

# A GOVERNAÇÃO DA INTERNET E O POSICIONAMENTO DE PORTUGAL

*Manuel da Costa Cabral*<sup>1</sup>

*ABSTRACT: Given the political, social and economic importance of the Internet, its Governance remains an open issue that is being vividly discussed in several international fora. Who controls the Internet? Who owns the information? Who may access to it? What is the role of Governments? Which is the best approach to implement the multistakeholder model? These are fundamental questions which remain unanswered. In this critical moment for the Internet Governance, the Author identifies the main controversial topics, describes how some of these topics are being addressed in Portugal and provides examples of alternative arrangements in other EU countries. Finally, the Author suggests a framework to address the Internet Governance in Portugal in a more effective and coherent manner and reflects about the role that Portugal can play in the international arena.*

SUMÁRIO: I. Introdução; II. O quadro global da Governação da Internet: identificação das grandes questões; 1. Considerações prévias; 2. Custos de acesso; 3. Qualidade de serviço e neutralidade de rede; 4. Domain Name System – DNS – Sistema de nomes de domínios; 5. Numeração e endereços IP; 6. Segurança e Privacidade; III. O debate institucional em torno da Governação da Internet; 1. Entidades de Direito privado; 2. Organizações internacionais; IV. Portugal e a Governação da Internet; 1. Situação Atual; 2. O confronto com outros países europeus; 3. Perspetivas de evolução em Portugal e algumas propostas; V. Notas conclusivas.

## I. INTRODUÇÃO

Quem controla a Internet? Quem é “dono” da informação? Quem a pode aceder? Qual o papel dos Governos? Qual a melhor solução para implementar

---

<sup>1</sup> Direção das Relações Exteriores da ANACOM. O presente artigo reflete opiniões pessoais, comprometendo em exclusivo o seu autor. Twitter: M\_CostaCabral

o modelo *multistakeholder*? Estas são questões fundamentais para as quais não existem respostas óbvias.

No *Global Agenda Outlook 2013*<sup>2</sup>, publicado no início de 2013 pela *World Economic Forum*, a Governação da Internet<sup>3</sup> é apontado como um dos quinze assuntos cuja resolução é mais urgente a nível global, num *ranking* liderado pela “instabilidade da economia mundial” e pela “fragilidade da zona euro”.

A Agenda de Tunis para a Sociedade de Informação<sup>4-5</sup> define Governação da Internet como “o desenvolvimento e aplicação de princípios, normas, regras e procedimentos de tomada de decisão, que moldam a evolução e o uso da Internet, por parte dos Governos, setor privado e sociedade civil, no âmbito das suas competências”. Lê-se ainda na Agenda de Tunis que “a Governação da Internet deve ser multilateral, transparente e democrática, compreendendo o total envolvimento de Governos, setor privado, sociedade civil e organizações internacionais. Deve assegurar uma distribuição de recursos equitativa, facilitar o acesso para todos e assegurar um funcionamento estável e seguro da Internet, tendo em consideração o multilinguismo”.

Está, pois, consagrado que a Governação da Internet assenta no modelo de *multistakeholder*, no qual entidades públicas e privadas cooperam para atingir os objetivos identificados.

Em termos práticos, poderemos ver a Governação da Internet de duas formas distintas: num contexto mais restrito, que aponta a Governação da Internet como a gestão de um conjunto de componentes técnicos que permitem a Internet funcionar; num contexto mais lato, onde, para além dos aspetos técnicos, se inclui um conjunto de fatores que moldam as políticas em torno da Internet, como os custos de acesso, a privacidade, liberdade de expressão ou segurança. É este segundo contexto que mais nos interessa, porque é nele que se desenvolve o debate em torno da Internet nos variados fóruns internacionais que abordam o tema.

---

2 World Economic Forum, *Global Agenda Outlook 2013*, 2013, disponível em: [http://www3.weforum.org/docs/WEF\\_GAC\\_GlobalAgendaOutlook\\_2013.pdf](http://www3.weforum.org/docs/WEF_GAC_GlobalAgendaOutlook_2013.pdf) [consultado em outubro de 2013].

3 Não existindo tradução óbvia da expressão anglo-saxónica “Internet Governance”, o autor opta por usar uma expressão frequente nos textos em Português: “Governação da Internet”.

4 Declaração consensual emanada da *World Summit on Information Society (WSIS)*, e adotada em novembro de 2005, em Tunis, Tunísia. Mais detalhes no capítulo III do presente artigo.

5 *Tunis Agenda for the Information Society*, 2005, disponível em <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html> [consultado em outubro de 2013].

Com base na análise feita sugerimos, por fim, um posicionamento para a atuação de Portugal nesta matéria.

## II. O QUADRO GLOBAL DA GOVERNAÇÃO DA INTERNET: IDENTIFICAÇÃO DAS GRANDES QUESTÕES

### 1. Considerações prévias

A urgência do debate da Governação da Internet não é alheia ao papel vital que a mesma assume nas sociedades atuais, nem à enorme controvérsia que o assunto tem vindo a suscitar, nomeadamente em fóruns internacionais como a União Internacional de Telecomunicações (UIT), agência das Nações Unidas para as Telecomunicações. Diversos países, nomeadamente Rússia, China, e alguns Estados Árabes, têm demonstrado desconfiança em relação ao *Internet Corporation for Assigned Names and Numbers* (ICANN), instituição que desempenha funções na gestão de recursos de numeração, nomes e endereçamento IPs. Para um conjunto de países, num cenário ideal, as funções do ICANN deveriam ser assumidas por um organismo de direito internacional, como a própria UIT. Não sendo tal cenário facilmente realizável, atendendo à oposição dos EUA, e seus aliados, tem vindo a ser exigido o reforço do poder dos Governos nestas matérias e em concreto no processo de tomada de decisão do ICANN. Por outro lado, Estados Unidos, diversos países da Europa e outros aliados, como Canadá, Austrália ou Japão consideram que algumas das exigências de reforma das instituições que controlam a Internet têm objetivos não confessáveis que passam pelo reforço das medidas de controlo e/ou barramento das comunicações, ou por outras palavras, pelo reforço da possibilidade de vigilância e censura. Consideram, assim, que as propostas de alguns Estados-Membros põem em causa a Internet livre e aberta que conhecemos. Os EUA garantem ainda que não dispõem de instrumentos para influenciar as decisões vitais do ICANN.

É neste cenário, de profunda divisão, que há quem sugira que nos encontramos perante uma Guerra Fria digital<sup>6</sup>.

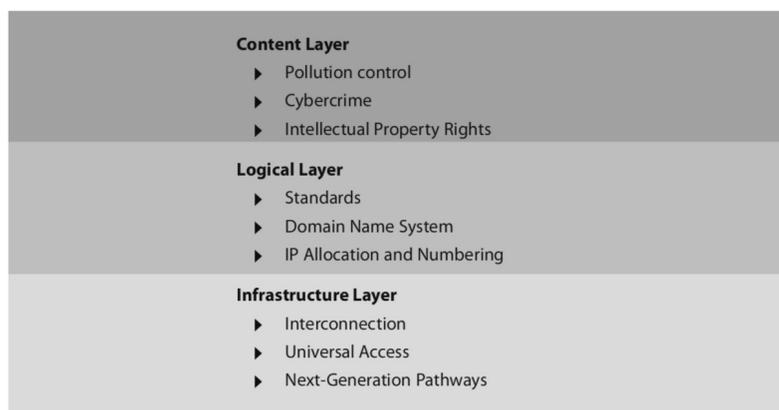
Mas a Governação da Internet está longe de se circunscrever a disputas entre países. O tema suscita debate entre Governos e Sociedade Civil; operadores

---

6 "Internet Regulation – A Digital Cold War?", *The Economist*, 14 dezembro de 2012, disponível em <http://www.economist.com/blogs/babbage/2012/12/internet-regulation> [consultado em dezembro de 2012].

tradicionais e prestadores *over-the-top* (OTT)<sup>7</sup>; ou entre a liberdade individual e a segurança nacional.

Procuraremos aprofundar o que está em causa nesse debate, sendo certo que dada a definição abrangente consagrada na Agenda de Tunis, a Governação da Internet respeita a um leque muito variado de assuntos. Akash Kapur<sup>8</sup> dividiu o tema da Governação da Internet em três níveis: Infraestrutura, lógico e conteúdo.



Consideramos que a sistematização em três níveis oferecida por Kapur continua útil, se bem que naturalmente, com o transcurso do tempo, a caracterização dos tópicos relevantes em cada um dos níveis se tenha vindo a alterar.

No presente artigo, exploraremos alguns dos tópicos mais controversos na atualidade a nível internacional, a saber:

- Custos de acesso (nível de infraestrutura);
- Qualidade de serviço e neutralidade de rede (nível de infraestrutura);
- *Domain Name System – DNS – Sistema de nomes de domínios (nível lógico)*;
- Numeração e endereçamento (nível lógico);
- Segurança (transversal a todos os níveis);

7 Prestadores de serviço/aplicações acessíveis através da Internet (eg. Google, Facebook e Skype).

8 kapur, 2005.

## 2. Custos de acesso

A *International Internet Connectivity* pode ser definida como o acesso internacional ao conjunto de meios através do qual um país pode aceder ao *backbone* da Internet Global. Este conjunto de meios inclui satélites e cabos de fibra ótica (terrestres ou submarinos).

O custo de acesso à Internet tem sido um tópico crucial para os países em desenvolvimento, em particular, em África e América do Sul, regiões onde os custos de acesso são elevados em comparação com outras regiões, o que condiciona o acesso à Internet pelas populações. Na verdade, o modelo em que assenta a Internet, a que alguns designam como “*receiver pays*” (no qual os *Internet Service Providers* – ISPs – que recebem a informação pagam o circuito internacional por completo), contribui para estes custos acrescidos. Uma vez que os conteúdos estão alojados fundamentalmente em países desenvolvidos, os países em desenvolvimento alegam estarem mais dependentes da largura de banda internacional<sup>9</sup>. Por isso mesmo, têm defendido, nos diversos fóruns internacionais, a revisão da fórmula para a repartição dos custos.

De notar contudo que a propagação de *Internet exchange points (IXPs)*, infraestruturas que permitem que diversos *players* se interliguem diretamente entre si, tem contribuído para melhorar a qualidade de serviço e reduzir custos de transmissão. Os IXPs contribuíram para um desenvolvimento da Internet na América do Norte, Europa e Ásia e têm gradualmente vindo a ser implementados nas regiões mais desfavorecidas de África ou América Latina<sup>10</sup>, muitas vezes com o apoio técnico e financeiro proporcionado por programas de desenvolvimento. A propagação de IXPs tem contribuído para diminuir os custos de acesso nos países em desenvolvimento, embora haja ainda um largo percurso a percorrer até porque se trata de uma infraestruturas que exige elevados investimentos e conhecimentos técnicos, que não estão ao alcance de grande parte desses países.

Esta questão parece ser, de resto, crucial para o desenvolvimento futuro da Internet, atendendo a que o crescimento mais acelerado de produção de conteúdos e de volume tráfego se verificará precisamente nos países em desenvolvimento.

---

9 “When an end user in Kenya sends E-Mail to a correspondent in the USA it is the Kenyan ISP who is bearing the cost of the International connectivity from Kenya to the USA. Conversely when an American end user sends E-Mail to Kenya, it is still the Kenyan ISP who is bearing the cost of the International connectivity, and ultimately the Kenyan end user who bears the brunt by paying higher subscriptions”: Bell, , 2002.

10 Mapa com a localização de IXPs no globo <http://www.datacentermap.com/ixps.html> [consultado em outubro de 2013].

### 3. Qualidade de serviço e neutralidade de rede

A qualidade de serviço e a neutralidade de rede expõem uma tensão crescente entre os operadores de telecomunicações tradicionais e os prestadores *over-the-top* (OTT).

Os operadores tradicionais de telecomunicações, e em particular a *European Telecommunications Network Operators' Association* (ETNO)<sup>11</sup>, têm defendido que o atual modelo de Internet resulta num desequilíbrio entre o esforço de investimento e a receita gerada. Assim, alegam que enquanto os operadores de telecomunicações investem na proliferação e melhoria das redes, têm sido os prestadores OTT a beneficiar desse investimento, dado que obtêm elevadas receitas pela prestação de serviços/aplicações que “correm” sobre as redes construídas por terceiros.

No processo de preparação para a *World Conference on International Communication* (WCIT-12), organizada pela UIT e realizada em dezembro de 2012, com o intuito de rever o Regulamento das Telecomunicações Internacionais<sup>12</sup>, os operadores tradicionais apresentaram propostas para diminuir o alegado desequilíbrio entre investimento e receitas. As propostas dos operadores apontavam para a criação de um novo ecossistema para a interligação IP, o que facilitaria a que paralelamente a uma qualidade de serviço baseada no princípio *best-effort*<sup>13</sup>, subsistisse uma qualidade de serviço *end-to-end*<sup>14</sup>. Com base no princípio *end-to-end* seria exequível estabelecer uma política de interligação que diferenciase a qualidade de serviço de acordo com o tipo de serviço e tráfego. No fundo, os operadores defendem que se um OTT pretende assegurar a “entrega” de um serviço/aplicação com um determinado nível de qualidade de serviço assegurado, terá de pagar um *fee* para o efeito. Deste modo, os operadores poderiam aumentar receitas e fazer face às exigências de investimento, nomeadamente em redes de nova geração. De notar, contudo, que estas propostas não mereceram o apoio da WCIT-12.

Ainda assim, as exigências dos operadores tradicionais têm-se feito ouvir não apenas no âmbito da UIT, mas também a nível europeu. Neste contexto, parece

11 A ETNO é a associação que reúne os operadores incumbentes europeus ([www.etno.be](http://www.etno.be)).

12 Site da WCIT-12 disponível em <http://www.itu.int/WCIT>. Mais detalhes no capítulo III do presente artigo.

13 A Internet tem vindo sobretudo a funcionar segundo o princípio do *best-effort*, segundo o qual as informações transmitidas serão entregues no destino caso existam recursos para tal, não existindo absoluta garantia de entrega.

14 Princípio que permite que um determinado nível de qualidade de serviço seja assegurado de ponto-a-ponto.

ser de particular relevância a proposta de regulação “*Connected Continent*” recentemente tornada pública pela Comissão Europeia<sup>15</sup>. No seu art.º 23 (“*Freedom to provide and avail of open internet access, and reasonable traffic management*”), a Comissão pretende consagrar a proibição de os operadores bloquearem, tornarem mais lento ou degradarem determinado tipo de conteúdo, aplicações ou serviços (art.º 23.º § 5). Por outro lado, a Comissão estabelece a possibilidade de os prestadores de conteúdo, aplicações e serviços acordarem com os operadores de telecomunicações a transmissão de determinado tipo de tráfego com uma qualidade de serviço pré-definida, ou com capacidade dedicada (art.º 23.º § 2). Salvo melhor opinião, a Comissão parecia abrir assim a porta às pretensões dos operadores, reforçando a legitimidade do princípio da qualidade de serviço garantida *end-to-end* na prestação de serviços de Internet.

Neste sentido, a proposta da Comissão para a revisão do enquadramento regulatório tem o mérito de inovar pois alarga o seu âmbito aos prestadores OTT.

No entanto, as discussões no Conselho Europeu (no qual têm assento países que adotaram legislação proibitiva de práticas que possam pôr em causa o princípio da neutralidade de rede, como a Holanda, Luxemburgo ou Eslovénia<sup>16</sup>), e especialmente no Parlamento Europeu<sup>17</sup> fazem prever que se deverão manter restrições à aplicação de um modelo baseado numa qualidade de serviço *end-to-end*.

Aguarda-se, assim, com expectativa o resultado de todas estas negociações.

#### **4. Domain Name System – DNS – Sistema de nomes de domínios**

No topo de uma pirâmide que gere os recursos críticos de Internet encontra-se o ICANN (*Internet Corporation for Assigned Names and Numbers*). O ICANN é uma organização norte-americana de direito privado, que se orgulha de atuar de acordo com o modelo *multistakeholder*, segundo o qual Governos,

15 “Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012”, 11 de setembro de 2013 <https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single>.

16 Olmos & Castro, 2013.

17 Ver Relatório aprovado pelo Comité de Indústria, Investigação e Energia (ITRE) do Parlamento Europeu sobre “Proposal for a regulation of the European Parliament and of the Council laying down measures concerning European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012”, 1 de abril 2014 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARG+PE-522.762+01+DOC+PDF+V0//EN&language=EN>.

setor privado, academia e sociedade civil têm a possibilidade de fazer ouvir os seus pontos de vista e contribuir para a tomada de decisão.

Na sequência de um memorando assinado entre o Departamento de Comércio (DoC) dos EUA e o ICANN em Novembro de 1998, a gestão do *Domain Name System – DNS* (Sistema de nomes de domínios) passou para o controlo do ICANN<sup>18</sup>. Este Memorando teve precisamente por objetivo libertar estas funções do controlo governamental dos EUA. Salienta-se contudo que o DoC dos EUA mantém a autoridade de alterar o detentor do poder de gestão do DNS, significando que em casos extremos o DoC poderia não renovar o contrato com o ICANN, o que na prática determinaria o fim desta organização. Por outro lado, o DoC tem o poder de aprovar modificações ao chamado *root zone file* (*Root Zone* refere-se ao nível mais elevado da estrutura do DNS, que contém a informação necessária ao funcionamento de todos os domínios de topo), pelo que a adição de novos domínios de topo passa também pela aprovação do DoC.

A influência dos EUA na Internet tem naturalmente uma razão histórica relevante: A Internet foi inventada pelos norte-americanos. É, assim, natural que as instituições que gerem alguns dos seus recursos críticos sejam o legado desse facto histórico.

De qualquer forma, a autoridade que os EUA detêm sobre o ICANN acaba por descredibilizar a ideia defendida pelos norte-americanos segundo a qual o seu poder de influência sobre o ICANN não se sobrepõe ao de outros Estados, sendo, por isso, crescente a pressão para que esse poder seja efetivamente reduzido

Foi neste contexto, sintomática, a Declaração de Montevideu, assinada por diversas entidades relevantes na comunidade da Internet, incluindo o próprio ICANN, em outubro de 2013, apelando, nomeadamente, a uma globalização do ICANN, subentendendo-se um apelo a um menor controlo dos EUA sobre o ICANN<sup>19</sup>.

---

18 No que respeita ao DNS, o ICANN é responsável pela gestão do conjunto dos domínios alfanuméricos (o chamado *Domain Name System - DNS*), funções que passam nomeadamente pela designação dos operadores dos domínios de topo (*top-level domains*, TLD). De relevar que os domínios de topo estão agrupados em duas grandes famílias Generic (gTLD. Exemplo: .com ou .net) e country code (ccTLD. Exemplo: .pt). O ICANN é responsável por contratualizar com *Registries* a coordenação de cada gTLD. No caso dos ccTLD, o ICANN atribui a competência de gestão, registo e manutenção dos domínios a uma entidade em cada país, através de uma delegação técnica.

19 Declaração de Montevideu, disponível em <https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm> [consultado em janeiro 2014].

Adicionalmente, conforme indicado anteriormente um conjunto alargado de países, incluindo alguns BRICS<sup>20</sup>, acredita que num cenário ideal, as funções do ICANN deveriam ser assumidas por um organismo de direito internacional, como a própria UIT. No lado oposto, EUA e diversos aliados opõem-se vivamente a todas as iniciativas que procurem dotar a UIT de poderes na gestão do DNS, considerando que o caráter dinâmico e inovador da Internet ficaria fortemente ameaçado se as decisões sobre a gestão dos seus recursos críticos passassem a ser tomadas por uma agência das Nações Unidas, cujos processos de tomadas de decisões alguns consideram lentos e pouco ágeis.

Atendendo à difícil concretização de reformas mais profundas, diversos países exigem, pelo menos, o reforço do poder dos Governos nestas matérias e em concreto no processo de tomada de decisão do ICANN. Neste contexto, têm sido particularmente audíveis as exigências de reforma do *Governmental Advisory Committee* (GAC)<sup>21</sup> do ICANN, organismo no qual se fazem representar os Governos, e cujas opiniões sobre políticas públicas deverão ser tomadas em consideração pelo *Board* do ICANN. Deste modo, tem vindo a ser pugnado um reforço dos poderes do GAC de modo a que os seus pareceres adquiram uma natureza tendencialmente vinculativa, pretendendo-se que o *Board* do ICANN<sup>22</sup> tenha uma menor margem de manobra para atuar ao arrepio dos pareceres do GAC. Na realidade, este grupo de países, do qual o Brasil se tem assumido como um dos líderes, considera que o GAC é um órgão fraco, que não garante as condições necessárias à efetiva participação dos governos nos processos de tomada de decisão.

Todo este contexto de pressão internacional terá seguramente contribuído para que os EUA, em março de 2014, tenham emitido uma declaração na qual convidam o ICANN a reunir os diversos *stakeholders* com o intuito de formular uma proposta de transferência das atuais funções dos EUA na coordenação do *Domain Name System* – DNS<sup>23</sup>.

É importante realçar, contudo, que muitos pontos de interrogação se levantam com esta declaração, desconhecendo-se, nomeadamente, quem assumirá

---

20 Brasil, Rússia, Índia, China e África do Sul.

21 <https://gacweb.icann.org/>.

22 <http://www.icann.org/en/groups/board>.

23 “NTIA Announces Intent to Transition Key Internet Domain Name Functions”, 2014, disponível em <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions> [consultado em março de 2014].

as funções de coordenação do DNS e quais são exatamente as funções a que os EUA se referem.

De qualquer modo, este parece ser um marco relevante, que abre a porta a que importantes desenvolvimentos venham a ocorrer na forma como o ICANN e em concreto a coordenação do DNS são organizados.

*a) Caso prático: A tensão em torno dos novos gTLDs*

A aprovação dos novos domínios genéricos de topo (ex: .hotel; .site; .nyc)<sup>24</sup> surge como uma das faces visíveis dos antagonismos patentes no processo de tomada de decisão do ICANN. O processo de criação destes novos domínios foi controverso desde a sua origem (2005), suscitando muitas reservas, nomeadamente por parte do GAC, quanto a questões de segurança, proteção de consumidores e defesa da propriedade industrial<sup>25</sup>. Paradigmático foi o caso dos novos domínios de topo “.Amazon” ou “.wine”/“.vin”. Em função das pressões do Brasil e de outros países daquela região, o GAC opôs-se à criação do “.Amazon”, que havia sido solicitada pela *Amazon*, empresa de vendas online. Na base da oposição do Brasil, esteve o facto de a Amazônia ser uma região do Brasil e de outros países sul-americanos, pelo que o uso desse domínio de topo deveria ser vedado a uma empresa privada. De notar que neste processo apenas os EUA apoiaram a pretensão da criação do “.Amazon” pela empresa Amazon. A decisão final sobre o domínio de topo “.Amazon” ainda está pendente, apesar do parecer do GAC, uma vez que o *Board* do ICANN ainda não tomou a decisão final.

Com base em argumentos similares, a Comissão Europeia contestou a possibilidade de virem a ser criados os domínios de topo “.wine” e “.vin”. Em carta remetida a Fadi Chehadé, Presidente e CEO do ICANN, em setembro de 2013, Nellie Kroes, Vice-presidente da Comissão, declarava “*under no circumstance can we agree having .wine and .vin and on the internet, without sufficient safeguards which efficiently protect the rights and interest of both Geographic Indicator right holders and consumers and wine and wine products*”<sup>26</sup>.

O ICANN ainda não tomou uma decisão sobre os domínios “.wine” e “.vin” devendo fazê-lo proximamente.

24 ICANN sobre os novos domínios de topo <http://newgtlds.icann.org/en/>.

25 Kruger, 2013.

26 Kroes, 2013.

Poderá dizer-se, para sintetizar, que os diferendos em torno da questão da gestão dos domínios têm uma dimensão política na qual alguns os governos procuram ter um maior poder no processo de tomada de decisão. Não se pode, porém, negligenciar uma dimensão económica: só por si a empresa Amazon terá investido cerca de 14 milhões de dólares em processos de candidatura de novos domínios de topo<sup>27</sup>.

## 5. Numeração e endereços IP

Cada equipamento conectado à Internet é identificado por um endereço IP. Estes endereços, que são usados para encaminhar os pacotes de dados, são um recurso finito. O ICANN, através da IANA (*Internet Assigned Names Authority*)<sup>28</sup>, tem também a função de gerir a alocação de endereços IP. Assim, o ICANN distribui as moradas IP a cinco *Regional Internet Registries* (RIRs) que por sua vez atribui os endereços aos ISPs ou diretamente a empresas que necessitem dos endereços IP para o desenvolvimento das suas redes internas. Na Europa, a função de RIR está atribuída à *Réseaux IP Européens Network Coordination Centre* (RIPE NCC)<sup>29</sup>.

Atualmente a maior parte dos equipamentos utiliza o chamado IPv4 (exemplo de endereço IPv4: 192.0.2.235), que permite em teoria gerar um conjunto de 4 mil milhões de endereços<sup>30</sup>. No entanto, devido ao crescimento galopante do número de equipamentos ligados à Internet, os endereços IPv4 acabaram por escassear, pelo que foi desenvolvido uma nova versão de endereços IP, o IPv6 (exemplo de endereço IPv6: 2001:0db8:85a3:0000:0000:08a2e:0370:7334) que permitirá gerar, em teoria, um número praticamente inesgotável de endereços IP.

A exaustão de recursos IPv4 disponíveis e a migração para o IPv6 tem servido de pretexto para exigências de reforma na Governação dos endereços IP. Estas reformas podem ser sistematizadas em dois níveis: operacional e institucional.

---

27 "Amazon Just Spent Millions Applying For Domain Names. Why?", 2012, Revista Forbes, disponível em <http://www.forbes.com/sites/chrisbarth/2012/06/13/amazon-just-spent-millions-applying-for-domain-names-why/> [consultado em outubro de 2013].

28 <http://www.iana.org/>.

29 <http://www.ripe.net/>.

30 Este número contudo não é estático, porque na prática a maior parte dos equipamentos estão ligados à Internet através de redes privadas que atribuem endereços IP de forma dinâmica.

No plano operacional, nos fóruns internacionais tem-se vindo a discutir a forma de alocação dos endereços IPv6. Alguns países sustentam que a política de alocação deve ser similar à realizada no IPv4, isto é, com base no “*first come, first serve*”, tendo como pressuposto uma necessidade demonstrável. Contudo, outro conjunto de países advoga que o princípio utilizado no IPv4 levou uma rápida ocupação de recursos finitos, pelo que se for novamente utilizado na distribuição de endereços IPv6, os países que procurem mais tardiamente tais recursos endereços IPv6, tipicamente os países em desenvolvimento, sairão prejudicados. Para estes países a alocação de endereços IPv4 não decorreu de forma eficiente, argumentando que existe uma proporção muito significativa de endereços que nunca foram usados, apesar de já terem sido atribuídos a diversas organizações<sup>31</sup>.

No plano institucional, enquanto alguns países advogam uma transformação profunda do modelo institucional, sugerindo, por exemplo, que a própria UIT atue como um RIR, ficando responsável pela atribuição de endereços, outros países referem que uma melhoria dos processos das atuais instituições será suficiente para garantir uma eficiente migração para o IPv6. Para este último grupo, a intervenção da UIT neste processo teria consequências negativas, uma vez que o iria tornar necessariamente mais pesado e burocrático.

## 6. Segurança e Privacidade

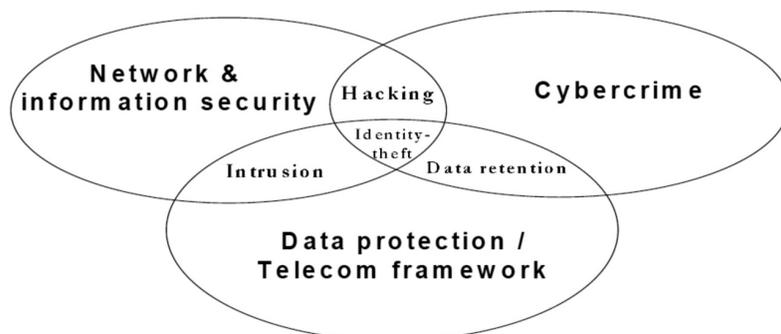
As questões de segurança e privacidade são para muitos o problema central da Governação da Internet. Assuntos como a recolha e retenção da vida de cada um de nós, o poder das corporações que armazenam tais dados, o papel e a eficácia do legislador para combater práticas abusivas, o combate ao cibercrime, e as ações de espionagem são incontornáveis na discussão da Governação da Internet.

De acordo com a Comissão Europeia, as questões de segurança podem ser sumarizadas no diagrama da página seguinte.

Considera-se que os três vetores são aplicáveis quando se discutem questões de segurança na Internet. No entanto será de realçar que, na sua maioria, os países desenvolvidos procuram limitar o âmbito da discussão da Governação da Internet ao vetor da “Network and Information Security”, alegando que as restantes dimensões alargariam o âmbito da Governação da Internet para

---

31 Algumas estimativas apontam para que a percentagem de endereços já atribuídos e não utilizados ronde os 30% do total dos endereços IPv4. Ver Asghari, 2012.



Fonte: Comissão Europeia<sup>32</sup>

assuntos como os de foro criminal. No entanto, os três vetores são, na prática, abordados nos principais fóruns internacionais, como a UIT ou o *Internet Governance Forum* (IGF), pelo que daremos breve nota de alguns aspetos que têm gerado polémica.

#### • “Network and Information Security”

A Comissão Europeia define: “*Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems*”.

Neste vetor de Segurança de redes e de Informação realça-se a importância de se construir redes resilientes e robustas, o que acaba por ser do interesse geral.

#### • Cybercrime

Esta é uma área que em geral os países desenvolvidos querem ver afastada dos fóruns de Governança da Internet, alegando que a mesma deverá ser tratada ao nível da cooperação judicial.

Um leque alargado de países desenvolvidos são subscritores da Convenção de Budapeste sobre Cibercrime, tratado internacional acordado no âmbito do Conselho da Europa para definir os crimes praticados por meio da Internet

<sup>32</sup> “Network and Information Security: Proposal for A European Policy Approach”, Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions, 2001, disponível em [http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001\\_0298en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf) [consultado em outubro de 2013].

e agilizar a cooperação para identificar e localizar os autores dos mesmos. Embora se trate de um texto acordado no âmbito de uma instituição europeia, países não europeus, como o Canadá, Japão, Estados Unidos e África do Sul, são igualmente signatários do Tratado. No total, 29 países, entre os quais Portugal, já ratificaram a Convenção de Budapeste, enquanto que outros 17 países já assinaram, mas ainda não ratificaram. Há, no entanto, Membros do Conselho da Europa que ainda não assinaram a adesão ao Tratado, destacando-se neste grupo Rússia e Turquia<sup>33</sup>.

Em Portugal, a Convenção sobre Cibercrime é concretizada na Lei n.º 109/2009, de 15 de setembro.

Apesar de poder ser considerado um assunto que ultrapassa o âmbito da Governação da Internet, diversos países, tipicamente os não signatários da Convenção de Budapeste, insistem para que algumas questões de cibercrime sejam analisadas em fóruns como a UIT, atendendo a que consideram que a prevenção de alguns crimes passa por ações de cariz técnico. Assim, são, por exemplo, frequentes debates em torno de temas como a *child online protection*, discutindo-se soluções técnicas e formas de cooperação que, por exemplo, impossibilitem o acesso a determinados conteúdos por crianças.

#### • Proteção de dados/Privacidade

Conforme referimos anteriormente Estados Unidos e diversos aliados consideram que as exigências de reforma da Governação da Internet constituem uma ameaça séria a uma Internet livre e aberta que hoje conhecemos, pois encobrem o desejo de um maior controlo dos conteúdos que são transmitidos pela Internet. Neste contexto, podemos dizer que o assunto da segurança sempre foi debatido nestes fóruns e que na base desse debate esteve latente uma desconfiança, ou uma suspeita, que determinados conteúdos pudessem ser, ou vir a ser, monitorizados por um determinado Estado-Membro.

A este propósito, as notícias sobre violações da privacidade por parte da *National Security Agency* (NSA), que denunciaram um programa de espionagem de larga escala (PRISM) visando comunicações estabelecidas através da Internet, deram ampla visibilidade pública a temas que têm vindo a ser debatidos em diversos fóruns mundiais, nomeadamente, na UIT. Contudo,

---

33 Lista de países aderentes da Convenção de Budapeste disponível em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG> [consultado em novembro de 2013].

estas denúncias parecem ter alterado a forma de encarar o tema da vigilância e de a discutir nestes fóruns internacionais.

Assim, as revelações em torno do PRISM serviram de pretexto para que o debate em torno da espionagem de comunicações deixasse de estar dissimulado em considerações técnicas ou jurídicas. Os relatos<sup>34</sup> que surgem do IGF de 2013, que se realizou em outubro, na Indonésia, são eloquentes quanto à forma clara e incisiva como o tema da espionagem foi tratado nesse fórum. Adicionalmente, estas denúncias contribuíram para reforçar o caráter político e de alto nível das discussões em torno da Governação da Internet, a ponto de Dilma Rousseff, Presidente do Brasil, ter transformado o assunto na sua principal bandeira, no seu recente discurso na 68.<sup>a</sup> Assembleia Geral das Nações Unidas<sup>35-36</sup>.

Finalmente, e não menos importante, estas revelações poderão estar a contribuir para alterar o xadrez geopolítico. A este propósito, saliente-se a proposta de resolução conjunta que Brasil e Alemanha apresentaram à Assembleia Geral da ONU, sobre o direito à privacidade na era digital<sup>37</sup>, e que viria a ser aprovada por unanimidade por aquela Assembleia em dezembro de 2013.

Na Europa, o debate sobre a privacidade das comunicações e em particular dos dados armazenados na Internet, também parece estar a ser influenciado com a revelação do caso PRISM. A Comissão Europeia, por intermédio da Comissária para os Assuntos de Justiça, Viviane Reding, havia apresentado uma proposta de reforma das regras de proteção de dados<sup>38</sup> em janeiro de

---

34 "Surveillance: the hot topic at Internet Governance Forum", 2013, Talking New Media, <http://www.talkingnewmedia.com/2013/10/25/surveillance-the-hot-topic-at-internet-governance-forum/> [consultado em outubro de 2013].

35 Rousseff, 2013.

36 A Presidente do Brasil pretende ainda aprovar um novo pacote legislativo, o designado "Marco Civil", o qual deverá estipular que "o armazenamento de dados de personalidades físicas ou jurídicas brasileiras por parte de fornecedores de aplicações de Internet que exerçam essa atividade de forma organizada, profissional e com finalidades económicas no país deve ser feito em território nacional", significando isto, caso esta redação seja aprovada, que OTTs globais como o Facebook ou Google terão de armazenar os dados que dispõem sobre cidadãos ou organizações brasileiras em território brasileiro.

37 Proposta de Resolução conjunta do Brasil e Alemanha, 2013, disponível em <http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/brasil-e-alemanha-apresentam-a-assembleia-geral-da-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital> [consultado em novembro de 2013].

38 Commission proposes a comprehensive reform of the data protection rules, 25 janeiro 2012, disponível em [http://ec.europa.eu/justice/newsroom/data-protection/news/120125\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm) [consultado em setembro de 2013].

2012. Esta proposta revelou-se, porém, muito controversa, com a Comissão a ser acusada, por alguns Estados-Membros, de ser demasiado exigente com determinados prestadores, incluindo os OTT.

As primeiras revelações de Edward Snowden, em maio de 2013, parecem ter contribuído para uma alteração das vontades políticas, o que tem sido aproveitado pela Comissão Europeia para dar novo fôlego à proposta sobre as regras para a proteção de dados. Referindo que, de acordo com algumas estimativas, as revelações sobre o PRISM poderão custar à indústria da *cloud computing* norte-americana, entre \$22 a \$35 mil milhões de dólares de receita nos próximos 3 anos, Viviane Reding<sup>39</sup> assumiu a necessidade de reforçar a confiança dos cidadãos na “economia digital”.

Concretizando o apoio político à reforma proposta pela Comissão, o Conselho Europeu de 24 e 25 de outubro de 2013, declarou que a mesma “é essencial para a realização do mercado único digital até 2015”<sup>40</sup>

Adicionalmente, em março de 2014 o Parlamento Europeu votou favoravelmente à reforma da legislação sobre proteção de dados, que assenta em 4 pilares fundamentais:

- Primeiro pilar: Um continente, uma Lei. Para ajudar a concretizar este pilar, a reforma aprovada pelo Parlamento Europeu compreende um regulamento e uma diretiva sobre o assunto. Sendo o regulamento de aplicação direta pelos Estados-Membros, não requerendo transposição, a harmonização legislativa é mais facilmente concretizável;
- Segundo Pilar: As empresas não europeias que operem na União Europeia, vão ter de obedecer às regras comunitárias;
- Terceiro Pilar: Consagração do direito a ser esquecido, isto é, sempre que um utilizador desejar que os seus dados pessoais não continuem a ser armazenados por um qualquer prestador de serviço, tais dados deverão ser removidos, desde que não existam razões legítimas que justifiquem o contrário;
- Quarta Pilar: Criação de um “One-stop-shop” para empresas e cidadãos, no sentido de facilitar a apresentação de denúncias contra uma empresa sediada noutro país.

---

39 R2013.

40 Conclusões do Conselho Europeu de 24 a 25 de outubro de 2013, disponível em [http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/pt/ec/139221.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/pt/ec/139221.pdf) [consultado em outubro de 2013].

A reforma aprovada pelo Parlamento terá ainda de ser adotada pelo Conselho da União Europeia.

### III. O DEBATE INSTITUCIONAL EM TORNO DA GOVERNAÇÃO DA INTERNET

Uma vez identificados alguns dos principais assuntos da Governação da Internet, importa indicar os mais relevantes fóruns de direito privado e direito internacional em que esta matéria é debatida internacionalmente e na qual os Governos têm vindo a participar ativamente.

#### 1. Entidades de direito privado

São de mencionar as seguintes:

- *GAC do ICANN*: Entidade a que nos referimos no ponto anterior;
- *Internet Society (ISOC)*<sup>41</sup>: Entidade que reúne milhares de membros, entre os quais os principais OTT, e que persegue diversos objetivos, como o desenvolvimento de normas, protocolos e infraestrutura técnica para a Internet;  
A ISOC procura ainda a criação de comunidades para a discussão de políticas nacionais e internacionais para o desenvolvimento da Internet. Esta função é atualmente distribuída por 90 comunidades nacionais, designadas “chapters”<sup>42</sup>;
- *The Internet Engineering Task Force (IETF)*: é uma das ramificações do ISOC, de particular relevância na área da normalização para a Internet, tendo desenvolvido, por exemplo, o IPv6.

#### 2. Organizações internacionais

Sistematizaremos as organizações internacionais que têm a Governação da Internet na sua agenda em três grupos: Nações Unidas, OCDE, e União Europeia.

##### a) Nações Unidas

A Assembleia Geral da ONU tem sido palco de variados debates e decisões sobre o Governação da Internet. Entre as decisões relevantes conta-se a criação

---

41 Internet Society em <http://www.internetsociety.org/>.

42 Portugal Chapter em <http://isoc.pt/>.

da *World Summit on Information Society* e a renovação do mandato do *Internet Governance Forum* (ver adiante Fóruns Internacionais).

Adicionalmente esta matéria é discutida em diversas agências das Nações Unidas, destacando-se, neste particular a:

- *União Internacional das Telecomunicações (UIT)* – como vimos anteriormente alguns Estados-Membros reclamam que esta organização assuma as principais funções do ICANN e/ou que assuma o papel de RIR, isto é, o papel de distribuição dos endereços IP aos ISPs. A UIT organiza como veremos seguidamente diversos fóruns relevantes para a Governação da Internet.
- *United Nations Education, Science and Cultural Organisation (UNESCO)* – a participação desta organização visa potenciar a Internet como catalizador do desenvolvimento humano, contribuindo para a consolidação de sociedades democráticas através da livre circulação de informação e ideias.
- *World Intellectual Property Organization (WIPO)* – Esta agência tem tido particular relevo no registo de novos domínios genéricos de topo, cujo processo tem levantado problemas de direitos de autor.

Ainda no âmbito das Nações Unidas saliente-se ainda o *High-level UN Group on Information Society (UNGIS)*, que tem por missão assegurar a coordenação das diversas agências da ONU.

Vários fóruns são organizados sob a égide das Nações Unidas:

- *World Summit on Information Society (WSIS)*: A WSIS consistiu de dois eventos sobre a Sociedade da Informação que ocorreram em 2003 em Genebra e em 2005 em Túnis (da qual resultou a Agenda de Tunis, referida no Capítulo da Introdução do presente *paper*). Esta Cimeira foi o resultado de uma Resolução da Assembleia Geral das Nações Unidas, em 2001, que atribuiu à UIT o papel de organizador do evento, em coordenação com outras agências das Nações Unidas.
- *World Conference on International Telecommunication (WCIT-12)*: A WCIT-12, organizada pela UIT, decorreu de 3 a 14 de dezembro de 2012, no Dubai, Emirados Árabes Unidos e reuniu 151 Estados-Membros, acabou por ser um marco importante para expor as fortes divergências que existem a nível global face à Governação da Internet. Na realidade, a Conferência foi agendada com intuito de rever o Regulamento das Telecomunicações Internacionais que estabelece princípios gerais para a prestação e operacionalização das telecomunicações inter-

nacionais, mas acabou por se centrar em larga medida no debate sobre o controlo da Internet e o peso dos Governos nessa matéria.

A divisão patente nessa Conferência, resultou em Atos Finais<sup>43</sup>, que não foram assinados pelos países da União Europeia, bem como pela maioria dos países desenvolvidos.

- *Internet Governance Forum (IGF)*: Estabelecido na WSIS de 2005, o IGF tem como objectivo a criação de um fórum *multistakeholder* em que Governos, Academia e Sociedade Civil debatem matérias da Governação da Internet. Por decisão de dezembro de 2010, da Assembleia Geral das Nações Unidas, foi renovado o mandato do IGF até 2015. Pela mesma decisão, a Comissão das Nações Unidas para a Ciência e Tecnologia (CSTD) foi mandatada a desenvolver propostas visando a melhoria do IGF, tendo sido criado, no âmbito desse mandato, um Grupo de Trabalho, no qual têm vindo a participar 22 Governos.

O IGF 2013, que se realizou em Outubro, na Indonésia, foi dominado pelas questões de segurança e privacidade.

*b) Organização para Cooperação e Desenvolvimento Económico (OCDE)*

Esta organização tem dado importantes contributos para abordagem de questões económicas da Internet. Em junho de 2011, a OCDE aprovou os Princípios para a Política para a Internet<sup>44</sup>, os quais pretendem contribuir para uma Internet propulsora da Inovação e do Crescimento.

*c) Europa e União Europeia*

Na Europa, devemos desde logo destacar a *European Conference of Postal and Telecommunications Administrations (CEPT)*, que integra 48 países da Europa, e que, entre outras competências, define a posição Europeia na UIT.

A União Europeia tem vindo a debater naturalmente matérias relacionadas com a Governação da Internet. Destaque-se, neste ponto, o *High-Level Group on Internet Governance (HLIG)*, que é presidido pela Comissão Europeia, no qual participam os Estados-Membros da UE, Noruega e Suíça, e onde se discute a posição da UE para fóruns como o GAC do ICANN ou o IGF.

---

43 Atos Finais da WCIT-12 disponíveis em <http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf> [consultado em janeiro 2013].

44 Princípios para a Política para a Internet, 2011, OECD, disponíveis em <http://www.oecd.org/internet/innovation/48289796.pdf> [consultado em abril de 2013].

Refira-se que em maio de 2013, a Comissão Europeia anunciou a criação da *Global Internet Policy Observatory (GIPO)*, que pretende ser uma plataforma *on-line* com vista a melhorar a participação de todos os *stakeholders* nos debates e decisões sobre política de Internet. O GIPO foi desenvolvido em ligação com países como o Brasil e a Suíça, e organizações como a União Africana e a *Internet Society*.

#### IV. PORTUGAL E A GOVERNAÇÃO DA INTERNET

##### 1. Situação atual

Procuraremos em cada uma das matérias tratadas anteriormente, identificar a entidade ou entidades com responsabilidade de acompanhamento/deliberação sobre as mesmas.

A questão dos *custos de acesso* é uma questão da responsabilidade do regulador setorial das comunicações, a ANACOM. Desde logo, a Lei 5/2004, de 10 de fevereiro, conforme revista pela Lei n.º 51/2011, de 13 de setembro (Lei das Comunicações Eletrónicas), confere à ANACOM a incumbência de “Eliminar os obstáculos existentes à oferta de redes de comunicações eletrónicas<sup>45</sup>, de recursos e serviços conexos e de serviços de comunicações eletrónicas a nível europeu” (conforme n.º 3 alínea a) do art 5.ª).

As questões de “*Qualidade de serviço e de neutralidade de rede*” estão igualmente sob a alçada do regulador das comunicações. Conforme referido anteriormente a proposta para nova revisão do enquadramento regulamentar europeu parece indicar que estas matérias tornar-se-ão ainda mais relevantes para as ARNs europeias.

No que concerne ao *Domain Name System*, a entrada em vigor do Decreto-Lei n.º 55/2013 de 17 de abril<sup>46</sup>, procedeu à extinção da FCCN, tendo as funções dessa entidade respeitante à gestão do domínio de topo “.pt”

45 «Rede de comunicações eletrónicas» são definidas na Lei n.º 5/2004, de 10 de fevereiro, como “os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos de rede que não se encontrem activos, que permitem o envio de sinais por cabo, meios radioelétricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes de radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida” (sublinhado nosso).

46 Decreto-Lei n.º 55/2013, de 17 de abril, disponível em [http://alfa.fct.mctes.pt/documentos/Lei\\_Organica\\_2013.pdf](http://alfa.fct.mctes.pt/documentos/Lei_Organica_2013.pdf) [consultado em outubro de 2013].

transitado para a Associação DNS.PT<sup>47</sup>, associação privada sem fins lucrativos, formalmente criada a 9 de maio de 2013. Assim, nos termos desse diploma, os direitos e obrigações até então por prosseguidos pela FCCN, no âmbito da delegação efetuada pela IANA a 30 de junho de 1988 (RFC 1032, 1033, 1034 e 1591), foram transmitidos para a Associação DNS.PT<sup>48</sup>. A Associação DNS.PT, tem como fundadores a Fundação para a Ciência e a Tecnologia, IP (FCT)<sup>49</sup>, Associação do Comércio Eletrónico e Publicidade Interativa (ACEPI), Associação Portuguesa para a Defesa do Consumidor (DECO) e o representante designado pela IANA como responsável pela delegação do ccTLD.pt. A Autoridade Nacional de Comunicações (ANACOM) é uma das entidades que integra o Conselho Consultivo da DNS.PT. Note-se ainda que com a extinção da FCCN todas as suas restantes funções foram transferidas para a FCT.

Ao nível da *Numeração e endereços IP (nível lógico)* as entidades nacionais têm reduzida margem para intervenção, uma vez que o processo está centralizado na RIPE NCC, que assume as funções de RIR na Europa e que atribui diretamente estes recursos aos ISPs.

Nas questões de *segurança e privacidade*, as responsabilidades estão partilhadas por diversas entidades. A Lei das Comunicações Eletrónicas atribui à ANACOM a incumbência de “assegurar que seja mantida a integridade e a segurança das redes de comunicações públicas” e confere à mesma entidade a responsabilidade de “Contribuir para garantir um elevado nível de proteção dos dados pessoais e da privacidade”. Em matéria de privacidade, destaque-se ainda a Comissão Nacional da Proteção de Dados que tem missão controlar e fiscalizar o processamento de dados pessoais, em respeito pelas liberdades e garantias consagradas na Constituição e na lei, devendo para o efeito cooperar com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Na vertente do *Cibercrime*, realce-se o Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade (Gabinete

---

47 Associação DNS em <https://www.dns.pt/home> [consultado em outubro de 2013].

48 Ver art. 21.º do Decreto-Lei n.º 55/2013, de 17 de abril.

49 Fundação para a Ciência e a Tecnologia, IP, disponível em <http://www.fct.pt> [consultado em outubro de 2013].

Cibercrime)<sup>50</sup> que tem sede na Procuradoria-Geral da República, de que é diretamente dependente. Este Gabinete tem por missão assegurar a coordenação interna do Ministério Público, nesta área da criminalidade, garantir a formação específica e estabelecer canais de comunicação com fornecedores de serviço de acesso às redes de comunicação, que permitam facilitar a sua colaboração na investigação criminal.

De destacar ainda alguns projetos que resultam de parcerias de diversas entidades que pretendem contribuir para uma Internet mais segura. Neste âmbito, destacamos o Projeto InternetSegura<sup>51</sup>. Trata-se de uma iniciativa que nasce de consórcio coordenado pela FCT e que envolve, nomeadamente, o Ministério da Educação e a Microsoft Portugal. Este Projeto tem como principais objetivos o combate a conteúdos ilegais; a promoção de uma utilização segura da Internet; e a consciencialização da sociedade para os riscos associados à utilização da Internet.

A representação internacional é, em larga medida, assegurada pela FCT, que acompanha o GAC do ICANN, o IGF e a nível da União Europeia, o *HLIG*, e a ANACOM que acompanha a UIT e a CEPT.

## 2. O confronto com outros países europeus

Em outros países da Europa, as questões de custos de acesso, qualidade de serviço e neutralidade de rede são em grande medida da responsabilidade das ARNs, até porque tal função decorre das Diretivas Europeias para o setor das comunicações eletrónicas.

A situação é bem mais complexa nas questões de segurança e privacidade<sup>52</sup>, uma vez que entre os países europeus convivem diferentes arranjos para tratar destas matérias. Se existe um traço comum entre os países europeus é o da multiplicidade de organismos com responsabilidades nestas áreas e a preocupação em criar mecanismos de coordenação entre os mesmos. Se alguns países atribuem à ARN uma responsabilidade central em matérias de segurança (como a Dinamarca, Finlândia, Suécia, Chipre ou Bulgária), a maioria dos países tende a atribuir esta responsabilidade a departamentos ministeriais

---

50 Gabinete Cibercrime da Procuradoria Geral da República <http://cibercrime.pgr.pt/index.html> [consultado em novembro de 2013].

51 Projeto InternetSegura, disponível em <http://www.internetsegura.pt/>.

52 "Country reports", 2011, European Union Agency for Network and Information Security (ENISA), disponível em <http://www.enisa.europa.eu/activities/stakeholder-relations/country-reports> [consultado em outubro de 2013].

(Reino Unido, Alemanha, França ou Espanha). Outra solução frequente entre os países europeus passa pela criação de plataformas ou grupos de trabalho interministeriais com o único objetivo de coordenar das entidades públicas e privadas relevantes (França, Irlanda, República Checa ou Bélgica).

No que respeita às questões de numeração, nomes e endereços, também subsiste uma considerável diferença na forma de acompanhamento destes assuntos.

Em alguns países a opção passou por atribuir aos reguladores de comunicações responsabilidades na gestão destes recursos críticos da Internet nos seus respetivos países.

Na Finlândia, a ARN (Ficora) tem um papel de regulação do domínio “.fi”. Neste contexto, incumbe à ARN: (i) submeter anualmente ao Governo uma proposta com o valor das tarifas dos domínios “.fi”; (ii) supervisionar os cerca de 1000 *registrars* (entidades que vendem os domínios aos utilizadores finais).

A PTS, regulador da Suécia, assume responsabilidades nesta matéria. A PTS é responsável pela coordenação de um Grupo de Trabalho para a Governação da Internet, que reúne aproximadamente 20 organizações suecas (Ministérios das Comunicações, da Justiça e dos Negócios de estrangeiros, ISOC-SE, Academia e algumas empresas).

A BIPT, Bélgica, é igualmente uma ARN com responsabilidades pelo acompanhamento de aspetos relativos aos recursos críticos da Internet (números, nomes, e endereços). No seu Relatório Anual de 2012 pode ler-se que está entre as preocupações da BIPT a escassez dos endereços IPv4 e as suas implicações ao nível da segurança<sup>53</sup>.

A RRT, Lituânia, assume as funções de gestão e supervisão dos recursos de numeração tradicionais e de outros “identificadores de rede”, o que inclui os recursos de nomes e endereçamento.

Fora da União Europeia, destaque-se também para a Ofcom, da Suíça, como outro caso em que a ARN é o principal interlocutor nacional para as questões da Governação da Internet, no seu conjunto.

Em todos os casos descritos, as ARNs garantem o acompanhamento dos principais fóruns de Governação Internet, como sejam o GAC do ICANN, IGF ou a UIT.

---

53 Relatório Anual da BIPT, 2012, disponível em <http://www.bipt.be/flash/AnnualReport2012/en/content/IBPT-13-12752-RapportAnnuel2012-EN-af-260813-web.pdf> [consultado em outubro de 2013].

### 3. Perspetivas de evolução em Portugal: algumas propostas

Não obstante a indefinição a nível internacional sobre o melhor modelo a adotar na Governação da Internet, estamos em crer que, a nível nacional, é possível aperfeiçoar, desde já, o modelo organizativo existente, de modo a adaptar o mesmo à realidade atual e a reforçar a coordenação e as sinergias das competências neste domínio.

Assim, para que a posição de Portugal se fortaleça a nível internacional, consideramos necessário um aprofundamento dos mecanismos de coordenação, entre entidades públicas, setor privado, academia ou representantes da sociedade civil com responsabilidade/interesse nas matérias identificadas no capítulo II do presente artigo. Deste modo, à semelhança do que se verifica noutros países poder-se-á enveredar pela constituição de plataformas/grupos de trabalho que permitam agilizar procedimentos de partilha de conhecimentos entre as entidades interessadas.

No fundo, propõe-se que, à escala nacional, sejam desenvolvidos mecanismos que permitam dar um impulso adicional ao modelo *multistakeholder*.

Em tese, poder-se-á equacionar ainda a evolução do modelo de regulador ‘tradicional’ de telecomunicações, para um regulador setorial que atue num ambiente convergente, com responsabilidades acrescidas em algumas das matérias identificadas.

Uma vez criadas as condições internas para abordar a Governação da Internet de forma mais abrangente e consistente, Portugal estará em melhores condições para fazer passar o seu posicionamento na matéria, a nível internacional. Na realidade, conforme se avançou no início deste trabalho, as cisões em torno da Governação da Internet são comparadas a uma Guerra Fria Digital, o que, no limite, poderá levar a que alguns países, não confiantes nas atuais instâncias de governação da Internet, avancem para a construção de um rede alternativa, que não passe por essas entidades. Ora, isto seria a fragmentação da Internet, com efeitos negativos para todos os países, e naturalmente também para Portugal.

As posições de Portugal nos diferentes fóruns deverão ser coordenadas a nível europeu, tanto a nível da União Europeia, como da CEPT. Nas organizações europeias, entendemos que Portugal deverá trabalhar ativamente no sentido de reforçar a sua capacidade de influência sobre as orientações estratégicas europeias. Noutro plano, Portugal deverá intensificar a sua atuação junto da CPLP no sentido de procurar harmonizar posições, identificando pontos de concordância e eventual discordância.

Nestes diferentes contextos, Portugal deverá defender alguns princípios fundamentais, a saber:

- O modelo *multistakeholder*, no qual Governos, sociedade civil, setor privado, organizações internacionais e academia participam e têm a oportunidade de se fazer ouvir.
- Uma abordagem *light touch*. O dinamismo e a capacidade de inovação que tem caracterizado tudo aquilo que rodeia a Internet não podem ser constrangidos por desnecessárias intervenções regulatórias, embora em determinados casos se admita como necessária uma regulação mais ativa (*vide* escassez de endereços IPv4, em parte explicada por recursos que não são usados).

Na defesa destes princípios, Portugal deve ter presente a importância histórica que os Estados Unidos tiveram na criação da Internet e que é dos Estados Unidos que continuam a surgir muitas das mais inovadoras aplicações que fazem com que a Internet seja um bem indispensável nos nossos dias, ao ponto de as Nações Unidas terem decretado o Acesso à Internet como parte integrante dos Direitos Humanos<sup>54</sup>.

Mas devemos ter também presente que é a universalização da Internet que faz da mesma aquilo que é hoje. O valor da Internet reside sobretudo nos cerca de 2,7 mil milhões de utilizadores em todo o mundo<sup>55</sup>. E esta universalização torna compreensível que vários países peçam mais poder de influência nas decisões que afetam a rede das redes, porque no fundo sentem que a Internet também é sua. Neste sentido, defendemos que deverão ser apoiadas as reformas que permitam a criação de um modelo institucional que melhor capte e traduza esta universalização, e que ao mesmo tempo deem garantias de salvaguarda do caráter livre, aberto, dinâmico e inovador da Internet.

Para sintetizar, consideramos que Portugal deverá ter como objetivo a mitigação dos fortes atritos que hoje ocorrem em torno da Governação da Internet e a criação de pontes entre os diferentes intervenientes.

Importa, por fim, não desprezar a influência que Portugal pode ter. Logicamente que não somos potência mundial, ou sequer potência regional. Mas Portugal é um país desenvolvido, da União Europeia e da OCDE, ao mesmo tempo que tem fortes ligações históricas, quer com o Brasil, já hoje um líder

---

54 La Rue2011.

55 UIT Stats, disponível em [http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU\\_Key\\_2005-2013\\_ICT\\_data.xls](http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls) [consultado em outubro de 2013].

global, e particularmente ativo nas questões da Governação da Internet, quer com vários países em desenvolvimento, de África, Ásia e demais América Latina. E, acima de tudo, não se pode negligenciar o facto de o Português ser a 5.<sup>a</sup> língua mais utilizada na Internet<sup>56</sup>.

## V. NOTAS CONCLUSIVAS

A análise constante do presente artigo suporta a ideia de que a Governação da Internet está longe de estar confinada à gestão técnica de recursos críticos da Internet, como os nomes e endereços IP. A Governação da Internet passa também pelo desenvolvimento de infraestruturas e acesso às mesmas, passa pela qualidade de serviço e pela polémica questão da neutralidade de rede, e passa necessariamente pelas cruciais questões de segurança e privacidade. Outros temas não aprofundados no presente artigo, como direitos de autor ou a liberdade de expressão, fazem igualmente parte do âmbito da Governação da Internet.

Ficou também patente que apesar de a Internet fazer, há largos anos, parte do dia-a-dia dos cidadãos, ainda subsiste uma indefinição a nível internacional, e inevitavelmente a nível nacional, sobre o papel dos Governos nesta matéria. Consideramos que na base dessa indefinição está precisamente a importância política, social e económica da Internet, o que faz com que qualquer eventual reforma na sua Governação seja analisada à luz de múltiplos interesses e critérios. Neste contexto, sublinhámos que a Governação da Internet suscita divergências não apenas entre países, mas também entre Governos e Sociedade Civil; operadores tradicionais e prestadores *over-the-top* (OTT); a liberdade individual e a segurança nacional.

Com base em exemplos de outros países da União Europeia, procurámos demonstrar que, a nível nacional, há espaço para aperfeiçoar o modelo organizativo existente em Portugal, através do reforço dos mecanismos de coordenação entre os *stakeholders* interessados, melhorando a eficácia e coordenação da intervenção nacional.

Para finalizar, reflectimos sobre o papel que Portugal pode assumir a nível internacional nesta matéria e estabelecemos aquele que deverá ser o desígnio último do posicionamento de Portugal: evitar a indesejável fragmentação da Internet e contribuir para a procura de soluções de compromisso e o aproximar de posições entre diferentes intervenientes, de diferentes latitudes. No fundo, julgamos que Portugal deverá fazer simplesmente aquilo que melhor sabe fazer.

---

56 Internet World Stats, disponível em <http://www.internetworldstats.com/stats7.htm> [consultado em outubro de 2013].

## BIBLIOGRAFIA

ASGHARI, Hadi

2012 “Thirty percent of IPv4 space is still unused”, Delft University of Technology, disponível em <http://www.internetgovernance.org/2012/08/17/thirty-percent-of-ipv4-space-is-still-unused/>.

BELL, Richard

2002 “The Halfway Proposition - Background Paper on Reverse Subsidy of G8 Countries by African ISPs,” disponível em [http://afx.afridns.org/technicaltraining/T1/AFRISPA\\_Halfway%20Proposition.pdf](http://afx.afridns.org/technicaltraining/T1/AFRISPA_Halfway%20Proposition.pdf) [consultado em outubro de 2013].

KAPUR, Akash

2005 “Internet Governance: A primer”, New Delhi: United Nations Development Programme–Asia-Pacific Development Information Programme (UNDP–APDIP), disponível em <http://www.unapcict.org/ecohub/resources/internet-governance-a-primer> [consultado em outubro de 2013].

KROES, Nellie

2013 *Carta da Vice-Presidente da Comissão Europeia a Fadi Chehadé, Presidente e CEO do ICANN*, disponível em <http://www.icann.org/en/news/correspondence/kroes-to-chehade-crocker-12sep13-en.pdf> [consultado em outubro de 2013].

KRUGER, Lennard

2013 “Internet Governance and the Domain Name System: issues for Congress”, disponível em <http://www.fas.org/sgp/crs/misc/R42351.pdf> [consultado em outubro de 2013].

LA RUE, Frank

2011 “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”, UN General Assembly, Human Rights Council, disponível em <http://documents.latimes.com/un-report-internet-rights/> [consultado em novembro 2013].

OLMOS, Ana & CASTRO, Jorge

2013 OpenForum Academy, “*Net Neutrality in the EU – Country Factsheets*”, disponível em <http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20%20Country%20Factsheets%2020130905.pdf> [consultado em outubro de 2013].

REDING, Viviane

2013 “Data protection reform: restoring trust and building the digital single market”, 4th Annual European Data Protection Conference, disponível em [http://europa.eu/rapid/press-release\\_SPEECH-13-720\\_en.htm?locale=en](http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm?locale=en) [consultado em setembro de 2013].

ROUSSEFF, Dilma

2013 Discurso na 68.<sup>a</sup> Assembleia Geral das Nações Unidas, disponível em <http://www2.planalto.gov.br/imprensa/discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua> [consultado em setembro de 2013].

## LISTA DE ACRÓNIMOS

UIT – União Internacional de Telecomunicações

BRICS – Brasil, Rússia, Índia, China e África do Sul

ICANN – *Internet Corporation for Assigned Names and Numbers*

IP – Internet Protocol

OTT – over-the-top

DNS – Domain Name System

IXPs – Internet exchange points

ISP – Internet Service Providers

ETNO – European Telecommunications Network Operators’ Association

WCIT-12 – World Conference on International Telecommunications 2012

DoC – Departamento de Comércio dos EUA

gTLD – Generic Top Level Domain

ccTLD – Country code Top Level Domain

GAC – Governmental Advisory Committee

IANA – Internet Assigned Names Authority

RIRs – Regional Internet Registries

RIPE NCC – Réseaux IP Européens Network Coordination Centre

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

IGF – Internet Governance Forum

NSA – National Security Agency

PRISM – Programa de vigilância

ISOC – Internet Society

IETF – The Internet Engineering Task Force

UNESCO – United Nations Education, Science and Cultural Organisation

WIPO – World Intellectual Property Organization

UNGIS – High-level UN Group on Information Society

WSIS – World Summit on Information Society

OCDE – Organização para a Cooperação e Desenvolvimento Económico

CEPT – European Conference of Postal and Telecommunications Administrations

HLIG – High-Level Group on Internet Governance

GIPO – Global Internet Policy Observatory

FCCN – Fundação para a Computação Científica Nacional

FCT – Fundação para a Ciência e a Tecnologia

ANACOM – Autoridade Nacional de Comunicações

Ficora – *Finnish Communications Regulatory Authority*

PTS – Swedish Post and Telecom Authority

BIPT – Belgisch Instituut voor postdiensten en telecommunicatie

RRT – Communications Regulatory Authority of the Republic of Lithuania

Ofcom – Federal Office of Communications, Switzerland

CPLP – Comunidade dos Países de Língua Portuguesa