse no acesso, mesmo quando deveríamos estar debatendo sobre outro assunto.

Então, acho que esse obstáculo pode ser superado se nós simplesmente nos concentrarmos primeiro na primeira etapa, que é finalizar a especificação temporária e entender exatamente o que será coletado e quais serão as finalidades e quais elementos de dados específicos serão necessários e quando eles deverão ser transferidos, e precisamos decidir essas coisas, se deixarmos de lado a questão do acesso para a próxima etapa, que é o que diz nosso regulamento.

Então, se não confundirmos as finalidades dos registros e registradores da ICANN na coleta de dados com o interesse legítimo de terceiros em acessar os dados e nos concentrarmos em corrigir a primeira parte, respondendo às perguntas relacionadas no regulamento, e depois pensarmos no acesso, acho que avançaremos muito mais rápido. Mas se toda discussão sobre finalidade e toda

discussão sobre coleta se tornar uma batalha de proxy pelo acesso, algo que não podemos resolver ainda, vamos ficar correndo sem sair do lugar por um bom tempo.

BRUCE TONKIN:

Tenho uma pergunta rápida para os participantes. Então, Milton, você disse que existe o medo de as pessoas acharem que deveríamos apenas voltar ao mundo antigo e voltar ao WHOIS como era antes. Quantas pessoas aqui na sala acham que essa é uma solução viável, de voltarmos a usar o WHOIS antigo? Uma pessoa. Então, acho que já desmistificamos esse mito. Ninguém acha que devemos fazer isso. Então, vamos seguir em frente. E acho que você tem razão, Milton, se você... se pensarmos nisso, se voltarmos aos princípios associados a qualquer lei de privacidade, qual é a finalidade da coleta e quais são as informações que precisam ser coletadas para atender a essa finalidade. Isso precisa obrigatoriamente ser o ponto de partida. Sim. Flip.

FLIP PETILLION:

Obrigado, Bruce. Na verdade, só quero lembrar a todos o que Cherine Chalaby disse na segunda-feira de manhã. Ele disse que precisamos encontrar um equilíbrio entre o que precisamos coletivamente e o que queremos individualmente. Eu achei a colocação dele brilhante. E essa é a essência do GDPR. E acho que precisamos, todos nós, nos lembrarmos o que é o GDPR. De onde ele surgiu. Qual é o objetivo dele. Francamente, quando todos estavam debatendo sobre a versão preliminar do GDPR, não pensaram nos problemas que estamos

tentando resolver hoje. Eles estavam pensando em proteger as pessoas contra propagandas e spam, etc. Mas não o problema com que estamos lidando hoje.

Precisamos é que todos que estão participando da discussão pensem: eu entendo qual é o verdadeiro objetivo aqui e o que eu quero está equilibrado com o interesse, não os direitos, mas os interesses dos outros. Eu não acho que, como algumas pessoas parecem achar, que é uma escolha entre o melhor e o (indiscernível). Temos um desequilíbrio agora. E esse desequilíbrio é certamente desagradável para várias pessoas da comunidade. Precisamos equilibrar as coisas novamente. Depois que entendermos isso, teremos discussões melhores. É disso que se trata. Do equilíbrio.

BRUCE TONKIN: Então, sua opinião é que, aceitar a... a comunidade precisa aceitar que existem necessidades que devem ser equilibradas. É isso?

FLIP PETILLION: Com certeza. O modelo da ICANN é todo baseado em um consenso, Bruce. Isso tem a ver com a confiança. Criamos gerar confiança em todos. E a confiança é a base para o consenso. E o consenso é a base para o equilíbrio. Um equilíbrio de interesses.

BRUCE TONKIN: Certo. Vamos fazer uma pequena votação. Quem acha que devemos nos concentrar aqui como parte do trabalho da nossa comunidade de

buscar um equilíbrio entre protegermos as informações e fornecermos as informações levante a mão. Parece que temos claramente a maioria. Então, isso é bom. Acho que estamos dizendo que, não podemos voltar ao WHOIS como era antes, mas também estamos dizendo para avançarmos, precisamos encontrar um equilíbrio. E temos bastante apoio na sala, eu acho, para isso. Acho que, novamente, essa é uma das suposições que temos, de que todos nós temos, que precisamos equilibrar esses interesses.

Como vocês acham que podemos conseguir esse equilíbrio? Qual é... qual é... essa é a parte difícil.

FLIP PETILLION:

Com bastante boa vontade e não pensando apenas no que é aplicável no GDPR, mas também externamente. Como as agências legais fiscalizadoras, proteção dos consumidores, tópicos muito importantes, proteção das crianças. Todas essas leis são aplicáveis. Não apenas na Europa. Não podemos nos esquecer de que temos uma diretiva de comércio eletrônico na Europa que, na verdade, tem uma disposição obrigatória sobre informações de contato do titular do site. Então, à primeira vista, isso vai diametricamente contra o que está no GDPR, mas não é. Não é porque cada item de lei na Europa, seja um regulamento, seja uma diretiva, ele sempre estabelecerá que a implementação e a aplicação do regulamento ou da diretiva devem ser equilibradas. Um equilíbrio com outras peças da estrutura regulatória que é aplicável. Então, na verdade, temos que ver o todo... a figura completa.

BRUCE TONKIN: Sim, acho que, quanto mais fizermos referência a esses detalhes específicos de algumas dessas outras leis nas discussões sobre políticas... porque, novamente, elas são apenas exemplos de como esse equilíbrio foi alcançado. Como eu disse no exemplo dos registros, todos eles têm um equilíbrio. Todos eles têm um equilíbrio entre fornecer informações suficientes ao público para permitir que as pessoas entendam quem é responsável por um determinado registro, mas também a capacidade de obter informações mais detalhadas quando realmente for necessário. Hadia.

HADIA EL MINIAWI: Hadia El Miniawi para deixar registrado. Na minha opinião, os desafios... quero falar sobre desafios de um ponto de vista prático, porque todos nós já sabemos que os dados de registro não são mais abertos. É um registro fechado de dados que estarão disponíveis... para divulgação com base nos interesses legítimos de terceiros. Então, eu gostaria de... e falando sobre equilíbrio, que você mencionou, precisamos reconhecer, é claro, que há... o equilíbrio é e será necessário. Mas também precisamos saber que não somos nós que faremos esse equilíbrio depois houver a divulgação, depois que houver a implementação. E, deixando isso de lado e...

NOME NÃO INFORMADO: WHOIS?

BRUCE TONKIN: Nós não faremos esse equilíbrio? Então, você está dizendo que não acha que nós faremos esse equilíbrio?

HADIA EL MINIAWI: Não, nós reconhecemos que o equilíbrio é necessário e que devemos equilibrar as necessidades entre terceiros ou as... as pessoas com interesses legítimos e os direitos dos registrantes. Mas, no que diz respeito à implementação e à divulgação, não estamos aqui que vamos... não vamos fazer esse equilíbrio caso a caso ou não vamos... não seremos nós que vamos implementar isso ou que vamos fazer esse equilíbrio agora.

Então, em alguns casos... os... os... reconhecemos o princípio, reconhecemos os fatos, mas na prática... de um ponto de vista prático, no que diz respeito à verdadeira implementação e divulgação dos dados, não seremos nós que vamos decidir nesse caso se o equilíbrio foi eficiente ou não. Então, precisamos ter isso em mente, na minha opinião.

Eu também gostaria de falar um pouco sobre os desafios de outro ponto de vista prático. Então, seja qual for o trabalho que fizermos ou as políticas que vamos criar, isso precisa ser prático, implementável e, é claro, além de estar em conformidade com o GDPR, mas prático e implementável também é muito importante, criar uma política que ninguém implementaria ou que não seja prático de implementar. É um desafio. E, na minha opinião, para lidar com isso, precisamos de alguns requisitos. Por exemplo, processos padronizados do setor. Isso

é obrigatório para a rede do registro, do registrador e do registrante, serviços de credenciamento e como vamos fazer isso.

E quem fará isso? Além disso, outros desafios relacionados a... correr os riscos de responsabilidade das partes contratadas. É importante... então, se tivermos uma política que não leve isso em consideração, ninguém implementará essa política, certo?

Então, na minha opinião, todos esses desafios precisam ser discutidos agora ou depois, em paralelo com o que estivermos fazendo agora, com o trabalho de políticas que estamos fazendo. E, espero, que consigamos alcançar o consenso para alguma coisa com que todos fiquem felizes.

Mas depois temos a pergunta: como implementar isso? E acho que é melhor trabalharmos com isso agora do que depois, e esse é nosso maior desafio, na minha opinião.

BRUCE TONKIN:

Sim. O que você está dizendo, em termos de criarmos uma solução em tempo hábil é a política certa. E Milton está ressaltando que precisamos ter uma comunidade concentrada em criar a política certa. Mas, para a solução final, precisamos pensar na implementação também, para que não comecemos a pensar sobre a implementação depois de concluirmos o trabalho da política. Precisamos pensar nisso em paralelo. Eu concordo.

Nick.

NICK WENBAN-SMITH: Obrigado. Nick Wenban-Smith. Estou aqui como representante das partes contratadas. E achei muito legal alguém ter mencionado o risco para as partes contratadas.

Quando olho para esse assunto, gosto dessa expressão “tempo hábil”, entre aspas. Porque estamos em outubro de 2018. E essa lei entrou em vigor em maio de 2018. Então, uma solução em tempo hábil teria sido há 12 meses.

Mas eu acho, em termos gerais, que embora tenha sido extremamente tarde e muito apressada considerando o que precisávamos fazer, a especificação temporária agradou as partes contratadas no geral. Então, quanto antes passarmos pelo processo de EPDP para formalizarmos isso, melhor. Depois poderemos falar sobre acesso.

Mas, na verdade, nós todos já tivemos que implicar nossas políticas de acesso. Porque, desde o dia 25 de maio, precisamos estar em conformidade com a lei. E isso inclui o acesso.

Então, um dos desafios muito interessante do GDPR diz respeito aos princípios. Precisamos equilibrar os princípios dos interesses legítimos com os direitos de privacidade dos objetos de dados de todas as pessoas que temos. E isso é um grande desafio. Nós tivemos, por necessidade, já que não há uma política global formal, que fazer isso por conta própria. Então, temos um tipo de colcha de retalhos, infelizmente, de diferentes políticas de divulgação.

E sei que o que fazemos no Reino Unido é legal porque recebemos centenas de solicitações de acesso. Na verdade, já recebi algumas reclamações. E a forma de saber se você está em conformidade no que diz respeito à lei de proteção de dados é olhando pelo espelho retrovisor. Se alguém não gosta do que você está fazendo, essa pessoa reclama para a autoridade de proteção de dados. E eles escrevem para você como a autoridade de proteção de dados para sua organização dizendo: “Recebemos uma reclamação”.

Eu recebi uma reclamação sobre divulgação de dados para um agente de fiscalização de direitos de propriedade intelectual. E essa reclamação foi rejeitada. Eu sei que o meu processo para divulgação é basicamente robusto o suficiente para pelo menos começar a suportar os tipos de desafios que enfrentamos dos objetos de proteção de dados que certamente exigem os direitos deles de fazer reclamações, caso não gostem da maneira que os dados deles são usados.

Então, estamos começando a construir um conjunto de experiências em lidar com fatos reais de implementação pós-GDPR. Acho que precisamos transformar isso em solução daqui para frente. Porque o que sabemos é que recebemos solicitações que não podemos atender. Recebemos cerca de... nos últimos três meses recebemos cerca de 750 solicitações. E atendemos a 96,5% delas. Mas algumas pessoas simplesmente não dão nenhum motivo. E claramente não são solicitações em conformidade, então, isso também precisa ser incluído nesses sistemas.

BRUCE TONKIN: Então, o que você está dizendo é que... como a Hadia disse... existem decisões que precisam ser feitas localmente com base nos fatos apresentados sobre fornecer acesso a um determinado elemento de dados. Mas também precisamos de mecanismos em conformidade para os dois lados, presumivelmente, para que a parte que solicitar os dados tenha uma forma de fazer uma reclamação se não receber o serviço. E o objeto de dados, se me permitem falar assim, precisa estar em conformidade com essas informações armazenadas ou divulgadas.

NICK WENBAN-SMITH: O mecanismo já está definido na legislação. Ele já existe.

BRUCE TONKIN: Que bom. Excelente. Greg.

GREG AARON: Obrigado, Bruce.

Parte das conversas sendo realizadas esta semana são sobre essas responsabilidades que o GDPR está colocando em todos. E isso é uma coisa boa.

Diz respeito à prestação de contas, de certa forma. Mas isso também se transforma em uma discussão sobre gerenciamento de riscos. Todos têm essas responsabilidades. E, é claro, às vezes temos

penalidades associadas quando essas responsabilidades não são cumpridas.

Certamente, o problema com o gerenciamento de riscos é que, às vezes, ele se transforma em uma discussão sobre custo.

O que preciso fazer para proteger os dados adequadamente? Que risco vou correr se por acaso compartilhar alguns dados?

E essa discussão sobre custo está permeando parte das conversas.

Um dos problemas é que todos estão avaliando os riscos e o que a lei diz. E essas avaliações são muito diferentes. Vemos isso até mesmo nos ccTLDs europeus, nos RIRs e assim por diante, onde eles tomam decisões diferentes com base no conselho que recebem e da disposição a riscos.

E essa imprevisibilidade é algo que estamos lentamente começando a discutir e descobrir. Porque, no final das contas, queremos um sistema onde possamos ter alguma certeza e confiança de que os dados estão sendo cuidados adequadamente por todos os envolvidos, aquele que os coletam e aqueles talvez os recebam e os usem.

E esse é o ponto de equilíbrio de que precisamos. Porque, no final das contas, para o pessoal de segurança cibernética, é importante para nós usarmos os dados. Porque precisamos proteger as pessoas. E a lei diz que precisamos... vocês sabem, podemos ter o acesso, se isso for feito adequadamente.

Então, queremos encontrar esse equilíbrio adequado. Mas precisamos fazer com que isso aconteça.

BRUCE TONKIN: Deixem-me passar para outra pessoa. Chris.

CHRIS LEWIS-EVANS: Obrigado. Primeiro, eu gostaria de ressaltar o progresso que este grupo já fez. E acho que sua primeira pergunta aos participantes foi muito boa. Porque, acho que, se você tivesse feito essa mesma pergunta no ICANN61, por exemplo, acho que teríamos uma resposta muito diferente dos participantes.

Acho que essa mudança na aceitação do que é necessário se deve ao entendimento dos diferentes requisitos exigidos de todas as partes da comunidade na ICANN.

Tanto do lado da proteção de dados quanto das partes que têm direito ao acesso pela finalidade legítima e legal. E, na verdade, esse entendimento surgiu do entendimento das exigências das pessoas, e não das soluções delas.

Acho que no EPDP, onde foi feita a maior parte do progresso, foi onde nós falamos sobre quais são cada uma das exigências das partes, em vez de quais seriam as soluções para atender aos requisitos delas.

E acho que essa é a melhor maneira de termos um bom entendimento das verdadeiras exigências de todos, para depois conseguirmos fazer

o equilíbrio disso, sobre o que já falamos. A questão é entendermos essas exigências para podermos tomar uma decisão bem equilibrada.

BRUCE TONKIN: Que é a finalidade da qual Milton falou, na verdade. Qual é a finalidade para você coletar os dados? Depois, quais dados você precisa para essa finalidade basicamente?

CHRIS LEWIS-EVANS: Exatamente. E acho que, para criarmos uma solução em tempo hábil, acho que realmente precisamos nos concentrar nessas exigências e depois equilibrá-las com um entendimento das necessidades de todos também.

BRUCE TONKIN: Interessante. Se analisarmos os projetos de TI... e as pessoas fazem revisões de projetos de TI... a principal razão para um projeto não ser finalizado é porque a equipe não passou tempo suficiente para entender os requisitos. Então, acho que é um ponto em comum isso, de que precisamos acertar isso. Cristina.

CRISTINA MONTI: Obrigada. Cristina Monti, Comissão Europeia. Quero ressaltar algumas observações dos meus colegas.

Se olharmos para o futuro e quais são os impedimentos, acho que também precisamos reconhecer que esses problemas já existem há muito tempo.

E talvez uma coisa que o GDPR conseguiu foi realmente trazer à tona o problema e nos obrigar a encontrar uma solução em pouco tempo.

Acho que muita coisa aconteceu. Percebemos nos participantes que ninguém mais hoje em dia pensa que a privacidade não é importante. Os dados... todos concordam que os dados... os dados pessoais são valiosos. E as pessoas que lidam com dados pessoais também devem ser responsabilizadas pela maneira que usam e administram esses dados.

Acho que também que, mesmo aqui no ambiente da ICANN, muito progresso já foi feito no sentido que agora pelo menos temos todos os nossos canais de comunicação abertos. O problema da reforma do WHOIS está agora na programação em muitas discussões de alto nível fora da ICANN. Então, acho que, nesse sentido, tivemos progresso e as discussões estão se encaminhando para uma fase mais madura.

Agora estamos nos concentrando de fato nas soluções. E é aqui que surgem os verdadeiros problemas. É claro que na operacionalização dos princípios que vimos é onde está o truque. E acho que, se, de certa forma, o modelo de múltiplas partes interessadas que temos aqui na ICANN está sendo desafiador porque temos muitos interesses diferentes... e às vezes as discussões ficam muito polarizadas... realmente acredito que somente em um ambiente de múltiplas partes interessadas é possível encontrar uma solução sustentável.

Também acho que neste exato momento sabemos que precisamos tomar medidas para garantir que o registro de WHOIS esteja em conformidade com o GDPR. Mas, novamente, ainda não estamos nessa etapa de uma solução final e previsível.

Acho que isso tem um impacto em muitos outros agentes, como sabemos bem. Às vezes, acho que é negligenciado o aspecto de que mesmo os registradores individuais ou os usuários individuais não sabem como os dados deles são gerenciados, quem devem contatar se quiserem fazer uma correção nos dados, e assim por diante.

Então, mesmo dessa perspectiva, agora estamos em uma situação em que estamos praticamente no meio.

BRUCE TONKIN:

Acho que foi uma boa observação sobre os usuários individuais. Porque minha experiência é que a maioria dos usuários individuais não sabe sobre a existência do WHOIS, por exemplo. A maioria das pessoas nesta sala, sim, porque a maioria das pessoas aqui são profissionais no setor de TI ou já participaram de um encontro da ICANN antes e já ouviram falar nisso.

Mas o usuário comum não pensa em usar o WHOIS. O usuário comum provavelmente, se tivesse uma experiência desagradável no site dele, ele provavelmente relataria isso para o departamento de assuntos do consumidor ou algum outro grupo sem ao menos saber que esses serviços existem. E eles certamente não sabem que as informações

deles possam ter sido publicadas em outro lugar. Tornar isso transparente, eu acho, é um princípio importante. Sim.

CRISTINA MONTI:

Com certeza. E apenas para complementar também e para relacionar à questão dos riscos que foi levantada, eu gostaria de fazer uma observação sobre o GDPR, que é baseado em regras que já existem há muito tempo, na verdade, ele deve ser entendido como um incentivo para todos os agentes que precisam... precisam lidar com dados pessoais, de fazer isso de maneira legal, transparente e responsável. E o GDPR agora, mesmo para os agentes fora da Europa, a situação melhorou de modo que agora temos uma uniformidade muito maior em como as regras são aplicadas, porque temos mecanismos em vigor para isso.

Então, antes do GDPR, tínhamos muitas leis nacionais diferentes. E com o GDPR temos uma uniformidade muito maior. Então, para um agente fora da Europa, será muito mais fácil do que lidar com esses problemas. Eu só queria acrescentar essas observações. Obrigada.

BRUCE TONKIN:

Certamente elevando o nível de padronização globalmente, eu acho. Hadia, e depois volto para o Nick.

HADIA EL MINIAWI:

Como já foi dito, desafio é um mal-entendido. Quero só observar rapidamente que não estamos coletando dados de maneira nenhuma

para a finalidade das partes com interesses de terceiro ou com interesses que... aqueles que têm interesses em acessar os dados. Porque isso é um mal-entendido.

Ouvi pessoas dizerem que nós estamos coletando dados para as agências legais fiscalizadoras. Que estamos coletando dados para crimes cibernéticos. Que estamos... exigidos por essas pessoas.

E quero garantir a todos aqui que os dados são coletados apenas para as finalidades necessárias para... para satisfazer o serviço, cumprir o serviço. Isso.

BRUCE TONKIN: Que é o princípio de minimização dos dados. Coletar apenas o que precisamos. Identificar a finalidade e coletar o que é necessário.

HADIA EL MINIAWI: E os terceiros acabarão tendo acesso ao que estiver sendo coletado para essas finalidades.

BRUCE TONKIN: Claro. Nick e depois Milton. Quero pedir que tenham cuidado de não entrar nos detalhes de determinados elementos de dados, mas sim o princípio.

Nick?

NICK WENBAN-SMITH: Eu ia dizer que há um risco, e o risco recai apenas nas partes contratadas. Isso é uma das coisas que nos motiva a buscar uma política mais conservadora. Acho que há um ponto de vista mais amplo. Na verdade, pessoalmente não tenho medo quando as pessoas falam das altas penalidades financeiras que poderão ser aprovadas. E para as organizações responsáveis isso apenas não é uma consideração muito relevante para mim.

Estou muito mais preocupado nesta era de cidadania digital com a reputação por administrar os dados adequadamente e legalmente, em conformidade com a lei, e isso é, na verdade, uma vantagem competitiva agora entre as nossas partes contratadas. É um tipo de reconsideração mais ampla, na minha opinião. Seria muito bom acrescentarmos isso também.

BRUCE TONKIN: Acho que você está falando em confiança.

Muitas pessoas estão perdendo a confiança agora porque descobriram que forneceram dados para um determinado serviço que contrataram. E, sem elas saberem, os dados estão sendo enviados a um terceiro ou sendo usados de uma forma que elas não compreendem.

Acho que um ponto importante, voltando aos objetivos gerais da ICANN, é que precisamos que as pessoas confiem no sistema de domínios, confiem que elas podem registrar um domínio, e confiem que nós vamos cuidar desses dados adequadamente. Caso contrário,

as pessoas não vão registrar nomes de domínio. Em vez disso, elas vão usar as mídias sociais. Acho que esse é um ponto muito importante.

Milton.

MILTON MUELLER:

Quero fazer uma observação sobre um comentário da Cristina Monti. Esse é um assunto bastante de alto nível sobre a função da ICANN enquanto uma instituição de governança global e como ela se relaciona aos estados e governos e as leis deles. Porque eu acho que essa é uma das questões fundamentais com as quais estamos lidando aqui.

Então, não sou um grande fã do regulamento de proteção de dados da Europa antes do GDPR. Mas preciso confessar que, em retrospectiva, acho que a Europa fez um favor ao mundo definindo um padrão.

Então, em termos de regulamentos e governança, temos algo chamado “efeito Califórnia”. Foi quando o Estado da Califórnia definiu os padrões de poluição para carros que eram muito mais rigorosos do que no resto do país. E os fabricantes precisaram decidir se faziam um carro para a Califórnia e um tipo diferente de carro para outras jurisdições ou se faziam apenas um carro? Essencialmente, é isso que está acontecendo agora com o GDPR e a privacidade, é que eles definiram um padrão. E acho que a questão é... enquanto agência global, a ICANN consegue atender a esse padrão? Ou vamos entrar em um conjunto de padrões concorrentes?

Por exemplo, se os Estados Unidos decidir que não gostam do que a Europa fez, eles vão definir um padrão diferente e conflitante, e teremos um sistema mais fragmentado? Acho que esse é um dos maiores problemas do qual precisamos estar cientes enquanto falamos sobre conformidade com o GDPR.

E estou usando apenas os Estados Unidos como exemplo. Qualquer outra jurisdição maior poderá criar os mesmos problemas. Pode ser a China. Pode ser a Índia. Pode ser talvez o Canadá? Não sei.

Mas vocês entenderam, o que quero dizer é que estamos lidando com um problema muito importante e complicado sobre o status da ICANN enquanto uma agência de governança global baseada no setor privado, a qual eu acredito que a maioria de nós aqui apoiemos, em comparação a um sistema baseado em estados de soberania fragmentada territorialmente onde poderíamos ter vários sistemas.

BRUCE TONKIN:

Sim. E acho que, se olharmos a história do GDPR, isso estava acontecendo na Europa, cada país falava sobre os princípios de alto nível, mas os interpretava de maneira diferente, o que gerou um custo para as empresas. E posso imaginar que as empresas talvez se interessem por um mercado maior e atendam aos requisitos da Alemanha ou algo assim. É um mercado maior. Mas, se você for um país europeu menor, elas diriam que poderiam fazer negócios ali porque as leis de privacidade são muito complicadas.

Então, acho que foi uma vantagem unificarmos para que as pessoas possam ver um mercado grande. Como na Califórnia... se fosse um dos outros estados nos EUA talvez com uma população menor e esse padrão de emissões fosse definido, provavelmente não teria feito diferença. Mas a Califórnia é uma economia enorme por si só. Os fabricantes de carros teriam que fazer carros para esse mercado. E os outros tirariam vantagem disso.

Sim. Flip.

FLIP PETILLION:

Obrigado, Bruce. Flip Petillion. Só quero acrescentar um comentário sobre confiança.

Existe confiança quando damos as informações, mas também deveria haver confiança quando há uma solicitação de informações. E todos deveriam mostrar o compromisso de contribuir para essa confiança. Acho que a Nominet tem dado um bom exemplo. Vimos outro exemplo apresentado pelo Sr. Noss de um determinado registrador. E esses são bons exemplos de compromisso, de boa vontade. Na Europa chamaríamos isso de boa-fé. Na verdade, é a disposição de encontrar uma solução viável. Eu só queria acrescentar isso.

BRUCE TONKIN:

Sim, e um dos principais pontos sobre o acesso aos dados, além disso, é que, quando uma parte solicita acesso, ela se torna responsável depois que recebe os dados e precisam prestar contas sobre o que acontece com os dados. Então, não é por que a parte tem acesso aos

dados, que ela tem o direito de fazer o quiser com eles. Essa prestação de contas precisa fazer parte da estrutura de confiança também. E as pessoas que acessarem os dados e não os usarem adequadamente, perderão o acesso. Isso é bastante simples.

Acho que vou passar para os participantes agora. Tenho algumas perguntas para fazer ao painel, mas considerando que várias pessoas da comunidade estão participando, que deixar aberto para perguntas ao painel, e particularmente aquelas que estão relacionadas a esse ponto. Como faremos para criar uma solução em tempo hábil? Como todos nós podemos ajudar a criar essa solução?

Não tenho certeza como as perguntas estão sendo feitas aqui. Vejo uma na primeira fileira. Vamos começar por aí.

HOLLY RAICHE:

Só uma pergunta. Em termos de finalidade, você precisa testar a finalidade em termos de ICANN, mas o escopo da ICANN é bastante amplo. Ouvi alguns argumentos de que o escopo diz respeito apenas a assuntos técnicos. Acho que, se pensarmos na missão da ICANN, ela é mais ampla do que isso. Se pegarmos os dados de alguém, não é apenas para dar uma superfície técnica. É para fazer coisas como permitir a transferência de algo, é para resoluções de disputas. Quando pensamos em finalidade, eu ficaria preocupada se não fosse algo pelo menos amplamente definido para que a missão seja, de fato, o gerenciamento de todo o sistema e da estabilidade dele.

BRUCE TONKIN: Sim. Boas observações. Algum comentário dos membros do painel? Ashley?

ASHLEY HEINEMAN: Sim, eu acho que demorou um pouco, mas o EPDP já reconheceu isso. Em termos de desenvolvimento das nossas finalidades, acho que capturamos praticamente tudo que você mencionou, e isso é bom. Acho que o nosso trabalho ainda não está bem finalizado, mas reconhecemos isso, particularmente com relação à segurança, estabilidade e resiliência do Sistema de Nomes de Domínio.

BRUCE TONKIN: Você tem outra pergunta? Ah, trabalhamos com essas coisas. Então, número 1, depois o número 2.

NOME NÃO INFORMADO: Sou o número 1.

BRUCE TONKIN: Agora estou vendo o sistema.

RACHEL POLLACK: Rachel Pollack pela UNESCO, e obrigada por essa discussão tão interessante.

No último encontro da ICANN do qual participei em Copenhague há mais ou menos um ano e meio, o Conselho... perdão, o Conselho Europeu havia trazido representantes da proteção de dados para ajudar a facilitar a discussão entre esses representantes e os membros

da comunidade e isso foi bastante esclarecedor. Entendo que eles têm... tem um pouco de eco aqui. Entendo que eles lançaram um guia no início deste ano sobre problemas relacionados à proteção de dados na ICANN. Então, eu gostaria de saber se algum dos membros do painel já... analisou esse guia e o que achou. Vocês imaginam que ter essas discussões novamente com os representantes da proteção de dados possa garantir que qualquer modelo adotado no final esteja, de fato, alinhado de maneira estruturada e sistemática?

Depois, só para falar diretamente pela minha organização e não relacionado à ICANN, mas nós publicamos dois estudos que analisaram problemas de liberdade de expressão, privacidade e transparência. E acho que aqueles comentários sobre um equilíbrio entre esses diversos direitos humanos e como... como encontrar um equilíbrio. Eu recomendo que vocês... que vocês deem uma olhada na série da UNESCO sobre liberdade na Internet.

Obrigada.

BRUCE TONKIN:

Apenas um breve comentário, sobre os representantes da proteção de dados. A ICANN entrou em contato para ver se poderíamos ter alguns palestrantes lá e participando do painel. Na verdade, eles têm um evento acontecendo nesta semana. É algum evento para representantes de dados europeus, então, foi uma coincidência infeliz.

Mas, voltando à pergunta... sim, Hadia.

HADIA EL MINIAWI: Então, respondendo à sua pergunta, certamente levamos em consideração todas as correspondências com a Diretoria Europeia de Proteção dos Dados e todas as cartas e conselhos que foram fornecidos à ICANN. Então... durante esse trabalho, no desenvolvimento da política, demos uma olhada em tudo que foi fornecido e levamos isso em consideração.

BRUCE TONKIN: Ótimo. Cristina.

CRISTINA MONTI: Talvez apenas para esclarecer e complementar a pergunta. É claro que estamos cientes do guia fornecido pelo Conselho Europeu, que é um documento muito útil. No entanto, ele entra na parte dos princípios. E agora estamos lidando com o GDPR, e o Conselho Europeu está mais encarregado da Convenção 108, que é um tipo diferente de instrumento. E precisamos ter isso em mente.

E sobre as autoridades de proteção de dados, você tem razão, eles não puderam vir a este encontro porque está sendo realizada uma grande conferência internacional em Bruxelas, mas eu também gostaria de garantir e enfatizar que as autoridades de proteção de dados europeias estão cientes desta discussão, estão acompanhando o progresso que foi feito e têm dado orientações, quando foram solicitadas a fornecer pareceres sobre questões específicas, e acho

que elas estão bastante abertas para continuar essa discussão. E isso também está relacionado ao medo de multas.

Eu gostaria de lembrar que as autoridades de proteção de dados, sim, têm poderes maiores agora, mas elas têm uma série de ferramentas à disposição. Então, antes de falarem sobre uma multa, acredito que elas usarão outras ferramentas, como emitir alertas ou isso... emitir uma ordem. Sendo assim, acho que estão também mostrando disposição para dialogar, nesse sentido. E isso é muito importante.

BRUCE TONKIN:

Sim, acho que isso é algo muito importante. Então, em outras palavras, o ponto de partida da conformidade ou fiscalização é uma abordagem cooperativa, que é ajudar as pessoas a entender quais são os requisitos dela, de certa forma. Depois, se elas estiverem ignorando, o caso seria encaminhado. Sim.

Número 2.

NOME NÃO INFORMADO:

Esta pergunta é para o Nick e é de um dos nossos participantes remotos. A experiência das partes contratadas sobre acessos é muito importante. Quais foram os números de solicitações de acesso de terceiros recebidos pela Nominet desde o dia 25 de maio de agências legais fiscalizadoras? Vocês estão publicando um relatório de transparência com essas solicitações, divulgações, cronogramas e recursos? O CPH está considerando publicar isso?

BRUCE TONKIN: É com você, Nick.

NICK WENBAN-SMITH: Obrigado pela pergunta. E ela é, talvez, uma forma de abordagem mais empírica ao desenvolvimento de políticas, de olharmos para trás e analisarmos nossas experiências.

Então, sempre tivemos políticas de acesso a dados, mesmo antes do GDPR, porque tínhamos alguns elementos de dados que não eram disponibilizados no nosso WHOIS público. Estou me referindo ao código de país .UK que é o maior... um dos maiores códigos de país. Temos 12 milhões de domínios, e só isso já dá a você uma boa ideia em termos de números.

Nós percebemos um aumento de solicitações de dados. Antes do dia 25 de maio, não publicávamos, de maneira alguma, endereços de e-mail nem números de telefone no nosso WHOIS público, então, as pessoas ainda podiam enviar uma solicitação por meio de um processo de liberação de dados, e tínhamos alguns desses todos os meses. Após o GDPR, nós tivemos... estamos coletando os números e analisando-os com cuidado. É um dos meus pequenos hobbies, a análise de dados. Então, sim, tivemos quase 800 solicitações por dados individuais de registros de nomes de domínio em um período de três meses. E, na verdade, o que vou fazer, eu acho, é que teremos uma análise desde o dia 25 de maio mais seis meses e depois farei um

breve relatório sobre as nossas experiências, porque ainda está muito cedo.

Mas nós... quando recebemos solicitações, obviamente as analisamos, e até formamos os objetos de dados de que os dados foram solicitados e se concordamos com a solicitação ou não. Então, isso também faz parte da transparência.

Temos vários diferentes elementos de relatórios que ocorrem em cada solicitação individual, mas acho que, sim, com certeza daqui para a frente, vamos analisar... analisar certamente com base na organização. E entre as partes contratadas temos grupos de discussão muito ativos sobre todos esses tópicos e a coleta das nossas informações e experiências juntos e tentamos usar isso para analisarmos as experiências reais e encontrarmos uma solução também, vemos o que não está funcionando bem. Eu diria que os números não foram tão altos em termos de solicitações de dados que algumas pessoas estavam sugerindo. Isso parcialmente porque nós fornecemos às agências legais fiscalizadoras muitos dados sem que sejam necessárias solicitações individuais. Mas... estou um pouco nervoso, e sei que a solução de RDAP é tecnicamente fornecer acesso, e as partes contratadas em geral apoiam isso totalmente, mas estou um pouco preocupado com base em algumas experiências anteriores com... com a forma como a ICANN tem implementado as coisas, que talvez tenhamos no final um sistema de implementação bastante complexo e caro, cheio muita engenharia para pessoas com grande conhecimento de engenharia para o número real de solicitações que as pessoas recebem. E precisamos lembrar disso... porque, embora o

.UK seja um registro grande, nós também somos um registro nacional para os domínios do País de Gales. Eles têm algumas dezenas de milhares de domínios e nós não recebemos nenhuma solicitação de dados. Então, implementar algo para... e isso, por sinal, para o Programa de Novos gTLDs, seria bastante representativo para muitos desses novos gTLDs.

Então, implementar algo muito complicado com um custo alto e despesas altas para algo que, na verdade... isso não se justifica em termos de escala e do custo da implementação. Isso seria outra coisa para... para analisarmos, porque eu gostaria de saber, entre os registros menores, eles chegaram a receber alguma solicitação?

BRUCE TONKIN: Então, apenas para mencionar o número novamente, acho que a pergunta foi, deixando de lado as agências legais fiscalizadoras, se ouvi direito, 800 por mês, certo?

NICK WENBAN-SMITH: 800 em três meses. Um trimestre.

BRUCE TONKIN: 800 em três meses. Então, 800 em um trimestre. Obrigado.

Microfone 1. Acho que você precisa pegar um número.

NOME NÃO INFORMADO: Obrigado, Bruce. Quero fazer uma pergunta, porque você fez uma afirmação sobre um dos princípios do GDPR sobre precisão, e você disse, mais ou menos, que o problema está solucionado, porque existem alguns padrões de precisão em vigor para atualizar uma vez ao ano pelo registrante todos os itens no WHOIS que são mencionados. E essa é uma discussão em andamento que também temos no EPDP. Acho que isso não está muito longe de uma boa solução, porque... a pergunta é, como vocês podem atender uma finalidade se tiverem dados imprecisos ou falso ou seja o que for? Como podem atender a uma finalidade? E não estou falando apenas do ponto de vista de terceiros, que não terão isso, mas também para as partes contratadas ou a ICANN ou quem quiser ter essas informações... por exemplo, para entrar em contato com alguém... e essa pessoa descobre que esses dados... que os dados que estão com ela não são precisos ou estão obsoletos ou algo assim.

Então, eu acho que esse é um assunto que varremos para debaixo do tapete. Entendo que o custo é alto, talvez, complicado ou é um problema chato, mas eu acredito que ainda não temos uma solução satisfatória para isso.

BRUCE TONKIN: Então, isso está relacionado à autenticação dos dados inseridos. Sim.

Algum comentário? Milton.

MILTON MUELLER: Sim, acho que o fantasma do antigo WHOIS ainda está assombrando muitas pessoas, e o problema da precisão é um bom exemplo disso.

Então, antes tínhamos o acesso indiscriminado a dados de contato pessoais, e pessoas boas e más, por motivos óbvios, colocavam dados imprecisos no WHOIS porque sabiam que eles seriam publicados. Depois que esses dados forem protegidos contra o acesso público indiscriminado, o problema da precisão será completamente diferente. Sim, ainda haverá pessoas que colocarão informações falsas, mas esse não será o caso da maioria dos registrantes legítimos.

Então... além disso, a discussão sobre a verificação dos dados é um problema ortogonal com os princípios no que diz respeito aos dados que coletamos e porque os coletamos. É um problema distinto de política. Temos um conjunto de políticas que já existe sobre precisão, como todos sabemos, e é... é um bom exemplo dos impedimentos ao progresso, porque as pessoas começam a anexar coisas ao processo de decisão, sobre quais dados estamos coletando e como estamos mantendo a conformidade com o GDPR, que são coisas ortogonais à conformidade com o GDPR e podem ser tratadas por meio de outros processos de políticas mais tarde.

BRUCE TONKIN: Certo. Número 2.

FIRDAUSI: Obrigado. Meu nome é Firdausi.

Eu gostaria de perguntar, talvez para o exemplo sobre o regulamento de conflitos. Por exemplo, se consultarmos o princípio legal como especialista (indiscernível) ou como (indiscernível). Então, um é o regulamento do especialista prevalecerá sobre o geral, e o outro é que o mais novo prevalecerá sobre o antigo.

Então, se analisarmos o exemplo, por exemplo, porque há uma finalidade para investigação, então, se analisarmos por exemplo, entre o GDPR e o RIPA, que é a Lei de Poder Investigatório de Regulamentos, então, como esse princípio legal pode ser implementado? Ou talvez exista outra teoria legal que possa ser implementada. Além disso, considerando que o GDPR se aplica não apenas na UE, mas também fora da UE, na prática, como um governo de outra região ou, talvez, outra região que tenha uma instituição semelhante, como a UE, por exemplo, a ASEAN, no sudeste asiático, como manteriam a conformidade com isso? Seria o caso de criar um acordo multilateral ou talvez um acordo bilateral ou talvez apenas caso a caso (indiscernível) com um assistente legal?

Além disso, porque... acho que ouvi um dos painelistas falando sobre reconhecimento da privacidade também do consumidor e assim por diante. Então, como vocês acham que será a função de uma autoridade de privacidade ou autoridade de proteção de dados no futuro? Porque isso significa que... quando a UE definiu o padrão do GDPR, acho que as necessidades de muitas empresas no mundo todo de ter uma autoridade de privacidade ou de proteção de dados tornou-se ainda mais urgente.

Obrigado.

BRUCE TONKIN: Obrigado. Vou pedir algumas respostas para a sua pergunta. Primeiro, vamos perguntar ao Nick. Então, vocês recebem respostas ou solicitações de dados de partes fora do Reino Unido que estão em jurisdições legais diferentes? E como vocês administram isso enquanto autoridades de proteção de dados?

NICK WENBAN-SMITH: Obrigado pela pergunta. Acho que... bem, temos um processo padrão e não importa quem você é. Nós recebemos algumas solicitações de fora do Reino Unido. A maioria das nossas solicitações vem da nossa jurisdição, e acho que isso parcialmente é porque a maioria dos nossos registros são baseados aqui e parcialmente onde está a nossa região legal, onde está o nosso governo e LEAs locais, as pessoas com as quais temos as melhores redes. Mas temos muitos registradores fora do Reino Unido, e temos muitos registrantes fora do Reino Unido. Então, a mesma política se aplica. É uma política global.

E acho que, quando olhamos como o GDPR tem funcionado na prática, é muito bacana perceber que, na verdade, temos visto um alto nível de padronização no nosso trabalho em geral.

Então, sim, é a mesma... a mesma... independentemente de quem faça a solicitação.

BRUCE TONKIN: Então, como vocês não estão aqui, porque estão localizados na Europa, estão vinculados à lei europeia, então, basicamente, vocês estão aplicando essa lei a todas as solicitações recebidas de fora. É isso que me parece.

NICK WENBAN-SMITH: Mas em termos de como isso é implementado, em termos de acesso, é a mesma política para todos. Não precisa ser, mas é muito mais simples para nós fazermos assim.

BRUCE TONKIN: Vocês tentaram padronizá-la.

NICK WENBAN-SMITH: Sim, certamente.

BRUCE TONKIN: Talvez, Ashley, se você puder fazer algumas observações de um governo diferente ou de um governo fora da Europa, como você acha que os registradores ou registros devem levar outras leis em consideração, talvez as leis nos EUA sejam diferentes do GDPR.

ASHLEY HEINEMAN: Não vou falar pelos EUA, porque não estou em uma posição para isso. Estou aqui para falar pelo GAC. Mas vou dizer que precisamos ter cuidado ao nos referirmos ao GDPR como um padrão para privacidade e proteção de dados global. É que... temos muitos regulamentos de

proteção de dados por aí. Acho que... não quero exagerar muito nisso, mas acho que o que realmente... trouxe isso à tona como um problema para a ICANN foi todos os riscos e as responsabilidades colocadas nas partes contratadas.

Então, acho que as pessoas esperam que a maior parte do GDPR seja em geral o mesmo tipo de conteúdo que as outras leis de proteção de dados, mas também temos o conflito com procedimentos de leis nacionais que ainda existem. Como isso será administrado é outra questão. Mas acho que o interesse dos governos, também, é... em termos de como isso tudo será implementado, é a capacidade das agências legais fiscalizadoras fora da Comissão Europeia... porque está muito claro que o GDPR permite uma certa, digamos, facilidade na justificativa de acesso para agências legais fiscalizadoras europeias. Não está muito claro se isso se aplica às outras agências legais fiscalizadoras do mundo todo. Então, é algo para considerarmos.

Obrigada.

BRUCE TONKIN: Obrigada. Ok.

Número 1.

NOME NÃO INFORMADO: Janis Sordie (fonética). Minha pergunta é sobre seu comentário sobre receber 800 solicitações em três meses.

Então, antes do GDPR, quantas solicitações vocês recebiam por mês, nos últimos, digamos, dois anos? Porque isso seria, me parece, dados mais interessantes sobre as solicitações reais que as pessoas enviam em geral, a comunidade em geral.

NICK WENBAN-SMITH: Obrigado pela pergunta. Então, não é exatamente o mesmo mês a mês, porque, às vezes, nós recebemos uma solicitação grande de uma determinada agência que está trabalhando em algo. Digamos, no período que antecede o Natal, temos mais investigações. Enfim...

Acho que a escala da mudança nas solicitações passou de aproximadamente 10 a 20 por mês para cerca de um terço de 800, que é 250 por mês. Essa é a escala do que mudou.

BRUCE TONKIN: Estou presumindo, Nick, que houve uma ampla divulgação sobre não apenas os serviços de vocês, mas sobre o GDPR em geral no Reino Unido? As pessoas estão sabendo sobre isso?

NICK WENBAN-SMITH: Na verdade, essa é uma pergunta muito interessante porque o mais curioso sobre o GDPR é que ele ainda não, eu não acho, ele não alterou significativamente a lei no Reino Unido. Mas o que ocorreu foi... em termos do conhecimento de cada pessoa e dos direitos que elas têm agora enquanto cidadãos aumentou muito. No site da BBC, por exemplo, eu acessei o site um pouco antes do GDPR e eles tinham

notícias de abertura. Foi... no dia 25 de maio, estava em todas as manchetes e todos estavam sabendo sobre isso.

BRUCE TONKIN:

Foi um aumento do conhecimento sobre isso pelos consumidores.

Sim, Greg.

GREG AARON:

Sim. Então, desde que o GDPR entrou em vigor em maio, estamos lentamente começando a entender quais são os efeitos. E estamos começando a ver algumas informações serem divulgadas sobre o uso e solicitações e assim por diante.

Um fato que ocorreu recentemente foi duas organizações compostas por profissionais de segurança cibernética e operadores de rede fizeram uma pesquisa. Foi uma pesquisa pelo grupo antiphishing no M3AAWG e os membros incluem... empresas de segurança são responsáveis por proteger redes, bancos, instituições educacionais e assim por diante.

E eles perguntaram aos membros: Você está fazendo mais ou menos solicitações? Como está sendo o processo? E cerca de 300 participantes deram algumas informações.

Uma dessas informações é que algumas pessoas não sabem mais como fazer essas solicitações. Isso ocorre parcialmente porque cada organização que armazena dados tem processos diferentes agora. Elas aplicam seus próprios procedimentos usando mecanismos

diferentes. Na verdade, de acordo com essas pessoas, isso as desanimou para fazer solicitações.

Então, se o número de solicitações é pequeno, isso pode ou não nos dizer algo sobre a demanda pelos dados, porque algumas pessoas desistiram de usar os dados do WHOIS pelo mecanismo disponível atualmente porque não vai mais dar as informações de que precisam. Eu acho que nos próximos meses saberemos muito mais sobre os efeitos disso nas pessoas.

BRUCE TONKIN:

Obrigado.

Número 3.

DIRK KRISCHENOWSKI:

Olá, Dirk Krischenowski do .BERLIN e .HAMBURG e vice-presidente do grupo de domínios de primeiro nível geográficos.

Fizemos recentemente... e publicamos isso na CircleID e no nosso site, geotlds.group... um estudo com 39 TLDs geográficos. Então, voltando à pergunta sobre como lidar com registros pequenos quanto ao GDPR. Desses 39, 25 deles eram TLDs geográficos europeus e 14 eram TLDs geográficos não europeus. Os resultados do estudo foram que, embora os registros de TLDs geográficos baseados na UE levem o GDPR a sério e tomaram medidas para proteger os dados pessoais dos cidadãos, o número de solicitações para acessar os dados é muito

pequeno. E essas solicitações estão sendo atendidas de maneira eficiente.

O estudo dos registros de TLDs geográficos mostra que não há uma necessidade corroborada por evidências para um modelo de acesso universal considerando a maneira como o GDPR funciona na prática. Deem uma olhada nesse estudo. É muito interessante. E diz quantas solicitações foram feitas, por exemplo, as solicitações de maio a setembro foram menos de 15 nos 39 TLDs geográficos, que têm mais de 700.000 nomes de domínio registrados, para dar uma ideia disso.

BRUCE TONKIN:

Obrigado, Dirk. Acho ótimo as pessoas compartilharem dados. Acho que todos podem fazer isso, aqueles que administram registros operacionais... compartilhar os dados, como Nick fez e Dirk também. Isso ajuda muito no desenvolvimento de políticas. Bom.

Um.

JOHN LAPRISE:

Oi, John Laprise, ALAC. Eu vou tirar o meu chapéu do ALAC e colocar o chapéu do meu trabalho fixo. Eu trabalho em uma pesquisa de mercado em um departamento de marketing nos EUA. Quero responder uma pergunta que Bruce fez antes sobre os efeitos nos EUA.

Particpei recentemente de um webinar pelo trabalho onde, embora muitas empresas nos EUA estejam cientes do GDPR, menos da metade delas estão preocupadas em adotá-lo. A postura delas é “esperar para

ver”. Em muitos casos, é o caso da... nos EUA, temos a expressão: “Você não precisa correr mais rápido que o urso, só precisa correr mais rápido que o outro cara”. Então, essa é a postura que muitas empresas nos EUA têm adotado, esperar para ver e rezar para que UE não procure elas depois.

Mas a pesquisa de mercado, em geral, em todo o setor está apreensiva. E temos outra... temos uma nova iniciativa de privacidade de dados na Califórnia que também entrará em vigor semelhante ao GDPR. Então, temos muito trabalho em andamento aqui.

BRUCE TONKIN:

Certo. Obrigado pela sua contribuição.

Dois.

THOMAS DE HAAN:

Sim, obrigado. Thomas De Haan, Holanda, representante do GAC.

Eu só gostaria de retomar a intervenção da Nominet, eu acho, que é muito importante para entendermos os mecanismos que estão sendo aplicados. É claro, está na jurisdição do Reino Unido, então, é um pouco menos complexo do que em uma escala mundial.

Mas a minha pergunta é: Você falou das solicitações... solicitações individuais de acesso a dados. E quanto ao acesso em lote ou acesso em lote limitado? Por exemplo, na Holanda, também um dos maiores ccTLDs do mundo, eles fizeram um acordo com as autoridades locais

de ter um acesso em lote limitado. Não sei bem os detalhes. Eles podem falar melhor sobre isso.

Mas esse mecanismo também é aplicado no Reino Unido? Basicamente, minha pergunta é: Os seus instrumentos ou os que estão em vigor, eles realmente atendem à demanda? Obrigado.

BRUCE TONKIN:

Se eu puder intervir um pouco nessa pergunta, só quanto à terminologia, você está falando em lote como em todo o banco de dados sendo fornecido à outra parte? E também temos a capacidade de fazer consultas automatizadas. Acho que são coisas um pouco diferentes. Mas vou deixar o Nick responder essas duas perguntas talvez. Então, vocês fornecem acesso em lote, em outras palavras, dão uma cópia completa do banco de dados às agências legais fiscalizadoras? E vocês têm acesso automatizado, e como são os índices de consulta nisso?

NICK WENBAN-SMITH:

Obrigado pela pergunta.

Então, respondendo à questão do acesso em lote, nós permitimos que as agências legais fiscalizadoras baseadas no Reino Unido tenham acesso em lote. Mas precisamos esclarecer que tipo de acesso estamos falando, porque não é ao conjunto inteiro dos dados.

O registro tem muitos mais dados do que os que são compartilhados com as agências legais fiscalizadoras. E muito menos dados são

exibidos no WHOIS público. Então, existem camadas diferentes, como uma cebola. Mas, certamente, o acordo que fizemos internamente com as nossas agências legais fiscalizadoras foi que elas teriam acesso a exatamente os mesmos dados do WHOIS que era disponibilizado publicamente antes do dia 25 de maio. Mas elas fazem isso usando um login seguro individualizado com verificações, e nós não vamos apenas dando os dados para ninguém. São agências que conhecemos e sabemos como são organizadas. Temos uma Agência Nacional de Crimes. Ela coordena esses tipos de coisas.

Mas, em termos de padrões locais de comércio, também temos os padrões locais de comércio em todo o país. Isso é feito por meio de um ponto de acesso, pela nossa autoridade nacional local.

BRUCE TONKIN: E quanto ao acesso automatizado?

NICK WENBAN-SMITH: Não temos acesso automatizado, certo.

BRUCE TONKIN: Milton?

MILTON MUELLER: Acho que é uma boa discussão sobre acesso, mas eu só quero ressaltar que estamos falando sobre acesso, certo?

E precisamos ter em mente que, primeiro, temos muitos dados interessantes sendo coletados sobre os efeitos reais. Acho que as informações dos TLDs geográficos são muito interessantes. Foi realizada uma pesquisa com ccTLDs. É bom saber pelo Greg sobre os pesquisadores de segurança.

E acho que todos estão entendendo como é complexo... quando a Nominet falou sobre os diferentes níveis e tipos de acesso, o quanto essa questão pode ficar complexa.

Então, precisamos chegar a uma conclusão. A conclusão do Dirk foi que não precisamos de acesso unificado. Mas também existem argumentos razoáveis de que precisamos, sim. Esse é um problema que precisamos resolver.

Mas, primeiro, precisamos decidir o que está no nosso WHOIS, o que é publicado, quais elementos de dados estamos coletando. E não podemos misturar esses problemas.

Precisamos resolver a primeira parte antes. Acho que isso é relativamente fácil de fazer em três meses. Se não concluirmos em três meses, teremos um grande problema. Nós não... o cronograma da política será prorrogado e todo o processo de múltiplas partes interessadas parecerá ter falhado. E nós temos, como eu disse antes, abutres nos cercando que gostariam de nos ver falhar, que gostariam de se meter e fazer intervenções governamentais e talvez começar a fragmentar o processo.

Então, vamos corrigir a especificação temporária, formalizá-la como uma política, e depois fazemos uma discussão interessante e produtiva sobre acesso.

BRUCE TONKIN:

Sim, uma das questões, do ponto de vista do desenvolvimento de software, é fazer o desenvolvimento de software em etapas. Então, fazemos uma parte e liberamos a etapa e lançamos isso, depois vamos para a próxima parte.

Até certo ponto, falando em tempo hábil, precisamos definir o tipo de finalidade, quais dados são realmente coletados e liberados, para definirmos isso. Depois poderemos começar a analisar outras coisas. Caso contrário, ficaremos andando em círculos. Então, acho que é uma observação válida.

Número 3.

BECKY BURR:

Olá. Sou Becky Burr, e falo como diretora executiva de privacidade da Neustar.

Eu só queria fazer uma observação sobre o comentário do John sobre metade das empresas americanas. Acho que muitas pessoas viram que a Microsoft, quando lançou a plataforma para o GDPR para solicitações de objetos de dados, a lançou no mundo todo. Eles agora relataram que, em comparação per capita e absoluta, estão recebendo mais solicitações e atendendo à mais solicitações de

americanos do que de qualquer outro lugar no mundo. Isso é certamente consistente com a nossa experiência.

O fato de todos na Europa estarem cientes do GDPR no dia 25 de maio também foi sentido no mundo todo. Então, na minha experiência, pelo menos esta empresa americana e outras empresas que conheço estão cientes e participando, em conformidade com o GDPR, e agindo rapidamente em resposta aos consumidores.

BRUCE TONKIN: Obrigado, Becky.

Número 1.

AMRITA CHOUDHURY: Meu nome é Amrita Choudhury da CCOUI, Índia.

Posso ter me enganado em alguns fatos, mas corrijam-me se estiver errada. Acho que existem aproximadamente 339 milhões de nomes de domínio registrados. E pelo que entendi, existem cerca de 120 milhões de nomes registrados no domínio da UE. Isso é menos que a metade dos domínios registrados no mundo todo, que estão na jurisdição da UE.

Embora haja muitas discussões na ICANN sobre como os nomes de domínio podem estar em conformidade com o GDPR em termos do registro do WHOIS, a ICANN também está analisando as... as leis de outras nações? A Europa está em uma área. No entanto, existem

outras regiões, também, nações. Os direitos delas estão sendo protegidos?

A segunda questão é: Existem nações que são bem desenvolvidas que têm um certo entendimento.

Mas também existem nações emergentes, por exemplo, a Índia, temos nomes de domínio que estão sendo vendidos por várias empresas, organizações da Europa e EUA também e até mesmo da Índia. Os registradores e registros talvez não tenham o mesmo nível de entendimento, capacidade.

Então, o que... há algo planejado para melhorar o conhecimento deles para que, no final, os consumidores também possam... os interesses deles sejam considerados? Porque estamos sentados aqui, conversando, mas, os novos usuários de Internet ou compradores de domínios não entendem muito bem de tecnologia, especialmente as pessoas de países emergentes.

BRUCE TONKIN:

Acho que são duas perguntas. Uma pergunta é: Como as leis de outros países estão sendo consideradas? E existem, obviamente, leis na Índia.

E a segunda pergunta é como o conhecimento das pessoas em outras partes do mundo está sendo aumentado sobre esses assuntos.

Talvez... vamos cuidar da segunda pergunta primeiro. Vou passar para a Hadia, porque a Hadia é do ALAC, e suponho que o ALAC esteja

realizando algumas atividades para melhorar o conhecimento disso em diferentes partes do mundo.

HADIA EL MINIAWI:

Sim. Falo enquanto membro do EPDP. Uma das recomendações que deverá resultar da equipe do EPDP é fazer uma recomendação para melhorar o conhecimento e ensinar os registrantes.

E acho que isso seria parcialmente feito pela ICANN e também pelos registros e os registradores, porque acho que é de interesse dos registradores que os registrantes estejam cientes do que está... o que aconteceu com as políticas.

Na verdade, estamos considerando no nosso trabalho outras leis de privacidade, porque agora a equipe de EPDP está autorizada a analisar a conformidade da especificação temporária com o GDPR. Mas isso não significa... é claro, esperamos que não haja conflitos com outras leis de privacidade.

Mas, no momento, não estamos fazendo esse trabalho como analisar outras leis de privacidade.

BRUCE TONKIN:

Obrigado. Ashley.

ASHLEY HEINEMAN:

Obrigada. Falando em nome do GAC, sim, no que diz respeito à nossa participação no EPDP e outras atividades em andamento relacionadas

ao WHOIS, temos nos esforçado o máximo possível para tornar isso... a palavra “genérico” não é a melhor opção, mas para garantir que todo o nosso trabalho reconheça que existem outras leis de proteção de dados.

Esperamos que possamos fazer isso usando o GDPR como alicerce, porque, digamos, foi ele que nos forçou a trabalhar. Mas, sempre que possível, estamos tentando não deixar esse trabalho tão específico ao GDPR. Acho que isso é importante, talvez acima de tudo, é uma questão de respeito com outras leis no mundo todo. Então, pelo menos é isso que estamos tentando fazer. Obrigada.

BRUCE TONKIN:

Obrigado. Cristina.

CRISTINA MONTI:

Eu queria fazer alguns comentários sobre essas perguntas que são recorrentes sobre a tensão, ou a possível tensão, entre diferentes leis em diferentes jurisdições e a natureza global da Internet. Então, sabemos que isso é um desafio, e sabemos que isso é um desafio e que continuaremos sendo confrontados não apenas em relação à proteção de dados, mas também em outras áreas. E é por isso que é tão importante acertamos essas questões aqui na ICANN, porque será pelo menos um caso de teste para o futuro.

No que diz respeito à proteção de dados, em geral, também gostaria de enfatizar que o que vemos... e talvez eu esteja sendo mais otimista que o meu colega Milton Mueller. Vemos uma tendência em direção à

convergência. Esses princípios consagrados no GDPR e que se baseiam na proteção de direitos humanos básicos são, eu diria, princípios de bom senso comum. E estão relacionados à boa administração dos seus dados.

Como eu disse no início, a dificuldade está nos detalhes e na implementação. E é nisso que precisamos ter atenção.

É possível que não encontremos todas as respostas aqui. E talvez possamos descobrir que precisamos produzir soluções criativas para fazer o sistema funcionar e ampliar o limite do assunto com o qual estamos lidando. Mas é por isso que temos esses processos, temos as partes interessadas ao redor da mesa, e devemos ser capazes de fazer isso funcionar.

Além disso, sobre... minha opinião sobre os diferentes processos, entendo que há, algumas... partes interessadas que gostariam de ter uma abordagem sequencial, e outras que têm um pouco de urgência para chegarmos a uma solução final.

Pessoalmente, não vejo problemas em termos um processo paralelo; mas está claro que precisamos ter um bom entendimento sobre essas questões. E, às vezes, alguns mal-entendidos ficam reaparecendo.

Sendo assim, é muito importante prestarmos atenção ao que as pessoas estão dizendo para que, nos diferentes grupos de trabalho, todos juntos coletivamente consigamos encontrar uma solução.

Se houver problemas que não possam ser resolvidos, vamos identificar juntos como podemos tapar essa lacuna.

BRUCE TONKIN:

Ótimo. Obrigado, Cristina.

Quero pular para outra pergunta, e depois vou voltar para os participantes. Apenas outra pergunta para o painel.

Uma das coisas, do ponto de vista do desenvolvimento de políticas, é que já foram desenvolvidas outras políticas recentemente relacionadas a este tópico.

Uma delas é a solução que os registros e registradores implementaram para proteger a privacidade de dados pessoais que foi a introdução do que eles chamaram de... às vezes chamaram de serviços de privacidade ou de serviços de proxy.

Mas nesse caso eles substituíam informações no WHOIS, que era de uma determinada empresa, referida como proxy, ou o nome e o endereço do registrador, por exemplo, em vez do nome e endereço do registrante. Depois elas basicamente operavam um serviço de encaminhamento. Então, se fosse enviada uma correspondência para o endereço no WHOIS, era possível que ela fosse encaminhada ao usuário final.

Uma das preocupações com o crescimento desses serviços de privacidade/proxy era que eles estavam fazendo um ótimo trabalho, dando aos consumidores a opção de proteger os dados pessoais deles. Mas o que não estava claro era em que circunstâncias os dados pessoais eram liberados para as agências legais fiscalizadoras, essas

agências legais fiscalizadoras e outros grupos ganhavam acesso a esses dados.

Então, um processo de desenvolvimento de políticas foi feito sobre esse tópico. Mas agora estamos tendo que lidar com isso desde o rascunho, então, minha pergunta para o painel é: como nós... precisamos voltar e analisar essas políticas novamente? Precisamos levar essas políticas em consideração quando estivermos desenvolvendo a política sobre o... o EPDP.

O outro tópico que ocorreu há alguns anos foi o conceito de um WHOIS thick. Alguns registros, principalmente o .COM, o registro central, basicamente, tem informações sobre o nome de domínio, como as informações do DNS, e também informações sobre o registrador... depois era necessário pedir ao registrador as informações sobre o titular do nome registrado. Então, é um sistema distribuído. Naquele momento, há alguns anos, era difícil fazer uma consulta a todos esses sistemas separados, porque os formatos de dados eram um pouco diferentes. E a única ferramenta disponível naquele momento era a porta 43 do WHOIS. Então, o processo de desenvolvimento de políticas disse: precisamos ter todas as informações em um registro central para que seja possível fazer as consultas em um só lugar. Mas o que está surgindo com os regulamentos em muitos países são restrições para a transferência de dados entre fronteiras. A opinião geral hoje em dia parece ser que, se você opera um registrador na Austrália e tem clientes australianos, então, seus dados ficam na Austrália. Da mesma forma, se você opera um registro na Alemanha ou na Irlanda ou algum outro país, você

mantém os dados sobre seus clientes no país onde está localizado o registrador e só liberaria esses dados por meio de padrões e convenções apropriadas.

Então, a pergunta para o painel é, considerando que existem essas duas políticas, elas podem estar em conflito com o trabalho realizado pelo EPDP. E eu mencionei na opinião do painel sobre como podemos levar em consideração o trabalho que já foi feito até agora, e será que precisamos voltar de alguma forma e atualizar ou analisar outras abordagens? Ashley?

ASHLEY HEINEMAN:

Falarei rapidamente porque talvez não seja a mais indicada, pelo menos com relação aos meus colegas das agências legais fiscalizadores e outras pessoas. Só quero observar que, como participei da equipe de revisão da implementação de privacidade/proxy, isso teve um impacto significativo no fato das coisas pararem neste ponto. O que é preocupante especialmente para as pessoas que querem ter acesso a essas informações. Também é preocupante porque, agora que estamos entrando neste mundo do GDPR, privacidade/proxy é uma opção disponível para mascarar dados e precisamos ter regras para isso também. Então, antes de mais nada, o impacto disso é que está interrompendo o trabalho de implementação. Obrigada.

BRUCE TONKIN:

Obrigado, Ashley. Alguém mais quer falar sobre esse tópico? Milton.

MILTON MUELLER: Não tanto sobre privacidade/proxy, mas sobre o WHOIS thick. Meu entendimento é que o WHOIS thick não seria mais necessário de acordo com... depois que estivermos em conformidade com o GDPR e tivermos implementado o RDAP, que a necessidade de um RDAP seria praticamente substituída pela existência... perdão, a necessidade de ter o WHOIS thick seria substituída pela existência do RDAP, e não precisaríamos de uma justificativa real para os registros armazenarem os dados.

BRUCE TONKIN: Então, só para esclarecer isso, por que esse seria o caso? As pessoas não conhecem necessariamente o RDAP, então, por que o RDAP solucionaria isso?

MILTON MUELLER: Ele forneceria um tipo de banco de dados federado pelo qual as pessoas que quisessem ter acesso poderiam acessar sem precisar mover... e armazenar isso em dois lugares diferentes, no registro e no registrador. Esse é o meu entendimento. Posso estar errado, mas... e eu achava que a justificativa para o WHOIS thick era fraca desde o início. Ele facilitava a transferência de domínios de diferentes registradores para outros, mas parece que isso deveria ser possível sem precisar do WHOIS thick. Além disso, alinhado com o GDPR, o princípio de minimizar a transferência e a coleta de dados parece

dizer que queremos que os dados fiquem parados com o registrador que faz a coleta.

BRUCE TONKIN: Certo. Greg.

GREG AARON: Uma das coisas que temos visto na nossa experiência nos últimos meses com a especificação temporária é que, embora o GDPR aborde certos tipos de dados, a especificação temporária está permitindo a inclusão de outros dados que não são tratados na lei. Por exemplo, o GDPR não aborda as informações do que chamados de pessoas jurídicas, entidades incorporadas. Mas esses dados podem ser adicionados pela especificação temporária e isso dá às pessoas acesso a menos informações.

Então, uma das coisas que o SSAC disse foi, disponibilizar as informações de acordo com a lei, isso é muito importante, mas não exagerar na aplicação da lei. Dar acesso de maneira equilibrada, conforme permitido por lei. E são duas coisas diferentes.

Então, com os dados de proxy, existem pessoas que não são sujeitas ao GDPR e que ainda poderiam usar os dados.

BRUCE TONKIN: Então, não são pessoas físicas, essencialmente.

GREG AARON: Por exemplo, se sou uma pessoa, digamos, no Brasil, não estou incluída no GDPR se o meu registrador não estiver localizado nesse país, mas talvez eu queira usar uma proteção de proxy. Temos uma sobreposição nesses dois casos.

Também preciso dizer que o SSAC afirmou que os registros thick são uma boa ideia por alguns motivos articulados de segurança e estabilidade, e eles não têm nada a ver com... alguns deles não têm nada a ver com a disposição das informações, então, eu discordo do Milton.

BRUCE TONKIN: Nick.

NICK WENBAN-SMITH: Não me incomodo de usar serviços de privacidade/proxy. Eu acho que a implicação dessa pergunta é que... e isso é apenas uma grande suposição... que o que está na especificação temporária que permite a inclusão de dados pessoais fique como uma política permanente com o tempo. Mas, se esse for o caso, então, eu acho que a pergunta é: os dados pessoais dos indivíduos não ficarão expostos em um WHOIS público, qual é o sentido da privacidade, certo? E nos sistemas... e existem muitos sistemas na Europa onde a privacidade foi integrada às operações do registro e algumas pessoas não têm a proteção de dados pessoais, como já foi dito antes, ainda assim, sempre houve uma demanda por serviços de privacidade e proxy. Às vezes apenas por conveniência administrativa. Às vezes por questão de

confidencialidade comercial. Digamos, se alguém quiser lançar uma nova marca, mas não quer que os outros saibam que estão fazendo isso. Essa pessoa registra os novos nomes usando serviços de proxy. Então, é isso... acho que ainda está muito cedo, não sabemos ainda, mas tenho quase certeza de que ainda teremos alguma demanda. Mas também tenho quase certeza de que essa demanda será menor do que antes.

BRUCE TONKIN: Hadia.

HADIA EL MINIAWI: Sim. Concordo com tudo que disseram. Quero apenas acrescentar que, de acordo com os provedores de serviços de proxy existentes ou anteriores ao GDPR, provedores de serviços de proxy legítimos também tinham o direito ou a permissão de fornecer os dados em determinadas circunstâncias. Então... não tenho certeza de realmente precisamos de serviços de proxy agora. Obrigada.

BRUCE TONKIN: Chris.

CHRIS LEWIS-EVANS: Obrigado. Sim, essa questão dos serviços de privacidade/proxy, isso enfatiza uma das perguntas anteriores, na verdade, que é, nesses serviços não havia um modo uniforme para solicitar dados a esses serviços. Isso provavelmente resultou na redução do número de

solicitações às pessoas que prestavam esses serviços. Então, acho que foi o .BERLIN que fez uma pergunta sobre... que não estamos vendo muitas solicitações. Acho que foi feita uma revisão do RDS2 e phishing... a revisão do Grupo de Trabalho Antiphishing e M3AAWG. Todos eles indicaram que há uma falta de conhecimento real sobre como ter acesso. E acho que isso está ocultando muitos problemas que estamos vendo. No momento, sei que ainda, como disse o Nick, é muito cedo, já passamos um bom período com o GDPR, mas realmente acho que ainda não estamos vendo todo o impacto da especificação temporária nas solicitações e nos níveis de solicitações. Acho que os números ajudam muito, mas não acho que sejam necessariamente relevantes.

Como Milton disse, precisamos primeiro criar essa política para que tenhamos um modelo de acesso uniforme em vigor e acertarmos essa política, para depois termos um modelo realmente bom e um modelo legal e justo para o acesso aos dados.

BRUCE TONKIN:

Certo. Cyrus da ICANN só quer fazer um comentário sobre a implementação da política de privacidade/proxy.

CYRUS NAMAZI:

Obrigado, Bruce. Meu nome é Cyrus Namazi. Faço parte do GDD (Global Domains Division, Divisão Global de Domínios) da ICANN. Só quero fazer um esclarecimento sobre o trabalho de implementação da política que fazemos no GDD e esclarecer que não paramos nada.

Particularmente, acho que a Ashley mencionou esse trabalho de privacidade/proxy. O esclarecimento é que, acho que percebemos que, neste momento, não há clareza suficiente para colocar uma estrutura legal apropriada, francamente, de essencialmente avançar com o modelo de credenciamento da maneira que consideramos justificada em termos de... da sua eficiência funcional e aplicabilidade. Há pouco clareza porque o GDPR não especifica como lidar com alguns componentes do modelo de credenciamento... que não é muito diferente, francamente, do modelo de credenciamento de registradores... como ele seria. E considerando a fluidez da situação e o fato de que a poeira ainda não abaixou muito bem sobre como interpretar algumas das implicações do GDPR, estamos basicamente adaptando a velocidade do trabalho de implementação com os fatos que estão surgindo que precisam ser considerados, ou seja, não estamos perdendo tempo avançando com algo que provavelmente precisará ser mudado daqui a pouco. E acho que isso, na verdade, não se limita apenas à privacidade/proxy. Estamos passando por uma situação parecida na implementação do WHOIS thick, que está na fase de implementação. A política foi definida, na verdade, ratificada pela Diretoria há algum tempo. E, nesse caso específico, o que está nos atrasando são os registros e os registradores acordando como eles devem lidar com o contrato entre eles, entre os registros e os registradores. O RRA, Contrato entre Registro e Registrador.

Existem outros programas. Existem 13 programas, na verdade, na organização que estão relacionados aos serviços de dados de registro, todos eles serão de alguma forma afetados, conforme

compreendemos melhor o GDPR e impacto que isso terá e como o trabalho de política e os serviços relacionados ao RDS precisarão talvez ser mudados no futuro.

BRUCE TONKIN:

Sim, acho que Cyrus está ressaltando algo importante que mencionei antes sobre o que chamo de solução em tempo hábil, porque estamos vendo... e usando o WHOIS thick como exemplo... esse desenvolvimento de política já foi feito há alguns anos. Há cerca de cinco anos. Talvez um pouco mais. Provavelmente... talvez tenha sido até quando eu estava no Conselho da GNSO, não consigo me lembrar. Mas... bem, já existe há muito tempo. Mas acho que o mundo está mudando. O regulamento nessa área mudou drasticamente nos últimos anos, e isso está nos forçando a repensar. Acho que, enquanto comunidade e enquanto organização, precisamos ser mais ágeis para conseguirmos responder a esses acontecimentos. Então, acho que o desafio, particularmente quanto ao WHOIS thick agora, é, como ele... ele ainda é a coisa certa, considerando as mudanças na lei de privacidade, particularmente o GDPR? Parece que o nosso trabalho precisa ser acertar este PDP e acertar os requisitos, compreender por que coletamos os dados, acertar alguns desses requisitos. Porque muitas dessas coisas foram feitas, digamos, de maneira parcelada, e agora precisamos voltar ao básico, que é revisitar o motivo pelo qual estamos coletando os dados. Certamente, quando comecei a trabalhar na ICANN por volta de 2000, o foco do WHOIS era permitir a concorrência, na verdade. Era uma forma de fazer transferências tranquilas entre um registrador que tinha a maioria dos nomes de

domínio na época, ser capaz de disponibilizar essas informações a outros registradores para ajudar nas transferências. Quero dizer, se formos descrever uma finalidade, essa era a finalidade em 2000. Eu não acho que demos um passo para trás enquanto comunidade agora e pegamos as opiniões de todos sobre qual deveria ser essa finalidade.

Então, isso precisa ser o fundamental, acertar a finalidade. E a privacidade/proxy é essencialmente uma discussão sobre acesso. O WHOIS thick é, na verdade, uma discussão sobre armazenamento de dados. Porque as tecnologias que existem hoje, quero dizer, não precisamos armazenar tudo centralmente. Podemos conseguir os mesmos resultados, como Milton disse, tendo... podemos ter uma página do WHOIS ou uma página de solicitação no site da ICANN. A solicitação pode ser enviada para o registrador relevante por essa página. O registrador pode aplicar a lei local ao responder a essa solicitação, basicamente.

CYRUS NAMAZI:

Obrigado, Bruce. Acho que você ressaltou outro componente desse ambiente em transformação. Porque, como devem saber, estamos prestes a implementar o RDAP, que é uma plataforma totalmente diferente do antigo e ultrapassado protocolo de WHOIS. E, na verdade, isso nos leva a fazer as perguntas que você está mencionando. Onde os dados são armazenados? Como temos acesso a eles? E acho que, com o RDAP, podemos realmente entrar no que eu considero uma plataforma do século XXI, que seja escalável, que pode realmente

mudar com o tipo de... com o cenário dinâmico e fluido das leis de privacidade no mundo todo e nos ajudar a desenvolver o tipo de sistema e serviços de registro de dados que funcione de maneira mais eficiente com as mudanças que ocorrerem no futuro.

BRUCE TONKIN: Obrigado. Certo, vamos voltar para o número 1.

VOLKER GREIMANN: Obrigado. Volker Greimann pela Key-Systems e NIC Central. Eu gostaria de retomar um dos... o que considero uma distração para o que foi levantado antes pelo painel, que é a distinção entre entidades legais e registrantes pessoais. Acho que essa distinção não está errada. A especificação temporária não está protegendo demais nem se estendendo além, por causa de um mal-entendido básico sobre o que o GDPR realmente protege. Ele não protege os dados pessoais propriamente ditos. Ele também protege os dados pessoais que podem ser incluídos nos dados fornecidos por uma entidade legal. Então, se tivermos o registro de uma empresa e essa empresa decide fornecer os dados pessoais de um dos funcionários no endereço de e-mail, no número de telefone, nos dados de registrante, isso são dados pessoais. Não podemos fazer essa distinção enquanto registrador. Não sabemos se um registro de uma entidade legal contém dados particulares. Mas esses dados particulares precisam ser protegidos da mesma forma que os dados de registro pessoais.

Então, essa distinção se um registro pode ser de uma entidade particular ou de uma entidade legal é absolutamente inútil para determinar se esses dados devem ser protegidos ou não de acordo com a especificação temporária. Obrigado.

BRUCE TONKIN: Obrigado, Volker. E número 2

DEAN MARKS: Olá. Dean Marks pela coalizão para a responsabilidade on-line. Quero retomar algo que a Cristina Monti da comissão falou, de que o GDPR é baseado nas regras que já existem há muito tempo. Pelo menos com relação ao processo de desenvolvimento de políticas de privacidade/proxy, isso não é algo que existe há muitos anos. Isso é algo que foi concluído em 2016, quando o GDPR já estava sendo mencionado. Havia uma grande conscientização sobre as preocupações com leis de privacidade quando o trabalho desse PDP estava em andamento. Então, eu entendo por que isso foi pausado para buscar clareza porque todos nesta sala concordam que o GDPR não responde a todas as perguntas. O GDPR por conta própria não traz clareza para todos os detalhes. Novamente, como disse a Cristina, este processo de múltiplas partes interessadas é um bom lugar para encontrarmos um equilíbrio. Nós conseguimos esse equilíbrio no PDP dos serviços de privacidade/proxy. Ele foi anonimamente aprovado pelo Conselho da GNSO. Ele foi anonimamente aprovado pela Diretoria da ICANN. É um grande passo à frente para encontrarmos esse equilíbrio. E quando essa conseguiremos alcançar esse nível de

clareza, Cyrus? Acho que dando prosseguimento com o serviço de privacidade/proxy, a comunidade de múltiplas partes interessadas estaria ajudando a estabelecer essa clareza. Acho que a Organização ICANN está fazendo um ótimo desserviço para toda a comunidade de múltiplas partes interessadas.

BRUCE TONKIN:

Cyrus, talvez você possa ser um pouco mais específico com alguns exemplos de quais são basicamente seus impedimentos para a implementação. Só para ser um pouco mais específico, talvez isso ajude...

CYRUS NAMAZI:

Sim. Muito obrigado. Na verdade, eu parei de falar para não tomar muito tempo da discussão do painel, que não era minha intenção. Dean, entendo perfeitamente o que você está dizendo. Novamente, quero esclarecer, não paramos com o trabalho de implementação das políticas que temos realizado com vocês e com outras pessoas na IRT há algum tempo. No meu ponto de vista, isso não está nem em questão, do nosso ponto de vista, da organização, sobre a relevância da política. Não preciso entrar nesse mérito. Isso cabe à comunidade decidir. Na verdade, isso tem a ver com criar uma estrutura legal apropriada para a implementação. E já falamos sobre isso com meus dados... os agentes de depósito de dados e os contratos que temos com eles. No momento, é mais ou menos o tipo de situação na qual não nos sentimos confiantes com a estrutura, a estrutura legal, que seria necessária para a implementação.

Isso não tem nada a ver com a relevância do trabalho. Na verdade, eu acho que precisamos de um serviço de privacidade/proxy no mundo pós-GDPR, por assim dizer. Mas, novamente, não cabe à organização decidir isso.

BRUCE TONKIN: Certo. Número 3.

SÉBASTIEN BACHOLLET: Sebastien Bachollet, vou falar em francês. Vocês dirão, “como sempre”.

A pergunta sobre a diferença entre uma pessoa... uma pessoa física e uma pessoa jurídica.

Isso me surpreende. É claro, existe uma diferença. Enquanto pessoa, uma pessoa física, tenho um nome, um endereço de e-mail. E, se eu precisar dar minhas informações, eu posso dá-las. Mas uma organização, uma empresa pode publicar essas informações. É uma escolha dela. Precisamos proteger as pessoas físicas. E a pessoa jurídica pode se organizar para que não... informações confidenciais não sejam publicadas. Todos nós podemos... podemos pelo menos nós mesmos ter as informações. Então, é normal para uma pessoa física obter as informações.

NOME NÃO INFORMADO: Concordo com Sebastien. Podemos ler o texto do regulamento. Vocês entenderão isso muito bem. O texto não precisa ser interpretado.

BRUCE TONKIN: Sim?

PETER KIMPIAN: Bom dia a todos. Sou Peter Kimpian, do Conselho Europeu. Serei breve hoje.

Só quero dizer que o Comitê do Conselho Europeu sobre proteção de dados acabou de adotar um guia sobre a ICANN e privacidade, que foi publicado esta semana. Sei que estamos nos concentrando no GDPR. E estamos aguardando uma opinião do EPDP. Mas o comitê do Conselho Europeu tem uma proteção de dados para todos os membros da União Europeia, além dos estados membros, como a Federação Russa, a Turquia, o México e alguns países africanos também.

Existem algumas indicações e orientações e entendimentos comuns e padrões de privacidade internacionais sobre isso, especialmente em se tratando do último tópico, objetos de dados e as outras definições e princípios também. Muito obrigado.

BRUCE TONKIN: Certo. Alguém quer comentar sobre isso? Não? Ok.

Ok. Temos uma pergunta aí no fundo? Não?

A outra pergunta que eu tinha acho que já foi mencionada, que é como podemos garantir a conformidade da solução com outras leis de

privacidade? Acho que essa pergunta já foi feita, de certa forma. Então, já tratamos disso.

Além disso, talvez seja bom voltarmos, tendo ouvido algumas discussões e comentários dos participantes, sei que o Milton... você disse que tinha alguns exemplos de como podemos facilmente nos dispersar para outras áreas.

O painel quer fazer mais algum comentário sobre o que vocês acham que devemos fazer para termos uma solução em tempo hábil? Como a comunidade pode ajudar no processo de desenvolvimento de políticas? O que podemos fazer para torná-lo eficiente?

Flip?

FLIP PETILLION:

Aumentar o conhecimento sobre ele. Acho que esta discussão claramente mostrou que as pessoas com dados e que compartilham os dados estão claramente ajudando a avançar essa discussão.

E isso ajuda as pessoas a terem conhecimento sobre o assunto.

Tivemos uma reunião ontem e Göran nos fez uma visita. E ele disse algo muito interessante. Ele disse: “eu gostaria que já tivéssemos tratado disso há muito tempo”, e é verdade. Mas esse é o fato. Quero dizer, é isso que temos.

Mas isso me fez... me fez pensar no futuro. E tenho prazer de apresentar uma ideia. Só quero pensar na mesma direção em que ele estava pensando.

E fiquei pensando: o que estamos deixando de ver agora que se mostrará para nós no futuro e que tem alguma relação ao acesso?

Suponhamos que todos os problemas com acesso sejam resolvidos. O que isso significa para a ICANN, enquanto organização? Isso significa que ela assumirá mais responsabilidades no futuro?

Há 20 anos temos um sistema de UDRP bastante eficiente. E que está ajudando os titulares de direitos de IP. Especialmente, os proprietários de marcas. Essa é uma solução para um determinado problema.

Fico pensando: existem outros problemas que deveríamos abordar e para os quais precisaríamos de abordagens semelhantes no futuro?

Por exemplo, o que é realmente preocupante é se os consumidores forem prejudicados, se as pessoas forem prejudicadas, se as crianças forem prejudicadas.

É apenas um exemplo, mas é muito importante.

Francamente, hoje eu preferia receber mais spam, mas sabendo que estamos lutando contra as violações e os danos causados, dependendo do EPDP.

BRUCE TONKIN:

Certo. Outras comunidades?

Ashley e depois Cristina.

ASHLEY HEINEMAN:

Obrigada. Representando o GAC. Acho que essa conversa sobre não nos distrairmos... sim, existem algumas áreas onde podemos evitar nos distrairmos e isso nos ajudará a fazermos o que precisamos fazer a tempo.

Mas, dito isso... especialmente, este painel não se limitando ao EPDP, acho que, do ponto de vista do GAC, apoiamos a conversa sobre o modelo de acesso universal que foi iniciada pela ICANN.

E somos muito gratos por ela ter sido iniciada, em grande parte porque isso nos permite começar o processo de pensar nela. Ela nos dá a estrutura para fazer isso. E ela também nos dá a oportunidade de começar a identificar e encontrar as respostas para perguntas importantes.

Não estou dizendo que começamos o desenvolvimento técnico nem nada disso. Isso virá na hora certa.

Mas receber perguntas, como as que foram feitas por Göran para a Diretoria Europeia de Proteção dos Dados, acho que isso nos ajudará a formalizar os nossos pensamentos e opiniões daqui para a frente. Novamente, acho que não é relevante caracterizar as conversas sobre o modelo de acesso universal como uma distração. Eu considero isso uma forma eficiente de começar uma conversa sobre outro problema com o qual teremos que lidar. Obrigada.

BRUCE TONKIN:

Cristina e depois o Greg.

CRISTINA MONTI: Rapidamente, eu só queria ressaltar que, na minha opinião, a coisa mais importante daqui para a frente é termos clareza, um acordo claro, e transparência sobre as diferentes atividades de processamento que envolvem o sistema de WHOIS e suas respectivas finalidades. Isso é o básico.

Depois que tivermos esse acordo sobre as diferentes atividades de processamento, então, ficará muito mais fácil lidar com outros aspectos. E eu gostaria de sugerir mantermos essas diferentes atividades de processamento separadas. Porque é possível que tenham embasamentos legais diferente. Então, acho que esse tipo de clareza realmente nos ajudará a seguirmos na direção certa.

Essa é minha sugestão.

BRUCE TONKIN: Obrigado. Greg.

GREG AARON: É importante pensarmos no futuro com relação a esta situação, porque não estamos pensando muito à frente. Então, olhar para a frente é importante.

O grupo de EPDP está trabalhando bastante em questões extremamente difíceis. E esta provavelmente seja uma boa hora para a GNSO e a organização como um todo pensarem sobre o que acontecerá em 2019.

Esse grupo trabalhará até onde for possível. Mas a especificação temporária chegará a um fim em algum momento, e esse grupo está trabalhando bastante. E veremos como o trabalho dele será recebido, mas é possível que o plano de projeto inteiro não seja aceito.

Então, em vez de sermos pegos de surpresa, vamos garantir que o trabalho continue e que as pessoas encarregadas por esse trabalho tenham os recursos de que precisam para concluí-lo.

BRUCE TONKIN: Hadia.

HADIA EL MINIAWI: Como membro do ALAC, nossa principal preocupação e nosso principal interesse é fazer da Internet ou manter a Internet como um lugar seguro para todos. Então, basicamente, detectar e impedir fraudes ou abusos do DNS... e abusos do DNS é algo que consideramos muito importante.

Disso isso, quero dizer novamente que é muito importante analisarmos agora... analisarmos agora os processos padronizados do setor e os serviços de credenciamento.

Porque, se concluirmos uma política e isso não estiver em vigor, quanto tempo precisaremos esperar para termos algo que realmente seja implementável e prático? Então, obrigada.

BRUCE TONKIN: Certo. Acho que temos uma pergunta dos participantes. Número 1.

RUDY DANIEL: Rudy Daniel. Sou um Fellow do ICANN 63 do Caribe. Uma pergunta geral: GDPR: Esse regulamento realmente mandou a ICANN e a comunidade a colocar a casa em ordem com relação ao WHOIS, por isso a definição de elementos de dados e o subsequente acesso e a metodologia de acesso com relação à lei aplicável existente e futura, especialmente já que o v6 está sendo cada vez mais adotado?

BRUCE TONKIN: Alguém quer comentar sobre isso ou responder?

Milton.

E obrigado a você, enquanto Fellow, por se levantar e fazer uma pergunta. Ficamos muito agradecidos.

MILTON MUELLER: Sim. Definitivamente o GDPR forçou a ICANN a colocar a casa em ordem. Acho que o Greg disse algo sobre que não olhamos para a frente e antecipamos o que iria acontecer. Alguns de nós têm falado à ICANN há 15 anos que o WHOIS era ilegal de acordo com a lei de proteção de dados. E eles simplesmente... não é como se não soubessem sobre isso. A questão é que eles não precisavam dar atenção a esses alertas.

É uma questão mais política do que uma falha de previsibilidade. E as penalidades do GDPR realmente nos forçaram a reorganizar tudo.

Apenas para resumir, falando no futuro, concordo totalmente com a Cristina de que a tarefa principal é identificar as finalidades e a coleta de dados necessários para atender a essas finalidades. Depois, passamos para definir quais elementos desses dados serão exibidos publicamente no WHOIS e quais não serão, que serão alterados. Depois podemos tratar do acesso.

Não quer dizer que a tentativa do Göran e do CEO de explorar o acesso legal sobre o modelo de acesso unificado seja uma distração, mas talvez seja uma atitude prematura. E talvez... não sabemos o que o modelo fará até que a primeira tarefa seja realizada.

Então, acho que o principal motivo pelo qual questioneei a discussão sobre o modelo de acesso unificado é que ela desperta nas mentes de muitas pessoas uma esperança de que, de alguma forma, esse modelo de acesso recriará o antigo WHOIS depois que forem credenciadas. E acho que isso é uma distração no sentido de que tira a atenção das pessoas do que realmente fará com o WHOIS que temos agora e não nos faz... pensamos, ah, como vou fazer para ter acesso... e não nos preocupamos com o que estamos fazendo com o WHOIS agora.

RUDY DANIEL:

Fiquei pensando: será que o modelo de acesso universal é uma solução rápida.

MILTON MUELLER: Ele pode ser uma solução rápida. É extremamente complicado. É complicado legalmente. É complicado tecnicamente. É complicado politicamente.

Então, não, acho que a principal justificativa para iniciar a discussão agora é que não será uma solução rápida. Será complicado.

E preciso dar algum crédito a Göran, ele está tentando iniciar logo essas discussões. Mas, ao mesmo tempo, ele está forçando uma direção para a conversa que talvez não seja a direção certa. Então, precisamos simplesmente deixar de lado a questão do acesso até que a primeira parte seja concluída, e isso deve ser rápido. Não deve ser muito difícil para nós solucionarmos o primeiro problema.

HADIA EL MINIAWI: Em resumo, não sabemos se é uma solução rápida porque simplesmente não estamos falando sobre acesso agora e não falaremos sobre acesso até que as primeiras perguntas sejam respondidas. Obrigada.

BRUCE TONKIN: Muito bem. Acho que vou encerrar por aqui. Gostaria de agradecer ao painel. E acho que no início da reunião tivemos uma conversa muito produtiva, porque, basicamente, as pessoas estão se entendendo, fazendo mais perguntas enquanto damos início a esta discussão. Como a Ashley falou, em termos de criarmos uma solução rápida, acho que entendemos rapidamente quais são os problemas para podermos resolvê-los. É um passo positivo à frente.

Acho que todos ouviram que não voltaremos ao antigo WHOIS. Temos pouco apoio para isso. E acho que o conceito que precisamos equilibrar é a proteção de objetos dos dados e fornecer o acesso a usuários legítimos... parece que há um forte apoio para isso de encontrarmos um equilíbrio, tanto entre os participantes quanto entre os membros do painel.

Então, muito obrigado a todos por participarem e esperamos que o PDP tenha uma conclusão eficiente.

[Aplausos]

[FIM DA TRANSCRIÇÃO]