
**40.ª edição da ICANN *meetings***

A primeira edição de 2011 da ICANN *meetings* decorreu na cidade de São Francisco, entre os dias 13 e 18 de Março. Na sessão de abertura foi assinalada a alocação dos últimos blocos de endereços IPv4 aos RIR's, já publicitada no passado mês de Fevereiro. A semana de trabalhos centrou-se em matérias como a segurança, estabilidade e resiliência do DNS, o DNSSEC, o WHOIS, e os novos gTLD's, desta feita sem qualquer expectativa de fechar um já longo processo. A sessão de abertura da 40.º edição da ICANN meetings ficou ainda marcada pela presença do "pai" da Internet, Vint Cerf, três anos passados sobre o termo do seu mandato como chairman do board do ICANN. Seguiram-se as apresentações de representantes governamentais dos EUA, onde se destacou a National Telecommunicaions and Administraton – uma das entidades que assinou o AoC com o ICANN –. A mensagem comum foi a da importância da manutenção do modelo de "multi stakeholder"/participado defendido pelo ICANN, e a necessidade da comunidade se empenhar na procura de soluções concertadas para matérias como a privacidade da Internet, a cibersegurança e a protecção dos direitos de propriedade industrial.

Dos diferentes tópicos em discussão um dos mais críticos foi o do *DNS abuse.* A pertinência da discussão em torno desta matéria deve-se não apenas à sua própria natureza mas, também, aos actores envolvidos que vão para além dos *registries* e *registrars* estendendo-se aos consumidores finais, aos órgãos de polícia criminal e, em última instância, aos governos dos próprios países envolvidos.

É neste cenário que representantes da indústria (Microsoft) da Interpol (188 países membros do National Central Bureau) e do US Federal Bureau of Investigation apresentaram os últimos desenvolvimentos a este respeito e as implicações de possíveis acções de combate à criminalidade via DNS, seja ela roubo de identidade, violação de direitos de autor ou propriedade intelectual, condutas fraudulentas e como não podia deixar de ser os designados "botnets". Nesta sede, foram apresentados dados estatísticos sobre o impacto que algumas destas acções criminosas têm hoje sobre o DNS: hoje estima-se que 500 000 domínios estão registados com o propósito de simplesmente gerar SPAM, sendo que 40% estão registados sob

.info; em Maio de 2009 foram condenadas nos EUA 14 pessoas pela venda ilegal de medicamentos online, tendo, nessa mesma data, sido publicado o On-line Pharmacy Consumer Protection Act fixando as regras aplicáveis à distribuição e venda de medicamentos via Internet.

Neste âmbito, o representante do CENTR veio reforçar o papel dos ccTLD's chamando a atenção para o facto de se começar a discutir se um ccTLD deve ter o papel de intermediário, figura dado pela directiva das comunicações electrónicas em exclusivo aos ISP´s. Na prática, isto significaria a assunção legal de um conjunto de obrigações que passariam pela obrigação de bloquear domínios sem uma ordem prévia do tribunal e o acesso incondicionado aos dados do WHOIS, sem fazer disso depender a natureza do demandante, leia-se, órgão de polícia criminal.

Associada a esta problemática está a questão de saber o que fazer com os domínios que estão na origem de acções criminosas: *Take down or block*? Aqui a comunidade não é unânime sobre a opção a tomar tendendo para a suspensão do domínio com a opção técnica de simplesmente o retirar da zona. Trata-se de uma opção mais específica, indo directa à fonte, bloquear pode contender, por exemplo, com o DNSSEC, o que se quer evitar. Nestes casos, a ideia é ser o registar a agir notificando de imediato o titular do domínio, o registry só agirá em última instância. Questão relacionada é a do WHOIS, já que se não estiver garantida a veracidade dos dados do titular do domínio este não será contactado nem, em última instância, condenado.

Foi ainda realizado um ponto de situação no processo *IDN ccTLD Fast Track*, aberto em 2009. Actualmente o ICANN já recepcionou 34 pedidos relativos a delegações de ccTLD, estando já na root 27 IDN ccTLD's correspondentes a 27 países. Trata-se de um processo com duas fases distintas: uma relativa à avaliação da "*string*" em si e a outra relativa à delegação da mesma. Este processo implica o pagamento prévio de 26 000 USD e, no caso de aprovação, de um montante anual entre 1% e 3% do lucro do registo de domínios sob o IDN em causa. Até à data foram recusados os pedidos da Bulgária e da Grécia e pela mesma ordem de razões: confundibilidade com ccTLD's pré existentes. Refira-se que o ICANN utiliza um algoritmo designado de SWORD que avalia o índice de confundibilidade entre a *string* solicitada e os diferentes ccTLD's. No caso da Bulgária, tratou-se de um processo iniciado em Junho de 2008 e com notificação de recusa do ICANN em Maio de 2010 pelo facto de, não obstante se tratar de caracteres cirílicos, são confundíveis com os caracteres (latinos) do ccTLD do Brasil, .br. Esta decisão foi mal acolhida na comunidade internet Búlgara, onde 65% dos inquiridos defendeu a manutenção da *string* inicialmente proposta. Neste momento o ICANN defende a impossibilidade de reabrir o processo já que o sistema de avaliação não prevê qualquer mecanismo de reavaliação ou recurso da decisão.

O caso da recusa ao pedido da Grécia foi idêntico, tendo sido comunicado no passado mês de Fevereiro. O argumento é que a *string* é similar com .ea, que, curiosamente nem um ccTLD é sendo antes uma das *string* reservadas na ISO-3166.

O impacto das regras e princípios decorrentes da propriedade industrial no registo de domínios, sejam eles ccTLD's ou gTLD's, é um dos assuntos mais debatidos no âmbito do ICANN. O WIPO ccTLD Program foi lançado no ano 2000 contando já com a adesão de 65 ccTLD's, representativos de 12 línguas diferentes. Até à data foram resolvidos neste âmbito

perto de 20 000 litígios. Sendo uma matéria onde a probabilidade de ocorrer conflitos relativos a direitos de propriedade intelectual é elevada – veja-se os casos conhecidos de cybersquatting em que uma marca de 3.º é registada como domínio por alguém, que não o seu titular, para disso obter vantagem – confrontamo-nos mesmo com a existência de legislação dispersa específica que tem feito doutrina para além fronteiras, referimo-nos em concreto ao Anti-Cybersquatting Consumer Protection Act, ao Anti-Cybersquatting Piracy Act, entre outros.

O ccTLD.cl (Chile) veio neste fórum apresentar o seu sistema de resolução voluntária de litígios que abrange matérias de propriedade industrial, que curiosamente vem trazer uma inovação no próprio quadro jurídico Chileno ao introduzir o sistema de arbitragem electrónica.

Em 2004 foi criado por iniciativa do Tribunal Arbitral Checo a ADR (Arbitration Center for Internet Disputes). Em 2005 foi aprovado pelo ICANN o .eu, hoje já com mais de 3.300.000 domínios registados. Tendo, nessa sequência, a ADR assumido-se como a plataforma de resolução de conflitos online por excelência do .eu e funcionando em exclusivo no formato electrónico. Esta plataforma estende hoje o seu campo de acção a gTLD's como o .com, .net, .mobi, entre outros, tendo totalizado até à data 11 000 disputas.

O crescimento da Internet anda lado a lado com o crescimento do registo de domínios, sendo a concorrência, também aqui, um factor que leva a que o mercado - neste caso os registries e registrars – se obrigue a prestar um melhor serviço. Assim sendo, a qualidade de serviço é hoje mais um dos *hot topics* em discussão entre gestores dos diferentes TLD's mundiais. O ccTLD .se (Suécia) ganhou recentemente no seu país o prémio "Organização do ano 2010 na qualidade", tendo partilhado o caminho percorrido e as acções desenvolvidas para atingir a dita distinção. Tratou-se do resultado de um trabalho iniciado há 4 anos atrás, tendo sido realizado internamente e após várias visitas a diferentes registries europeus e a empresas de sucesso na área do IT, onde foi recolhida informação e boas práticas que depois foram adaptadas ao funcionamento da fundação que gere o .se. Para além do princípio constante no RFC 1591 de onde se retira que os ccTLD têm um "(…) dever de servir a comunidade (…)", na base deste prémio esteve uma consciência generalizada da organização na importância de apostar na qualidade de serviço e que a mesma só podia ser atingida com empenho interno e olhando para aquilo que os parceiros de sucesso hoje fazem.

Um dos assuntos que figura hoje como uma das grandes preocupações de muitos ccTLD's são os ataques informáticos – hacking – à infra-estrutura técnica por estes gerida e que, por regra, suporta o DNS do país em causa. O DNS.PR (Puerto Rico) veio neste fórum partilhar a experiência que teve com um ataque às suas máquinas que afectou, em Abril de 2009, registos importantes como o google.com.pr, a nike.com.pr a coca-cola.com.pr. Na prática, tratou-se de um *SQL Injection* para o interface do nic.pr, que acabou por ser resolvido no espaço de 2 horas.

Na sequência desta experiência – com reflexos a 3 níveis: registry, registrar e registrants – foram tomadas um conjunto de medidas tendo em vista minorar a possibilidade de ataques futuros, a saber: acesso à plataforma online por parte dos registrars baseado no respectivo endereço IP; contas bloqueadas ao fim de 3 tentativas falhadas de acesso; log-in de acesso feito com recurso a *token*; actualizações de domínios feitas apenas via telefone e sempre através dos mesmos interlocutores com a indicação prévia de um *passcode*.

No âmbito dos gTLD's e em sede do previsto no AoC (Affirmation of Commitments) o WHOIS Policy Review Team lançou no passado mês de Outubro uma consulta pública sobre o qual a informação que deve ser disponibilizada pelo sistema de WHOIS. Da proposta em apreciação resulta o princípio que cabe ao ICANN promover acções no sentido dos diferentes TLD's disponibilizarem o mesmo tipo de informação por forma a que fique garantido o princípio da transparência de forma equilibrada com o principio da salvaguarda da privacidade, confidencialidade de dados e protecção dos direitos dos consumidores. Assim sendo, conclui-se pela disponibilização pública do contacto do titular do domínio, de informação técnica sobre o mesmo e de alguma informação de cariz administrativo.

No que respeita aos ccTLD's europeus (em concreto aos seus 50 associados) o CENTR fez recentemente um inquérito onde aferiu que dos 25 ccTLD's que responderam, 15 dão acesso condicionado aos seus dados às entidades competentes, sendo que 10 deles o fazem sem quaisquer limites.

Como se antevia, a 40.ª edição da ICANN meetings fechou sem a aprovação do "Applicant Guidebook for New gTLD's". Porém, ficaram já agendados os próximos passos: 15 de Abril, será a data limite para responder aos pontos em aberto deixados pelo GAC na sequência da reunião que decorreu no passado mês de Fevereiro com o Board, sendo então publicada e disponibilizada para consulta pública a versão final do AG; a 15 de Maio fecha o espaço reservado aos comentários da comunidade; 20 de Maio reunião entre o GAC e o Board; 30 de Maio publicada a versão final fechada; 20 de Junho (durante a reunião de Singapura), data em que o Board estima aprovar, em reunião extraordinária, as regras e princípios que presidirão ao lançamento dos novos gTLD's. De qualquer forma, foi já antecipado, em termos macro, o modelo a seguir no processo de avaliação de cada novo gTLD. O processo começará com a submissão, seguida de uma avaliação inicial e de um período aberto de discussão pública (45 dias). Este espaço temporal foi definido como o tempo necessário e suficiente para o ICANN ter o feedback da comunidade, onde se incluem os governos dos países eventualmente interessados (questão com especial acuidade relativamente aos nomes geográficos) e o próprio GAC. Volvido este prazo o registry candidato é livre de desistir da aplicação que submeteu, sendo-lhe então devolvido 70% do valor pago aquando da submissão. Caso avance, será feita uma avaliação mais profunda num prazo que se estima ir até aos 4 meses e meio e tomada a decisão final que, se positiva, culminará na assinatura de um contrato com o ICANN.

Nota final, e especialmente relevante para a aprovação do *sponsored* gTLD .xxx – patrocinado, neste caso e nesta fase, significa que o respectivo registo só estará acessível à industria de conteúdos para adultos -. Diga-se que o ICM (registry do .xxx) declarou ter já 200 000 pré registos, indo brevemente lançar um *sunrise period* para os titulares de marcas registadas.

Fazendo uma breve resenha histórica o .xxx começou por ser recusado na reunião de Abril de 2006 em Wellington, recusa reforçada em Março de 2007 em Lisboa. Destas decisões resultou uma acção proposta pelo ICM contra o ICANN, que correu nos tribunais dos EUA. A sentença foi conhecida em Fevereiro de 2010, tendo sido favorável ao ICM, impondo ao ICANN a revisão do processo de registo do .xxx. Nessa sequência foi reaberto o processo interno de avaliação, tendo-se concluído não ter havido alterações às condições iniciais submetidas pelo ICM. Em Agosto foi submetida a consulta pública os termos do possível acordo a celebrar entre o ICANN

e o ICM. No comunicado de Cartagena o GAC reiterou os termos do comunicado de Wellington no sentido de não aprovar o .xxx. O Board deliberou então considerar estarem preenchidas as condições para aprovar este novo gTLD, bastando apenas o parecer último do GAC. A posição inicial deste órgão foi mantida e mesmo reforçada em São Francisco. O argumento seria o de que não havendo representantes governamentais a favor, havia claramente países que estavam enfaticamente contra. O que pesou na decisão do GAC foi o facto do lançamento do .xxx poder levar a que alguns governos comecem a bloquear este domínio, servindo tal de precedente legitimante de outros bloqueios. Em suma, seria um passo para pôr em causa a estabilidade e resiliência do DNS.

No dia 18 de Março de 2011 foi aprovado com unanimidade o .xxx, após discussão acesa que, de resto, reflectiu o que se tinha passado, um dia antes, no *public forum*, marcado pela presença de vozes discordantes, curiosamente oriundas de representantes da indústria dos conteúdos para adultos/pornográficos. A ordem de argumentos do ICANN foi clara, não está em causa o princípio da liberdade de expressão, não está em causa a estabilidade e resiliência do DNS, o que está ao fim destes anos está em causa é a obrigação de cumprir procedimentos e fechar um processo cuja manutenção em aberto não tem qualquer justificação à luz das regras aplicáveis. O futuro o dirá.