ICANN57
HYDERABAD
3-9 November 2016
ANNUAL GENERAL

RELATÓRIO DNS.PT

ÍNDICE

Sumário Executivo

Neste relatório, para além daquilo que seja o enfoque puramente técnico, iremos debruçar a nossa atenção em três assuntos amplamente debatidos nesta edição da ICANN, e cujos potenciais desenvolvimentos se afiguram de particular interesse para o ccTLD nacional.

Referimo-nos em concreto à possibilidade de apropriação futura pelos novos gTLDs dos códigos dos países - Alf 2 e 3/ISO 3166 -; das questões relativas à proteção de dados; do impacto global da nova regulamentação comunitária e, por fim, da questão da possível intervenção dos registries e, em última análise, da ICANN, nos conteúdos online.

Introdução

A edição 57 da ICANN decorreu entre os dias 3 e 9 de novembro na Índia, em Hyderabad, o segundo país com mais população do mundo, com uma diversidade linguística assinalável, marcada por um registo oficial de 22 línguas faladas e 15 diferentes alfabetos. Atualmente o ccTLD .IN tem cerca de 2.5 milhões de domínios registados, num país com uma taxa de penetração da Internet de cerca de 36%. Esta reunião foi identificada como histórica. Primeiro, porque foi a maior reunião pública de sempre da ICANN, com um total de 3.141 participantes[1], em segundo lugar porque assumiu o modelo novo de 7 dias de duração, que ocorre uma vez ao ano, inaugurando uma nova era no modelo de funcionamento destas reuniões, em terceiro lugar, e como corolário da relevância dada à interação da comunidade com o board, porque foi a primeira reunião que contou com dois Fóruns Públicos de discussão. A este propósito o provedor da ICANN, Herb Waye, defendeu que, passamos a citar, "*Devemos estar conscientes de nossas diferenças e abraçá-las como sendo a força da comunidade*".

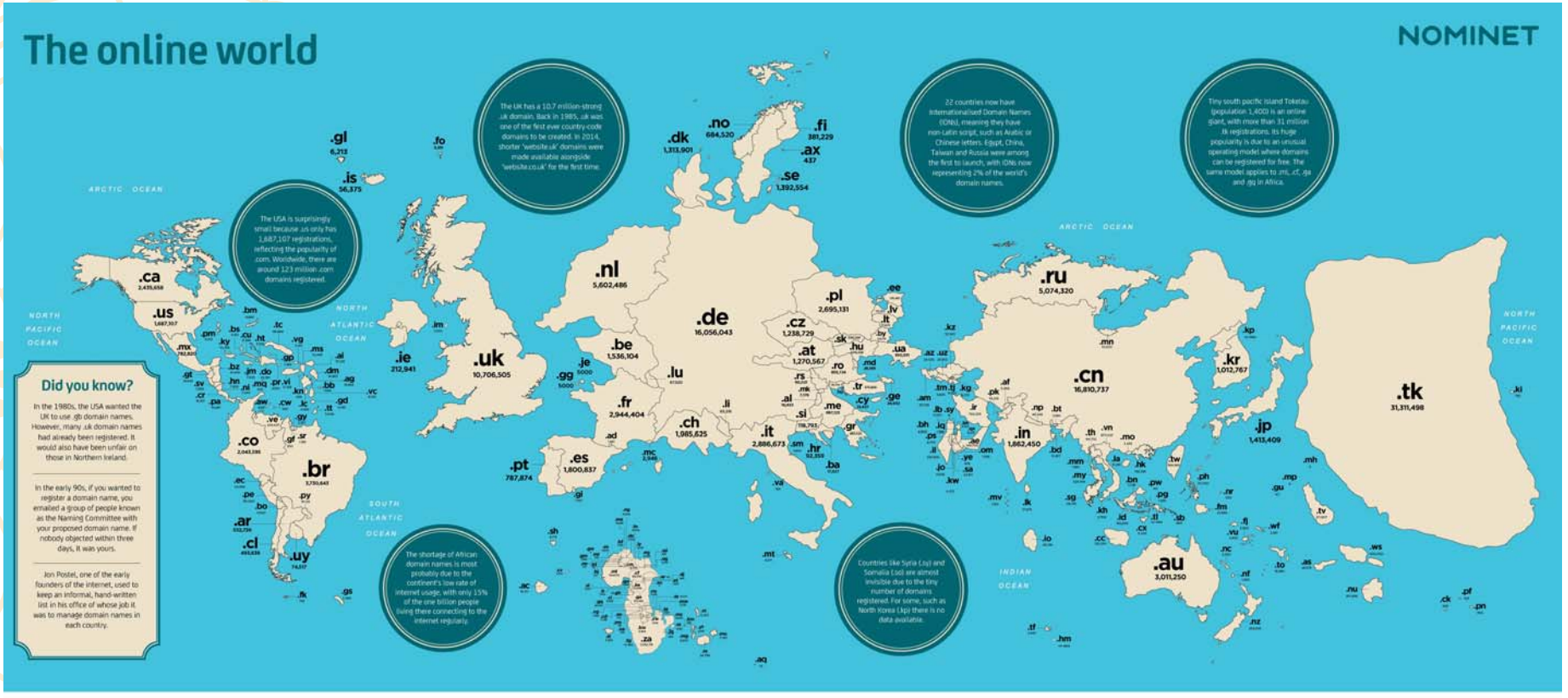
[1] *Número que porém esteve perto da reunião 50.º, em Londres, com 3.115 participantes registados.*

A estas três razões acresce uma última que, pela sua relevância, merece nota à parte: esta foi a primeira reunião pública após a conclusão do processo de transição das funções da IANA anunciado a 30 de setembro último. Como é sabido na sequência do anúncio público da NTIA, a 14 de março de 2014, a ICANN lançou um processo aberto e participado para reunir a posição da comunidade multistakeholder envolvida sobre os princípios e mecanismos aplicáveis para a transição da administração da NTIA das funções da IANA. Na base do trabalho a desenvolver estariam sempre presentes um conjunto de premissas, a saber: uma participação multistakeholder; a manutenção da segurança, estabilidade e resiliência do DNS, a obrigação de atender às necessidades e expectativas dos clientes e parceiros da IANA e, por fim, a manutenção da abertura da Internet. Por fim, foi ainda condição que a nova organização a criar não poderia ter uma natureza governamental ou intergovernamental. Assim, a partir do passado dia 1 de outubro, as funções da IANA passaram a ficar garantidas por uma afiliada da ICANN a, PTI - Public Technical Identifiers.

Assim, se enquadra parte do discurso feito pelo Presidente da ICANN na sessão de abertura, do qual se extrai a declaração:

Thank you, you´re now in charge – Göran Marby, Presidente da ICANN
Discurso completo em: https://youtu.be/AEBn8ezNxWQ

O Mundo online



Utilização de Nomes e Códigos de Países e Territórios pelos novos gTLD's

A possibilidade dos novos gTLD's incluírem domínios coincidentes com a classificação adoptada na norma ISSO 3166 - códigos Alfa 2[2] ou 3[3] – vem a ser debatida há largos meses, tendo agora merecido especial atenção em várias sessões que decorreram nesta última edição da ICANN. Se pensarmos que a nova ronda para submissão de candidaturas a novos gTLD's não se perspetiva para antes do final de 2018, esta questão pode não ter qualquer tipo de acuidade, porque não é, digamos, suficientemente oportuna. Porém, já será diferente nos casos em que se desenha a possibilidade de códigos como .pt ou .prt poderem ser registados como domínios de segundo nível nos mais de 1900 domínios já delegados neste processo com início no longínquo ano de 2013.

Se pensarmos que estamos a falar de códigos que fazem parte da identidade de cada país e que são marcas ou símbolos nacionais e de soberania, a questão em presença facilmente se converte num problema a resolver.

Vejamos pois o enquadramento que julgamos dever ser considerado para melhor compreender a matéria em análise.
O contrato celebrado entre a ICANN e cada um dos registries dos novos gTLD's prevê que estes últimos estejam vinculados à reserva, no segundo nível, dos códigos elencados no ISO 3166, salvo acordo em contrário com o governo/registry do país em questão. Esta é pois a realidade vigente. Até à data Portugal[4] foi contactado para liberar o registo de .pt por apenas dois registries, tendo defendido a posição que o código PT, no imediato não seria disponibilizado para registo de segundo nível.

O GAC[5] emitiu parecer formal[6] sobre esta matéria em ocasiões distintas. A título de exemplo, no comunicado de Los Angeles (15 de outubro de 2014) o GAC defendeu que os nomes de domínio de dois caracteres são amplamente utilizados em todos os TLDs existentes e não têm posto em causa a segurança, estabilidade ou, em última análise, não têm sido fonte de questões de natureza técnica ou mesmo concorrenciais, no entanto, esta situação deveria ser ponderada e levada a discussão pública. Sob este contexto, o board adotou uma resolução ao abrigo da qual o staff da ICANN era nomeando para desenvolver e implementar um procedimento eficiente para a liberação futura de domínios de dois caracteres. Nos comunicados de Singapura (11 de Fevereiro de 2015) e Dublin (21 de Outubro de 2015), defendeu não estar ainda em posição de emitir um parecer consensual sobre a matéria, merecendo a mesma discussão suplementar. No Comunicado de Helsínquia (30 de Junho de 2016), o GAC arguiu a importância de ser sempre levado ao conhecimento do governo e do registry respetivo qualquer tentativa de registo coincidente com um ccTLD.

2 *PT para Portugal.*
3 *PRT para Portugal*
4 *Estes contactos têm sido realizados via representante nacional no GAC, neste caso a FCT-DSI.*

5 *GAC, Governmental Advisory Committee. Funciona como órgão consultivo junto da ICANN, representando hoje 171 governos mais 35 observadores. Portugal é representado pela Dra. Ana Cristina Neves, diretora do departamento da sociedade da informação da Fundação para a Ciência e a Tecnologia, FCT. Informação adicional em: https://gacweb.icann.org/display/gacweb/About+The+GAC*

6 *Os pareceres do GAC são emitidos no formato "Communiqué", no termo de cada reunião pública da ICANN. Este Communiqué, sendo público, é formalmente dirigido ao board da ICANN.*

A ICANN iniciou vários períodos de comentários públicos e consultou várias partes interessadas sobre o assunto durante um período de quase dois anos e meio. Entre junho a setembro de 2014, a equipe da ICANN tinha já conduzido cinco fóruns públicos no sentido de obter feedback da comunidade. Mais de 646 comentários foram recebidos ao longo do processo. No passado dia 8 de julho, a ICANN publicou para comentário público um conjunto de propostas e medidas que os registries poderiam adotar para evitar a eventual confusão com os códigos dos países correspondentes. Foram recebidos quarenta e três comentários, a maioria favorável à liberação de nomes de domínio de dois caracteres.

Que especiais preocupações ou questões foram levantadas pela comunidade?

I. A introdução de nomes de domínio de dois caracteres aumentaria a concorrência, uma vez que as atuais restrições criam constrangimentos, em particular para os novos gTLDs, que estão a competir com os designados legacy TLDs;

II. A introdução de nomes de domínio de dois caracteres apresenta um risco limitado de confusão, como de resto já ficou demonstrado pelo uso prévio de nomes de domínio de dois caracteres em TLDs existentes;

III. A liberação de nomes de domínio de dois caracteres criaria novas oportunidades para empresas e marcas aumentando a escolha do consumidor e impulsionando o crescimento económico, em particular nos países em desenvolvimento.

Aos argumentos aduzidos anteriormente contrapõem-se aqueles já acima identificados e que se prendem com o reconhecimento geral e o uso associado dos dois nomes de domínio aos códigos de países, para o propósito aos ccTLDs, o que claramente pode gerar confusão aos consumidores e utilizadores globalmente considerados.

Nesta sequência, o board deliberou na reunião de Hiderabad, conforme comunicado público de 8 de novembro, deverem ser desbloqueados os domínios de duas letras que correspondam aos códigos de países que figuram na lista ISO 3166, a maioria dos quais ccTLDs, com exceção dos reservados, de acordo com a Especificação 5, Seção 6 do contrato registry/registrar. O GAC reagiu de imediato a este comunicado expressando uma "séria preocupação" pelo facto de o board não ter respondido formalmente[7] ao seu comunicado de Helsínquia. "É nossa convicção que a nossa resolução é consistente com o parecer do GAC", afirmou, em tom de resposta, Bruce Tonkin, membro do board da ICANN, aditando ainda que ninguém pode reivindicar direitos exclusivos sobre qualquer sequência de caracteres, independentemente da sua natureza.

[7] *Refira-se que de acordo com o Artigo XI, Seção 2.1 dos Estatutos da ICANN, o GAC pode "submeter questões ao board diretamente, por meio de comentários ou pareceres prévios, ou recomendando especificamente ações ou novas políticas de desenvolvimento ou revisão de políticas existentes". Os Estatutos da ICANN exigem que o board tome em consideração o parecer do GAC em questões de política pública na formulação e adoção das políticas. As recomendações não são pois vinculativas.*

O processo decisório, para além de moroso, tomou em consideração um conjunto de fatores e ordens de razão, sobretudo de cariz formal e que, pela sua pertinência, reproduzimos abaixo:

- Specification 5, Section 2 of the New gTLD Registry Agreement
- RSTEP Report on the Proposal for the Limited Release of Initially Reserved Two-Character Names
- Correspondence from the Board to the GAC regarding requests for release of two-character labels as second-level domains in New gTLDs
- Correspondence from the GAC to the Board regarding requests for release of two-character labels as second-level domains in New gTLDs
- GAC Los Angeles Communiqué
- ICANN Board Resolution 2014.10.16.14: Introduction of Two-character Domain Names in the New gTLD Namespace
- Authorization Process for Release of Two-Character ASCII Labels
- GAC Singapore Communiqué
- ICANN Board Resolution 2015.02.12.2016: Release of Two-Letter Codes at the Second Level in gTLDs
- Correspondence from RySG to the President of the Global Domains Division regarding the treatment of government comments on requests to release two-character ASCII labels
- Response from the President of the Global Domains Division to the RySG regarding the treatment of government comments on requests to release two-character ASCII label
- Joint Correspondence from the BRG, the BC and the IPC to the Board regarding the release of 2-letter labels and country names for Specification 13 registries
- Response from the President of the Global Domains Division to the BRG, the BC and the IPC regarding the release of 2-letter labels and country names for Specification 13 registries
- Correspondence from GAC to the President of the Global Domains Division re-garding two-character codes as Second Level Domains
- Response from the President of the Global Domains Division to the GAC regard-ing two-character codes as Second Level Domains
- Two-Character Letter/Letter Labels Comments Consideration Process
- GAC Dublin Communiqué
- Correspondence from RySG to the Board regarding advice contained in the GAC's Dublin communiqué regarding the use of two-letter country codes
- Response from the Board to the RySG regarding advice contained in the GAC's Dublin communiqué regarding the use of two-letter country codes
- GAC Helsinki Communiqué
- Proposed Measures for Letter/Letter Two-Character ASCII Labels to Avoid Confu-sion with Corresponding Country Codes
- Public Comment Summary and Analysis Report on Proposed Measures

Ficam agora as questões de saber qual o impacto na comunidade, na própria ICANN (plano estratégico, plano de atividades, orçamento); e, tão ou mais importante, na segurança, estabilidade ou resiliência do DNS. Os próximos meses irão já trazer algumas respostas às quais deveremos estar atentos, sobretudo olhando para o panorama nacional do .pt.

Outra das questões que referimos anteriormente e que se prende igualmente com a utilização pelos novos gTLDs de códigos de países ou territórios, é a de saber qual o enquadramento que deve ser adotado no que respeita à possibilidade de registo destes códigos, já não no segundo nível mas antes e logo no primeiro nível. Clarificando, estamos agora a falar, por exemplo, no hipotético registo de um .PRT ou de um .GBR[8].

A acuidade desta questão levou mesmo à criação do CWG UCTN[9] ,cujo mandato se resume à preparação de um documento de trabalho concertado entre as constituencies[10] que representam os diferentes interesses na matéria, a enviar em tempo oportuno ao board da ICANN. No entretanto, já foram apresentados alguns resultados. Primeiro a reserva pelo ICANN dos domínios com duas letras deve manter-se, o que é de resto consentâneo com o RFC 159, segundo, não cabe à ICANN a definição de que determinada composição de carateres corresponde ou não a um país ou território. Já relativamente aos códigos Alfa 3 há divergência entre os que entendem que estes deve ser tratados como ccTLD's e aqueles que consideram que devem vir a ser permitidos numa segunda ronda, embora com algumas restrições, por exemplo, terem o apoio, ou pelo menos, uma não objeção, por parte do governo e/ou do registry do país em causa. Nota para dizer que hoje se encontram já delegados 66[11] gTLD's geográficos. Uma outra possibilidade vislumbrável seria o próprio registry do ccTLD com dois carateres passar a gerir também o código de três carateres. Perante esta última possibilidade, levantaram-se vozes discordantes (caso da Holanda), invocando violação clara das regras da concorrência. Questão paralela é a de países como a Tailândia que defendem estarmos perante uma questão de natureza puramente técnica, havendo designações que são muito mais ilustrativas daquilo que define o país devendo, essas sim, serem protegidas, no caso vertente, a designação Thai. Paralelamente, e na senda do litigio que tem rodeado a questão do registo do gTLD .africa em confronto com o registo do .dotafrica, a African Telecommunication Union Administrations submeteu no passado mês de outubro ao ITU[12] uma proposta de alteração à Resolução 47[13] da World Telecommunication Standardization Assembly (WTSA/Dubai), sobre nomes de domínios.

8 *ISO 3166/cód Alfa 3 correspondente ao Reino Unido.*

9 *Cross Community Working Group on Use of Country and Territory Names.*

10 *Generic Names Supporting Organization, GNSO; Country Code Names Supporting Organization, ccNSO; GAC, etc.*

11 *Exemplo: .berlin; .budapest; .paris; .cologne, vários IDN como o correspondente a .moscow,* москва*, etc.*

12 *(Versão em inglês) The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of tele¬com¬mu-ni¬ca¬tions. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU T study groups which, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. Disponível para consulta em: http://www.itu.int/pub/T-RES-T.47-2012*

13 *http://www.itu.int/pub/T-RES-T.47-2012*

Em suma, o objetivo seria o de criar mecanismos acrescidos àqueles hoje em prática pela ICANN, que, segundo estes se têm revelado insuficientes, para proteger os nomes geográficos associados ao continente Africano, vindo chamar a si o direito de veto a qualquer resolução do ICANN que viole os princípios acordados e contratualizados relativamente a nomes geográficos, nomeadamente a candidatura apresentada para o dotafrica. Entretanto, da WTSA que decorreu na Tunísia, entre os dias 25 de outubro e 3 de novembro, não resultou qualquer alteração à resolução 47 que assim se mantém na versão original.

Concluindo, no que concerne ao primeiro nível o registo de dois ou três carateres coincidentes com ccTLD's e/ou com o código ISO 3166, por parte dos novos gTLD's continua expressamente vedada, no entanto, o caminho e a discussão estão abertos. Aguardam-se novos desenvolvimentos.

Proteção de Dados Pessoais

A matéria relativa à proteção dos dados pessoais, sobretudo na vertente relativa à recolha, tratamento e disponibilização dos dados dos titulares e gestores técnicos e administrativos dos domínios, tem sido desde sempre objeto de discussão no seio da ICANN. Ao nível técnico, por exemplo, a evolução tem sido salutar, do WHOIS[14] aos desafios agora lançados pelo muito recente novo protocolo de acesso a dados de registo, o RDAP[15], muito se tem feito mormente tendo como objetivo a qualidade, na aceção, de veracidade e exatidão dos dados que são fornecidos por quem regista e gere um domínio. Ou seja, neste campo a ICANN 57 pouco nos trouxe de novo.

Temos, no entanto, um contorno que fez acender as discussões e acelerar qualquer ideia que estivesse em curso de alteração das políticas de tratamento de fluxo de dados pessoais em matéria de DNS: falamos do novo Regulamento Geral sobre a Proteção de Dados - Regulamento (EU) 2016/679, de 27 de abril de 2016 - proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), transposta em Portugal pela Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro. Este diploma, prevendo um período transitório de dois anos para adaptação às novas regras, passará a ser diretamente aplicável aos 28 Estados-Membros a partir do dia 25 de Maio de 2018.

14 *Ferramenta WHOIS disponibilizada pelo DNS.PT: https://www.dns.pt/pt/ferramentas/whois/*

15 *Informação atualizada e relevante em: https://participate.icann.org/p6s8aawsot6/?launcher=false&fcsContent=true&pbMode=normal*

Principalmente quando se trata de partilhar os dados dos cidadãos da UE com os EUA, a UE assume-se como o bastião da proteção de dados. No entanto, as paredes da proteção são mais finas dentro da própria UE, especialmente com os desafios da globalização trazidos pelo mundo online, pelo mercado único digital. Urge pois a definição de medidas claras e eficazes mas que em simultâneo não comprometam a abertura, a resiliência e a estabilidade da Internet. Foi sob este contexto que assentaram grande parte das discussões que decorreram a respeito nesta última edição da ICANN.

Não sendo este o fórum para explorar aquilo que nos vai trazer este Regulamento há elementos que foram amplamente reiterados e que, por esse facto nos merecem aqui nota. A importância da harmonização da legislação de proteção de dados no Espaço Económico Europeu, a adaptação das regras de privacidade à nova era digital e criação de confiança nos meios digitais, os requisitos mais exigentes ao nível da informação e da obtenção do consentimento, as exigências reforçadas para o tratamento de dados de perfil com o reforço dos direitos dos titulares dos dados e, depois, o tratamento das matérias relativas à segurança/notificação dos incidentes de segurança. Importante ainda o reforço do quadro sancionatório[16].

Estando nós no âmbito do online onde o conceito geoespacial e o princípio da territorialidade são desafiados a cada segundo, relevante é pois saber a forma como o Regulamento vai tratar, nomeadamente, as transferências de dados para fora da EU. Aí temos a regra geral do Artigo 44º, que dispõe que " As transferências de dados pessoais só podem ser realizadas no estrito cumprimento do disposto no RGPDP". Se relativamente ao tratamento de dados num Estado-Membro cada autoridade é responsável por monitorizar os termos de tratamento de dados e assegurar o cumprimento do Regulamento, a nível supra-fronteiriço qualquer autoridade passa a poder gerir queixas e reclamações por um titular dos dados ou entidade, se a questão for referente a um estabelecimento localizado no seu Estado-Membro ou se afetar substancialmente titulares dos dados localizados apenas na sua jurisdição.

16 *As penalidades pelo incumprimento podem ascender a 20 milhões de euros ou a 4% do volume total de negócios anual.*

Novidade, neste âmbito, é ainda a criação de um mecanismo de "One-Stop-Shop"[17] para tratamento de dados transfronteiriços na EU. Relevante aqui é também a questão da transferência de dados UE-EUA[18], como é sabido os safe harbour principles foram declarados inválidos pelo TJUE em outubro de 2015. A nível nacional, a CNPD[19] deliberou que todas as transferências de dados à luz do Safe Harbour iriam ser revistas e as empresas deveriam suspender os fluxos internacionais de dados pessoais com base neste mecanismo. Hoje, a cobertura legal para a transferência de dados da UE para os EUA está suportada no designado Privacy Shield Framework, aprovado em julho de 2016 e desenhado pelo Departamento de Comércio dos EUA e pela Comissão Europeia, no sentido de disponibilizar mecanismos que cumpram o quadro legal da transferência de dados pessoais da União Europeia para os Estados Unidos.

Comparativamente com o quadro legal vigente, o Regulamento é claramente mais tentacular em termos de aplicação já que irá, a título de exemplo, aplicar-se às operações de tratamento que incidam sobre titulares de dados pessoais europeus, independentemente de o responsável pelo tratamento (ou o subcontratante) se encontrar ou não localizado na UE.

Ora foi todo este enquadramento que levou a que a matéria do tratamento e proteção de dados fosse trazida a este largo fórum de discussão. 2018 ainda está longe porém, sobretudo os registries e os registrars, têm de começar a preparar as suas infraestruturas e políticas internas para este novo paradigma que terá certamente impacto no negócio e no funcionamento diário do DNS, na componente de privacidade e gestão de dados pessoais.

Conteúdos Online:A Possível Intervenção dos Registries e da ICANN

A reflexão centrou-se em dois pontos distintos: primeiro o de saber se os registries ou, em última análise a ICANN, têm competência para intervir na remoção de conteúdos online, por exemplo, bloqueando sites e, em segundo, o de identificar as situações em que os conteúdos, per si, se configuram como ilícitos e se, ainda assim, e em nome de princípios constitucionais como a liberdade de expressão[20] devem ser removidos.

Relativamente à primeira questão os novos estatutos[21] da ICANN parecem não levantar dúvidas. No capítulo relativo à missão, compromissos e valores, em concreto no artigo 1.º, secção 1.1., al (c)[22] é afastada a possibilidade de serem aplicadas regras ou

17 *Mecanismo de balcão único (one-stop-shop) para empresas multinacionais, com base na determinação de um estabelecimento principal.*

18 *https://www.privacyshield.gov/welcome*

19 *https://www.cnpd.pt/bin/relacoes/comunicados/Comunicado_CNPD_SafeHarbor.pdf*

20 *A Constituição da Republica Portuguesa consagra no artigo 37.º o direito à liberdade de expressão e informação http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx*

21 *https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf*

22 *"ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority."*

restrições relativamente aos conteúdos. Esta disposição é particularmente relevante no universo dos gTLD's no âmbito da qual, como é sabido, a ICANN mantém uma relação contratual[23] com os respetivos registries onde são impostos direitos e obrigações que, de alguma forma, espelham, entre outros, aquilo que são os princípios base que regem a ICANN. Este será pois um deles. Ou seja, no imediato, as políticas aplicáveis ao registo de domínios sob gTLD's refletindo as obrigações assumidas *à priori* com a ICANN, não preveem qualquer obrigação ao nível da monitorização de conteúdos. Relativamente às regras aplicáveis aos diferentes ccTLD's reconhece-se a mesma tendência. A título de exemplo, em Portugal o registo de um domínio está unicamente dependente da análise que recai sob o nome do domínio em si e nunca sob os conteúdos que a este fiquem posteriormente associados. Pós registo as causas de remoção estão expressamente tipificadas nos artigos 32.º e 33.º das Regras aplicáveis[24] e não incluem no seu articulado qualquer referência aos conteúdos. Não obstante este facto, um domínio pode ser removido na sequência de decisão arbitral ou judicial[25] para o efeito, a qual pode ter obviamente na sua origem a existência comprovada de conteúdos ilícitos de natureza diversa. O .pt nunca divulgou uma posição formal relativamente a esta matéria, porém, face ao articulado das regras de registo de domínio vigentes e aos termos e abrangência da recente subscrição do Memorando Ofertas Legais[26] será simples inferir a política que tem sido seguida a respeito, de resto consentânea com o recentemente sufragado pelo CEO da nossa congénere do Reino Unido, Nominet:

> *"As guardian of the UK namespace for 20 years, we invest significantly to help all .UK owners protect their domains and take seriously our role in helping to protect internet users from criminality online. Collaborating with law enforcement agencies we are helping more people be safe and networks stay secure."*
>
> Russell Haworth, Nominet CEO

A este propósito merece-nos nota a proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO[27] , publicada no passado mês de maio, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação coerciva da legislação de defesa do consumidor e que estabelece as condições em que as autoridades competentes designadas pelos Estados-Membros como responsáveis pela aplicação coerciva da legislação de defesa dos interesses dos consumidores devem cooperar entre si

23 *No caso do ccTLD nacional, o .pt, a relação formal com a ICANN baseia-se apenas numa troca de cartas, não tendo sido firmado qualquer contrato, este é de resto o panorama comum à maior parte dos ccTLD's.*

24 *https://www.dns.pt/pt/dominios-2/regras-de-dominios/capitulo-iv/*

25 *No reino Unido, onde o número de registos ascende a mais de 10 milhões, entre novembro de 2015 e outubro de 2016 foram removidos mais de 8000 domínios na sequência de sentenças relativas a conteúdos ilícitos online. Este número traduziu um crescimento de mais de 50% relativamente a período homólogo.*

26 *No dia 30 de julho de 2015 foi assinado, em lisboa, o Memorando de Entendimento cujo objeto central passou pela promoção da cultura, da criatividade e a defesa dos Direitos de Propriedade Intelectual, em geral, e na Internet em particular. Neste âmbito, e após várias sessões negociais, juntaram-se um conjunto de players interessados em subscrever. Referimo-nos em concreto ao leque de todas as entidades que, em Portugal, têm voz e responsabilidades nesta matéria, em concreto: à IGAC – Inspeção-Geral das Atividades Culturais, à DGC – Direção-Geral do Consumidor, à APRITEL – Associação dos Operadores de Telecomunicações, em representação dos operadores de comunicações eletrónicas nacionais, à MAPINET – Movimento Cívico Anti Pirataria na Internet, à SPA – Sociedade Portuguesa de Autores, AFP – Associação Fonográfica Portuguesa, à APEL – Associação Portuguesa de Editores e Livreiros; à API – Associação Portuguesa de Imprensa; à AUDIOGEST – Associação para a Gestão e Distribuição de Direitos; à ASSOFT – Associação Portuguesa de Software; à FEVIP – Associação Portuguesa de Defesa de Obras Audiovisuais; à GDA - Cooperativa de Gestão dos Direitos dos Artistas, Intérpretes ou Executantes, CRL; à GEDIPE – Associação para a Gestão de Direitos de Autor, Produtores e Editores; à VISAPRESS – Gestão de Conteúdos dos Media, CRL, à APAP – Associação Portuguesa das Agências de Publicidade, Comunicação e Marketing, à APAME – Associação Portuguesa das Agências de Meios, à APAN - Associação Portuguesa de Anunciantes e, por fim ao DNS.PT - Associação DNS.PT.*
O acordo entrou em vigor na segunda quinzena de agosto e corporiza um acordo pioneiro a nível europeu de auto-regulação no que respeita à proteção do direito de autor e dos direitos conexos em ambiente digital. Por esta via, foi criado um mecanismo expedito de notificação que culmina no encerramento de sites que disponibilizem de forma não autorizada obras ou prestações e que, como tal, violem a lei aplicável.
Em concreto ao DNS.PT está adstrita a função de disponibilização do alojamento e do domínio de suporte ao portal – www.ofertaslegais.pt -, onde será disponibilizada uma lista dinâmica de sítios com ofertas legais nas áreas da música, videojogos, livros, audiovisual e eventos desportivos.

27 *https://ec.europa.eu/transparency/regdoc/rep/1/2016/PT/1-2016-283-PT-F1-1.PDF*

e com a Comissão, de forma mais eficiente e célere, a fim de assegurar o cumprimento dessa legislação e o bom funcionamento do mercado interno, e de reforçar a proteção dos interesses económicos dos consumidores. Designadamente, para tomada de medidas provisórias de bloqueio dos chamados websites infratores. A proposta passa por no campo da esfera digital, as autoridades competentes deverem deter o poder de pôr cobro a infracções, nomeadamente se o operador que vende bens ou serviços online ocultar a sua identidade ou deslocar as suas atividades no interior da União ou para um terceiro país, no intuito de evitar a aplicação coerciva da lei aplicável.

As autoridades competentes devem dispor dos poderes necessários para fechar, ou notificar para o propósito o prestador de serviços, websites, domínios ou quaisquer outros serviços ou contas digitais similares. Isto caso se verifique um risco de prejuízo grave e irreparável para os consumidores. Ao abrigo desta proposta de Regulamento, os registries (por exemplo a Associação DNS.PT) podem ser notificadas para remover domínios que alojem conteúdos ilícitos.

O CENTR[28] já emitiu uma opinião formal sobre o articulado desta proposta de Regulamento vindo defender que apoia o objetivo de melhorar a regulamentação de proteção do consumidor em toda a Europa, muito embora tenha dúvidas sobre a eficácia do mesmo.

Na realidade as medidas estabelecidas podem revelar-se ineficazes, na medida em que a remoção de um domínio do ficheiro da zona não obvia à consulta do website em questão, basta para o efeito aceder ao respetivo enderenço IP. Assim sendo, e pensando naquilo que são os interesses dos diferentes ccTLD's representados pelo CENTR, foi no imediato encontrada a seguinte posição concertada:

Verificando-se a existência de conteúdos ilícitos num website dever-se-á iniciar o processo notificando o respetivo titular e solicitando a remoção dos mesmos, sendo esta solução ineficaz o recurso seguinte será à entidade que aloja o website, só pois em última instância deve o registry ser notificado no sentido de remover o domínio do arquivo de zona. Nota final do CENTR no sentido que esta obrigação deve ser igualmente extensível aos gTLD's.

[28] *https://www.centr.org/*

A segunda questão debatida no capítulo dos conteúdos prende-se com a definição ou âmbito daquilo que podem ser considerados conteúdos ilícitos, ou melhor, do que deva ser censurável do ponto de vista jurídico no mundo online. Aqui a discussão foi mais participada, se por um lado se defendeu que os conteúdos que violem disposições legais devem ser eficaz e atempadamente removidos[29], por outro, e em nome de princípios como, nomeadamente, a liberdade de expressão e a neutralidade da rede[30] foi defendido que em caso algum um website deve ser removido em função da natureza dos conteúdos que encerra. A virtude estará certamente numa posição moderada onde, acima de tudo, fique garantida a proteção do consumidor e dos utilizadores da Internet em geral, consolidada na confiança e segurança relativamente ao que se transaciona e consulta online. Esta é uma discussão que se perspetiva longa e participada, estaremos pois atentos.

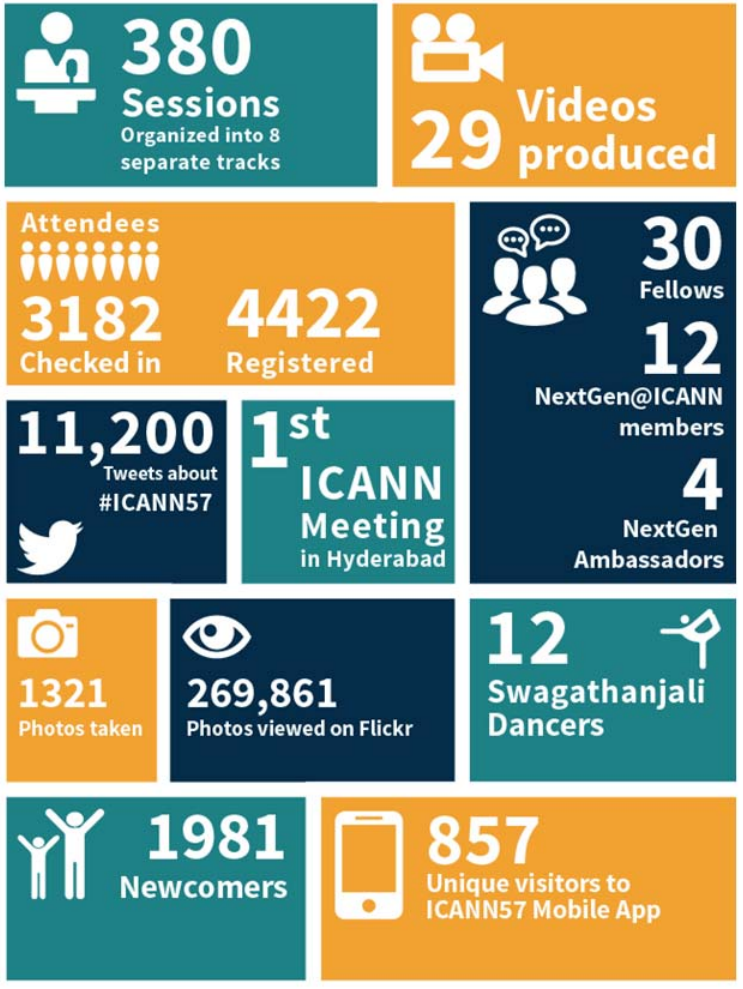
"*A neutral network might be designed without legal prodding – as in the original internet. In an ideal world, either competition or enlightened self-interest might drive carriers to design neutral networks*".- Tim Wu, Professor at Columbia Law School

29 *Veja-se o impacto para a saúde pública do comércio online de medicamentos falsificados. Só em 2015 foram encerrados mais de 2400 websites que operavam nesta área. Informação útil em: https://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea*

30 *(Versão em ingles) "Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized – when they are a platform for multiple uses, present and future. (For people who know more about network design, what is just described is similar to the "end-to-end" design principle).*
Em: http://www.timwu.org/network_neutrality.html

Conclusão

Os números:



No encerramento da ICANN57 em Hyderabad, Índia, Liana Teo, diretora de comunicação da ICANN para a região Ásia-Pacífico, reuniu Stephen Crocker e Göran Marby, e registou esta breve análise retrospetiva, que sumariza, na perspetiva dos lideres da ICANN o que de mais importante se passou ao longo desta longa semana de trabalhos.

Assista o video em: https://youtu.be/sg8wfjWWk1E

Informação complementar:

RELATÓRIO CENTR:
https://www.centr.org/library/library/external-event/centr-report-on-icann57.html;

COMMUNIQUÉ DO GAC:
https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee

BOARD RESOLUTIONS:
https://www.icann.org/resources/pages/2016-board-meetings

ICANN | 57 • TECH DAY

Nomulus

Richard Roberto da Google apresentou a solução *Nomulus*, uma solução de serviços *Registry* desenvolvida e utilizada pela Google na gestão e operação dos seus domínios de topo, nomeadamente .GOOGLE, .HOW, .SOY e .みんな (.MINA em Japonês).

Esta solução suporta todos os requisitos de funcionalidades exigidos pelo ICANN, os protocolos *Extensible Provisioning Protocol (EPP), Whois e Registration Data Access Protocol (RDAP)*, produz relatórios, tem mecanismos de proteção de marcas e salvaguarda da informação *Data Escrow (RDE/BRDA)*. Suporta ainda DNSSEC, não o processo de assinar domínios, mas sim a submissão do registo DS para a hierarquia superior. Corre na plataforma *Google App Engine*, e os dados são armazenados na plataforma *Google Cloud Datastore*. O código está escrito maioritariamente em Java, e no passado mês de outubro foi disponibilizado publicamente sob a licença *open source Apache 2.0*.

A Google não recomenda a utilização desta plataforma localmente '*On-premises*' exceto para efetuar testes à plataforma. A forte ligação aos serviços *Cloud* da Google é um fator desencorajador à adoção desta plataforma por outras entidades *Registries*.

IDN e Virtual Keyboard

A associação *CORE Internet Council of Registrars*[1] apresentou o domínio de topo (TLD) "xn--mgbab2bd"[2] (notação *Punycode*) composto unicamente por caracteres da língua árabe e cuja tradução para inglês é 'bazaar', uma expressão que significa um local de atividade comercial onde produtos e serviços são comercializados.

Esta expressão é utilizado num território vasto que inclui o médio Oriente, o sudeste Asiático, Ásia central e o norte de Africa. É reconhecido por mais de 600 milhões de pessoas que falam Árabe, Curdo, Afegão, Persa e Urdu entre outras linguagens. O objetivo deste domínio de topo é providenciar uma plataforma que promova a adoção em larga escala de iniciativas de comércio eletrónico num mercado emergente e em rápido crescimento.

O registo de domínios neste TLD é aberto a qualquer entidade, sendo que têm que ser composto exclusivamente por caracteres árabes.

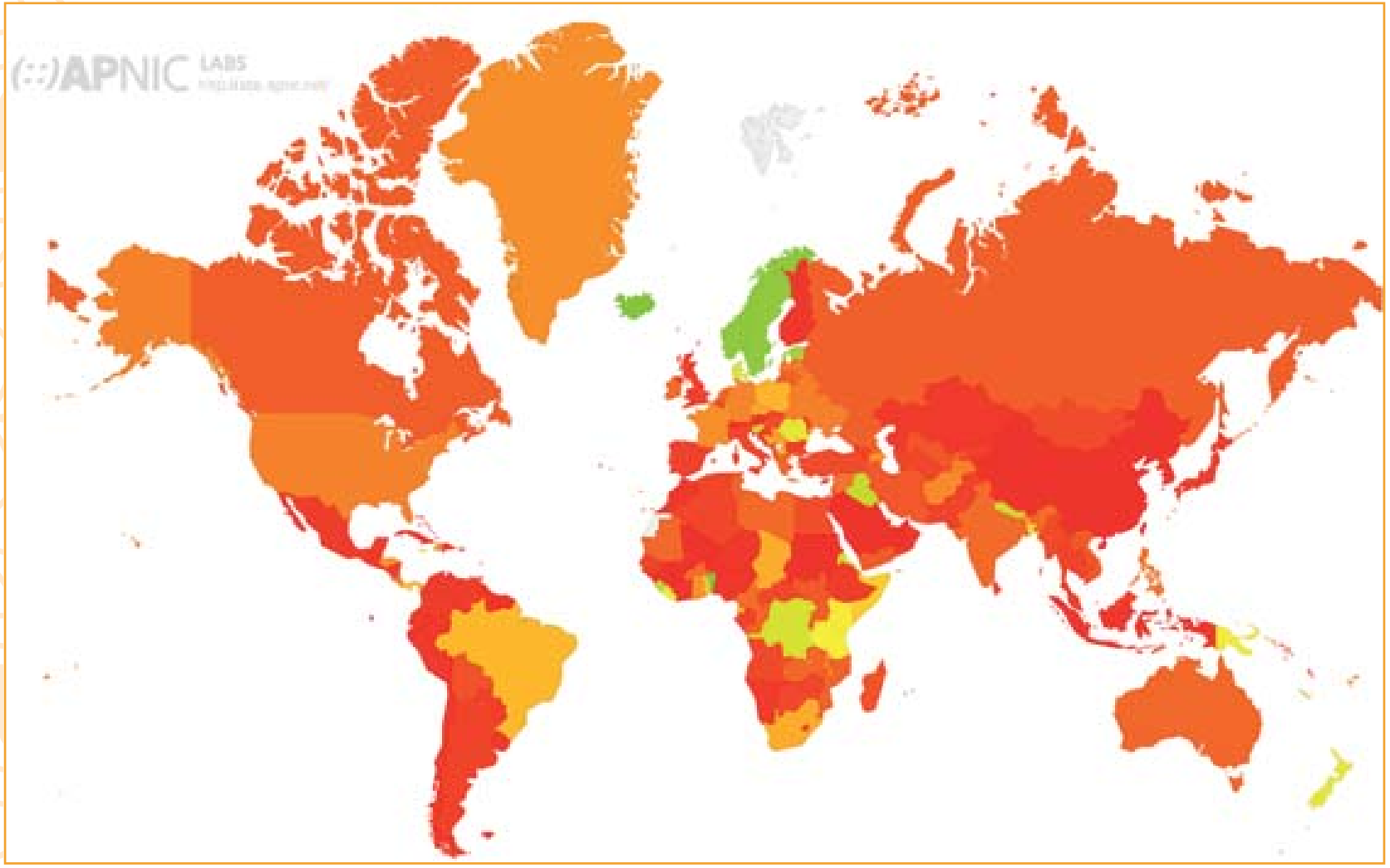
Para agilizar o registo de domínios neste TLD, a associação CORE desenvolveu um teclado virtual[3] com suporte para várias línguas árabes.

1 *http://www.corenic.org/*
2 *http://dotbazaar.net/*
3 *http://keyboard.nic.بازار/s#*

Território onde a expressão “bazaar” é reconhecida

Valibox: Bringing DNSSEC Validation to the Home

O funcionamento do DNSSEC assenta em dois componentes base, assinar a informação DNS com chaves criptográficas, e validar a informação DNS. No primeiro, o DNSSEC já percorreu um longo caminho que resultou na implementação na maioria dos domínios de topo, onde .PT foi pioneiro, mas ainda é necessária uma forte adesão dos domínios registados sob a grande maioria dos TLDs. Contudo, a componente de validar a informação DNS ainda é muito incipiente, segundo dados recolhidos pela APNIC apenas 14.34% do tráfego DNS global é validado com DNSSEC, sendo que o serviço DNS da Google por si só, é responsável pela validação de 13,74%. Ou seja, a validação DNSSEC neste momento é garantida quase em exclusivo pela Google, quando deveria ser garantida pelos provedores de serviços Internet (ISPs).



Taxa de validação DNSSEC por país

Tendo por base este cenário, *Cristian Hesselman* da SIDN, o Registry responsável pela gestão do ccTLD .NL da Holanda apresentou a solução *Valibox*[4] . Trata-se de um *software* de validação DNSSEC para dispositivos com sistemas embebidos do tipo *OpenWRT*, onde todos os componentes são optimizados para operar em dispositivos de dimensão reduzida, com capacidade de armazenamento e memória limita, por exemplo routers e telemóveis.

Esta solução permite a configuração dum vasto espectro de equipamentos, em dispositivos com capacidade para validar trafego DNS com DNSSEC, que uma vez instalados nas instalações dos utilizadores assumem o controlo da segurança da resolução DNS. Desta forma o utilizador elimina a dependência dos ISP's para a validação DNSSEC. Estes dispositivos podem no futuro desempenhar funções adicionais de segurança no serviço DNS.

Este tipo de soluções são a consequência direta da demora da implementação de DNSSEC pelos ISP's e atuam como provocações para o surgimento de soluções definitivas que ultrapassem as dificuldades atuais.

S/MIME Dane Demo

Atualmente, a comunicação encriptada por email entre dois utilizadores requer que ambos tenham os certificados um do outro, o que implica a comunicação prévia dos certificados com os consequentes riscos associado.

Contudo, é possível tornar este processo mais seguro e simples, utilizando o protocolo *DNS-based Authentication of Named Entities (DANE)* e DNSSEC. O protocolo DANE permite autenticar titulares de certificados com base na validação DNSSEC. A utilização de registos TLSA e SMIMEA conjuntamente com DNSSEC, permite obter os respetivos certificados a partir do serviço DNS duma forma segura e transparente, possibilitando o envio e a receção de emails encriptados sem a troca inicial de certificados.

Richard Lamb do ICANN fez uma demonstração do envio e receção de emails encriptados com DANE e DNSSEC no software Outlook. A escolha da aplicação Outlook é óbvia, uma vez que é a aplicação mais utilizada para envio e receção de emails. O objetivo destes trabalhos é a integração desta solução nas aplicações de email, nomeadamente o Outlook, para agilizar a comunicação encriptada por email, de uma forma segura e transparente para o utilizador.

Este é um assunto ao qual vamos certamente voltar, uma vez que está intimamente ligado à privacidade dos dados uma área que está atualmente a sofrer transformações.

[4] *https://valibox.sidnlabs.nl/*

Introduction to Mirai

Mirai é o nome dum pequeno software que se propaga e instala autonomamente em dispositivos ligados à Internet, conhecidos pela expressão "*Internet of Things (IoT)*", formando uma *botnet* com capacidade para efetuar ataques *Distributed Denial-of-Service (DDoS)* de grande dimensão. Ainda recentemente, esta botnet foi utilizada no maior ataque da história da Internet, contra uma empresa de serviços DNS norte americana causando indisponibilidade em várias dezenas de sites bem conhecidos nomeadamente Twitter, Paypal, Spotify, Netflix, Amazon, BBC, CNN entre outros.

Luis Espinoza da *Akamai* mostrou os resultados da análise que fez a esta botnet nos seus tempos livres. De destacar que esta botnet explora dispositivos IoT com credenciais de acesso francas ou inexistentes, e o seu código fonte foi publicado na Internet, tendo surgido desde então várias réplicas com ligeiras alterações o que dificulta em muito a implementação de medidas de controlo e mitigação da ameaça.

DNSSEC automation of [Fred]

Jaromir Talir do CZ.NIC, o *Registry* responsável pela gestão do ccTLD .CZ da República Checa, apresentou os desenvolvimentos mais recentes em autonomização DNSSEC do software *Free Registry for ENUM and Domains (FRED)*. Foi introduzido o objeto *KeySet* para armazenar informação de chaves DNSSEC. Estes trabalhos ainda estão em curso e tem como objetivo a implementação de mecanismos que facilitem a manutenção da cadeia de segurança no DNSSEC.

ICANN | 57 • DNSSEC

Workshop DNSSEC

A sessão pública do *workshop* DNSSEC organizada pelo *Security and Stability Advisory Committee (SSAC)* do ICANN e com o apoio do programa *Deploy360* da *Internet Society*, ocorreu no dia 07/11/2016 com a habitual presença de especialistas em DNS ativamente evolvidos na implementação e utilização de DNSSEC, e representantes de ccTLD's de vários países e entidades *Registrars* com forte expressão do país organizador e de países vizinhos.

Wes Hardaker iniciou esta sessão com os últimos dados relativos à utilização de DNSSEC nas componentes de assinatura de domínios e validação de consultas. Destaque para os ccTLD's de .SG de Singapura e .SN do Senegal, assinados com DNSSEC no passado mês de setembro e que assim se juntam ao atuais 1.349[5] (89%) domínios de topo (gTLD's e ccTLD's) assinados com DNSSEC. Em termos globais cerca de 15% das consultas DNS são validadas com DNSSEC[6] , grande parte devido ao serviço *Public DNS* da Google, no entanto em alguns países com o Nepal há sinais de suporte de DNSSEC pelos ISPs a operar localmente. Em relação ao mapa de implementação de DNSSEC dos ccTLDs[7] , as regiões de Africa, Asia-Pacífico e algumas áreas da América Latina continuam a ser a zonas geográficas com trabalho por desenvolver nesta área, como se pode verificar na figura abaixo.

Mapa de implementação DNSSEC a 07/11/2016

5 *https://rick.eng.br/dnssecstat/* 6 *http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=0&w=7&r=1* 7 *http://www.internetsociety.org/deploy360/dnssec/maps/*

Ainda, *Wes Hardaker* relatou o atual estado de implementação do protocolo *DANE* que ainda é muito incipiente mas no qual o DNS.PT é pioneiro. Atualmente há cerca de 102.000 domínios com registos TLSA (registos associados ao protocolo DANE) para o serviço de email (SMTP).

Por último, *Wes Hardaker* referiu a publicação "*DNS-Based E-Mail Security*"[8] do *National Institute of Standards and Technology (NIST)* e do *National Cybersecurity Center of Excellence (NCCoE)* ambos do departamento de comércio dos Estados Unidos da América, que promove a utilização de DANE e DNSSEC para incrementar os níveis de segurança da utilização do serviço de email.

[8] *https://nccoe.nist.gov/file/811/download?token=vmUaouWR*

Processo de rotação de chave KSK da root

O tema da rotação das chaves DNSSEC da raiz da Internet "*Root Zone KSK rollover*"[9] já foi referido em relatórios anteriores no âmbito das reuniões do ICANN 56 e ICANN 56, contudo importa continuar a referir este tema porque há novos desenvolvimentos e pelo relevo da matéria em si.

O documento "*Root Zone KSK Rollover Plan*"[10] foi publicado em julho de 2016, e incorpora as recomendações do grupo de trabalho "*Design Team*" composto por uma equipa de especialistas da comunidade técnica Internet que se debruçou sobre as implicações do processo de "*Root KSK rollover*" sobre a coordenação do ICANN. Na elaboração deste documento muito completo que descreve todo o processo de rotação da chave, esteve envolvido o ICANN no papel de operador das funções da IANA, a *Verisign* como gestor da zona raiz, e o *Department of Commerce's National Telecommunications and Information Administration (NTIA)*, cujas funções na gestão da Internet cessaram no passado dia 1 de outubro como resultado do processo de transição da IANA.

O plano para a rotação das chaves tem a seguinte calendarização, ainda sujeita a alterações.

27/10/2016: O processo de *rollover* começa de com a geração da nova chave KSK

11/06/2017: A nova chave KSK é publicada no DNS

[9] *https://www.icann.org/resources/pages/ksk-rollover/*
[10] *https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf*

19/09/2017: A resposta do registo DNSKEY nos servidores root servers aumenta de tamanho

11/10/2017: A nova chave KSK começa a assinar a zona raiz

11/01/2018: A antiga chave KSK é revogada

22/03/2018: O último dia em que a antiga chave KSK aparece na zona raiz

08/2018: A chave antiga é eliminada dos sistemas de gestão chaves DNSSEC do ICANN

O primeiro passo já foi dado, com a criação da nova chave KSK durante 27ª cerimónia trimestral de assinatura das chaves DNSSEC[11] que decorreu a 27 de outubro nas instalações do ICANN na cidade de Culpeper no estado da Virgínia perto de Washington D.C.

O próximo passo irá ocorrer em julho de 2017, com a publicação da nova chave KSK no sistema DNS.

O principal ponto operacional a reter deste processo, nomeadamente para os provedores de serviços Internet (ISP's) é a importância de manter a chave KSK da raiz da Internet permanentemente atualizada, caso contrário a validação DNSSEC irá falhar depois de substituída a chave KSK atual.

11 *https://www.iana.org/dnssec/ceremonies*

Painel de discussão/apresentação de atividades relacionadas com DNSSEC na região Ásia Pacífico

O painel de discussão/apresentação de atividades relacionadas com DNSSEC na região Ásia Pacífico contou com a presença do ccTLD do país anfitrião .IN, e ainda os ccTLD's .SG de Singapura e .VN do Vietnam.

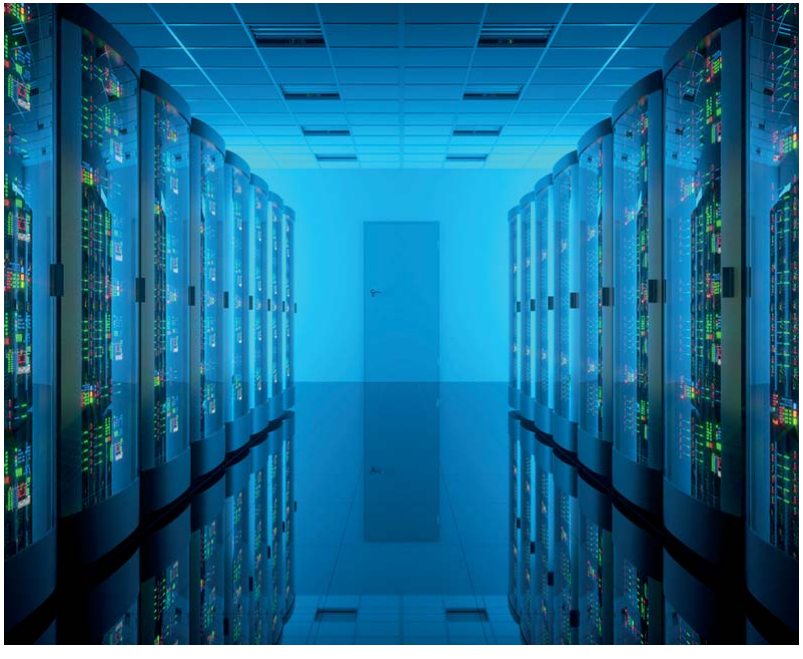
O ccTLD .IN é o que está mais desenvolvido nesta área, foi assinado com DNSSEC em 2010 e em 2011 disponibilizaram uma plataforma de testes. No entanto apresenta uma taxa de adesão muito reduzida, dos 2,19 milhões domínios registados apenas 0.05% (1.173) estão assinados com DNSSEC.

O ccTLD .SG iniciou o projeto de implementação de DNSSEC em 2009, através da formação de um grupo de trabalho para avaliar os requisitos e as implicações da adoção de DNSSEC. Posteriormente em 2015 decidiu avançar com os trabalhos, tendo concluído o projeto em setembro deste ano. A taxa de adesão é nula, o .SG tem 176,769 domínios registados nenhum deles assinados com DNSSEC. No primeiro trimestre de 2017, as entidades governamentais de Singapura tencionam assinar a hierarquia "gov.sg".

Por último o ccTLD .VN, começou por analisar o protocolo DNSSEC em 2012 e em 2014 aprovou a sua implementação no plano estratégico para o triénio de 2015 a 2017. Os trabalhos estão a decorrer conforme planeado, sendo que no final de 2016

está prevista a assinatura do .VN com DNSSEC, e no início de 2017 está previsto a disponibilização do serviço às entidades *Registrars*.

Yoshiro Yoneya do Registry *JPRS*, entidade responsável pela gestão do ccTLD .JP do Japão apresentou os conteúdos das sessões de sensibilização executadas por este Registry no âmbito do processo de rotação das chaves da raiz do DNS, mais conhecido por "Root KSK rollover". O objetivo destas sessões é preparar os Registrar's e ISP's que se encontram a operar no território para o processo de rotação de chaves que está a decorrer.



Aggressive Use of NSEC/NSEC3

Warren Kumari, engenheiro sénior da Google, apresentou a solução "*Aggressive use of NSEC/NSEC3*", atualmente em fase final de discussão no *Internet Engineering Task Force (IETF)*. Trata-se duma resposta à crescente vaga de ataques conhecidos por "*Random Qname Attacks*". Estes ataques são executados com recurso a BotNets que enviam um volume massivo de consultas de subdomínios gerados aleatoriamente que não existem para o serviço DNS, criando indisponibilidade do serviço através da sobrecarga do serviço DNS.

A solução "*Aggressive use of NSEC/NSEC3*" consiste na utilização dos registos NSEC/NSEC3 para criar respostas DNS negativas para um intervalo entre domínios, libertando o DNS do processamento de consultas para domínios inexistentes que se encontram dentro desse intervalo. Esta solução permite aumentar o desempenho do serviço DNS, através da redução de recursos envolvidos na resolução de nomes. Simultaneamente aumenta a resiliência do serviço DNS a ataques de negação de serviço (DoS).

Mais uma vez, e à semelhança do protocolo DANE, estamos perante o desenvolvimento de soluções que utilizam DNSSEC como base para novas soluções de segurança.

Root Key Rollover Discussion - Recursive Resolver Software Readiness

Moderator: Jacques Latour, CIRA

A sessão moderada por *Jacques Latour* responsável técnico do ccTLD .CA do Canada, expôs o nível de preparação de três soluções de *software* para servidores *resolvers*, para o processo de rotação das chaves da raiz do DNS "*Root KSK rollover*". Os servidores *resolvers* situam-se no fim da cadeia de resolução DNS, são responsáveis pelo processo de validação DNSSEC e por responder ao cliente que fez a consulta DNS inicial.

Este processo reveste-se de importância uma vez que o processo de rotação de chaves da raiz da Internet já está a decorrer. As soluções de software apresentadas foram *Unbound, BIND* e *Knot*.

A solução *Unbound* da *NLNet Labs* suporta DNSSEC desde que foi criada em 2007, posteriormente em 2009 foram adicionados mecanismos de atualização automática da chave pública KSK da root. Trata-se de uma ferramenta que suporta a rotação das chaves, ainda assim os seus criadores estão a melhorar a solução para reforçar alguns aspetos de segurança. De destacar o envolvimento da *NLNet Labs* na preparação do processo de rotação de chaves da raiz da Internet, através da participação de colaboradores seniores da organização no grupo de trabalho "*Design Team*" que elaborou um conjunto de recomendações.

Mukund Sivaraman do Internet Systems Consortium (ISC) falou da solução BIND, trata-se da ferramenta de servidores DNS mais utilizada em todo o mundo. Esta ferramenta pode ser configurada de forma manual através da diretiva de configuração "*trusted-keys*" e automática através da funcionalidade "*managed-keys*". *Mukund Sivaraman* explicou o processo com ambos métodos e deixou um conjunto de recomendações para o correto uso da ferramenta durante o processo de rotação das chaves da raiz da Internet.

Jaromír Talíř do ccTLD .CZ da República Checa, falou da ferramenta *KNOT* uma solução *Open-source* para servidores *resolvers* desenvolvida em 2006. Foram apresentadas algumas das principais características e funcionalidades, nomeadamente o suporte para a rotação automática das chaves DNSSEC da raiz da Internet.

DS Automated Provisioning (DSAP)

Jacques Latour, CIRA

Um dos desafios com DNSSEC é a comunicação do material criptográfico, o registo *Delegation Signer (DS)*, a chave DNSKEY ou ambos, para o domínio da hierarquia DNS superior. Esta informação é a base das cadeias de segurança conhecidas por "*trust-anchors*". Esta comunicação deveria ocorrer sem dificuldades, mas como o DNS é gerido por um conjunto heterogéneo de entidades e organizações, por vezes esta comunicação traduz-se num processo difícil e complexo. Para ajudar a resolver este problema foram desenvolvidos os registos CDS

(*Child DS*) e CDNSKEY (*Child DNSKEY*) conforme especificação no *RFC 7344*.

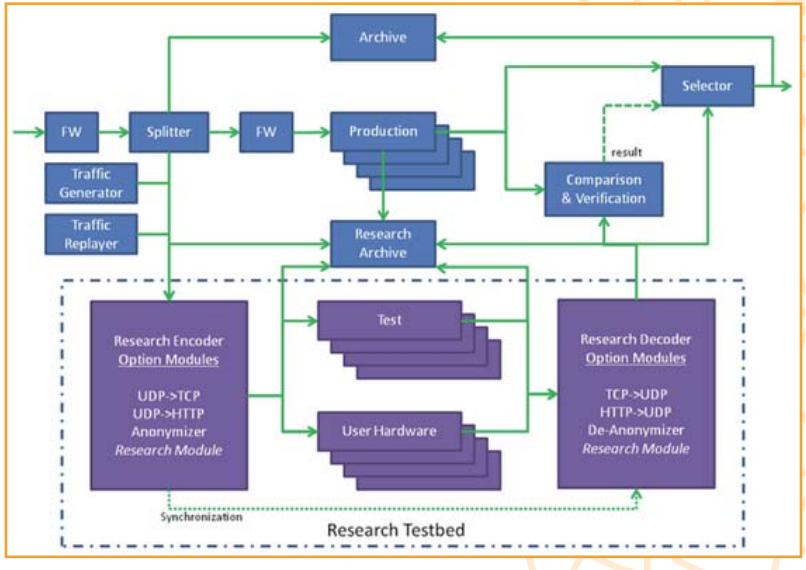
Jacques Latour apresentou a plataforma *DS Automated Provisioning (DSAP)*, que faz uso desses registos para automatizar a comunicação dos registos DNSSEC.

CIRA, o Registry do ccTLD .CA, já desenvolveu um protótipo e está atualmente a promover a implementação desta solução.

Critical Infrastructure DNS Research Testbed
Wes Hardaker, USC/ISI

O serviço DNS teve origem no meio académico, mas a evolução do acesso à Internet nos últimos 30 anos colocou o serviço DNS maioritariamente no mundo comercial, o que dificulta em muito a evolução tecnológica do serviço. Assente nesta realidade, *Wes Hardaker do Information Sciences Institute (ISI) da University of Southern California (USC)* apresentou a ideia de construir uma plataforma de pesquisa e investigação com dados reais da utilização do serviço DNS, que permita testar de uma forma segura vários cenários de utilização do serviço DNS. De uma forma geral esta plataforma irá recuperar e aumentar o envolvimento do mundo académico, o que irá acelerar a evolução tecnológica do serviço, e permitir uma melhor colaboração entre a academia, a indústria, os governos e organizações não-governamentais.

Este projeto chama-se *Naming and Internet Protocol Experimentation Testbed (NIPET)*[12], e está numa fase inicial de levantamento de requisitos, angariação de fundos e recolha de apoio da comunidade para colaborar.



Proposta de arquitetura da plataforma NIPET

12 *http://ant.isi.edu/researchroot*

DNSSEC in Windows for DNS Server

Kumar Ashutosh, Microsoft

Kumar Ashutosh da Microsoft, fez uma demonstração num sistema real (*live demo*) do suporte de DNSSEC no sistema operativo *Windows Server 2012 R2*. Esta apresentação é muito importante, pois apesar da comunidade de especialistas em DNS preferir a utilização de sistemas Linux, as várias versões do sistema operativo Windows são de longe as mais populares em qualquer segmento de utilização, nomeadamente servidores empresariais e computadores pessoais.

A Microsoft disponibiliza informação para implementação DNSSEC no Windows Server 2012 nos conteúdos "Deploy DNSSEC with Windows Server 2012"[13]

[13] *https://technet.microsoft.com/en-us/library/dn593684(v=ws.11).aspx*

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

Produção: julho 2016
Grafismo: dns.pt