

## LACIGF 11

Quarta-feira 1 de agosto, 15:00h

### Sessão 7 “Desafios na Gestão de Identificadores da Internet”

Sob a premissa "Privacidade sob a abordagem do GDPR e seu impacto no DNS" apresentada por Rodrigo de la Parra, vice-presidente para a América Latina e o Caribe da ICANN, um grande grupo de participantes reuniu-se para discutir o assunto.

Rodrigo apresentou os antecedentes do GDPR, um tema que ocupou a agenda da ICANN, e que lida com as medidas de proteção e privacidade de dados de cidadãos e moradores da União Europeia (GDPR)

Esta questão tornou-se relevante para a comunidade técnica e, nesta oportunidade, foi dada uma abordagem mais ampla e não tão técnica, para gerar maior interesse para a comunidade em geral. Algumas perguntas foram feitas para trabalhar hoje no grupo que não estão focadas apenas em questões técnicas, mas nas implicações que esta questão tem para a governança da Internet.

#### Antecedentes

O GDPR entrou em vigor em 25 de maio passado e visa proteger os cidadãos e residentes da UE contra violações à privacidade e uso indevido de dados pessoais. "O regulamento é um passo essencial para fortalecer os direitos fundamentais dos cidadãos na era digital e facilitar os negócios simplificando as regras para as empresas no mercado único digital."

O mesmo é aplicado a todas as empresas que processam e mantêm dados pessoais de indivíduos residentes na UE, independentemente da sua localização geográfica.

O descumprimento pode resultar em multas de até 20 milhões de euros ou 4% do faturamento total anual. As autoridades europeias de proteção de dados interpretarão os acontecimentos que ocorram e farão cumprir o regulamento e os tribunais europeus resolverão qualquer disputa.

Disse que não é muito diferente das leis ou regulamentos de proteção de dados existentes nos nossos países.

Mas qual é o vínculo disso com o DNS, com a Internet e com a ICANN?

A ICANN é afetada de duas frentes:

Internamente, como qualquer organização que recebe **dados pessoais**, tem que observar o cuidado em seu tratamento. Refere-se a dados que coleta e processa para fornecer serviços internos ou externos.

Mas há também uma dimensão especial que afeta as partes contratantes da ICANN, que são os **registros e os registradores dos domínios**, que seguem as regras estabelecidas pela

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt, Negrita

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt, Negrita

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

ICANN: toda vez que um registrante, seja uma pessoa ou uma empresa ou organização, registra um domínio, serão solicitadas certas informações relacionadas aos dados pessoais, que se coletam em um diretório público chamado **WHOIS**. O WHOIS contém as informações de cada domínio: registrador e o registro. Anteriormente tinha mais dados de caráter pessoal. Este WHOIS está em contradição com a disposição da União Europeia e isto, conseqüentemente, afeta qualquer empresa que registre domínios e mantenha dados de cidadãos da UE. Há quase dois anos, a comunidade da ICANN começou o processo de discutir sobre como cumprir a disposição e, ao mesmo tempo, como preservar os dados do diretório do WHOIS. Nesse sentido, está acontecendo uma discussão participativa de baixo para cima.

Desta forma, dois tópicos muito importantes para a governança da Internet são apresentados:

-Privacidade e Proteção de dados na Internet **vs.**

- Manter este diretório de informações que faz parte da missão da ICANN, de um lado, para manter a estabilidade técnica e operacional da Internet e, ao mesmo tempo, fornecer informações para a aplicação da justiça. Por exemplo, nos casos em que um delito relacionado a um site ou uma página web é investigado, a justiça usa as informações desse diretório para localizar a pessoa ou o local em que a rede é usada maliciosamente.

Esse processo de discussão está ocorrendo entre os diferentes grupos da Internet para chegar a uma política que defina muito bem esse aplicativo.

A discussão sobre o WHOIS vinha acontecendo antes, em que alguns setores buscavam um WHOIS mais robusto e outros queriam um mais enxuto sem informações confidenciais, mas o aplicativo do GDPR acelerou esse processo na comunidade. Disso surge a pergunta: "Especificação temporária", ou seja, um modelo provisório que garanta um quadro comum para o gerenciamento dos dados de registros dos gTLDs, enquanto continua o processo de discussão entre os diferentes grupos de interesse da ICANN para levar a uma política que defina como continuar usando o WHOIS.

Algumas das medidas propostas colocam que não deve haver uma única camada de informações para as pessoas que consultam o WHOIS, mas sim diferentes (modelo estratificado/escalonado), levando em conta o nível de informações necessário e, assim, cumprindo o GDPR. Quer dizer, que o WHOIS só mostre de maneira pública uma parte da informação e o restante que seja acessível somente para aqueles que solicitem através de registradores ou operadores e demonstrem ter um interesse legítimo (legal, por exemplo). De acordo com essa especificação temporal, as partes contratadas da ICANN (registros e registradores) devem continuar compilando as informações dos usuários que registram domínios. Esta proposta ainda continua em discussão.

Dominique2 17/11/18 13:13

**Con formato:** Fuente: 12 pt, Negrita

Dominique2 17/11/18 13:13

**Con formato:** Fuente: 12 pt

Dominique2 17/11/18 13:13

**Con formato:** Fuente: 12 pt

As seguintes perguntas são deixadas para o grupo reunido para discutir essa questão.

#### O GDPR e seu impacto no DNS

- Como pode ser alcançado um equilíbrio entre os objetivos de privacidade/proteção de dados pessoais e os objetivos de segurança e a estabilidade operacional?
- Quais foram as lições aprendidas em relação ao impacto de um regulamento regional sobre os aspectos globais da Internet?
- Como o modelo de múltiplas partes interessadas conseguiu reagir de forma eficiente perante eventos externos?

Como mencionado na apresentação, esta questão tem sido parte da agenda de todos os atores envolvidos no ecossistema da Internet durante este ano.

As principais posições discutidas no grupo frente às questões colocadas foram:

Johanna Falliero (setor acadêmico): afirma que a dicotomia entre privacidade e proteção de dados vs segurança está errada.

Enrique Chaparro (Sociedade civil): acredita que a questão principal é uma contradição. A coleta excessiva de dados no DNS não faz a estabilidade do DNS, isso faz o lobby dos direitos autorais. Para que um pacote chegue a um endereço de destino, não é necessário saber o endereço social. Para a função do DNS, os dados de endereço físico da pessoa não fazem sentido. Sim há uma contradição em relação às agências de aplicação da lei. Também o lobby de proteção de dados que vai contra o poder principal na ICANN.

O GDPR não nasceu da noite para o dia e, portanto, tem sido uma falha institucional da ICANN não tomar uma decisão a tempo. Existe algum mecanismo diferente para o armazenamento de dados para grandes entidades que permitam, perante um incidente de segurança poder agir rapidamente para superar o problema de segurança. Os dados que serão salvos com uma necessidade específica não deveriam gerar um problema. No fundo, não deveria existir uma contradição entre os dois. A ICANN está trabalhando hoje em uma definição final.

É esclarecido que na ICANN existem dois tipos de domínio. Códigos de país ou genéricos: ccTLDs e gTLDs. Las políticas globais da ICANN afetam os genéricos, os códigos de país têm certa flexibilidade dependendo do tipo de administração que possuam.

Erick Iriarte .pr: Ele disse que o GDPR não é aplicável no seu país por dois conceitos. Existe legislação própria de dados pessoais de 2011 e é funcionalmente operacional, protegemos os dados que nos foram entregues sob a legislação peruana (Lei 29733 Art 3 inc 23). Quando se trata de um serviço que é entregue e é transfronteiriço, ai é aplicado o GDPR, somente quando é fornecido serviço direto a eles, em sua moeda (euro) Atualmente,

apenas 3 dados são armazenados: endereço postal, e-mail e DNS. Menciona que para ele, o padrão para a publicação de dados do WHOIS não existe.

Luis Aranciabía, .cl: Sim existem casos de registro e registradores, e a maioria são europeus. Lá, se tiverem uma função de controlador e estão a caminho de um padrão diferente ao da indústria, é uma tutela dos dados dos usuários.

Alberto Soto: Cada governo pode ter sua lei de proteção de dados pessoais, mas o fato é que o problema da ICANN é que ela é uma organização global que deve respeitar as leis do estado da Califórnia e qualquer assunto em qualquer parte do mundo. Para abordar os dados de WHOIS há que listar 1, 2 e 3, se estiver ocupado. A partir daí, há interesses particulares e devemos começar a partir daí para ver qual é acessado e via solicitação através da lei.

Outras perguntas que surgem no debate:

Qual é o balanço de que os crimes não sejam investigados e quais a proteção?

Quais são os dados mínimos necessários para operar?

Nome de domínio, método para contatar o usuário. O problema operacional é poder nos comunicar rapidamente com o registrante para solucionar algum problema técnico ou criminal.

Quais são esses dados?

E.C.: Pode se ter um ponto de contato, intermediado ou não. O restante dos dados é usado para outro propósito.

Atualmente, existe um juízo entre a ICANN e EPAG, que quebrou contrato com a ICANN (a ICANN iniciou esta ação porque a EPAG informou-lhe que, a partir de 25 de maio de 2018, deixaria de coletar informações de contato técnico e administrativo ao vender novas inscrições de nomes de domínio). EPAG considera que a coleta desses dados seria contrária ao GDPR. A coleta dessas informações é exigida pelo contrato entre a ICANN e EPAG.

J.F.: Problemas como regulamentos de corte local e segurança de dados acontecem aqui ou em qualquer lugar. Deveríamos avançar todos nós a partir dos mesmos princípios. Pensar padrões para todos além dos regionalismos. Entende-se que existe uma reticência institucional para aplicá-lo, porque eles são mais abrangentes e não menos do que temos.

Quais serão os princípios aos que iremos aderir dos levantados no GDPR? Deve-se levar em conta o consentimento expresso e tácito.

#### **Conclusões do debate:**

Privacidade vs. Segurança: Foi acordado que não há antagonismo entre privacidade e segurança, que são dois princípios fundamentais que devem existir e coexistir. Também

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt

foi acordado que devem ser coletados os dados pertinentes ao uso pretendido e não levantar dados em excesso, pois seria um abuso. Por exemplo: para garantir a função do DNS, não é necessário ter o endereço postal do detentor do domínio.

Conversou-se sobre a discussão e definição que está sendo dada pela ICANN sobre a necessidade de combinar o próximo funcionamento do WHOIS com base na aplicação do GDPR.

Foi colocada a diferença entre os ccTLDs e os gTLDs, pois os genéricos têm um contrato com a ICANN que devem cumprir e, portanto, continuar a coletar os dados do WHOIS, enquanto os ccTLDs variam em sua forma de gerenciamento e têm uma situação mais flexível. Concordamos em manter um ponto de contato com o titular, seja médio ou não. Foi dito que não pode existir um padrão do WHOIS para todos.

Atualizou-se sobre a legislação local dos países representados no grupo e foi expresso que, independentemente de haver legislação ou não a esse respeito, suas práticas não eram modificadas, uma vez que não afetavam o GDPR em seu território.

Finalmente disseram que todos nós, de alguma forma, deveríamos visar os mesmos princípios para além dos regionalismos e particularidades de cada país, e pensar em uma definição global onde o centro seja o cidadão, e que seja um acordo comum para todos dado que a proteção de dados na região e no mundo deveria ser a mesma.

Dominique2 17/11/18 13:13

Con formato: Fuente: 12 pt