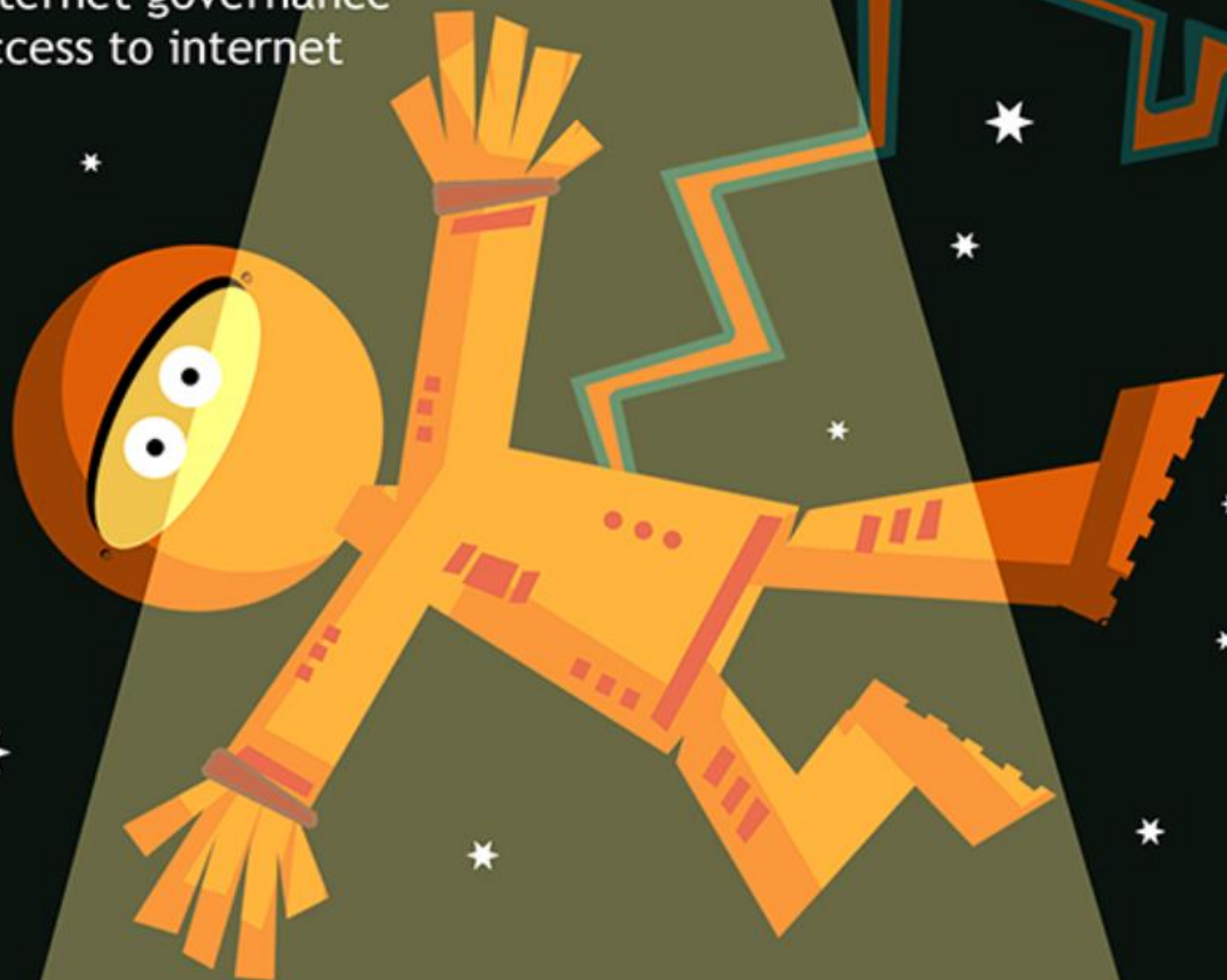


DIREITO:

A PENSAR TECNOLOGICAMENTE

internet:

- international tribunal for the internet
- open and free Internet
- internet governance
- access to internet



OUTROS: • international cooperation



EDIÇÃO N.º II – JUNHO DE 2016

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO
CENTRO DE INVESTIGAÇÃO JURÍDICA DO
CIBERESPAÇO – CIJIC – DA FACULDADE DE
DIREITO DA UNIVERSIDADE DE LISBOA**

CYBERLAW

by CIJIC

CYBERLAW

by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e GONÇALO SOUSA

DESIGN & GRAFISMO: ISABEL BAPTISTA e ANTÓNIO OLIVEIRA

DIRECTOR DO CIJIC: EDUARDO VERA-CRUZ PINTO

COMISSÃO CIENTÍFICA:

- ALFONSO GALAN MUÑOZ
- ANTÓNIO R. MOREIRA
- DANIEL FREIRE E ALMEIDA
- ELLEN WESSELINGH
- FRANCISCO MUÑOZ CONDE
- MANUEL DAVID MASSENO
- MARCO ANTÓNIO MARQUES DA SILVA
- MARCOS WACHOWICZ
- ÓSCAR R. PUCCINELLI
- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW

by CIJIC

EDITORIAL NOTES :

In an ideal world, the fruition of Internet and its *inspiring* capabilities – as almost everything in the real world - should occur in respect for human fundamental rights. Thereby, the need and the demand for an open, free and secure Internet present itself as natural corollaries. Nevertheless, *homo homini lupus*, times and actions have proven over the years that we tend to live in *troubled* times.

Regarding only to Internet, and to its governance model – *per se* one core subject of our present edition – in a glimpse of one *back to basics*, the transition process going on aims to promote Internet governance under a "*multi-stakeholder*" model, and, thereby, is keen to avoid the control of the online ecosystem by any kind of just one single governmental bodie.

Over the years many countries expressed concern conveyed by the perception – real or not, in a quite *petulant* interjection - that the United States were holding the reins of the Internet. By "*doing it*" - potentially - such an American action would lead to its fragmentation insofar as many countries would feel tempted to prompt their "*specific*" *regional* "*domains*". To avoid it, and to boost Internet governance under a "*multi-stakeholder*" model - with a system of checks and balances – the current process of transition intends to prevent that no single entity can exert control over the Internet. According to the gist of it, it is likely to assume itself as *the click* to a more *democratized perception* of such an indispensable and *worldwide* human tool as the Internet. We do follow the underlying generosity of the motivation behind this transition. That is, the motto to "*preserve a free and open Internet*" as we know it. But, we will leave this stage for our guest authors.

At this «**Cyberlaw by CIJIC**» 2nd edition, we intend to bring to one legal and technological debate some of the most worrying questions related with the weakness of the traditional concepts of public law. Take Cyberspace. Currently it dominates daily life. Where can we find the protection of the legal-subjective positions of individuals in it? More, traditional juridical and legal programs will lose all effectiveness, sliding into *nominal*, if the rule of law gives up to respond to the daily problems of *netizens*. So, we seek to bring to discussion either «Internet governance» models, either one future court to its global regulation. Making always our point of honor on safeguarding human fundamental rights, which - if any - new international, *worldwide*, legal solutions do we must strive for?

Celebrating the arrival of CIJIC as a member of the *Network of Centers*⁽¹⁾, we made the decision to have more articles in English language. However, true to our goal of producing scientific content in our native portuguese language, we present this edition of «Cyberlaw by CIJIC» with articles either in Portuguese or in English.

Thereby, seizing the opportunity, on my own behalf and on behalf of the Cyberlaw Research Centre - CIJIC - at The University of Lisbon, Faculty of Law, our sincere «Muito Obrigado!» to all the authors who have decided to participate in this edition.

At long last, and for the remarkable relevance, I just would like to call into play Sir Antonio Genesio Maria Panizzi by quoting and suiting his ideal of free and equal access to learning, back in the 19th Century, to the nowadays – where a flourishing digitized economy, the 4th industrial revolution, and, one universal access to knowledge must match - «*I want a poor student to have the same means of indulging his learned curiosity, of following his rational pursuits, of consulting the same authorities, of fathoming the most intricate inquiry as the richest man in the kingdom, as far as books go, and I contend that the Government is bound to give him the most liberal and unlimited assistance in this respect.*»

Lisbon, June 2016

Nuno Teixeira Castro

1 More at: <http://networkofcenters.net/centers>

CYBERLAW

by CIJIC

**INTERVIEW WITH PORTUGUESE NATIONAL
CYBERSECURITY CENTER COORDINATOR : PROFESSOR
PEDRO VEIGA**

**ENTREVISTA COM O COORDENADOR DO CENTRO
NACIONAL DE CIBERSEGURANÇA PORTUGUÊS:
PROFESSOR PEDRO VEIGA**



Professor PEDRO VEIGA

RESUMO

O novo Coordenador do Centro Nacional de Cibersegurança⁽¹⁾, Pedro Veiga, admite, à «*Ciberlaw By CIJIC*», que tem havido “défice de discussão” sobre a proteção dos Direitos Fundamentais no Ciberespaço. Garantiu-nos, todavia, que tudo fará para que a internet possa ser um espaço seguro e de confiança para todos os portugueses. Mais, após ter assumido funções há dois meses, Pedro Veiga apela, ainda, a um maior envolvimento de entidades públicas e privadas, prometendo um papel de charneira do CNCiber na divulgação das actuais leis e das boas práticas de Cibersegurança junto de todos os sectores da sociedade.

1 <http://exameinformatica.sapo.pt/noticias/mercados/2016-04-18-Pedro-Veiga-e-o-novo-coordenador-do-Centro-Nacional-de-Ciberseguranca>

O catedrático apaixonado pela Cibersegurança revela que uma das suas prioridades é criar pontes com entidades públicas e privadas para trazer mais recursos humanos para uma área que considera ser “tão promissora, aliciante, de elevada empregabilidade e desafiante.”. Pedro Veiga lembra que o factor humano é crucial para a Cibersegurança. Num paralelismo, questiona, “(D)e que serve um automóvel ter airbags, ABS, cintos de segurança e muitos outros dispositivos de segurança se o condutor estiver distraído a usar um telemóvel, não respeitar um sinal de proibição de ultrapassagem numa curva ou um semáforo no vermelho?”. Podemos ter à mão tecnologias fantásticas, mas se não forem correctamente utilizadas, o resultado pode ser desastroso, conclui o recém-empossado Coordenador do CNCiber.

Ao longo da nossa conversa, Pedro Veiga revela as suas principais prioridades e mostra-se confiante no empenho do actual Governo na superação dos desafios, velhos e novos, do Ciberespaço.

Interview Questions

Propusemos⁽²⁾ uma conversa, ao Professor Pedro Veiga, subordinada a alguns tópicos, para que dela possamos suscitar discussões necessárias. Em traços gerais, pretendemos problematizar em torno da construção, do estabelecimento e do fomento de uma cultura de confiança (no anglicanismo de «*Trust*») do utilizador (em sentido lato, compreendendo desde o utilizador-médio, às organizações e ao próprio Estado) no uso da internet e na fruição do ciberespaço. Conseguiremos ancorá-la na vitalidade, que assim se espera, do nosso CNCiber?

Q) Começemos, por exemplo, pela comparação, bastante *ilustrativa*, trazida a discussão por Peter Singer⁽³⁾. Poderemos esperar que o CNCiber tenha por «(...)missão de contribuir para ganhos em cibersegurança pública, através de atividades de investigação e desenvolvimento tecnológico, atividade laboratorial de referência, observação da segurança e vigilância epidemiológica informática, bem como coordenar a avaliação externa da qualidade laboratorial, difundir a cultura científica, fomentar a capacitação e formação e ainda assegurar a prestação de serviços diferenciados, nos referidos domínios⁽⁴⁾»? Agora que tomou as rédeas do CNCiber, o que podemos esperar deste?

P.V.) O CNCiber tem um mandato que está definido na Estratégia Nacional de Segurança no Ciberespaço (Resolução do Conselho de Ministros nº 36/2015) e esta estratégia deve ser alvo de uma revisão regular e periódica, segundo este diploma. Numa altura em que a crescente digitalização da sociedade avança, quando a informação sob a forma digital cresce a um ritmo muito elevado, e, quando cada vez mais serviços se desenvolvem sobre as redes globais, a missão central de garantir um ciberespaço nacional seguro free que inspire confiança aos cidadãos assume-se como muito importante. Não é só ao CNCiber que está atribuído o papel de garantir um ciberespaço seguro, na medida em que muitas outras entidades, públicas e privadas,

2 Conduzida por Nuno Teixeira Castro.

3 Singer, Peter W., em «How to Save the Net: A CDC for Cybercrime» em: <http://www.wired.com/2014/08/save-the-net-peter-singer/>

4 Embora adaptada à temática da cibersegurança, esta informação foi, *ipsis verbis* retirada do sítio do INSA - Instituto Nacional de Saúde Dr. Ricardo Jorge, e da missão a que este se propõe prosseguir. Disponível em: <http://www.insa.pt/sites/INSA/Portugues/QuemSomos/Paginas/Missao.aspx>

tem que estar envolvidas e contribuir para elevados níveis de resiliência e robustez do nosso quotidiano neste mundo digital. Mas o CNCiber tem que contribuir para uma confluência de esforços na mesma direcção, quer através do desempenho de um papel charneira na difusão da legislação existente, quer levando o conhecimento das boas práticas de cibersegurança ao conhecimento de todos os sectores da sociedade. Há sectores e recursos que devem merecer uma especial importância como as infraestruturas críticas, a informação que é detida pelas instituições públicas ou a resiliência das redes que prestam os serviços aos cidadãos ou às empresas. A reduzida dimensão dos recursos humanos e materiais atribuídos ao CNCiber limitam a abrangência e diversidade da intervenção, por exemplo na vertente de investigação e desenvolvimento que é referida na sua questão, mas pela sua relevância é algo que será necessário repensar e reforçar no contexto da revisão regular e periódica atrás referida, sempre numa abordagem de colaboração e de procura pela excelência na implementação.

Q) - O factor humano continua a ser o «*tendão de Aquiles*». A este respeito, por um lado, comecemos com uma afirmação, curiosa, de Vint Cerf⁽⁵⁾: «(...) *“The thing I worry more than anything about is not the hackers and the people who are attempting to somehow change the function of the Internet. (...) Some of the worst problems that happen on the Internet are not because somebody deliberately caused the problem. It’s because somebody made a mistake. We’ve lost half the network’s ability to transport traffic or route it to the right destinations because somebody made a configuration mistake.”*». O que se passa? Ensino deficitário? Demasiada pressão organizacional focada no lucro? Incúria na segurança? *Maus* alunos?

P.V.) Em todas as áreas da segurança o factor humano é sempre um dos elos mais fracos. Na minha actividade de professor universitário costumo fazer analogias, na exposição nas aulas, com outros sectores da sociedade onde a segurança é um elemento crucial, tais como a segurança rodoviária, a segurança em edifícios ou a segurança contra os incêndios que nos devastam a cada verão. Nestas áreas podemos

5 Mais em: <https://www.washingtonpost.com/blogs/post-live/wp/2016/05/18/meet-father-of-the-internet-vinton-g-cerf/>

usar tecnologias fantásticas, mas se não forem aplicadas de modo adequado por todos os agentes envolvidos, o resultado final é desastroso. De que serve um automóvel ter *airbags*, ABS, cintos de segurança e muitos outros dispositivos de segurança se o condutor estiver distraído a usar um telemóvel, não respeitar um sinal de proibição de ultrapassagem numa curva ou um semáforo no vermelho? Também no ciberespaço existem soluções tecnológicas que podem mitigar muitos dos problemas que existem. Mas, se os gestores não estiverem cientes dos problemas não as aplicarão nas organizações e nas empresas que gerem, ou não atribuirão os recursos humanos e meios materiais necessários para garantir a cibersegurança organizacional. Os cidadãos não as usarão nos seus sistemas pessoais ou domésticos. Os técnicos informáticos não aplicarão as tecnologias necessárias por falta de meios materiais ou por puro desconhecimento. E a estonteante velocidade de evolução tecnológica, o crescente uso das tecnologias da informação em todos os sectores da nossa sociedade, não têm sido acompanhadas pela capacitação de recursos humanos em quantidade e com as competências necessárias, o que conduz a que o factor humano seja um dos principais problemas que urge resolver.

O nosso sistema de ensino não tem tido capacidade para formar todos os recursos humanos necessários para esta área; mais preocupante ainda quando aliado ao facto de os jovens não escolherem carreiras ligadas às tecnologias da informação e da comunicação (TIC). E isto parece um absurdo, na medida em que há muitas saídas profissionais nesta área e os estudos internacionais apontam para que o problema da falta de recursos humanos em TIC vá aumentar, em especial devido à, já referida, digitalização da economia. O CNCiber também procurará articular-se com outras iniciativas públicas e privadas para trazer mais recursos humanos para esta área tão promissora, aliciante, de elevada empregabilidade e desafiante.

Q) - Ainda e quanto ao factor humano. O comportamento e os hábitos, de uma grande parte dos *netizens* (autodidatas), resvalam para o risco. Como sabemos, o perigo não está somente no *software* e no *hardware*, mas, pelo contrário, antes e muito no *manware*. Sem uma formação de base mínima, muitas das vezes, pequenas dicas de comportamento *online* poderiam mitigar os efeitos associados a tais acções ou omissões. Poderá o CNCiber preencher esta falta de formação? Veja-se, por exemplo,

o caso dos EUA, no seguimento da campanha levada a cabo pelo *DHS (Department of Homeland Security)- Stop.Think.Connect*⁽⁶⁾, desde o seu lançamento em 2010, a mensagem de divulgação e sensibilização assume uma dimensão nacional. O objectivo é o de criar uma verdadeira compreensão destas ameaças virtuais, segundo o *DHS*. A mensagem, forte, apela ao esforço de todos, cidadãos, organismos públicos e privados. Complementada com alguns recursos tecnológicos, regra geral ao nível de *software*, ainda segundo o *DHS*, tem permitido assegurar aos cidadãos comportamentos, recursos e ferramentas essenciais à sua protecção e, indirectamente, do próprio Estado, contra as crescentes ameaças cibernéticas. Um modelo que poderemos seguir?

P.V.) Esta pergunta já foi, em parte, respondida anteriormente. Com efeito é crucial criar uma cultura de segurança no ciberespaço. Mas chegar a todos é um desafio monumental, que obriga a recorrer a meios e a instrumentos que são difíceis de serem geridos por um centro com a nossa dimensão e os nossos recursos. Mas é uma vertente que pode marcar a diferença, pelo que iremos tentar reunir esforços de outras entidades, como o sistema de ensino superior (politécnico e universitário) e não superior ou ainda, por exemplo, associações de vários tipos para podermos atingir os vários actores que são mais relevantes. Desde associações empresariais, associações sem fins lucrativos do terceiro sector ou empresas interessadas em contribuir para uma sociedade digital mais segura, tentaremos uma confluência de esforços e acções para que todos tenhamos um uso mais seguro do ciberespaço.

Q) – Quanto ao contexto empresarial. O CNCiber, sendo vitalíssimo para todas as nossas organizações, à semelhança da estratégia nacional de cibersegurança alemã⁽⁷⁾, poderia assumir uma postura activa - eventualmente por equipas especializadas CERT ou CSIRTS - de especial "policimento" e/ou apoio às nossas PME's⁽⁸⁾? Ainda a tempo

6 Disponível em: <http://www.dhs.gov/stopthinkconnect>

7 Em: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf>

8 Um *ciberpolícia* para as PME's? O tecido empresarial português é essencialmente composto por PME's. Precisamente pelo peso que estas representam na nossa economia e pela dimensão da sua estrutura - a qual mais das vezes relega a sua ciberprotecção para segundo plano - as recentes e constantes notícias sobre ataques de *ransomware* têm privilegiado o ataque a estas. Os riscos associados a tais omissões de protecção estarão devidamente consciencializados?

para construirmos um CNCiber útil e vital⁽⁹⁾, para que Portugal não perca as inúmeras potencialidades do, já prometido, Mercado Único Digital para a Europa, estará o caminho para essa construção e os objectivos últimos suficientemente definidos para a prossecução dos mais elementares fins do estado? E de todos?

P.V.) O CERT.PT, que foi criado no seio da FCCN enquanto a dirigi, é uma peça importante mas não a única. Claro que a existência de CERTs é reconhecida pela ENISA como de especial importância, mas há outras formas de preparação das organizações e de resposta a incidentes que podem ser exploradas. Aliás, várias iniciativas europeias sugerem o modelo de parcerias público-privadas para reforçar a capacidade de garantir segurança no ciberespaço. O modelo alemão é um dos que estudaremos para ver qual o mais adequado a Portugal. Não há modelos óptimos e o que venha a ser decidido deve ter em conta a estrutura e as entidades nacionais. Ainda e em relação ao caso que refere, da Alemanha, há dimensões que se justificam num estado federal e que não podem ser transpostos de modo directo para a nossa realidade. Mas, sem dúvida que o desenvolvimento do Mercado Único Digital exige, de todos, uma confiança acrescida em relação à segurança do ciberespaço.

Q) – Um pouco de contexto da política legislativa e a essencialidade de mecanismos legislativos de cibersegurança, eficientes, perceptíveis e concretos no terreno da acção, quer para juristas quer para engenheiros, quer para o utilizador-médio-comum. Reflexo da crescente dependência tecnológica, as infraestruturas críticas, enquanto manifestações essenciais no regular funcionamento do estado, encontram-se cada vez mais manietadas por esta, carecendo de uma efectiva e eficaz protecção (por cada dia que passa, a tónica deverá incidir mais sobre a ciberprotecção⁽¹⁰⁾). Só assim o Estado poderá estar melhor capacitado para alcançar os seus fins. Existirá uma percepção correcta, por parte da vontade política, sobre a necessidade de legislar sobre cibersegurança e sobre as nossas infraestruturas críticas?

9 Enquanto farol coordenador, especializado, entre o governo-sector público, as empresas, a academia e o cidadão.

10 Assustador? <http://exameinformatica.sapo.pt/noticias/internet/2016-05-24-Internet-das-coisas-em-Portugal-ha-redes-de-agua-gas-e-centrais-eletricas-sem-autenticacao>

P.V.) Em primeiro lugar e relativamente ao aspeto da “*vontade política*” tenho dificuldade em responder de modo directo, na medida em que as múltiplas dimensões dos problemas ligados ao *ciber* são tratados por muitas entidades e para umas o tema terá mais relevância do que para outras. Mas do ponto de vista da Ministra da Presidência e da Modernização Administrativa, que me desafiou para estas funções, sempre senti que atribui uma enorme importância a esta área, na medida em que o crescente uso da internet e dos paradigmas associados ao digital são fundamentais para uma administração mais ágil, eficiente e eficaz. Acresce que a directiva NIS, cuja versão final foi terminada há pouco tempo, contempla uma série de aspectos que têm de ser transpostos para a legislação nacional e que terão implicações em várias vertentes legais e em que muito trabalho terá de ser feito.

Em relação às infraestruturas críticas devo dizer que se trata de algo em que já estamos a desenvolver actividades, mais especificamente, com reuniões com várias entidades que têm responsabilidade em relação a este tipo de recursos, para ver como nos podemos articular para termos garantias de que são resilientes relativamente aos diversos desafios que podem surgir.

Q) – Por fim, a temática mais apetecível aos juristas: os Direitos fundamentais. Na senda da ideia da edificação de uma *Magna Carta*⁽¹¹⁾ para a internet, *Stefan Decker*, membro do Centro irlandês *Insight Centre for Data Analytics*, proferiu uma afirmação deveras pertinente. As pessoas «*are not looking for web protection and web privacy. They are looking for data protection and data privacy.*”⁽¹²⁾». Concorda? Protecção da rede e da sua privacidade, ou, Protecção de dados e da privacidade das pessoas? E por falarmos em protecção, com tantas formas, estaduais ou não, de interferência na normalidade *online*, no mundo *virtual* e no processo completo de transmissão da

11 <http://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy> e <http://www.networkworld.com/article/2688401/microsoft-subnet/tim-berners-lee-wants-internet-magna-carta-to-guarantee-netizens-privacy.html>

12 *Stefan Decker*, ao *Irishtimes* em: <http://www.irishtimes.com/business/technology/how-collective-insight-could-make-the-data-deluge-work-to-society-s-advantage-1.2108295>

Informação e na garantia da sua ulterior superioridade, até que ponto fará sentido a exigência de um centro nacional cripto?

P.V.) Concorde com a afirmação e queria salientar que é uma área em que creio que existem múltiplas dificuldades. E até diria que o que as pessoas querem é poder beneficiar do mundo digital em segurança, sem saberem, sequer, o que são dados. E estarem protegidos de intrusos ou criminosos.

É difícil o equilíbrio entre, por exemplo, o que está preconizado no documento do Conselho da Europa “Guia dos Direitos Humanos para os Utilizadores da Internet” e a necessidade da protecção e da segurança do ciberespaço. Diferentes entidades, públicas e privadas, ou diferentes indivíduos, consoante o seu domínio de responsabilidade e a sua visão do Mundo, têm diferentes abordagens sobre os instrumentos que se podem, ou não, usar para que o uso do ciberespaço seja de progresso para a humanidade. É algo em que tem havido défice de discussão e é algo onde ainda não tenho ideias sólidas sobre o papel que deve ter o CNCiber, especialmente porque o nosso mandato e os recursos que temos disponíveis não nos permitem abrir áreas de intervenção em todas as vertentes possíveis neste mundo cada vez mais digital. As alterações relativamente à protecção de dados, e que são da responsabilidade directa de outras entidades, também são uma das frentes a que temos que estar atentos pelas implicações que pode ter no modo como o ciberespaço se desenvolve.

Quanto ao Centro nacional de criptografia, não considero que seja necessária a existência de um centro assim. É uma área de investigação que deve ser financiada como outras áreas já são financiadas, numa base competitiva a nível nacional ou internacional, mas considero que a tecnologia criptográfica que existe a nível internacional é adequada às exigências de privacidade e segurança do ciberespaço. O que considero que é muito relevante é o uso livre, adequado e apoiado em tecnologias de *software* robustas que assegurem implementações sólidas.

CYBERLAW

by CIJIC

INTERNET GOVERNANCE ON THE MOVE

INTERNET GOVERNANCE EM MOVIMENTO

ROLF H. WEBER ¹

¹ Faculty of Law, University of Zurich.

RESUMO

Parece-nos evidente a necessidade de regulação da Internet por lei; o ciberespaço não poderá estar totalmente dissociado do espaço real (físico). Ademais, as actividades desenvolvidas na Internet, inevitavelmente, reflectem a sua influência sobre os indivíduos e sobre outras entidades no mundo real. Concomitantemente, o actual quadro regulamentar da Internet sendo traçado por diferentes legislações nacionais, orientações autorreguladoras e um número considerável de tratados multilaterais, apresenta graus variados de incidência. Pese embora nos últimos 20 anos tenhamos vindo a assistir a múltiplas actividades dentro do ecossistema de Internet Governance, quer a internet quer a sua governance, denotam um estado contínuo de desenvolvimento, que vale a pena observar com mais acuidade.»

Palavras-Chave: cosmopolitanismo; fragmentação; Multistakeholderism; Soft Law; Direito transnacional.

ABSTRACT

The necessity of the Internet's regulation by law seems clear; given that cyberspace cannot be entirely dissociated from real (physical) space, activities on the Internet inevitably have an influence on individuals and other entities in the real world. Accordingly, the existing regulatory framework of the Internet is composed of different national laws, self-regulatory guidelines and a number of multilateral treaties having relevance in varying degrees. Although within the last 20 years manifold activities within the Internet Governance ecosystem have been made, just as the Internet also the Internet Governance is in a continuous state of development that is worth to be looked at more closely.

Keywords: *Cosmopolitanism, Fragmentation,
Multistakeholderism, Soft Law, Transnational Law*

Table of Contents

1. Starting Point	
1.1 2015 Events	
1.2 2016 Challenges	
2. Tensions in the Regulatory Environment of Cyberspace.....	
2.1 General Principles vs. Detailed Norms	
2.2 Multilateral Agreements vs. Soft Law	
2.3 United Nations vs. United Constituencies.....	
2.4 Harmonization vs. Fragmentation	
2.5 Macrosystem vs. Microsystem.....	
3. Ongoing Hot Topics	
3.1 Cybereconomy	
3.2 Human Rights.....	
3.3 Cybersecurity	
4. Ongoing Important Platforms	
4.1 United Nations.....	
4.2 UNESCO and IGF.....	
4.3 Other Intergovernmental Bodies	
4.4 ICANN and IETF	
4.5 Multistakeholder Fora	
5. Outlook: Rise of Transnationalism	

1. STARTING POINT

1.1 2015 Events

Looking back to 2015 two main regulatory events are noteworthy, namely (i) the decisions of the United Nations (UN) and of UN special organizations to proceed with and intensify the cooperation in the field of Internet Governance and (ii) the ongoing efforts to make the transition of IANA functions to a new multistakeholder body a successful event.

(i) In December 2015, 193 governments participating in the UN General Assembly agreed on the so-called “WSIS 10+ Outcome Document” (A/Res/70/125).⁽¹⁾ Substantively the decision is an expression of the acknowledgment that the activities initiated by the two World Summits on the Information Society (WSIS) of 2003 (Geneva) and 2005 (Tunis) should be continued. In particular, the governments agreed to extend the mandate of the Internet Governance Forum (IGF) for another ten years, to strengthen the multistakeholder approach and to bring the next billion users online until 2010. Furthermore, the UN Group of Governmental Experts (GGE) expressed the intention to develop confidence building measures in order to improve cybersecurity. In addition, the collaboration between ITU and ICANN should be improved and the UN Human Rights Council appointed a new rapporteur on privacy in the digital age.

(ii) The self-regulatory approach of the Domain Name System has been the object of increasing criticism mainly by less developed countries. Since US-President Barack Obama announced in 2013 that the partly US “supervised” IANA functions could be transferred to a new multistakeholder body intensive efforts have been undertaken to work out the respective transition agreement. In 2015, within ICANN, the IANA Stewardship Transition Coordination Group (ICS) agreed on the details how to manage the transition of the IANA functions. The intensively discussed issue of the ICANN bodies’ accountability is still debated but in October 2015 a preliminary

1 United Nations, Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes, A/Res/70/125, adopted on 16 December 2015, online available at: <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf>.

agreement on a so-called “Designator Model” has been entered into by the members of the Cross Constituency Working Group on Accountability.⁽²⁾

1.2 2016 Challenges

In particular, the decision of the UN General Assembly can be seen as a milestone in the further development of the IGF and the multistakeholder approach. Nevertheless, the mentioned understandings reached in 2015 constitute “agreements in principle” having the consequence that many details are still not settled or even quite open. Political tensions due to different understandings of public policy will continue in 2016. Therefore, the design of the legal framework for cyberspace merits further attention. Different regulatory approaches are to be balanced in view of the ongoing hot topics and the existing established platforms.

In 2016, the net community could celebrate the 20th anniversary of the “Declaration of Independence of Cyberspace”, emphatically proclaimed by John Perry Barlow in February 1996.⁽³⁾ But in the meantime it has become clear that many wishes of Barlow remain unfulfilled,⁽⁴⁾ even if the Internet has indeed created a new world with many benefits, challenges and risks.

The following contribution attempts to shed light on the regulatory environment in Internet Governance and to path ways for future successful actions in this field. On that regard, the existing tensions in the cyberspace’s regulatory environment particularly need to be discussed in respect of aspects like cybereconomy, human rights, cybersecurity and the ongoing platforms’ actions.

2 See Wolfgang Kleinwächter, Internet Governance Outlook 2016: Cooperation & Confrontation, online available at: http://www.circleid.com/posts/20160111_internet_governance_outlook_2016_cooperation_confrontation/.

3 John Perry Barlow, A Declaration of Independence of Cyberspace, 8 February 1996, online available at: <https://www.eff.org/de/cyberspace-independence>

4 Rolf H. Weber, Realizing a New Global Cyberspace Framework – Normative Foundations and Guiding Principles, Zurich 2014, p. 17

2. TENSIONS IN THE REGULATORY ENVIRONMENT OF CYBERSPACE

A philosophical and sociological assessment of the regulatory environment of cyberspace allows to identify several theoretical tensions occurring between different normative systems. Before discussing the ongoing developments in the cyberspace area it appears to be valuable to theoretically analyze the respective tensions.

2.1 General Principles vs. Detailed Norms

Rule-making can be conceptualized in two different ways: On the one hand, general principles are able to provide for a normative framework designing guidelines for an expected fundamental behavior; on the other hand, detailed norms specify the concrete behavior expected from the addressees of the regulations.

(I) General principles need to be founded on very basic values such as good faith, public interest, or the proportionality principle. As a consequence, the addressees remain with a relatively wide area of discretion in the implementation of the principles. Correspondingly, the addressees are responsible to comply with the general guidelines in a suitable and reasonable way. A liberal interpretation is possible as long as the underlying objectives of the principles are observed. In the field of Internet Governance a special positive feature of this approach consists in the independence from the vast technological advances: The general principles are applicable notwithstanding the prevailing technology and changes in the techniques do not have an immediate repercussion on the regulations.⁽⁵⁾

(II) Detailed rules give clear and precise directives to the addressees. If properly drafted, such provisions should not lead to major interpretation problems since they regulate specific situations. Apart from the length of detailed rules, an important

⁵ For a general overview see Marcelo Thompson, *Evaluating Neutrality in the Information Age – On the Value of Persons and Access*, Oxford (Bodleian) 2013.

weakness of this approach consists in the dependence from the given technology; a change therein might lead to the need of adapting the regulatory framework.

2.2 Multilateral Agreements vs. Soft Law

The traditional legal instruments dealing with global issues are multilateral agreements. Ideally, most (at least the concerned) countries ratify and implement the respective normative frameworks. In reality, however, unanimous consent cannot easily be achieved. Good examples of the past are the telecommunications regulations under the auspices of the International Telecommunications Union (ITU) and the international trade regulations designing the framework of the World Trade Organization (WTO).⁽⁶⁾

In the Internet Governance field multilateral agreements covering a broad field of topics do not exist. Moreover, the normative framework is based on so-called “soft law”. This situation with “half-governmental” rules has revitalized the relatively old discussion to what extent “hard law” is necessary and to what extent “soft law” could exercise a substituting function, respectively. Indeed, a robust regulatory system does not necessarily have to be founded on hard law.⁽⁷⁾

Soft law is a model developing and establishing rules independently of the principle of territoriality, mainly through the concerned organizations; in accordance with the subsidiarity principle the concerned participants of a specific community are attempting to achieve suitable solutions themselves.⁽⁸⁾ The legitimacy of soft law is based on the fact that private incentives lead to a need-driven rule-setting process. Therefore, soft law is justified if it is more efficient than hard law and if compliance with traditional hard law is less likely than compliance with self-regulatory rules.⁽⁹⁾

6 See Rolf H. Weber, Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises, *Journal of Governance and Regulation*, Vol. 1/1, 2012, p. 8, p. 10.

7 Weber (supra note 6), pp. 10/11.

8 For a general overview see Chris Brummer, *Soft Law and the Global Financial System: Rule Making in the 21st Century*, 2nd ed. New York 2015.

9 Weber (supra note 6), p. 12.

As far as the legal quality of soft law is concerned, it should not be underestimated that soft law can encompass several functions previously tied to hard law. Therefore it is arguable that the notion of legalization entails a specific form of discourse as far as justification for certain rules is concerned; furthermore, the often expressed assumption that hard law is qualitatively better than soft law does not hold anymore in today's environment of Internet Governance.⁽¹⁰⁾

2.3 United Nations vs. United Constituencies

Developments in many political fields have shown that the State-centric approach of traditional international relations does not anymore fulfil the requirements of today's regulatory needs. In particular, the involvement of other stakeholders apart from States is suitable in order to improve the quality of rule-making. Even if the approach as such is known for many decades, the most recently coined term is called "*multistakeholderism*": This concept attempts to include all potentially concerned stakeholders in the relevant decision-making processes.⁽¹¹⁾

The first international organization to recognize the relevant role of multiple stakeholders in the discussion of global issues was the International Labor Organization (ILO) having created a model including representatives from governments, employers and unions. The ITU also accepted the participation of private telecommunications providers in its deliberations. The probably best known example for a multistakeholder undertaking in the past was the World Conference on Environment and Development (UNCED) held in Rio de Janeiro (1992). The stakeholders of many segments were invited to discuss and integrate different views and interests to realize practical solutions leading to a more sustainable world. More recently, the multistakeholder concept has again been taken up by the UN Commission on Sustainable Development (CSD) in the context of the "Agenda 21" that envisages different stakeholders' roles in a global sustainability arrangement.⁽¹²⁾

10 Weber (supra note 6), p. 11.

11 Rolf H. Weber, Legal foundations of multistakeholder decision-making, ZSR 2016 I, pp. 259 et seq.

12 See Virgilio Almeida/Demi Getschko/Carlos Afonso, The Origin and Evolution of Multistakeholder Models, IEEE Internet Computing 2015, Vol. 19, p. 74, 75.

In the context of Internet Governance, the multistakeholder approach goes back to the Report of the Working Group on Internet Governance” (WGIG) which introduced a widely accepted working definition of multistakeholder Internet Governance referring to the “development and application by governments, the private sector, and civil society, in their respective role, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet”.⁽¹³⁾ Based on this notion some five years ago a sophisticated model composed of the “United Nations” encompassing sovereign States and international organizations and of the “United Constituencies” representing networks, non-governmental groups, businesses, technical/academic communities and civil society was developed. Even if the two governance cultures are rather different, they do not need to be antagonistic, but can co-exist in a meaningful way. A formal and rough comparison between the “national hierarchies” of the “United Nations” and the “global networks” of the “United Constituencies” could be designed as follows:⁽¹⁴⁾

Issue	United Nations	United Constituencies
Actors	Governments	Private Industry/Civil Society
Structure	Hierarchies	Networks
Codification	National Laws	Universal Codes
International Agreements	Legally Binding Treaties	Memorandum of Understanding
Mission	Broad	Narrow

13 Report of the Working Group on Internet Governance, June 2005, p. 4, online available at: <http://www.wgig.org/docs/WGIGREPORT.pdf>.

14 Wolfgang Kleinwächter, A new Generation of Regulatory Frameworks: The Multistakeholder Internet Governance Model, in: Rolf Sethe et al. (Eds.), Kommunikation, Festschrift für Rolf H. Weber, Bern 2011, p. 559, pp. 571/72.

Policy Development	Top Down	Bottom Up
Decision-Making	Formally specified Majority Voting	Informally specified Rough Consensus
Representation	Elections by All	Delegation by competent Constituencies or via NomComs
Policy-Making	Formally Restricted Access and limited Participation	Formally Open Access and broad Participation
Negotiations	Mainly closed to outsiders	Mainly transparent and open for outsiders
Result	Stability and Predictability	Flexibility

The table shows that both the “real places” and the “virtual places” are linked to each other. Since reality does not allow a separation, an objective need for collaboration in a multistakeholder model is given. Thereby, all stakeholders need to recognize the dynamic nature of their respective roles in the cyberspace environment. Not only do new actors appear and have to be integrated, but also iterative consultation processes and governance workflows change over time. Appropriate participatory processes need to ensure inclusive participation by fighting information overload, by synthesizing debates, by preventing capture(s), and by complying with the neutrality principle.⁽¹⁵⁾

15 Weber (supra note 4), p. 135.

2.4 Harmonization vs. Fragmentation

The Internet is a global information and communication network. Therefore, ideally, its governing rules would also be globally acknowledged. In part, mainly as far as technical standards are concerned, coherence is needed in order to allow cross-border data delivery. Since the infancy of the Internet, requirements related to protocols and domain names are harmonized based on technical recommendations of the Internet Engineering Task Force (IETF).

Such kind of harmonization is more difficult to achieve in respect of issues having a social and political nature. But generally, interventionist measures of Nation States have become more frequent during the last few years, often with the objective to “protect” the own civil society from foreign influence. Tendencies to split the global network into smaller parts (national Internet segments, special Internet economic zones) through firewalls and wallet gardens cannot be overlooked. The building of fences around sub-systems can be justified in order to secure the functionality of the specific services, at least in the form of checkpoints avoiding the access to the dark side of the Internet.

However, the re-erection of frontiers should not jeopardize the developments that have enhanced the individual rights/freedoms and the social/economic advances (innovation) of the last twenty years.⁽¹⁶⁾ For good reasons, therefore, fragmentation has become subject of scholarly research; in the recent past concerns have been expressed about the Internet being in some danger of breaking up into “loosely coupled islands of connectivity”.⁽¹⁷⁾

2.5 Macrosystem vs. Microsystem

Similarly to the distinction between macroeconomic and microeconomic elements in the societal developments, a differentiation can be made between the

16 Kleinwächter (supra note 2).

17 See William Drake/Vint Cerf/Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, January 2016, p. 3, online available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

macrosystem and the microsystem in Internet Governance. The not identical topics of the two systems are also reflected in the differing actors being involved.

The macrosystem addresses substantive issues such as cybereconomy, human rights, and cybersecurity. Since these issues have a global reach, the platforms and fora for negotiations, discussions and decision-making procedures must also be global. Looking from a general perspective, the respective normative framework mainly encompasses substantive/material issues.⁽¹⁸⁾

The microsystem relates to the more formal operating structure of the Internet as the most important international data exchange network and encompasses the issues of names/numbers and of protocols. In this field, private initiatives and expertise are of major relevance. Taken from a general point of view this system rather entails operational and procedural issues.⁽¹⁹⁾

18 See below Ch. 4.1-4.3.

19 See below Ch. 4.4.

3. ONGOING HOT TOPICS

3.1 Cybereconomy

Without any doubt, the digitization of private and business life is a major achievement of the last twenty years. But the full benefits of the digitization depend on the global access to the infrastructure. Therefore, with good reasons the “WSIS 10+ Outcome Document”⁽²⁰⁾ pleaded for bringing the next billion Internet users online. In particular the European Commission, for example in its Agenda for a Digital Market Strategy of May 2015, pointed out that the development of a digital economy is crucial for economic growth and job creation.⁽²¹⁾

The European Union is keen of bringing Europe up to speed in the digital ecosystem even if some past initiatives have not been very successful. Otherwise, Europe risks of being dominated by a US-China digital race with the Silicon Valley giants (Google, Facebook, Apple, Amazon, eBay) on the one hand and the Chinese giants (Baidu, Weibo, Alibaba, Tencent) on the other hand.⁽²²⁾

Cybereconomy requires the possibility to trade goods and services without being confronted with impediments such as trade barriers. The international trade framework has been established by the WTO, however, improvements in the regulation of digital trade have hardly been made during the last ten years. As a consequence, regional trade agreements such as the Trans-Pacific Partnership Agreement (TTP) and the Transatlantic Trade and Investment Partnership Agreement (TTIP) as well as bilateral treaties are concluded in order to overcome the standstill in the WTO negotiations. Nevertheless, such preferential trade agreements lead to a fragmentation

20 See note 1 above.

21 European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 6 May 2015, online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192>.

22 See also Kleinwächter (supra note 2).

of the legal landscape; providers of goods and services always have to check which country is covered by which regulatory regime.⁽²³⁾

A further cross-border problem has arisen in connection with data protection. Obviously, privacy is a fundamental right and the protection of the personality constitutes an important value. From a cybereconomy perspective, however, data protection could (at least theoretically) become a trade barrier if the applicable regulations substantially differ between countries.⁽²⁴⁾ This assessment does not mean that privacy considerations should be given up but an obvious need exist to attempt at achieving harmonized data protection standards.

3.2 Human Rights

At the end of 2013 the UN Human Rights Council agreed that human rights should apply in the online world equally as in the offline world.⁽²⁵⁾ This principle has been reconfirmed by the governments in the “WSIS 10+ Outcome Document”: The UN Resolution 70/125 reiterates the principle of equal level of protection and also links the WSIS process to the Millennium Development Goals (MDG).

If an agreement on fundamental principles exists, its implementation in reality is often more cumbersome. As already mentioned, governments have different appreciations of privacy around the globe. In the post-Snowden era it has also become obvious that the issue of mass surveillance to fight criminals and terrorists is not identically interpreted by the governments around the world. Furthermore, many examples show that notions such as “public order” or “illegal content” are quite

23 Rolf H. Weber, Digital Trade and E-Commerce: Challenges and Opportunities of the Asia-Pacific Regionalism, Asian Journal of WTO & International Health Law and Policy (AJWH), Vol. 10, 2015, pp. 321-347.

24 Rolf H. Weber, Regulatory Autonomy and Privacy Standards under the GATS, Asian Journal of WTO & International Health Law and Policy (AJWH), Vol. 7, 2012, pp. 26-47.

25 United Nations, The right to privacy in the digital age, A/RES/68/167, adopted on 18 December 2013, online available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

differently understood and applied in the UN countries, usually depending on the political and social system.⁽²⁶⁾

The strengthening of human rights also means that in less developed countries more people should have online access: in 2015, more than 80% of the developed world was online, but only 34% of the developing countries. The “WSIS 10+ Outcome Document” correctly states that bridging the digital divide “requires greater sustainable investment” (para 35), that “private investment” is “critical” (para 38), and that “an ongoing evaluation of “new innovative financing options” is needed (para 40). But the realization of these objectives, even if unanimously agreed upon, remains quite open.

3.3 Cybersecurity

Peace is a general objective of the UN since 1945. In particular, Chapter 7 of the UN charter gives the governments a right to self-defense in cases of an attack. The problem with this provision consists in the fact that “cyberwar” is not a generally acknowledged term. In the physical world, war leads to death, destruction, and damages but neither the attack against Estonia (2007) nor the Stuxnet case (2010) caused death and destruction. Therefore, the rights of individual Nation States in case of cyberattacks are uncertain.⁽²⁷⁾

The UN Group of Governmental Experts (GGE) agreed on a set of confidence building measures in cyberspace⁽²⁸⁾ however, these measures are not generally acknowledged as legally binding instruments for cybersecurity. The Budapest Convention on Cybercrime released by the Council of Europe⁽²⁹⁾ and signed by many Western countries has not been ratified by politically important countries like China, Russia, India and Brazil, i.e. its scope of application is limited. The Shanghai

26 Kleinwächter (supra note 2).

27 Kleinwächter (supra note 2).

28 United Nations Group of Governmental Experts (UN GGE), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, online available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

29 Council of Europe, Convention on Cybercrime, 23 November 2001, online available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf.

Cooperation Organization (SCO) has announced to be interested in negotiating a new treaty under the auspices of the UN; so far, however, progress has not been made.

The “WSIS 10+ Outcome Document” states that the members will “review their procedures, practices and legislation regarding the surveillance of communications, as well as their interception of personal data, including mass surveillance” (para 46). This wording is derived from the NETMundial Declaration of April 2014 (São Paulo).⁽³⁰⁾ Again, the practical implementation of the principle is difficult. How can mass surveillance directly and justifiably be targeted at combating terrorism to be differentiated from illegal espionage? Countries around the globe also do not share a consensus about the notion of “terrorism”.⁽³¹⁾

30 NETmundial Multistakeholder Statement, 24 April 2014, p. 4, online available at: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

31 See also Kleinwächter (supra note 2).

4. ONGOING IMPORTANT PLATFORMS

4.1 United Nations

After the adoption of the “WSIS 10+ Outcome Document” in the UN General Assembly the practical work on Internet Governance is now conducted by the UN Commission for Science and Technological Development (UNCSTD). The UNCSTD is vested with enlarged functions and a more important role in cooperation with other international bodies.⁽³²⁾ In particular, the Working Group on Enhanced Cooperation (WGEC) is reactivated and mandated to produce a report about Internet Governance matters for the UN General Assembly in 2017 (Session 72). The WGEC is a multistakeholder body allowing all participating members to act on equal footing. In contrast, the UNCSTD is still an intergovernmental body and allows the participation of non-governmental stakeholders only to a very remote extent.⁽³³⁾

During the UN General Assembly 2016 (Session 71) three reports are expected to be discussed, namely the GGE-report on cybersecurity (Committee 1), the UNCSTD-report on economic and social developments (Committee 2) and the report of the special rapporteur on privacy/human rights (Committee 3).⁽³⁴⁾

4.2 UNESCO and IGF

UNESCO has become more active in the field of Internet Governance during the last few years. In 2014 a special framework encompassing several important elements of Internet Governance was published (so-called R-O-A-M approach, standing for Rights, Openness, Accessibility, and Multistakeholder).⁽³⁵⁾ In 2015 a special rapporteur delivered a hundred pages comparative analysis of Internet Governance frameworks and guidelines.⁽³⁶⁾ In addition, UNESCO called all

32 See <http://unctad.org/en/Pages/CSTD.aspx>.

33 See <http://unctad.org/en/Pages/CSTD/WGEC.aspx>.

34 Kleinwächter (supra note 2).

35 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_university_en.pdf; see also Weber (supra note 4), p. 142.

36 Rolf H. Weber, *Principles for governing the Internet: A comparative analysis*, UNESCO Series on Internet Freedom, Paris 2015.

stakeholders for an important conference “Connecting the dots” in Paris (March 2015). UNESCO is particularly suited to promote Internet Governance issues since this UN organization is strongly devoted to social, cultural, educational, and development issues.

For quite some time it was not certain whether the IGF would survive after the first ten years’ period. With the mentioned decision of the UN General Assembly of December 2015 it is now clear that the IGF will be held for another ten years, the next time in December 2016 in Guadalajara (Mexico). This assurance for a long-term institutionalization facilitates the organizers of the IGF to tackle new topics and to initiate additional policy-making projects, subject to the availability of sufficient financial resources. Furthermore, the foundational ideas of the IGF have successfully spread out to the regions (for example EURODIG, the European IGF) and to a large number of countries knowing a national IGF.⁽³⁷⁾

4.3 Other Intergovernmental Bodies

The OECD mainly representing the Western world addresses its attention to issues of digital trade; as mentioned, the respective rules do have an impact on Internet Governance debates. Some initiatives such as the OECD Principles for Internet Policy Making (2012) did not reach full acceptance but new efforts to be taken at the Cancun Summit of June 2016 might lead to further harmonization attempts in the assessment of digital trade and Internet Governance.⁽³⁸⁾

The G-20 meeting and the G-7 meeting are supposed to take up topics like cybersecurity, digital trade and human rights in 2016. Further intergovernmental organizations, particularly regional organizations such as the Council of Europe, the OSCE, the OAS, the APEC, and the African Union, also look at Internet Governance issues.⁽³⁹⁾

37 For example, most of the European countries hold a yearly national IGF.

38 See <https://www.oecd.org/forum/>.

39 For more details see Kleinwächter (supra note 2).

4.4 ICANN and IETF

Similarly to 2015, the gTLD program again plays an important role in the ICANN agenda of 2016. However, as the ICANN meeting in Dublin (October 2015) and in Marrakesh (March 2016) have shown more emphasis will now be put to the completion of the IANA transition.

After the Marrakesh meeting, the National Telecommunications and the Information Administration (NTIA) of the US Department of Commerce was notified that the agreed mechanisms should now be put in place. This step has been celebrated as one of the most successful outcomes of the multistakeholder approach. Whether all activities can be finalized prior to 30 September 2016, the date of termination of the existing contract, remains to be seen. This assessment is based on the assumption that the US Congress also wants to consider the final package (although a formal approval of the US Congress is not needed). In particular, the US presidential election can cause certain drawbacks for political reasons.

ICANN also needs to tackle organizational questions such as the accountability issue. On 10 March 2016, the ICANN board submitted a plan developed by the international Internet community to the U.S. Government, among others containing recommendations on how to enhance the organization's accountability.⁽⁴⁰⁾

Furthermore, the newly established "Competition, Consumer Trust and Choice Review Team" (CCT-CRT) is burdened with many tasks. Representing an array of geographic regions and areas of expertise the review team's 17 members are expected to complete a final draft of the CCT-CRT's report by December 2016.⁽⁴¹⁾

The IETF realized that new challenges in respect of how standardization could move forward will have to be met. As mentioned, privacy issues in protocols do have

40 IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations, 10 March 2016, online available at: <https://www.icann.org/en/system/files/files/iana-stewardship-transition-package-10mar16-en.pdf>.

41 See <https://www.icann.org/news/announcement-2-2015-12-23-en>.

political, cultural and social implications. Furthermore, new technical aspects are worth to be dealt with.⁽⁴²⁾

4.5 Multistakeholder Fora

A large number of multistakeholder fora have been established during the last few years. Activities can be expected from the following platforms:⁽⁴³⁾

- The New Mundial Initiative (NMI) has the task to implement the principles and the roadmap of the NETMundial conference, particularly the strengthening of the multistakeholder approach.
- The World Economic Forum (WEF) has initiated the project “Future Internet Initiative” (FII) in 2015. Topics of the FII are the digital transformation of industries, digital trade and strategies, cybersecurity, Internet for all, etc.; at the Davos meeting in January 2016, a first rather extensive report on Internet fragmentation was presented.⁽⁴⁴⁾
- The Global Internet Governance Commission (GIGC), managed by Chatham House and the Center for International Governance Innovation (CIGI), is preparing a final report on the governance of the future Internet (June 2016). In addition, CIGI is producing a series of very valuable expert papers.⁽⁴⁵⁾
- The Global Forum for Cyber Expertise (GFCE), initiated by the Dutch government in 2015, attempts to prepare a declaration on cybersecurity issues. Notwithstanding several conferences, the document is not yet agreed upon but work of governments and big private companies is advancing.

42 For more information regarding the IETF’s recent activities see <https://www.ietf.org/>.

43 For more details see Kleinwächter (supra note 2).

44 See Drake/Cerf/Kleinwächter (supra note 17).

45 See <https://www.cigionline.org/publications/cigi-papers>.

- The Freedom Online Coalition (FOC), established in 2011, has the objective to promote human rights in cyberspace; the FOC has working groups producing policy recommendations and has already published two documents on human rights.
- The Wuzhen Internet Initiative (WII), initiated at the World Internet Conference in Wuzhen (December 2015) by the Chinese government, attempts at enhancing the role of China in the global Internet Governance framework. The WII is mainly driven by governmental efforts but ignores the multistakeholder approach driven by the IGF and the NETMundial declaration.

Apart from the mentioned multistakeholder fora, a large number of Internet Governance programs and projects are going on. The respective activities encompass research, knowledge production, documentation, and education. The outcome should serve policy makers, civil society, technical experts, and business leaders in their attempt to deal with the relevant issues in the Internet ecosystem. The following projects fall into this category:⁽⁴⁶⁾

- The Global Internet Governance Academic Network (GigaNet), already implemented in 2006, assembles a large number of Internet Governance experts from almost all countries around the World; GigaNet regularly organizes an annual symposium back-to-back to the IGF and additional regional conferences; many research books and papers have been published based on these events.
- The Geneva Internet Platform (GIP), initiated by the Swiss government close to many international organizations in Geneva and managed by Diplo Foundation is very active in capacity building programs and documentation of the manifold Internet Governance events attracting a large number of diplomats.

46 Kleinwächter (supra note 2), p. 9.

- The Global Internet Policy Observatory (GIPO) has been launched by the European Commission in 2013 and provides for an Internet Governance database.
- The Internet & Jurisdiction Project (I&J Project) in Paris is making available a large (permanently increasing) database related to multistakeholder processes and to jurisdictional issues (transnational cooperation).
- Since 2007, the Summer School on Internet Governance (SSIG) in Meissen (Germany) offers high level multistakeholder education; similar educational facilities are now also established in Latin America, Africa and Asia.

This short overview evidences that Internet Governance debates are not anymore restricted to a small circle of specific experts but spread out to large communities of multistakeholder participants around the world.

5. OUTLOOK: RISE OF TRANSNATIONALISM

The aforementioned description of the manifold activities within the Internet Governance ecosystem shows that valuable guidance can be drawn from the observance of general substantive principles being conceptually able to complement the existing formal structures. As Fukuyama said more than ten years ago, modern constitutional structures and the rule of law were established to limit discretion in the exercise of governmental power.⁽⁴⁷⁾ Assuming that this kind of political system is effective in implementing cosmopolitical principles of good governance, an appropriate policy framework must encompass those values that motivate both democratic and sound governance on the global level.⁽⁴⁸⁾ In delineating the respective substantive principles a stronger focus should be directed to the concept of transnationalism. In overcoming the State-centricity of traditional law, collective regulation operating among economic actors or social actors with transnational ties must gain importance.

Transnational law allows designing governance patterns in not coherent structures. The presence of transnational law also indicates a flow of legal rules that is dynamic in form and contents and includes understandings from non-state actors. Therefore, globalization of legal developments involving manifold legal sources leads to a shift of the locus of political engagement from sovereign States to functional regimes.⁽⁴⁹⁾ Norms put into the pipeline of “*transnationalization*” and achieving normativity in international relations do have important common characteristics⁽⁵⁰⁾ such as legitimacy, transparency, and accountability, i.e. foundational characteristics of a sound Internet Governance ecosystem.

47 Francis Fukuyama, *State Building – Governance and the Order in the Twenty First Century*, London 2004, pp. 98/99.

48 See Rolf H. Weber, „Cosmopolitically“ Founded Concepts for the Cyberworld, in Giovanni Biaggini et al. (eds.), *Festschrift für Daniel Thürer*, Zürich 2015, p. 779, p. 781.

49 See Martti Koskenniemi, *The Politics of International law – 20 Years Later*, *European Journal of International Law*, Vol. 20, 2009, p. 7, p. 11.

50 See also Weber (supra note 48), pp. 781/82.

CYBERLAW

by CIJIC

REFLECTIONS ON INTERNET GOVERNANCE AND REGULATION WITH SPECIAL CONSIDERATION OF THE ICANN *

REFLEXÕES SOBRE O GOVERNO E A REGULAÇÃO DA INTERNET COM PARTICULAR ÊNFASE SOBRE A ICANN

LUÍS DE LIMA PINHEIRO ¹

* - A first version of this work has been published in the *Estudos de Direito Intelectual em Homenagem ao Professor José de Oliveira Ascensão*, Coimbra, 2015.

¹ Full Professor at the Law School of the University of Lisbon

SUMMARY:

INTRODUCTION.....	
I. INTERNET GOVERNANCE AND REGULATION.....	
A) Internet governance.....	
B) Internet regulation.....	
II. ICANN EVOLUTION IN THE PERSPECTIVE OF A MULTISTAKEHOLDER MODEL.....	
A) ICANN scope of activity and the domain names system.....	
B) Characterization of the ICANN and the stewardship of the domain names system.....	
C) Formal issues of the ICANN evolution.....	
D) Substantial issues of the ICANN evolution.....	
III. FINAL REMARKS.....	

ABSTRACT

This article is focused on very general issues of Internet governance and regulation and on the potentialities of the adopted general conceptions with respect to the ICANN evolution. It advocates for an autonomous governance of the Internet, based upon a model of multistakeholder and globalized organizations. This autonomous governance is connected with a co-regulation of the Internet, through a combination of the principle of autonomous regulation with public regulation in all areas where autonomous regulation is insufficient. This public regulation should be fundamentally of international source. Regarding the evolution of ICANN, it is considered the very recent Proposal to Transition the stewardship of the Internet Assigned Numbers Authority (IANA) functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community and suggested the assumption by ICANN of the political role of a Non-Governmental Organization and the conclusion with the interested States and international organizations of standard quasi-treaties containing appropriate arbitration clauses.

Keywords: Internet governance; Internet regulation; ICANN; Domain name; Control of the Domain Name System

INTRODUCTION

Internet governance may be understood in a broad sense as comprising the legal regulation of the Internet as well as the organization and the action of the entities that coordinate its operation ⁽¹⁾. It is beyond doubt that these aspects are connected, but it seems appropriate to distinguish them, reserving the term “governance” for the institutional coordination of the network.

The *Internet* is a worldwide decentralized network of open computer networks that share a common communication technology. Its *genesis* still has today significant influence on the manner in which it is governed and regulated. The Internet was born in the U.S.A. as a project of the *Advanced Research Project Agency*, linked to the Defense Department ⁽²⁾. Since then, it has been developed through the interconnection of the networks created mainly by the civil society, giving rise to decentralized governance and regulation essentially carried out by autonomous entities. These entities undertake the task of assuring its operation and development, especially in respect to the definition of standards concerning communication protocol and the allocation and assignment of domain names and addresses that identify the computers connected to the network, working together with the U.S. Administration.

With the *globalization of the Internet*, its growing importance as a means of communication and information in all the spheres of social, political, economic and cultural life, these marks of origin raised new challenges. In face of its primarily private nature, the challenge of coordination with the values and policies pursued by the States and international organizations. Before the decentralized structure of the net governance and regulation, the need to ensure its internal consistency. Last but not the least, given the umbilical link with the U.S. Administration, the concern with the globalization and even, for some, with the intergovernmentalization of the entities that coordinate the Internet.

1 - See the conclusions of the United Nations Summit on the Information Society – Geneva 2003/Tunis 2005, in <http://www.itu.int/wsisis/index.html>.

2 - See “A Brief History of the Internet”, in <http://www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet>.

Presently, the Governments of the main democratic countries, namely at the EU and USA level, ⁽³⁾, as well as the main fora in which the global Internet community has found its expression ⁽⁴⁾, converge towards a multistakeholder model of Internet governance, which includes not only Governments and international organizations, but also the civil society, namely the academic and technical communities, the economic actors, and the associations of Internet users. This does not exclude, naturally, some divergence in the details of this model.

This multistakeholder model corresponds, at the regulation level, to a co-regulation in which the applicable rules are created primarily by autonomous sources which are the expression of the Internet global community, but which needs to be complemented by State and supranational regulation.

This multistakeholder model should, for instance, be applied to the entity which coordinates the systems of exclusive identifiers of the Internet: the *Internet Corporation for Assigned Names and Numbers* (ICANN). It has just been delivered a proposal by the *IANA Stewardship Transition Coordination Group* to transfer the stewardship of the functions concerning the domain name system to the Internet multistakeholder community that must be referred in this context.

This article will focus, in first place, on very general issues of Internet governance and regulation (I). Thereafter, it will examine the potentialities of the adopted general conceptions in respect to the ICANN evolution (II). It will conclude with a few general remarks (III).

3 - See Communication from the European Commission "Internet Policy and Governance Europe's role in shaping the future of Internet Governance" COM (2014) 72 final and *Press Release* of the U.S. Commerce Department's *National Telecommunications and Information Administration (NTIA)* of 14/3/2014.

4 - See, namely, the *NETmundial Multistakeholder Statement* issued by the *Global Multistakeholder Meeting on the Future of Internet Governance* held in Brazil in 2014, in <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>, the *Report by the Panel on Global Internet Cooperation and Governance Mechanisms* "Towards a Collaborative, Decentralized Internet Governance Ecosystem", 2014, in http://Internetgovernancepanel.org/sites/default/files/ipdf/XPL_ICAN1403_Internet%20Governance%20iPDF_06.pdf, and the "Perspectives on the IANA Stewardship Transition Principles", issued by the *Internet Society* in 2015, in http://www.Internetsociety.org/sites/default/files/IANA-Transition-Perspectives-20150728-en_0.pdf.

I. INTERNET GOVERNANCE AND REGULATION

A) Internet governance

As a global reality, the Internet should be subject to a prevailing global governance and regulation ⁽⁵⁾. The main alternative that arises in this context is between intergovernmentalization and globalization based upon a model of participation of all the interested parties ⁽⁶⁾. It is in the light of the *policies that should guide Internet governance* that the issue must be considered.

Internet governance should, in the first place, assure the unity, openness, gratuity and freedom of access to the Internet, countering the tendencies to segment or restrict access to the Internet by countries that intend to limit the freedoms of expression and information on the net.

Internet governance should also grant efficiency, stability and security in the operation of the net, taking as much advantage as possible of the entities and expertise that have been providing it, and preserving the innovative spirit that has been shaping Internet development.

Last but not the least, Internet governance should allow sufficient participation in decision-making processes by the entities that are in charge of the pursuance of public legitimate interests as well as an appropriate coordination between the autonomous mechanisms of governance and regulation and the exercise of normative powers of States and international organizations.

There is no intergovernmental organization in position to adequately assume the tasks of Internet governance. The Internet, affecting many aspects of social life, also touches the sphere of action of several intergovernmental organizations, as it is the case of the World Trade Organization (WTO), but the scope of activity of organizations like these does not embrace the central issues of Internet governance and regulation ⁽⁷⁾.

5 - See, namely, the remarks I made in “Portugal, Europe and Globalization in the Private Law Perspective”, in *Portugal, Europe and the Globalization of the Law*, ed. by Vasco Pereira da Silva, 46-57, Ebook, Lisbon, 2015 (also accessible in SSRN: <http://ssrn.com/abstract=2465349>, 52-53, with more remarks.

6 - On the different Internet governance models, see Michael RUSTAD – *Global Internet Law*, 2nd ed., St. Paul, MN, 2016, 94 et seq.

7 - See also Pedro MIGUEL ASENSIO – *Derecho Privado de Internet*, 5th ed., Cizur Menor (Navarra), 2015, 43-44.

The intergovernmental organization that could be more suited for this purpose is the International Telecommunication Union (ITU), which is today a specialized agency of the United Nations ⁽⁸⁾. Among other areas of activity, the ITU develops the communications infrastructure's technical standards of operation. The ITU aims to extend its activity to the technical standards of all the technology of information and communication, but its organizational structure, based upon representatives of the Member States with equal voting rights, is unsuited for the reality of the Internet.

As remarked by Miguel Asensio ⁽⁹⁾, the ITU does not seem able to overcome the divergence that arises at the international scale regarding protection of fundamental and intellectual property rights on the Internet and the warranty of access and information exchange in the net by everybody. This has been expressed by the refusal of a high number of States, among which the EU Member States, the U.S.A., and Japan to sign the Final Acts of the World Conference on International Telecommunications, held in 2012, which included a revision to the International Telecommunications Regulation. Some of the rules of this instrument have raised doubts which could facilitate a higher control of Internet traffic and the new version adopted certain provisions on the net control of uncertain reach in its applicability by States which are not favorable to the Internet openness and do not share the same conceptions regarding fundamental rights.

These problems could be mitigated by the constitution of an intergovernmental organization with weighted voting and control of new members' admission. Nevertheless, it is doubtful that an organization of this type could shoulder all Internet governance tasks in an advantage position in relation to autonomous entities that represent not only the States and international organizations but also civil society and, in particular, the most dynamic forces that have been steering the Internet's efficient operation and development.

An indirect representation of civil society through representatives of autonomous entities and stakeholder groups of each Member State (like it happens, for instance, with the International Labor Organization), would not proportionate an

8 - See João MOTA DE CAMPOS (ed.) – *Organizações Internacionais*, 4th ed., Coimbra, 2010, 601 et seq.

9 - N. 7, 44-45.

appropriate representation of civil society, since, first of all, in the sphere of the Internet the civil society is more institutionalized in transnational organizations and fora than in national entities. On the other hand, such an organization would hardly count with the membership of all States. This could potentially lead to net fragmentation.

Therefore, *preference should be given to a globalization based on a multistakeholder model*. Accordingly, Internet governance should be entrusted to autonomous entities that are inclusive, transparent, and accountable, in which the Internet global community is appropriately represented ⁽¹⁰⁾.

The transparency of the processes embraces a certain degree of democratic legitimacy and credibility through active participation of interested parties as well as through a certain amount of control over the decision-making processes ⁽¹¹⁾. The accountability should be understood in wide sense, implying a justification of the decisions and an assumption of liability for any errors and failures ⁽¹²⁾.

At present, *the Internet is mainly governed by autonomous entities that form a decentralized structure with complex interrelations* ⁽¹³⁾.

In first place, it should be mentioned the *Internet Society* (ISOC), which is an association constituted under the law of the District of Columbia with an important role in Internet coordination, albeit it only intervenes indirectly in the adoption of rules, to the extent in which it contributes to the appointment of the members of the entities that adopt or draft them. Many of the rules governing the Internet are adopted by the *Internet Architecture Board* (IAB) based upon the works carried out by the *Internet Engineering Task Force* (IETF), which is an open community in which technicians, economic actors and other parties interested in the evolution of the Internet participate voluntarily and which takes charge of issues concerning net protocols and architecture; by the *Internet Research Task Force* (IRTF) focused on the research and development of new technologies in the sector, with a structure based on small research groups; and by the

10 - See also Rolf WEBER – *Shaping Internet Governance: Regulatory Challenges*, in collaboration with Mirina Grosz and Romana Weber, Zurich, Basel and Geneva, 2009, 63, 78 and 116-117.

11 - See, with more development, WEBER (n. 10) 121 et seq.

12 - See, with more development, WEBER (n. 10) 132 et seq.

13 - Cf. WEBER (n. 10) 43 et seq., RUSTAD (n. 6) 89 et seq., and MIGUEL ASENSIO (n. 7) 46 et seq.

Internet Engineering Steering Group (IESG) which concretizes the development of standards.

The *World Wide Web Consortium* also adopts “recommendations” which contain specifications and standards, especially on software, fundamental for the uniformity and operation of the world web. These “recommendations” deal with technical issues like the specifications concerning the languages and formats that may have projection in the users’ activities such as the selection and filtration of contents and data protection technology.

Besides these entities whose activities have a worldwide scope, there are autonomous entities with a geographically limited scope, such as those coordinating the assignment and use of domain names at regional and national levels, whenever such a role is not performed by public entities. In effect, these autonomous entities adopt regulations on the registration of domain names and take decisions on their allocation.

The autonomous entities that govern the Internet should reflect its global nature, reinforcing and perfecting the multistakeholder model, performing the main role in Internet coordination and regulation, and establishing with interested States and international organizations agreements and coordination structures meant to overcome the insufficiencies of the autonomous governance and regulation in a harmonious manner when strictly needed. It is conceivable that a central entity of coordination could stand out, and that this entity, in collaboration with the States and the international organizations, creates a standard agreement to be concluded with each of them.

B) Internet regulation

Internet regulation faces limits and constraints by virtue of the *net global character*, which in most cases involves more than one national legal order, and which prevents the chance of its coordinated and harmonious operation being provided by national regimes; the diminished role that the States’ territory plays in the cyberspace, triggering, among other aspects, the difficulty in localizing Internet users and the activities they carry out online; and its *decentralized structure*, coordinated by various entities, as a rule autonomous, with specific scopes and, sometimes, also geographically limited.

For this reason, there is a *normative production by autonomous centers* that perform a role in Internet regulation, although of limited reach. It essentially deals with the definition of the technical standards required by Internet operation and the allocation and assignment of domain names and IP addresses.

The autonomous rules on the operation of the Internet are normally called “*Request for Comments*” (RFC), a denomination that evokes the cooperative and voluntary nature that the normative creation in the Internet assumed at its genesis. They are frequently drafted by the IETF, revised and approved by the IESG, and published by the IAB, under the control of the ISOC, which delegates this function to the editor of RFC. The RFCs include the basic rules of the allocation of IP addresses and the structure of the domain names system ⁽¹⁴⁾.

The standards of behavior and decision created by these autonomous centers are true rules of law, since they are characterized by generality and binding force: they bind a plurality of addresses that are not determinable at the moment of their creation. For instance, an interested party cannot register a domain name if it does not fulfil the established pre-requisites and procedures. This binding effect precedes the registration agreement, which spells out the conditions for domain name use and alternative resolution procedure for the respective disputes ⁽¹⁵⁾.

Furthermore, there are soft law instruments with a wider scope, namely the codes of conduct adopted by professional or consumer organizations. However, its binding force is limited to cases in which they express customary rules or relevant trade usages, sometimes in connection with social sanctions – such as the publishing of transgressors lists or the exclusion of the organization promoting the code of conduct –, and with alternative dispute resolution methods.

According to the *subsidiarity principle* ⁽¹⁶⁾, the Internet should be regulated by rules created by autonomous sources which are the expression of the Internet global

14 - See MIGUEL ASENSIO (n. 7) 48.

15 - Therefore, these provision are not general contract conditions, which only bind through their incorporation into the individual contracts. For a different view, Dário MOURA VICENTE – *Direito Internacional Privado. Problemática Internacional da Sociedade da Informação*, Coimbra, 2005, 135; *A Tutela Internacional da Propriedade Intelectual*, Coimbra, 2008, 180.

16 - On the meaning and scope of the subsidiarity principle on the regulation of transnational relationships, as a corollary of the freedom value, see Luís de LIMA PINHEIRO – *Arbitragem Transnacional. A Determinação do Estatuto da Arbitragem*, Coimbra, 2005, § 40, and *Direito Internacional Privado*, vol. I – *Introdução e Direito de Conflitos/Parte Geral*, 3rd ed., Coimbra, 2014,

community, namely rules originated from entities which represent this community and customs and usages observed by its members except to the extent in which the protection of rights or public policies that cannot be appropriately pursued by autonomous law is at stake ⁽¹⁷⁾.

The *priority of autonomous regulation*, besides corresponding to a democratic and open conception of society ⁽¹⁸⁾, is justified by several advantages, namely:

- autonomous rules are adjusted to the technical reality of the Internet, tend to adjust to the interests of its stakeholders and stimulate the participation of all interested parties in their creation;
- its origin assures a high degree of compliance;
- rules created by autonomous entities are more easily modifiable than the rules created by international instruments and, therefore, are more suited to follow the evolution of the Internet ⁽¹⁹⁾.

Naturally, these advantages depend, to some extent, on a balanced representation of all the stakeholders; on the efficiency, transparency and suitability of the normative creation process; and on the foundation of the stakeholders representatives' conduct on the mutual respect, on the warranty of an essential core of fundamental rights and on the due consideration of the interests of the other stakeholders and of the common good in order to assure that the adopted rules are suited for the pursuance of common values before the conscience of the global Internet community members and are compatible with the conceptions prevailing in the international community ⁽²⁰⁾.

The phenomenon of autonomous regulation of the Internet is a particular manifestation of a broader phenomenon of development of autonomous law applicable to transnational relationships. This phenomenon has special importance in the realm of international business relationships, originating a new *lex mercatoria* ⁽²¹⁾. For this

333-334. More in general, on its meaning for the general theory of law, see Miguel TEIXEIRA DE SOUSA – *Introdução ao Direito*, Coimbra, 2012, 64 et seq.

17 - See also WEBER (n. 10) 17 et seq.

18 - See also WEBER (n. 10) 78-79.

19 - Their production costs are also lower than the costs of the rules created by international instruments.

20 - See the convergent remarks of WEBER (n. 10) 22-23, 96 et seq., 120 e 207 et seq.

21 - On the autonomous law of international business, see Luís de LIMA PINHEIRO – *Contrato de Empreendimento Comum (Joint Venture) em Direito Internacional Privado*, Coimbra, 1998, §§ 18-19;

reason, the autonomous law of the Internet is sometimes referred to as *lex electronica*, though this expression tends to be employed in broader senses ⁽²²⁾.

It stems from the stated above that, so far, autonomous regulation has had a limited material scope, confined mainly to the definition of technological standards, the regulation of the technical issues required by the proper functioning of the network, and the allocation and assignment of domain names and IP addresses. The *lex electronica* does not yet perform a significant role in the shaping and regulation of the majority of private law relationships between Internet stakeholders. Nonetheless, an evolution towards the widening of its scope of regulation is entirely conceivable, namely the relationships between the involved telecommunications, hardware and software enterprises, the contracts between service providers and users, the electronic contracting, and the online provision of goods and services in interaction with the development of the *lex mercatoria* regarding international business relationships. It should be stressed that the expansion of the *lex electronica* does not mean that it should necessarily be the exclusive source of regulation in the above matters.

In parallel to the *lex mercatoria*, the binding force of the autonomous rules and principles of the *lex electronica* does not depend on their insertion in a legal order. Instead, it is grounded on the pursuance of the values shared by the majority of the global Internet community stakeholders; on the suitability of their content in the pursuance of these values, and to assure the Internet operation before the conscience of these stakeholders; on their formation through autonomous processes suited for the creation of binding rules according to the same stakeholders; on their conformity with the general principles of law and the fundamental values widely recognized by Public International Law and by the large majority of national legal orders; and on their application in alternative dispute resolution methods regardless of their reception by a national legal order ⁽²³⁾.

The values at stake in Internet regulation do not exclusively concern private law and there are cases in which the autonomous regulation does not appropriately assure

Direito Comercial Internacional, Coimbra, 2005, nos 37 et seq.; *Direito Internacional Privado* (n. 16) § 6, with more references.

22 - See, namely, Pierre TRUDEL – “La *lex electronica*”, in <http://www.chairelrwilson.ca/cours/drt3808/Lexelectronicastrudel.pdf>.

23 - See, regarding *lex mercatoria*, LIMA PINHEIRO, *Arbitragem Transnacional*...(n. 16) 431-432, with more references.

the protection of private law values. Even the definition of technical standards affects electronic contracting, the manner in which goods and services are provided online, the reach of some fundamental rights, such as freedom of the press, freedom of information, freedom of expression, privacy, personal data protection, and, regarding the domain names and IP addresses system, is related to important legislative policies ⁽²⁴⁾.

In the areas in which public regulation is needed – especially, in the fields of cybercrime, protection of personality and intellectual property rights ⁽²⁵⁾, tort, and consumer protection —, the global nature of the Internet justifies, in principle, endeavors of international unification through international conventions ⁽²⁶⁾. In effect, only international regimes may provide the effectivity, the certainty, and the foreseeability of legal solutions in those areas, as well as international legal harmony, and avoidance of concurrence of norms and conflict of duties which burden users and service providers on the net.

Although it is not inconceivable to entrust the drafting of these international conventions to an international organization specifically created for that purpose, with weighted voting and control of new member admissions, it seems that such a task may in principle be performed by preexisting organizations, such as the UNIDROIT, the World Intellectual Property Organization (WIPO), WTO, the United Nations Commission for International Trade Law (UNCITRAL), and the Hague Conference on Private International Law. This point of view has already obtained some acceptance, namely with the WIPO Treaties on Copyright and on Performances and Phonograms of 1996, which were mainly designed to develop and improve the regimes in force attending to the issues raised by new information and communication technologies and, especially, the Internet.

Whenever the creation of an international regime of a universal scope faces severe difficulties, and there is interest in regional regulations, it should also be accepted, in the areas in which public regulation is needed, the drafting of regional

24 - As remarked by MIGUEL ASENSIO (n. 7) 49-50.

25 - See, namely, Luís de LIMA PINHEIRO - “Algumas considerações sobre a lei aplicável ao direito de autor na Internet”, *ROA* 74 (2014) 13-34, Introdução and I.B (regarding the risk to the protection of the right of making the work available to the public resulting from the delocalization of operators who provide access to protected works, through the establishment in States with low copyright protection level).

26 - See also WEBER (n. 109) 16-17.

international conventions or legislation enacted by international organizations, as it is the case of the EU legislation.

To sum up, albeit Internet should be essentially autonomous governed, it will be more appropriate to tackle its regulation in a perspective of complementarity between autonomous and public regulation and, therefore, of *co-regulation* ⁽²⁷⁾.

27 - For the same view, WEBER (n. 10) 5. For a partially divergent view, Alexandre DIAS PEREIRA – “Direito Ciberespacial: ‘Soft Law’ or ‘Hard Law’?”, in *Est. José Gomes Canotilho*, vol I., 685-710, Coimbra, 2012, 704 et seq., based upon legitimate concerns, but without taking into due account, in my opinion, the corollaries of the subsidiarity principle and the relativity which, in the global or transnational sphere, the interests and public policies of the single States assume.

II. ICANN EVOLUTION IN THE PERSPECTIVE OF A MULTISTAKEHOLDERS MODEL

A) ICANN scope of activity and the domain names system

The ICANN is an autonomous entity. While it has a rather limited scope of activity, it performs especially important functions to the Internet operation and it may constitute the embryo of a central entity of Internet coordination. In effect, the ICANN has the mission to coordinate, on a general level, the global Internet's systems of unique identifiers, and, in particular, to ensure the stable and secure operation of the Internet's unique identifier system (Article 1(1) of the ICANN Bylaws).

In particular, the ICANN coordinates the allocation and assignment of the Internet's three sets of unique identifiers, which are domain names (forming a system referred to as "DNS"), the Internet protocol ("IP") addresses and autonomous system ("AS") numbers, and protocol ports and parameter numbers. It coordinates the operation and evolution of the DNS root name server system and coordinates policy development reasonably and appropriately related to these technical functions.

The ICANN does not operate as registry of domain names or IP addresses, but it accredits the entities which may act as registries of domain names under certain top level domains.

The *top level domains* may be generic or geographic. Generic top level domains are assigned worldwide, based upon material criteria (for example, .com). Geographic top level domains are assigned by countries (for example, .pt, for Portugal) or regions (for example, .eu).

The administration of geographic top level domains is entrusted, by delegation of the ICANN, to the national or regional Internet registries (*Network Information Centers*). There is a trend towards governmental control of these national register centers, but the compliance with the limitations of the ICANN delegation and the

coordination between these centers and ICANN are fundamental to the proper operation of a unified system of domain names ⁽²⁸⁾.

The *top level generic domain names* are subdivided into sponsored and non-sponsored domain names.

The policies of the assignment of non-sponsored top level domain names, such as “.com” and “.net”, are defined by the ICANN, with which the operators of these domains conclude Registry Agreements regulating the generality of the assignment and use issues concerning these domain names ⁽²⁹⁾.

The sponsored top level domain names are coordinated by organizations that represent the sectors affected by these specialized domain names. These organizations have concluded agreements with the ICANN, which delegates the sponsors’ power to define the policies of assignment and use of these domain names taking into account their respective Charter.

An important part of the powers of the ICANN, namely the coordination of allocation of IP addresses and of autonomous numbers, and the management of the DNS root server is entrusted to the *Internet Assigned Numbers Authority* (IANA), which is presently an ICANN department.

The IANA delegates the allocation of blocks of IP addresses in different geographic areas to 5 regional Internet registries ⁽³⁰⁾.

In order to understand the reach of the ICANN’s powers it is important to examine the functions and nature of domain names.

Domain names have a double function. One is a *localizing function*, since they are the Internet address of websites, which provides access to its content. The other is a website’s *identifying function*, which may also be relevant for the identification of the

28 - For this view, see MIGUEL ASENSIO (n. 7) 70.

29 - See MIGUEL ASENSIO (n. 7) 65-66.

30 - These regional registries created an organization which represents their collective interests and assures the coordination of their policies: the Number Resource Organization.

enterprise which operates the website and of the goods and services offered on the website, performing then a function analogous to other distinctive signs of trade ⁽³¹⁾.

The domain name is an intangible good with patrimonial value. *The holder of the domain name has the exclusive of its use as such.* This should not be confused with its use as a trademark or other distinctive sign of trade. Nonetheless, the right referring to the domain name is not usually deemed a right of intellectual property ⁽³²⁾.

A different issue is the possibility of the domain name holder benefiting from an autonomous right or other mode of protection by virtue of using the domain name as a firm, distinctive sign of the enterprise or work title, or of its register as trademark ⁽³³⁾.

In the face of the limitations or difficulties met by claims grounded on the infringement of trademarks or on unfair competition due to the use or registration of a given domain name in State courts, in 1999 the ICANN established a dispute resolution procedure called *Uniform Dispute Resolution Policy* (UDRP). This Uniform Policy has been mainly based upon a WIPO recommendation.

The most evident practical advantages of this dispute resolution procedure are the speed and the comparatively low cost. These disputes are dealt with by “administrative panels” normally composed of just one member. The center in which the procedure is held may be chosen by the claimant among the centers authorized by ICANN. The most important is the center operating in the WIPO framework.

31 - See, for a convergent view, Gerald SPINDLER and Fabian SCHUSTER – *Recht der elektronischen Medien*, 3rd ed., Munich, 2015, Vorbemerkung: Allgemeine Grundsätze des Kennzeichenrechts..., nos 43 et seq.

32 - See, namely, SPINDLER/SCHUSTER (n. 31) Vorbemerkung: Allgemeine Grundsätze des Kennzeichenrechts... nos 47 and 70, who make reference to an enjoyment right analogous to property. On the main conceptions regarding the legal nature of the industrial property rights, see José de OLIVEIRA ASCENSÃO – *Direito Comercial. Direito Industrial*, vol. II, Lisbon, 1988, 389 et seq. The characterization as an intellectual property right faces two type of difficulties. On one hand, the principle of *numerus clausus* of the intellectual property rights associated with the territoriality principle regarding their effects. On the other hand, the fact that the right on the domain name is not assigned *ope legis* nor, in the great majority of the cases, by a public authority applying the law. Both difficulties may be relativized, because the statutory law is not the only source for the recognition of an intellectual property right – see OLIVEIRA ASCENSÃO, op. cit., 26, the assignment of the domain name has a global scope and the register of some domain names is legally regulated and/or organized by public authorities.

33 - See SPINDLER/SCHUSTER (n. 31) Vorbemerkung: Allgemeine Grundsätze des Kennzeichenrechts... no 73.

The dispute resolution procedure is governed by a set of Rules. According to these Rules, the applicable decision criteria are the ICANN rules and the rules and principles that the panel deems applicable (Article 15(a)). Often the decisions are based upon internationally accepted general principles of law, especially when the parties are not habitually resident in the same country ⁽³⁴⁾.

It is not an arbitration, because this procedure does not exclude the jurisdiction of the State courts and doesn't have jurisdictional effects. Its sole effect is the cancelling, modification or transference of the domain name registration ⁽³⁵⁾. It may be said, however, that it is an alternative dispute resolution method (ADR), different from either arbitration or mediation, in the sense that it allows the resolution of the dispute by a private person, outside the State courts (and not in the sense of a tribunal which would exclude the jurisdiction of a State court).

Every registry accredited by the ICANN is bound by this dispute resolution procedure. The domain name users, in turn, become bound by virtue of their registration agreements ⁽³⁶⁾.

In effect, the registration of second level domain names subordinate to certain top level domain names is dependent on the acceptance of this dispute resolution procedure. Presently, more than 50 States apply the Uniform Policy or extrajudicial procedures inspired by it regarding disputes concerning domain names registered under the respective national top level domain names ⁽³⁷⁾.

For instance, in *Portugal*, the management, registration and maintenance of the *domain names pt.* are entrusted to the *Associação DNS.PT* ⁽³⁸⁾. This is an association of Private Law constituted by the public entity that supports the research on science and technology – the FCT – *Fundação para a Ciência e a Tecnologia*, IP –, by private entities – the *Associação do Comércio Eletrónico e Publicidade Interativa* (ACEPI), and the *Associação Portuguesa para a Defesa do Consumidor* (DECO) –,

34 - See MIGUEL ASENSIO (n. 7) 487 et seq., and SPINDLER/SCHUSTER (n. 31) Verfahren in Kennzeichenstreitsachen..., nos 1 et seq.

35 - For a different view, SPINDLER/SCHUSTER (n. 31) loc. cit.

36 - Cf. SPINDLER/SCHUSTER (n. 31) no 9.

37 - See MIGUEL ASENSIO (n. 7) 487-488.

38 - See <http://www.dns.pt/pt/>.

representatives of business and consumers, and by the representative appointed by the IANA as the entity in charge of the delegation of the top level domain.

At the international level, the DNS.PT participates actively, as a member, in meetings and working groups of organizations accredited in the realm of the Internet such as the ICANN and the *Council of European National Top Level Domain Registries* (CENTR).

The registration of domain names under .pt is not conditioned to the acceptance of an alternative dispute resolution method. However, the Rules of Register of Domains .PT allows the settlement of disputes between holders of domain names, that when registering the holder undertakes to settle the disputes on domain names by arbitration under the auspices of the ARBITRARE (*Centro de Arbitragem para a Propriedade Industrial, Nomes de Domínio, Firmas e Denominações*), and the undertaking of the Associação DNS.PT, which is entrusted with the registration of domain names under .pt, to settle any dispute concerning domain names by arbitration under the auspices of the same center (Article 38). The criteria for the settlement of disputes concerning domain names, defined in the same Rules (Article 40), follow the provision contained in Uniform Policy of the ICANN.

At the EU level, the domain name .eu is governed by the Regulation (EC) no 733/2002 on the implementation of the .eu Top Level Domain and by the Regulation (EC) no 874/2004 Laying Down Public Policy Rules Concerning the Implementation and Functions of the .eu Top Level Domain and the Principles Governing Registration.

Article 22 of the Regulation no 874/2004 provides for an alternative dispute resolution procedure (ADR) based upon the Uniform Dispute Resolution Policy of the ICANN. The ADR is compulsory for the holder of a domain name and for the Registry (no 2). The results of ADR are binding to the parties and the Registry unless court proceedings are initiated within 30 calendar days of each party's receipt of the notification of the ADR procedure results. (no 13) ⁽³⁹⁾.

After these very general remarks on the domain names system, I turn now to the structure and nature of the ICANN and the stewardship of the domain names system.

39 - In general, on the ADR, see SPINDLER/SCHUSTER (n. 31), *Allgemeines...*, nos 113 et seq.

B) Characterization of the ICANN and stewardship of the domain names system

The ICANN is a legal person of State law, constituted in 1998 under the *California Corporation Code* as a non-profit corporation with seat in Los Angeles, California. In comparison with the types of legal persons known in Civil Law systems, it is not an association, nor a foundation, nor a company (since it does not have a profit purpose), but a *sui generis* legal person.

It is managed by a Board of Directors of 16 members who are directly or indirectly appointed by stakeholder groups, by autonomous entities, or by the stakeholder community at large which is somehow designed to represent the global Internet community ⁽⁴⁰⁾.

Furthermore, ICANN has advisory organs and mechanisms aimed at receiving the contributions of the stakeholders who do not participate directly in the *Supporting Organizations*. This includes the Governmental Advisory Committee, which is composed of representatives of a high number of Governments of all over the world. ICANN has been coordinating its activity with intergovernmental organizations, especially with the WIPO, regarding the organization of the domain names system and its coordination with the protection of distinctive trade signs.

[The ICANN has had operational platforms in Istanbul and Singapore since 2013.](#)

The control of the US Department of Commerce over the ICANN ceased in 2009, but the ICANN continued to be linked to the same department by a contract [*Affirmation of Commitments*] during a period ending in 2015. It was later extended

40 - According to Article 6(2) of the ICANN Bylaws, the Board is composed by:

- 8 members appointed by a Nomination Committee (the delegates of this committee are selected from the *Generic Names Supporting Organization*, being one delegate from the Registries Stakeholder Group, one delegate from the Registrars Stakeholder Group, two delegates from the Business Constituency, one delegate from the Internet Service Providers Constituency, one delegate from the Intellectual Property Constituency and one delegate from the consumer and civil society groups, selected by the Non-Commercial Users Constituency, one delegate selected by the *Council of the Country Code Names Supporting Organization*, one delegate selected by the *Council of the Address Supporting Organization* and one delegate selected by the IETF);
- 2 members selected by the *Address Supporting Organization*;
- 2 members selected by the *Country Code Names Supporting Organization*;
- 2 members selected by the *Generic Names Supporting Organization*;
- 1 member selected by the At-Large Community; and
- the President *ex officio*.

until September 2016. The above mentioned policy of the US Administration, (*supra* Introduction) pointed to the transference of the functions it performs regarding the domain names system to the Internet global community of stakeholders and considered the ICANN as the entity most well positioned for the drafting a plan for this transition.

The path followed was, however, to entrust two groups composed of representatives of the global Internet community – the *IANA Stewardship Transition Coordination Group* (ICG) and the *ICANN Cross Community Working Group on Accountability* (CCWG) – with the draft a proposal for the transference of stewardship of the domain names system to the global Internet community.

The IGP presented a *Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community* in march 2016 ⁽⁴¹⁾. This document is composed of a ICG report, which contains a summary of the proposal, by the proposals of the *Domain Names Community*, of the *Internet Numbers Community* and of the *Protocol Parameters Registries Community*, which develop it ⁽⁴²⁾. This proposal obtained the support of the *Internet Society* ⁽⁴³⁾ and has started being reviewed by the NTIA ⁽⁴⁴⁾.

The proposal includes the constitution of an affiliate of the ICANN – the *Post-Transition IANA (PTI)* –, to which would be transferred the human and material resources of IANA, designed to be the IANA functions operator ⁽⁴⁵⁾. According to the proposal, the ICANN maintains its seat in the U.S.A. and subcontracts the IANA functions with PTI ⁽⁴⁶⁾. The *Domain Names Community* proposal expressly states that PTI should be, along with ICANN, a non-profit corporation constituted under the California law ⁽⁴⁷⁾, and that its Board of Directors should be appointed by ICANN ⁽⁴⁸⁾. The oversight function until now performed by the US administration regarding the

41 - <https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf>.

42 - No 12.

43 - Press release *Internet Society Statement in Support of the IANA Stewardship Transition*, 24 may 2016, in <https://www.Internetsociety.org/news/Internet-society-statement-support-iana-stewardship-transition>.

44 - Cf. Lawrence STRICKLING – “Reviewing the IANA Transition Proposal”, Blog of 11 march 2016, in <https://www.ntia.doc.gov/blog/2016/reviewing-iana-transition-proposal>.

45 - Nos 13 e 23.

46 - *Ibidem*.

47 - No 1108.

48 - No 1112.

domain names system will be transferred to a *Customer Standing Committee* ⁽⁴⁹⁾ composed mainly by representatives of the registry operators of domain names elected by the respective communities ⁽⁵⁰⁾.

The ICG's Proposal embraces only a limited aspect of the Internet governance, which concerns mainly the control of the domain names system. Notwithstanding, having in mind the policies stated by the EU Commission (*supra* Introduction) and the US Administration, which follow the conclusions of the main global Internet community fora (*supra* Introduction), there is the chance of the ICANN evolving into a central multistakeholding structure of this community of Internet governance.

Regarding the ICANN evolving into a global multistakeholder entity, there are more formal and more substantial issues to be considered.

C) Formal issues of the ICANN evolution

Regarding the most formal issues, one may ask what nature ICANN, or the entity succeeding it, should assume.

The ICANN powers, in particular the coordination of the domain names system, is not confined to strictly technical issues, since it affects the operation of several legal regimes of supranational and national sources and is, as previously remarked, connected to the pursuance of given public policies (*supra* I) ⁽⁵¹⁾. Such is the case with the definition of the criteria which determine the top level domain names as well as the fundamental decisions on their allocation and assignment. The democratic legitimacy of ICANN is controversial, because it does not assure the democratic control of its

49 - No 13 and P1. Annex G, nos 1308 et seq.

50 - Nos 1327 e 1328. The Committee is composed in the minimum by 2 representatives of top level generic domain names registry operators, 2 representatives of geographic domain names registry operators, eventually 1 representative of a registry operator of domain names not included in the previous categories and 1 liaison from the PTI. It may be appointed liaisons from other organizations. The representatives and liaisons are appointed by the respective communities (no 1334), which are the *Country Code Names Supporting Organization*, the *Registry Stakeholder Group* and the *Generic Names Supporting Organization* (no 1336). On the structure of the supporting organizations, see Articles IX-X of the ICANN Bylaws. On the structure of the Registry Stakeholder Group, see Charter adopted by the ICANN Board of Directors, in <http://gnso.icann.org/en/about/stakeholders-constituencies/rys>.

51 - See also WEBER (n. 10) 61 and MIGUEL ASENSIO (n. 7) 50 et seq.

decisions by all interested parties, it does not exercise its powers through the delegation of international community bodies and does not hold merely technical powers ⁽⁵²⁾.

For this reason, it could be thought that this mission should be entrusted to the national political power or that, taking into account its global repercussion, it should be in charge of an international organization.

A *stricto sensu international organization*, i.e., an intergovernmental or supranational organization, is an association of International Law entities (traditionally States) constituted by act of International Law (international treaty or resolution of international organization) which pursues common goals of the Member States, has organs that express its own will, and has a legal personality distinct from the Member States ⁽⁵³⁾.

In the *intergovernmental organizations* the deliberative organs are composed of representatives of the Member States. Their deliberations, addressed to the Member States, are usually taken by unanimity. The most common solution is the equality voting of the Member States, but some international organizations take into account the real inequality between them and adopt weighted voting (for example, Security Council of UN, IMF, World Bank, BERD).

Nonetheless, as stems from the above stated (*supra* I), since the Internet is a global reality, it should be governed by *global entities*. Not only is the creation of an intergovernmental organization assuring the pursuance of policies which should guide that governance hardly feasible, but is also fundamental that civil society is appropriately represented in those entities and does not see its dynamic curtailed by intergovernmental mechanisms.

It should be pointed out that the constitution of a legal person under a State law does not prevent that this legal person pursues international goals and has a global scope of action.

52 - See, namely, Markus KÖHLER, Hans-Wolfgang ARNDT and Thomas FETZER – *Recht des Internet*, 7th ed., Heidelberg et al., 2011, nos 26 et seq.

53 - See, for a convergent view, ANDRÉ GONÇALVES PEREIRA and FAUSTO DE QUADROS – *Manual de Direito Internacional Público*, 3rd ed., Coimbra, 1993, 411 et seq.

In the present context, the national nature of the legal person essentially means that its incorporation, transformation and winding up, the internal affairs, the patrimonial autonomy, the binding of the legal person by the acts of its organs and the liability of its organs towards third parties are ruled by a State law ⁽⁵⁴⁾. It should be added regarding internal affairs that the governing State law may allow for a wide freedom of choice.

The localization of the seat or establishment in a given State may also be relevant, at least in the absence of the choice of another law by the parties, to the determination of the law governing contractual and non-contractual relationships to which the legal person is party, as well as, in the absence of an arbitration agreement or of a jurisdiction agreement, to the determination of the State jurisdiction competent for the settlement of the disputes arising therefrom.

The incorporation of a legal person with an international scope of action under a State law, as well as the localization of its seat in the respective State, do not imply, in principle, that other aspects of its activity are governed by its law, nor that they are not governed by other laws.

To consider a legal person who pursues international goals and has a global scope of action as a mere national law entity, however, may constitute a too narrow vision.

In the last decades, the category of non-governmental organizations (NGOs) has assumed growing importance, which, in a first approach, are precisely organizations with transnational activity, not having been created by act of Public International Law, but which pursue international goals, i.e., collective goals that transcend the scope of a State ⁽⁵⁵⁾. Many of these organizations tend to avoid the applicability of any State law and jurisdiction, subjecting the disputes arising from the relationships which have been established with persons of domestic law to international arbitration.

The designation “non-governmental organization” expresses the idea that it is an international organization (in a broad sense) different from an intergovernmental

54 - See Luís de LIMA PINHEIRO – *Direito Internacional Privado*, vol. II – *Direito de Conflitos/Parte Especial*, 4th ed., Coimbra, 2015, § 58 e 59.

55 - See LIMA PINHEIRO (n. 44) § 60, with more references.

organization, because it is not an association of States created by act of Public International Law.

The growing influence of the NGOs has been one of the most important developments at the international level ⁽⁵⁶⁾. They are one of the entities with transnational activity with which the States tend to share their powers – including political, social and security roles which are in the core of sovereignty –, in an era dominated by the end of the Cold War and by globalization. “A world that is more adaptable and in which power is more diffused could mean more peace, justice, and capacity to manage the burgeoning list of humankind's interconnected problems. At a time of accelerating change, NGOs are quicker than governments to respond to new demands and opportunities” ⁽⁵⁷⁾.

Very important organizations in the humanitarian field, such as the International Committee of the Red Cross, or in the economic field, such as the International Chamber of Commerce and the International Air Transport Association, are examples of NGOs. Nevertheless, there is no uniform concept of NGO. Some authors define it as an international association with members of different nationalities and non-profit aim ⁽⁵⁸⁾. Meanwhile, for the European Convention on the Recognition of the Legal Personality of International Non-Governmental Organisations (Strasbourg, 1986), a NGO is an entity with a non-profit-making aim of international utility, established by an instrument governed by domestic law, carrying out their activities with effect in at least two States.

In the face of this concept of NGO, *ICANN would be a NGO*. A future entity succeeding ICANN and which was not created by an act of Public International Law, as well as the proposed PTI, would also be NGOs.

What is *the relevance of the legal characterization of a legal person as NGO?*

The Strasbourg Convention lays down a special regime for the NGOs which have been created by act of domestic law of a party State or which have its statutory

56 - Cf. Barry CARTER, Phillip TRIMBLE and Allen WEINER – *International Law*, 5th ed., Austin et al., 2007, 144-145.

57 - Jessica MATHEWS – “Power Shift”, 76 *Foreign Aff.* 50, 50-64 (1997), also accessible at <https://www.foreignaffairs.com/articles/1997-01-01/power-shift>.

58 - Cf. Patrick DAILLIER, Mathias FORTEAU and Alain PELLET – *Droit international public*, 8th ed., Paris, 2009, no 417.

seat and its management and control in the territory of party States. This Convention provides for the recognition of the legal personality and capacity acquired under the law of the statutory seat. In legal systems, such as Common Law systems, in which domestic law legal persons are subject to the law of the State of incorporation (incorporation theory), this does not raise special difficulties. But in systems like the Portuguese, in which legal persons are, in principle, subject to the law of the main and effective seat of their administration (Article 33 of the Civil Code), is there a segmentation of the law governing the legal person or a choice of law rule defining the law governing the legal person as a whole?

The issue is very controversial ⁽⁵⁹⁾. It seems to me there is a segmentation. The personality and the capacity become subject to the law of statutory seat ⁽⁶⁰⁾. The determination of the law applicable to other aspects of the legal person will still depend on the domestic choice of law rule.

The relevance of NGOs in the international legal order is a different issue. There are acts of International Law assigning a consultative status to some NGOs regarding given international organizations (namely UN Resolutions). There are also States that assign to some NGOs a status relevant to the International Law. Thus, it seems that these NGOs have acquired an international personality, albeit very limited, which has been assigned to them by international organizations and States ⁽⁶¹⁾.

The Strasbourg Convention has only 11 party States, which are members of the Council of Europe, and it is obvious that the ICANN has not been created by an act of a party State nor has its seat in the territory of a party State.

Notwithstanding, *relevant issues regarding the determination of its status may arise.*

One of these issues, which is still open in legal systems such as the Portuguese, is the possibility of including these entities in the concept of *international legal person*

59 - See Albert BLECKMANN – “Nongovernmental Organizations”, in *Universal Economic Organizations, IECL*, vol. XVII, ch. 25, 1981, no 14.

60 - This will often cause difficulties, because some of these organizations do not provide for a statutory seat. In this case, resort should eventually be made to the effective seat of their direction.

61 - Cf. BLECKMANN (n. 59) no 14.

for choice of law purposes ⁽⁶²⁾. This would lead, for instance in the Portuguese Private International Law, to apply to these entities the law (domestic or international) chosen in the constitutive act and, in the absence of a choice, the law of the country where the man seat is located (which is not necessarily the administration seat) (Article 34 of the Civil Code) instead of the law of the country where the main and effective seat of the administration is located ⁽⁶³⁾.

Another issue deserving reflection is whether the role recognized to ICANN or to a future entity which succeeds it by some international organizations (namely the UN and the WIPO) or by States, may be *relevant to International Law*.

Keeping in mind the doubts raised by the determination of the status of these type of entities, the possibility of an international convention to define their legal framework, without prejudice for its incorporation under a State law, could also be considered. A possibility which, naturally, would only have direct relevance to the States that became party to that convention. In this case, the NGO, or analogous entity, would have an international legal framework, which would be compatible with a model of autonomous multistakeholder governance.

In any case, it seems advisable that ICANN, or the entity succeeding it, politically assumes its role as a NGO.

Furthermore, in the relationships between this NGO and the public and private entities, namely in the standard contract to be concluded with the interested States and in the registration rules of domain names, *arbitration of the disputes* arising therefrom ⁽⁶⁴⁾, the seat of the arbitration, and the rules of law applicable by the arbitral tribunal to the merits of the dispute, which would not always be State law, could be provided. It

62 - ISABEL DE MAGALHÃES COLLAÇO – *Direito Internacional Privado*, parte II – “Sistema de normas de conflitos portuguesas”, t. I – “Direito das pessoas. § 2,º Pessoas Colectivas” (students notes), Lisbon, 1971, 49-50, advocated at the time being that could be included in Article 34 associations and foundations which, although not created by international convention, are designed for an activity at the international scale. She exemplified with the International Chamber of Commerce and the Institute de Droit International. On the contrary, João BAPTISTA MACHADO – *Lições de Direito Internacional Privado*, 2nd ed., Coimbra, 1982, 350, and António MARQUES DOS SANTOS – *Direito Internacional Privado. Sumários*, Lisboa, 1987, 261-262 exclude all the legal persons that are not created by an International Law instrument.

63 - See LIMA PINHEIRO (n. 44) § 60, with more references.

64 - Compare the alternative proposal of an international tribunal for Internet put forward by Daniel FREIRE E ALMEIDA – *An International Tribunal for the Internet* (Ebook), Coimbra, 2016, Part II, Chapter 1. In my opinion, this proposal triggers the risk of contributing to the intergovernmentalization of Internet governance.

would also be appropriate to adopt rules of arbitration, or even eventually create an institutionalized center, at least for the arbitrations concerning the assignment, modification or cancelling of domain names. This would constitute an important step in the globalization of this entity.

D) Substantial issues of the ICANN evolution

Regarding the more substantial issues, one must reflect on the mode of representation of the Internet community multistakeholders and on its coordination with the interested States and international organizations.

The subcontracting of the IANA functions in an affiliate of ICANN is a possible solution to transfer the stewardship of the domain names system to the community of Internet multistakeholders because ICANN is oversighted by a *Customer Standing Committee* mainly composed by representatives of the communities of domain names registry operators. The merits of this solution require further analysis. I will only point out that, on one hand, this solution is supported by organizations representing the global Internet community. On the other hand, it seems depend to a larger extent on the structures and internal procedures of the communities concerned with the registration of domain names, and on the nature of their members (*supra* B).

In general terms, I believe that the evolution of ICANN towards a multistakeholder structure of Internet governance, which I consider desirable, requires further steps.

First of all, in the direction of a *more balanced, inclusive and transparent representation* of the Internet community stakeholders in the appointment of the members of the Board of Directors.

This should include the *direct or indirect participation of delegates of States and international organizations* in that appointment, although without a hegemonic position and through a weighted voting which takes into account their relative political-economic weight. The mere participation in an advisory organ does not express appropriately the contribution that the States should give to the definition of some

policies and to the decision-making where are at stake public interests that they should pursue.

With respect to the *external coordination of the entity's activity with the interested States and international organizations*, it seems advisable that these States and international organizations assign to it a status relevant to International Law, namely accepting its participation in advisory organs of international organizations and in conferences and fora even having an intergovernmental nature, as well as its contribution to the drafting of international conventions and in the preparatory work of normative acts of supranational organizations (such as the EU).

The entity may also participate in other *coordination structures* together with the interested States and should conclude with them agreements which, while not being international treaties in strict sense, may amount to *quasi-treaties*, since they are not exclusively subject to the law and the jurisdiction of the contracting State and are, by the procedures observed by the public party and by the position of the public organs that intervene in their conclusion, or authorize it, materially comparable to international treaties ⁽⁶⁵⁾.

In these ways, the autonomous entity may acquire a *limited international legal personality*, which consolidates its institutionalization as a global multistakeholder entity and reinforces its role as a global political actor.

As previously remarked, the agreements to be concluded with the interested States may conform to a standard contract assuring the uniformity of the entity's rights and obligations, and in which the inclusion of appropriate arbitration and choice of law clauses – which do not refer necessarily to State law –, may increase its autonomy and global nature.

65 - See LIMA PINHEIRO, *Contrato de Empreendimento Comum...* (n. 21) § 15 C and (n. 44) § 67, with more references. The exceptional possibility of agreements between NGOs and States constitute international treaties seems to be accepted by DAILLIER/FORTEAU/PELLET (n. 48) no 417.

III. FINAL REMARKS

This study does not intend to advance definitive conclusions nor to propose a plan of action. It is essentially comprised of a set of reflections that are mainly aimed to find some clues related to possible solutions for the evolution of Internet governance and regulation.

The transference of the stewardship of the domain names system to the community of Internet multistakeholders is on the table and may constitute a first step towards the governance of the Internet by a globalized autonomous entity based on a multistakeholder model, which seems to be the option most suited for the goals and values that should guide it.

In this evolution, the assumption of the role of an NGO by ICANN, or by the entity which succeeds it, and the recognition to this NGO, by States and international organizations, of status relevant to Public International Law, seems appropriate to its consolidation as an *autonomous global multistakeholder entity*.

For this purpose, however, improvements are required in the representation mechanisms of the global Internet community stakeholders. These include namely an increased emphasis in the role of the States. A network of coordination structures and agreements involving the autonomous entity, on one side, and the States and international organizations, on the other, is also required.

If this transition is successful, the autonomous entity may play a more important role in Internet governance than that presently played by ICANN and, eventually, may constitute the embryo of central structure of Internet governance.

The autonomous governance of the Internet, here advocated, is indissociably connected with a co-regulation of the Internet, through a combination of the primacy of autonomous regulation with public regulation in all the areas and issues in which the autonomous regulation is insufficient. This public regulation should be fundamentally of an international source, in principle of universal scope, but also regional whenever justified by the circumstances.

The autonomous regulation of the Internet (the so-called *lex electronica*), constitutes a particular manifestation of a phenomenon of development of autonomous

sets of rules governing transnational relationships. This assumes, together with its practical importance, a major theoretical interest for legal science. It raises the question whether these sets of rules may be seen as specific areas of International Law understood in a broad sense, or as subsystems of a complex global legal system ⁽⁶⁶⁾.

In the first case, International Law would be understood as the legal order of an international society comprised both of the interstate relationships and of the transnational relationships between private people.

In the second option, the global legal system would be the legal expression of a world society, integrating the universality of human interactions and of all the other societies, namely the State societies. No doubt globalization, and the Internet as its catalyst and tool, favor an evolution towards the formation of this world society and, with it, a global legal system.

66 - See, with more development and references, LIMA PINHEIRO, *Contrato de Empreendimento Comum...* (n. 21) 936 et seq.; and *Arbitragem Transnacional...* (n. 16) 433 et seq.

CYBERLAW

by CIJIC

IS MULTISTAKEHOLDER THE NEW BLACK? BRAZILIAN EXPERIENCES IN INTERNET GOVERNANCE AND DIGITAL RIGHTS POLICYMAKING

MULTISTAKEHOLDER É A NOVA ONDA? EXPERIÊNCIAS BRASILEIRAS DE GOVERNANÇA DE INTERNET E DE POLÍTICAS PÚBLICAS SOBRE DIREITOS DIGITAIS

CLÁUDIO LUCENA ¹

¹ PhD Candidate, Católica Research Center for the Future of Law, Católica Global School of Law, Universidade Católica Portuguesa. Researcher, Foundation for Science and Technology, Ministry of Science, Technology and Higher Learning, Portugal. Professor, Center for Legal Studies (CCJ), Department of Private Law, Universidade Estadual da Paraíba (UEPB), Brazil.
Claudio.Lucena@uepb.edu.br

RESUMO

Arranjos de governança multistakeholder têm o propósito de envolver atores para além dos tradicionais e assim buscar ampliar o escopo de sua representação, de forma a trazer novos atores, como sociedade civil, indústria e academia, para as discussões gerais de gestão, elaboração de políticas, decisão e aplicação de normas, levando em consideração a necessidade de ampliar a legitimidade no ambiente em que operam. Este trabalho analisa de maneira crítica processos multistakeholder conduzidos no Brasil, como o Comitê Gestor da Internet (CGI.br), a elaboração do Marco Civil da Internet e a discussão de outros projetos que afetam o exercício da cidadania, de direitos e liberdades no ambiente digital com o objetivo de contribuir para ampliar a visão sobre as perspectivas, os aspectos positivos e as armadilhas que uma abordagem multistakeholder dirigida a tais iniciativas pode apresentar.

Palavras-Chave: modelos multistakeholder; governança de internet; políticas de tecnologia.

ABSTRACT

Multistakeholder arrangements are meant to involve players beyond traditional ones and search to widen the scope of their representation so as to bring new actors, such as civil society, industry and academia, to overall management, policy-making, decision and enforcement discussions, taking into consideration the need for improved legitimacy in the environment they operate. This work critically analyzes multistakeholder processes carried out in Brazil, such as the Internet Governance experience through the Brazilian Internet Steering Committee (CGI), the elaboration of Marco Civil and the discussion of other bills that affect the exercise of citizenship, online rights and freedoms with the objective of contributing to a broader view of the perspectives, strengths and pitfalls that a multistakeholder approach to such initiatives can bring.

Keywords: multistakeholder models; internet governance; technology policy.

1. INTRODUCTION

Unconventional governance arrangements commonly referred to as multistakeholder models, have evidently grown in importance and presence in the last decade. They are meant to involve players beyond traditional ones, and search to widen the scope of their representation so as to bring new actors, such as civil society, industry and academia, to overall management, policy-making, decision and enforcement discussions, taking into consideration the need for improved legitimacy in the environment they operate.

Multistakeholder structures, thus, are those in which parts with interests at stake recognize the importance of factors like equitable representation, accountability, communication, transparency and participation in structuring and taking decisions that affect each other, and the system itself⁽¹⁾. The general notion carries an underlying overall idea of enhancing participation in decision-making processes, and as such has been rapidly emerging and assuming significant importance in recent years, due to its adoption, in different layouts and degrees, by different entities throughout the world. Understanding how diverse governance groups which are structured in such a way and with different geographical and material scopes are formed, operate, how they measure success and feel internal and external sources of impact has been the object of recent studies⁽²⁾. They do not always behave in the same way, not every stakeholder exercises the same influence in the interaction, it is common for stakeholders without direct law enforcement or policy-making capabilities to play non-conventional roles that still need clarification, in summary, not all stakeholders interact in the same level for every step of every kind of process.

1 In fact, Hemmati describes multi-stakeholderism as “processes which aim to bring together all major stakeholders in a new form of communication, decision-finding (and possibly decision-making) on a particular issue. They are also based on recognition of the importance of achieving equity and accountability in communication between stakeholders, involving equitable representation of three or more stakeholder groups and their views. They are based on democratic principles of transparency and participation, and aim to develop partnerships and strengthened networks among stakeholders. MSPs cover a wide spectrum of structures and levels of engagement. They can comprise dialogues on policy or grow to include consensus-building, decision-making and implementation of practical solutions. The exact nature of any such process will depend on the issues, its objectives, participants, scope and time lines, among other factors.” Hemmati, Minu. *Multistakeholder Processes for Governance and Sustainability: Beyond Deadlock and Conflict*, Earthscan, 2002.

2 Gasser, Urs, Budish, Ryan, West, Sarah Myers. *Multistakeholder as Governance Groups: Observations from Case Studies*. The Berkman Center for Internet & Society Research Publication Series: Cambridge, 2015. http://cyber.law.harvard.edu/publications/2014/internet_governance

Multistakeholder governance evidently does not occur only in the internet environment, though it is interesting to notice that Internet processes have always been governed like this and that the universe of the Internet was perhaps the one which contributed the most to the recognition of the important political development that demonstrates that a governance model based on other values, mechanisms and structure is possible. Told from the other side, the story is also true. Internet would probably not have turned into what it is today if it were not for the governance model in which it developed. It seems, thus, that the structure of Internet model draws the multistakeholder model as a proper fit. Essentially technical multistakeholder cooperation, for example, has been in place for almost 50 years in the environment of the Internet Engineering Task Force (IETF), a community in which the practice of decisions by rough consensus (and running code) not only works, but also fits better than traditional law-enforcement practices. The same may hold true for some other global dynamic issues. Evidently, the interests of early times were much less complicated than transversal issues which are on the spotlight today as long as Internet Governance is concerned.

This work attempts to critically analyze multistakeholder processes carried out in Brazil, such as the Internet Governance experience through the Brazilian Internet Steering Committee (CGI), the elaboration of Marco Civil and the discussion of other bills that affect the exercise of citizenship, online rights and freedoms, through the lenses of the arguments expressed above, with the objective of contributing to a broader view of the perspectives, strengths and pitfalls that a multistakeholder approach to such initiatives can bring.

2. MULTISTAKEHOLDERISM

2.1 What is multistakeholder?

When current discussions refer to the term *multistakeholder* they are invariably invoking ideas from governance theory that are indeed closely connected to administration issues, but which are also evidently important in other aspects, since multistakeholder implies a political, a legal, a communicational dimension, to name but a few. In the relevant literature it is possible to address the construction starting from a core assumption that the State alone can no longer deal with all the pressing needs and challenges of society, From that comes a description of a viable new arrangement to tackle this new situation in terms of some of its characteristics such as “‘responsive regulation’, informal cooperation, public-private partnerships, and multistakeholder processes”.⁽³⁾

A multistakeholder governance initiative, as already mentioned, is one meant to involve players beyond traditional ones, and search to widen the scope of their representation so as to bring new actors, such as civil society, industry and academia, to overall management, policy-making, decision and enforcement discussions, taking into consideration the need for improved legitimacy in the environment they operate.⁽⁴⁾

2.2. What is multistakeholder for?

Issues of transnational, global reach currently seem to demand such an approach naturally, because it seems like no other option can efficiently fit as an optimal solution when governance matters cross borders. However, the fact that the problems transcend geographical limits does not seem to be an essential characteristic for the proposition and adoption of a multistakeholder model. In fact, such initiatives have expanded and are being explored in virtually any circumstance where it is clear that the State is no

3 John Gerard Ruggie, THE GLOBAL FORUM Global Governance and “New Governance Theory”: Lessons from Business and Human Rights, *Global Governance* 20 (2014), 5–17

4 (Adelman and Morris, 1997), (Abbott and Duncan Snidal, 2013), (Gillies, 1993), (Pattberg and Widerberg, 2014).

longer in the best position to face the problems exclusively with the resources at its hand.

The purposes of the adoption of such an arrangement also include the necessity of an increment in the perception of legitimacy and representation that the situation demands. Goals in law and public policy are essentially shaped by complex institutional processes and an institutionalist view allows a better analysis of the multi-stakeholder inputs that are apparently relevant to understand the factual of the context, given the scale, the nature and the diversity of the interest groups that legal mechanisms affect in this field, and the intertwined way they collaborate and interact. An institutional perspective is also suitable to try to establish a relationship between the norms of action which are currently applicable to this dynamic environment of broad range institutional experimentation, and norms of being that are eventually identified or proposed as the ones that ought to govern the realm.

A number of relevant global digital-technology-and-innovation-related governance processes are already based on multistakeholder arrangements, in a search to widen the scope of their representation, bringing actors such as civil society, industry and academia, to overall management, policy-making, decision and enforcement discussions. The justification for this new sort of settlement, as already referred to, is the need for improved legitimacy in the environment they operate.

One key question for the present and for the future is to understand if this model which was enough to deal with the simpler questions of early times, full of trust and dreams, remains sufficiently sustainable nowadays so as to be useful in the task of tackling and managing the very delicate issues that range from the existence of adequate legislative procedures currently in place to face the dynamics of social and economical digital models to government surveillance, security, citizenship and democracy, the exercise of freedoms in its various forms, cyberwarfare and ultimately national security. Technological decisions are now clearly much more politically charged than they might have been in the beginning of the development of the Internet, and no other global multistakeholder governance structure faces a similar scale of challenges in the decisions it has to take, or has ever had to go through such increasingly and evolving complexity tests, which will only get more complex as new issues come to the stage. Internet Governance is currently the widest multistakeholder process in

the world, the one that potentially affects more people and global issues, and it is undeniably important because it involves the technical mediation of the public sphere and the privatization of some conditions for freedom in that public sphere⁽⁵⁾, a technical mediation which in the end decides what kind of space unfolds, and which is growingly assisted, fed back and automated by technology, based on the amount of data collected and algorithmically processed in a way we most of the times do not properly understand or even attempt to scrutinize or validate.

Finally, transparency and accountability also appear as desired byproducts of this multidimensional point of view of problem solving.

2.3. Who is multistakeholder?

To consider that a certain initiative has a multistakeholder nature it is not enough that its representatives come from various sectors or backgrounds. It is essential to observe in which capacity they act and which interests they support while acting in the process. If representatives have initial access to the governance structure from different sectors but are institutionally required to abandon the interest of that original group once they take their place, a so to speak multistakeholder model is not precisely what is being described. For that to be configured, it is necessary that representatives hold on to the interests of their original group or sector while developing their activities, although some institutional common grounds for collective action are indispensable for the experience to produce results, much like an “informal parliament”.

That being said, such structures have been concretely adopted in a number of real-life situations⁽⁶⁾, such as in the case of the Worldwide Slot Guidelines (WSG), agreements under the auspices of the International Air Transport Association (IATA) in order to allocate airport capacity, in the *Enquete-Kommission Internet und digitale Gesellschaft*, a parliamentary inquiry body of the German *Bundestag*, in a water resource management initiative in the White Volta River Basin, spanning across Ghana, Burkina Faso, Benin, Togo, Mali, and Cote d’Ivoire, and in some directly technology-

5 DeNardis, L. *The Global War on Internet Governance*. New Haven, CT: Yale University Press, 2014.

6 Gasser, Urs, Budish, Ryan, West, Sarah Myers. *Multistakeholder as Governance Groups: Observations from Case Studies*. The Berkman Center for Internet & Society Research Publication Series: Cambridge, 2015. http://cyber.law.harvard.edu/publications/2014/internet_governance

related initiatives such as the development of the Brazilian Internet Bill of Rights *Marco Civil* and in the NetMundial Initiative, allowing insights and evaluations of their impact and of the consequences of their adoption.

2.4. What is not multistakeholder?

A brief final word to reflect upon this initial conceptual analysis may be necessary to point out some criticism and limitations to the idea of what is to be expected from a multistakeholder model of governance.

The most important one seems to be the general recognition that giving civil society 5 minutes of say just the day before a meeting when decisions have all been already taken is anything but multistakeholder. It is paramount to “observe if stakeholders are participating, how participation is balanced, how the body and the stakeholders are accountable to each other for their roles in the process and if the body constitutes an empowered space”⁽⁷⁾. There is not an initiative where we can say governance is truly shared among interested parts to some extent where “social actors are not actual political actors⁽⁸⁾”, if they do not become real interlocutors in the processes, because this will mean that they do not participate, engage and actually influence the formation of the political discourse. This is probably the reason why the idea in many cases is still considered rather as an abstraction with narrow practical use and impact. Trying to give it a more politically relevant sense would mean facing shortcomings such as those which were highlighted, along with issues of enforcement, sovereignty and jurisdiction, as well as data curation concerning contributions that come from multiple inputs.

7 Malcolm, Jeremy. Criteria of meaningful stakeholder inclusion in internet governance. Internet Policy Review, 4(4). 2015 DOI: 10.14763/2015.4.391 <http://policyreview.info/node/391/pdf>

8 Durante, Massimo. The Democratic Governance of Information Societies. A Critique to the Theory of Stakeholders. Philosophy & Technology 2015.

3. A MULTISTAKEHOLDER EXPERIENCE OF INTERNET GOVERNANCE – BRAZILIAN INTERNET STEERING COMMITTEE (CGI)

3.1. Description and Organization

[Interministerial Ordinance 147](#), of May 31st, 1995, later amended by [Presidential Decree 4,829 of September 3rd, 2003](#), established The Brazilian Internet Steering Committee (CGI.br) “with the purpose of coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the services available”⁽⁹⁾. The importance of its role has recently been strongly reinforced with the recognition of the legal obligation that it be heard and consulted in several Internet Governance-related matters, according to Marco Civil⁽¹⁰⁾. The pursuit of its missions include the proposition of policies and procedures regarding the regulation of Internet activities, the recommendation of standards for technical and operational procedures for the Internet in Brazil, the establishment of strategic directives related to the use and development of the Internet in Brazil, among others. It is also responsible for the administration and the coordination of the allocation of Internet addresses (IPs) and registration in the <.br> domain.

It gathers members appointed by the government, by the internet industry, by the civil society and by the academic community. It is a successful experience of participatory model of governance for the Internet in decisions involving network implementation, management and use. Members have been elected since July 2004 to participate in discussions and to debate priorities for the Internet, together with the government.

3.2. Recent Developments

The Brazilian Internet Steering Committee has been playing an important role in Brazil in general since its establishment, but some more recent episodes can clearly point out specific trends and demonstrate relevant interventions and points of view

⁹ <http://www.cgi.br/about/>

¹⁰ Article 9º, §1º, and Article 24, II, of Marco Civil, Lei n.º 12.965, de 23 de Abril de 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm

stemming from this multistakeholder structure, that are worth highlighting for the purposes of the present analysis.

3.2.1. Marco Civil

Brazil has enacted a Bill of Rights for the Internet, widely known throughout the world as Marco Civil. It is legally binding in Brazil as of 2014, and it structures basic principles for the protection of civil liberties regarding the use of Internet in the country, specially considering personal data, liability and the so-called issue of *NetNeutrality*. The Steering Committee had a very important role in the way public consultations for the discussion of the bill were conducted, by enabling a public open platform through which contributions to the process could come from anyone, anywhere, at any time, and also through the promotion of seminars, events, through the participation in public hearings in various commissions in the National Congress and through awareness and capacity building initiatives. It was a very important moment of consolidation for the Committee, and this was reflected in the importance CGI was given in the final enacted text of the Law, which recognized, as already stated, its relevance as an actor in internet governance issues and decisions in Brazil. The diversity of the composition of CGI.br, the different backgrounds and interest groups which its members represent and the several points of view that are shared in its environment certainly contributed to the adequate and successful acting of the organism during the process.

The initiative of Marco Civil contains imperfections, in spite of all the celebration around it. In theory the Statute still permits fractures in the fundamental rights it intends to guarantee. It happens when it establishes, for example, a detailed legal framework for personal data collection and retention without setting – because it does not exist – a similar framework for data protection in Brazil, not even an equivalent one in terms of the level of detailed legal treatment.

These fractures are putting Marco Civil under a stress test. Along the latest weeks, the Committee has been pressed to act in the course of the work of an Inquiry Commission which was established in Brazil in 2015 with the purpose of investigating the scenario of cybercrime in Brazil and its social and economic effects. [The final report](#)

of the Commission was released in April 2016, and it carries unsettling conclusions like that “E-commerce is a wide category of criminal practices (...).” The way the final text was written and presented, showing that there was not even enough time and attention to perceive and correct such an absurd statement gives a good idea of the inconsistency of the work. This has been urging CGI to act towards preventing amendments of Marco Civil that essentially dismantle it as the important, collectively constructed Bill of Internet Rights that it represents. These bills attempt to fill this important piece of legislation with substantive criminal and criminal procedure matters, instead of dealing with these questions in a different and more appropriate legal instrument or debate.

It would not even be necessary to amend Marco Civil and risk its core text, when there is an ongoing process of regulation of the Law, also under the oversight of the Steering Committee, through which minor adjustments are possible without compromising the key issues, without a setback in the rights which are more difficult to guarantee and negotiate under a harder, more controversial legislative process. Marco Civil is not a space to detail strategies of Public Security. Marco Civil is a Bill of Rights for the Citizen. It is not a statute to ensure State prerogatives. It is an affirmation of individual rights and guarantees. Of course it should – and it does – contain general exceptions designed to reconcile the individual interests it protects with other public ones, should conflicts arise. But if this essential conception is not taken into consideration, each and every attempt to amend Marco Civil in Brazil will result in a distortion of its purpose, because of a lack of understanding of the very reasons why it exists. This is a position which is being endorsed by the CGI during this process.

3.2.2. *WhatsApp*

More recently, a judicial order determining the suspension of the service provided by WhatsApp application in Brazil called once again for the intervention of CGI, through a [clarification note](#). The suspension was decided and determined in the course of a lawsuit in which a first instance judge ordered representatives of Facebook (since Brazilian justice holds that for the purpose of the incidence of national jurisdiction Facebook and WhatsApp are part of the same industry conglomerate) to hand in information deemed essential to the investigation and prosecution in a drug traffic case. The content of certain communications was among that information. Apart

from other arguments, the company raised the issue that the recently default-enabled end-to-end cryptography that it adopted and implemented to protect its users does not allow even the developer to access the content of messages. Controversy established, the order searching to compel the company to hand in the information was implemented for some hours before a suspension order was issued by a higher court.

The episode urged the Steering Committee to take stand as an interpreter of Marco Civil, clarifying that Article 12 of the Statute, used as the judge as legal ground for the suspension order, does not refer to the possibility of suspending services due to general illicit activities, but merely as a sanction against data protection violations, which would hold the suspension order in the case inadequate and illegal, since outside the scope of the mentioned provision. The Committee also pointed out to the disproportional nature of the adopted measure and to the fact that any imposition of liability of Internet stakeholders should be limited “to the specific extent of the activities they perform”¹¹. The Inquiry Commission Report mentioned in the last section also intends to amend issues in this respect, and the clarification from CGI also addresses those particular questions, in an attempt to keep any eventual new measures closely connected with the values and interests which this statute intended to protect, preventing liberties and guarantees which are protected in Marco Civil from being affected by the proposed bills.

11 CLARIFICATION NOTE in virtue of the decision issued by the Honorable Judge of the 1st Lower Criminal court of São Bernardo do Campo, ordering the suspension of the Internet application “Whatsapp” in the national territory of Brazil. <http://www.cgi.br/esclarecimento/clarification-note-december-2015/>

4. CONCLUSIONS – A MATTER OF PERSPECTIVE

There is no perfect governance model ready and thoroughly developed to be adopted in order to face the new challenges that a networked society presents. If the search is for an easy answer in the form a miracle model, then multistakeholderism is a fail, as it is, as a matter of fact, any other governance structure applied to organize and discipline the digital dimension of a modern society.

If, however, the search takes into consideration the specific needs of the time, multistakeholderism, even with its clear limitations, can very well be a way forward. It is in fact hard to think of an adequate strategy in this realm today that does not rise from the multistakeholder perspective. Multistakeholderism may not yet be very well understood, even by the ones who are closest involved with it, not all players are equal, nor all of them have the same weight or exercise the same influence in the same issues, it is certainly not a perfect governance model, but the experiences where it is being employed – internet governance as a main successful example – show that it is still a very interesting and constructive option for managing conflicting interests from different segments of society and to coordinate governance processes in organizations where these different segments must be heard and take part in decision and policy making. In times when issues such as representation and legitimacy can no longer be taken for granted and face a serious crisis, the rise of the alternatives that multistakeholderism present should not be neglected. Such a multi-participative process had already been thought of before, but is now finally possible due to the effective existence of a digital and interconnected environment where necessary interactions can take place. And internet governance is probably the first large and certainly the most relevant global issue that can be conducted under such paradigm. There has to be balance, and it has to be found.

Also, it is an initiative that demands alignment but not necessarily agreement. It is a process of constant consultation among stakeholders, which may ensure that different points of view of a certain issue are looked at each time the discussion is back on the table. In fact it allows the matter never to completely leave the table, with a certain recognized cost to stability, but also with a clear gain in legitimacy, transparency, accountability and oversight. Given the nature of the activities that are connected to the digital environment, the potentially massive and transnational scale of

its activities and consequences to come and the dynamics of this realm, an approach which takes into consideration a greater amount and more diverse inputs makes it plausible to expect a positive impact in the quality of decision-taking and policymaking.

In Brazil, the experience of the Internet Steering Committee, and the recent processes in which it is involved stress out the importance not only of the multidimensional actor itself, but also of innovative problem-solving methods for law discussion, creation and implementation, opposing, for instance, an exclusively court-centric, rights-focused approach to law. Approaching this dimension of normativity through this multiparty and unconventional lens sounds promising, and it is not exclusively an initiative coming from Brazil. The Government in India has recently announced an inclination to a multistakeholder model, though more carefully reserving to the State the functions of security.⁽¹²⁾ It is inevitable to recognize that Jurisdiction, as the prerogative to "tell the Law", evidently remains an essential State function, but at the same time it is essential to understand that exploring possibilities of multistakeholder engagements that involve some degree of delegation of that function, possibilities which have already been experienced, sometimes with more, sometimes with less success in a number of situations is a serious alternative, as the one proposed above – mainly in a transnational scenario where both the distinction and the intersection between the private and public spheres seem to be *digitally* thin.

12 <http://thewire.in/2015/06/22/indias-new-multistakeholder-line-could-be-a-gamechanger-in-global-cyberpolitics-4585/>

CYBERLAW

by CIJIC

AN OVERVIEW OF AN INTERNATIONAL TRIBUNAL FOR THE INTERNET

UMA VISÃO SOBRE UM TRIBUNAL INTERNACIONAL PARA A INTERNET

DANIEL FREIRE E ALMEIDA ¹

¹ Postdoctoral researcher - Visiting Researcher at Georgetown University (Washington-DC). Professor of Internet Law, International Law and International Relations. PhD in International Law, Faculty of Law, Coimbra University, Portugal. PHD Thesis: “*An International Tribunal for the Internet*” (2008-2012).

Lawyer. E-mail: da616@georgetown.edu

RESUMO

Este artigo tem como principal objetivo demonstrar a proposta de criação de um Tribunal Internacional para a Internet. O documento de trabalho é dividido em duas secções. Primeiro, levanta alguns argumentos e aspectos inovadores introduzidos pela Internet e os consequentes desafios na aplicação jurisdicional. Mais especificamente, na segunda parte, apresenta a proposta de que um Tribunal Internacional para a Internet deve ser estabelecido em resposta aos desafios que as jurisdições nacionais estão enfrentando para impor seu Direito.

Palavras-Chave: Direito na Internet; Tribunais Internacionais; Direito Internacional; Tribunal da Internet; Jurisdição na Internet.

ABSTRACT

This article has as its main goal to demonstrate the proposal to establish an International Tribunal for the Internet. The working paper is divided into two sections. First, it raises some arguments and innovative aspects introduced by the Internet and the consequent challenges on jurisdictional enforcement. More specifically in the second section, it suggests that an International Tribunal for the Internet shall be established due to the challenges that national jurisdictions are facing to enforce its law and judicial decisions.

Keywords: Internet Law – CyberLaw - International Courts – International Tribunals - International Law.

INTRODUCTION

The world has witnessed a significant increase in activities of the Internet. This unbridled trend has resulted in the emergence of a number and increasing complexity of private and public disputes, both at the domestic level, and the international dimension.

However, the transnational aspects of the Internet and Electronic Commerce also present international challenges, requiring new forms of global governance to deal with these global issues.

The global nature of the Internet and its global reach, provided by a worldwide architecture, presents a series of jurisdictional complexities to any country wishing to exercise its sovereign power ordinarily. Still, this new system has transformed our lives and our society in shaping judicial aspirations.

This working paper has as its principal objective show the proposal to establish an International Tribunal (Court) for International Law on the Internet⁽²⁾.

For this, the work is divided into two parts. In Part one, raises some of the reasons and innovative aspects introduced by the Internet and the consequent challenges in law enforcement.

More directly in Part two, introduces an overview on the proposal of an International Tribunal for the Internet, to be established due to the challenges that national jurisdictions are facing to enforce its judicial decisions.

2 This working paper is based on our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

1. SOME REASONS TO IMPLEMENT AN INTERNATIONAL TRIBUNAL FOR THE INTERNET

Initially, in a diverse set of legal systems, from the United States of America to the United Kingdom, from India to China, from Norway to France, from Greece to Israel, from Denmark to Brazil, from Portugal to Germany, the problems arising from new technologies, especially those promoted by the different uses of the Internet are seen increasingly as a challenge, complementary and innovative, to traditional national legal systems.

On the same line, users of these new computer systems, leveraged by the Internet, have already required a new type of behavior in the provision of legal services.

Within this new context of digital relationships, and in addition, countries around the world seek closer ties with its citizens, to improve their communication systems and services offerings, as well as trying to follow the changes in society, increasingly digitized⁽³⁾.

In fact, as well, there are disputes arising from new activities on the Internet, which due to the arguments of speed, immediacy, **internationality**, and lodging in the

3 Vide BOEHME-NEßLER, Volker. *CyberLaw. Lehrbuch zum Internet-recht*. München: Verlag C.H. Beck, 2001, p. 333 et seq. In fact, governments around the world are increasingly looking to strengthening their communication links and provision of services to citizens, such as: In Germany - <http://www.deutschland.de> ; in Italy- <http://www.italia.gov.it> ; in the United Kingdom- <http://www.direct.gov.uk> , Cfr. HOUSE OF COMMONS COMMITTEE OF PUBLIC ACCOUNTS. *Government on the Internet: Progress in delivering information and services online*. London: The Stationery Office Limited, Sixteenth Report of Session 2007–08, 2008, p. 01/33. Vide DUTTON, Willian, HELSPER, Ellen, GERBER, Monica. *The Internet in Britain 2009*. Oxford: Oxford Internet Institute, 2009, p. 01/72. Vide, also, NORTON, Pedram. *Directgov: The Right Direction for E-government or a Missed Opportunity?* Journal of Information, Law & Technology, 2008, p. 01/16, Vide GREAT BRITAIN. *Government on the internet: progress in delivering information and services online*. London: The Stationery Office, 2007, See OXFORD INTERNET INSTITUTE at: <http://www.oii.ox.ac.uk/> ; in the United States- <http://www.firstgov.gov> ; in France- <http://www.service-public.fr> ; Austria- <http://www.help.gv.at> ; Spain- <http://www.administracion.es/> ; Brazil- <http://www.brasil.gov.br> ; Portugal- <http://www.portaldocidadao.pt/PORTAL/pt> ; about Greece Vide IGLEZAKIS, Ioannis. *The development of E-Governance and the issue of digital inclusion in Greece with particular regard to the constitutional right of e-participation*. Journal of Information, Law & Technology, 2008, p. 02/24. For an international overview, Vide GRIFFIN, David, TREVORROW, Philippa, HALPIN, Edward. *Developments in e-government: a critical analysis*. Washington, DC: IOS Press, 2007, Vide PAVLICHEV, Alexei, GARSON, David. *Digital government: principles and best practices*. Hershey: Idea Group Publishing, 2004, Vide REMØE, Svend, ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Governance of Innovation Systems*. Paris: OECD, 2005. Vide ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Resolving E-commerce Disputes Online: Asking the Right Questions about ADR*. Paris: OECD publishing, n° 63, 2002, p. 01/07. Vide ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Shaping Policies for the Future of the Internet Economy*. Paris: OECD publishing, n° 148, 2008, p. 09 et seq.

information abroad, among others, cannot wait for the slow and traditional resolution of their disputes, through the national courts⁽⁴⁾.

Indeed, the Internet has created a "tangled web" of legal and scientific complexity that has exceeded the capacity of judicial systems to manage these cases only with traditional and national solutions.

We conclude that to the extent that the new media advance, it seems clear that the current structures and supervision models are not properly prepared to face a world where challenges transcend national boundaries, and in such a constant and numerous way.

In fact, many of the processes that affect individuals, countries and businesses in the Internet world are beyond the jurisdictions of national Judicial Power exercise mechanisms.

We can find several cases around the world showing the global context of the Internet challenging the national context of the courts or tribunals, like Uber's cases, EU-USA data transfer, Google, Facebook, WhatsApp, Apple, Twitter, Microsoft, Alibaba, Netflix, Amazon, cases of Cyber espionage of China, the United States of America, Brazil, European Union, Russia, WikiLeaks, Snowden, among many others.⁽⁵⁾

Also explicitly is the importance that even Judicial Powers being aware of the practical limits of execution of judgments or subjecting decisions against people abroad

4 In this regard, in substance, of deserved prominence is the opinion of WALD (2001), *in verbis*: "Now, we continue to live with legal techniques of the past, without noticing that often become obsolete and that the new economic and technological context must match a new Law, which is not a strait-jacket to prevent the development, but rather, a catalyst for new social aspirations." Vide CALLIESS, Galf-Peter. *Online Dispute Resolution: Consumer Redress in a Global Market Place*. German Law Journal, Volume 07, nº 08, 2006, p. 659. Vide HÖRNLE, Julia. *Cross-border Internet Dispute Resolution*. Cambridge: Cambridge University Press, 2009, p. 26 et seq. Vide POLANSKI, Paul Przemyslaw. *The Internationalization of Internet Law*. In: KLABBERS, Jan, SELLERS, Mortimer. *The Internationalization of Law and Legal Education*. Helsinki & Baltimore: Springer, IUS GENTIUM COMPARATIVE PERSPECTIVES ON LAW AND JUSTICE, 2008, p. 191/210; Cfr. WALD, Arnoldo. *Prefácio*. In: CHALHUB, Melhim Namem. *Trust*. Rio de Janeiro: Renovar, 2001, Preface.

5 A complete list of cases, with details, can be found in our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

(that is, to exercise its jurisdiction), they are reluctant to openly admit the limits of their power over the Internet.

However, the reality prevails and many Internet judgments of the Internet remain unforced.

In other words, there is nothing more international than the Internet, and the national States, originally territorial, are being challenged in the exercise of their sovereign power in this virtual space.

In this context, the needs grow to require new forms of global governance to deal with these global issues. Also, with the increase of Internet users, and to the extent that international problems brought to light also grow, the answers should also be international.

In this course, it's important to emphasize that the traditional Law faces growing challenges. Beginning with the clear internationality of the Internet. In the same line of reasoning, there is no physical barriers to online mobility, and the forms of control, therefore, have not been prepared in order to focus on the new virtual activities. In fact, one of the challenges faced by the judge is to achieve effectively the subordination of a certain foreign defendant in a lawsuit initiated in his country, like we observed by the recent case of WhatsApp in Brazil⁽⁶⁾.

On the other hand, we find that in some cases the applicants did not even have access to a meritorious decision, by the simple fact that the Tribunals deviated from the jurisdiction. Equally, we can admit that to the extent that more people are subject to different spatial domains, it leads to a conflict or sometimes convenience between the sovereign powers.

Still, we look into as to what legislation could subject the behavior of a citizen or company linked to multiple sovereignties, in time of any trial. In addition, the situations caused by the Internet and the solutions offered by the Treaties and Regulations were not prepared taking into consideration this new context.

6 See REUTERS, "Brazil judge orders WhatsApp blocked, affecting 100 million users". Available at <http://www.reuters.com/article/us-facebook-brazil-whatsapp-idUSKCN0XT1KB>, 05.03.2016.

Moreover, fundamentally, we must emphasize that the freedom that both attracts people to the Internet at the same time, and paradoxically, to be properly maintained need some sort of order, either by new regulatory means, whether by new judicial means.

The new spaces created by the Internet, or cyberspace, have increased this debate considerably⁽⁷⁾.

In this sense, we consider the need for a new plan, due to the current lack of ability to respond to all electronic issues facing forward to the national Judicial Powers⁽⁸⁾.

For all titles, it arises therefore the need for a new paradigm⁽⁹⁾. Everything therefore in the direction of an international judicialization, more efficient and suitable for the world of the Internet:

- **AN INTERNATIONAL TRIBUNAL FOR THE INTERNET⁽¹⁰⁾.**

Under the new materials that Law, as well as International Law has absorbed, it is highlighted the need of an effective international justice, arising from the supplementary assimilation of issues that were of absolute (*or not*) dominance of the States⁽¹¹⁾.

7 Also, we realized that international cooperation mechanisms such as letters rogatory, *in exemplis*, are too slow for the days of the Internet, and urgently need to be improved if they are to meet the legitimate aspirations of their jurisdictional. Vide KLEINWÄCHTER, Wolfgang, DORIA, Avri. *Internet Governance Forum (IGF). The First Two Years*. Paris: UNESCO, 2010, p. 324. Vide DIZARD, Wilson. *Digital diplomacy: U.S. foreign policy in the information age*. Washington: Praeger, 2001, p. 99 et seq.

8 A complete list of arguments and reasons can to be found in our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

9 Cfr. VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism and Particularism as Paradigms of International Law*. New York: International Law and Justice Working Paper 2008/3, p. 57 et seq. Cfr. RABINOVICH-EINY, Orna. *Beyond Efficiency: The Transformation of Courts Through Technology*. UCLA Journal of Law & Technology, Volume 12, n° 01, 2008, p. 03.

10 See our book: FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

11 In general, Vide RÖBEN, Volker. *The Enforcement Authority of International Institutions*. In: GOLDMANN, Matthias VON BOGDANDY, Armin, WOLFRUM, Rüdiger, VON BERNSTORFF,

In this perspective, CASELLA, ACCIOLY and NASCIMENTO E SILVA (2008), believe that the understanding and the scope of International Law only consolidate to the extent that it has the impossibility awareness and operational inadequacy of national systems to confront current needs⁽¹²⁾.

The new dimension brought by the Internet, entitled cyberspace, did not ask the consent of the States to constitute a global scale. The International Law, then, if it does not wish to position itself as inefficient or ineffective, must incorporate the real problems, and star in its actions aimed at establishment of justice, also on a global scale⁽¹³⁾.

In the segment of the Internet, it should be put into perspective its future evolution. In fact, today's importance of International Law is revealed by the many areas that came to absorb, such as the International Economic Law, International Communication Law, International Law of Outer Space, the International Environmental Law, International Human Rights Law, the International Criminal Law and International Sports Law, among others⁽¹⁴⁾.

Jochen, DANN, Philipp. *The Exercise of Public Authority by International Institutions: Advancing International Institutional Law*. Heidelberg: Springer, 2010, p. 819/840. Vide VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism and Particularism as Paradigms of International Law*. New York: International Law and Justice Working Paper 2008/3, p. 57 et seq. Vide LEITE DE CAMPOS, Diogo. *Preface*. In: GOMES, Fabio Luiz. *Direito Internacional. Perspectivas Contemporâneas*. São Paulo: Saraiva, 2010, p. 5/8.

12Cfr. CASELLA, Paulo Borba, ACCIOLY, Hildebrando, NASCIMENTO E SILVA, G. E. do. *Manual de Direito Internacional Público*. São Paulo: Saraiva, 2008, p. 99.

13 Vide UERPMANN-WITZACK, Robert. *Internethölkerrecht*. Archiv des Völkerrechts, Volume 47, Number 3, September 2009, p. 261/283.

14Cfr. MACHADO, Jónatas E. M. *Direito Internacional. Do Paradigma Clássico ao Pós-11 de Setembro*. Coimbra: Coimbra Ed., 2006. p. 96. About the International Economic Law, Vide SALACUSE, Jeswald. *The Emerging Global Regime for Investment*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010, p. 427/473. Vide MELLO, Celso D. de Albuquerque. *Curso de Direito Internacional Público*. Rio de Janeiro: Renovar, 2º Volume, 2004, p. 1683 et seq. Vide ROBERTS, Paul. *Comparative Criminal Justice Goes Global*. Oxford Journal of Legal Studies, Volume 28, Number 02, 2008, p. 369/391. Vide CLAPHAM, Andrew. *The Role of the Individual in International Law*. The European Journal of International Law, Volume 21, Number 01, 2010, p. 25/30. Vide, also, LIMA PINHEIRO, Luís. *Direito Internacional Privado*. Coimbra: Almedina, Volume 1, 2008, and LIMA PINHEIRO, Luís. *O Direito aplicável aos Contratos Celebrados através da Internet*. In: PINHEIRO, Luís de Lima. *Estudos de Direito Internacional Privado*. Coimbra: Almedina, Volume II, 2009.

In all dimensions to what it was called, International Law sought to give their contribution. Whether on land, at sea, in the air or in space, new international legality thresholds were tacked⁽¹⁵⁾.

But to do so, it cannot and it should not be based on previous paradigms on which were based several theories "inter / nationalist", largely negating the possibility of a, complementary or shared Law, in a Global scale⁽¹⁶⁾.

Many of them supported by facts and acts situated in anterior temporal moment in which there was not even the airplane as a means of international transport, and to increase international relations⁽¹⁷⁾. The importance of such a claim is covered on the premise that international relations have become more commonplace to the extent that new international means of transport emerged, *in casu* the airplane.

But now, transportation is also virtual, digital, instantaneous, and global with the Internet.

In other words, the needs, conditions, prospects, and dimensions established are also international, global.

15 Regarding the international legal treatment of the various dimensions of the territory in its terrestrial, maritime, aeronautical fields, as well as in the legal treatment of outer space, Vide CASELLA, Paulo Borba. *Direito Internacional dos Espaços*. São Paulo: Atlas, 2009. Vide SIMMA, Bruno. *Universality of International Law from the Perspective of a Practitioner*. The European Journal of International Law, Volume 20, Number 02, 2009, p. 265/297. Vide OWADA, Hisashi. *The Rule of Law in a Globalizing World – An Asian Perspective*. Washington University Global Studies Law Review, Volume 7, Number 02, 2008, p. 193/194. Vide SALACUSE, Jeswald. *The Emerging Global Regime for Investment*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010, p. 427/473. Vide UERPMANN-WITZACK, Robert. *Principles of International Internet Law*. German Law Journal, Volume 11, nº 11, 2010, p. 1245/1263. Vide BÚRCA, Gráinne de. *The European Tribunal of Justice and the International Legal Order After Kadi*. Harvard International Law Journal, Volume 51, Number 1, Winter 2010, p. 01/49. Vide MACHADO, Jónatas E. M. *Direito Internacional. Do Paradigma Clássico ao Pós-11 de Setembro*. Coimbra: Coimbra Ed., 2006. p. 96/97. Vide FREIRE E ALMEIDA, Daniel. *Bioterrorism Act – A Nova Política Externa dos EUA e a Eleição Presidencial sob a Perspectiva Diplomática do Brasil*. In: SAVINO, Luis María (Org.). *Las Elecciones de los Estados Unidos y El Impacto Global*. Buenos Aires: Fundación Centro de Estudios Americanos, 2004, p. 157/173. Also, see FREIRE E ALMEIDA, Daniel. *The Taxation of Electronic Commerce in the United States of America and in the European Union*. São Paulo: Almedina, 2016.

16 Cfr. In a favorable position to the universalism, VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism and Particularism as Paradigms of International Law*. New York: International Law and Justice Working Paper 2008/3, p. 57 et seq. On the conduct for a Universal International Law, Vide LORCA, Arnulf Becker. *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010, p. 475/552.

17 Vide VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism Renewed: Habermas' Theory of International Order in Light of Competing Paradigms*. German Law Journal, Volume 10, nº 01, 2009, p. 05/30.

The benefits of global judicialization of international disputes on the Internet, with proper organization, would allow for greater efficiency in the search for justice and legal security. In this sphere, international Law arises with promising fundamental perspective⁽¹⁸⁾.

The Internet constitutes a topic that concerns all peoples, and it is used across the globe, the different computer systems are interconnected, the various languages find their universal terminology⁽¹⁹⁾.

On the other hand, the arguments seeking to overturn the additional possibility of a World Law, Global or a *Universelles Völkerrecht* in no time mention the phenomenon of the Internet.

The paradigms have changed, we need to understand them, formulate new international routes, and address them.

Because of this goal, and in order to resolve the issues raised, we are to propose the unprecedented **International Tribunal for the Internet**, presenting it in its essential aspects⁽²⁰⁾.

18 Vide CASSESE, Sabino. *Regulation, Adjudication and Dispute Resolution Beyond the State*. Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008, p. 25 et seq. Vide KASTO, Jalil. *New International Order and International Law After the Millennium*. London: International Law Series n° 07, 2002, p. 12 et seq. Vide WESTON, Burns, FALK, Richard, CHARLESWORTH, Hilary, STRAUSS, Andrew. *International Law and World Order*. St. Paul: Thomson/West, 2006. Vide VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism and Particularism as Paradigms of International Law*. New York: International Law and Justice Working Paper 2008/3, p. 57 et seq. Vide SIMMA, Bruno. *Universality of International Law from the Perspective of a Practitioner*. The European Journal of International Law, Volume 20, Number 02, 2009, p. 265/297. Vide OWADA, Hisashi. *The Rule of Law in a Globalizing World – An Asian Perspective*. Washington University Global Studies Law Review, Volume 7, Number 02, 2008, p. 187/205. Vide LORCA, Arnulf Becker. *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010, p. 475/552. Vide UERPMANN-WITZACK, Robert. *Internetvölkerrecht*. Archiv des Völkerrechts, Volume 47, Number 3, September 2009, p. 261/283.

19 Vide HUNTINGTON, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster, 2003, p. 59/64. Vide CASTELLS, Manuel. *A Era da Informação: Economia, Sociedade e Cultura. (O Poder da Identidade- Volume II)*. Lisboa: Fundação Calouste Gulbenkian, 2003, p. 63. Vide SCHOR, Miguel. *Mapping Comparative Judicial Review*. Washington University Global Studies Law Review, Volume 7, Number 02, 2008, p. 281.

20 A complete list of arguments and reasons can to be found in our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

2. AN OVERVIEW OF AN INTERNATIONAL TRIBUNAL FOR THE INTERNET

Initially, we can state that, purposely, we seek rather take utility of assessing the experiences and best practices implemented previously in international legal areas. On the other hand, it is explicit the importance of the efforts of developing analysis related to Internet governance.

Preliminarily, this initial focus lead us to a coherent integration to the desired starting point the International Tribunal for the Internet.

In the original point, we dedicate, then, our investigations and reflections concerning the International Legal System to be adopted by the Tribunal, with the outlined solution, with the possible models focused on its Starting Point, as well as the establishment of its headquarters.

In continuation, we cover the national scope of the Tribunal for the Internet, with its main purposes. In this order, and in order to resolve the issues raised, we try to discuss the fundamental concerning admissibility criteria and the stipulations relating to the Applicable Law.

Starting from the essence of the investigated points⁽²¹⁾, we consider, in this part of our study, the need for a prospective deepening on organizational composition of the Tribunal, with its basic tasks.

In this context, regarding the Rules of Procedure to be implemented as of now, it is focusing on the desire and the need for such a Tribunal to gather assumptions passing through Procedural innovations (*Scanning of Procedural Parts, Celerity of Formalities, online audiences*), Technological Innovations (*appropriate technological means for Law operators to carry out the changes raised*), and Organizational Innovations (*Personal and Functional*). Everything, therefore, to be addressed, along with the Procedural Phases idealized, and aligned with the proposed innovations.

21 See our book: FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

By position, it is not intended, here, to define in detail thorough all the ins and outs of a future founder treaty, but the essential aspects involving the issues discussed during this working paper⁽²²⁾.

It is appropriate to alert at this point that, even if they have different views on the following topics, and of course there will be, the suggestions that follow are the result of further reflection, deep reading (over 2,500 authors), constant monitoring of digital practice, fundamental jurisprudential analysis, search for the best technique available, alignment to the evolutionary future of Digital Society, and above all, a spirit of wellness for global collective (*us*)⁽²³⁾.

Changes, obviously, will be the result of suggestions and subsequent negotiations around the most sensitive points to countries, individuals, and participating companies.

It is under this perspective, then, we present our conclusions about the contours of the **International Tribunal for the Internet**, listed below, topically⁽²⁴⁾.

1. First, the Tribunal would possess the specific purpose of judging international disputes relating to the Internet and International Electronic Commerce.
2. Accordingly, in becoming an international organization focused on the prosecution of international conflicts of the Internet and Electronic Commerce, possess legal personality of International Law, provided also the international legal capacity necessary for the performance of all its functions, and the full attainment of its objectives.

22 A complete list of arguments, reasons and details can to be found in our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

23 Vide, about this perspective, LEITE DE CAMPOS, Diogo. *O Direito em NÓS*. New York: Lawinter Review, Volume I, Issue 1, March 2010, p. 05/30.

24 This working paper is based on our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

Two important points result of this condition, namely, the Tribunal could negotiate and conclude treaties, and still would be independent of States, companies and other International Organizations. These points are extremely important in international judicial activity.

3. The Tribunal's headquarters will be in location that fulfills the conditions necessary for the implementation of the agency under review, and the Tribunal would own regional headquarters in the territory of any State Party. In these places, besides the exercise of its powers and purposes, people and businesses have the opportunity to access the Tribunal.
4. The Tribunal should have universal jurisdiction, encompassing natural persons, companies, States and International Organizations, with the key objective to judge international disputes relating to the Internet and Electronic Commerce.
5. However, international cases from the Internet and Electronic Commerce would be jurisdiction of the Tribunal, where not properly appreciated, tried or executed previously by national or international courts, in judicial exercise.
6. But, if the country, the company or person you want to drive directly an international demand in the International Tribunal for the Internet, this would be possible without the prior need to establish the proceedings in another national authority, judicial or extrajudicial.
7. In a complementary purpose, the Tribunal may be called upon to run earlier international decisions that have become difficult to implement by countries with meritorious discussion, with *res judicata*.
8. Similarly, cases that require the cooperation of other countries or the Internet companies may be mediated by the Tribunal, by communication, request an investigation and interconnection between the parties involved.
9. Finally, in this area, the Tribunal would be able to advise on relevant and international issues involving Internet Law.
10. The Member State, or Compliant with the founder Treaty, shall accept the universal jurisdiction of the International Tribunal for the Internet, including its jurisdictional, individuals and companies.

11. In cases where the applicant or defendant, company or person, under the jurisdiction of a non-member of the Treaty, the Tribunal shall conduct proceedings for possible acceptance of the country in question, in the specific case, and for all other subsequent cases involving the non-member country.
12. Another possibility of cases before the Tribunal admission would be one resulting from the acceptance of forum clause, or international agreement, established in terms of service of the Internet Web sites that sets out the jurisdiction of the International Tribunal for the Internet.
13. Likewise, the Tribunal judge demands set forth by international Treaty establishing the Tribunal's jurisdiction by interested countries and international organizations.
14. In order to avoid national legal delays, the Tribunal's jurisdiction could be thrown by the person who does not receive appropriate legal treatment of a Member State for a period of twelve (12) months from the filing date of the lawsuit, in case option of the plaintiff by the adjudicative nationally.
15. In consequence of the difficulty of national trial in cases of great international repercussion, the Tribunal may exercise jurisdiction.
16. However, it must be that the Tribunal only enjoy in investigative or adjudicative headquarters, cases occurring after the entry into force of its founder Treaty.
17. But, the issues of judgment of the Tribunal does not decay or prescribe.
18. Likewise, there would be no exclusion of jurisdiction in relation to the age of the person concerned or defendant⁽²⁵⁾.
19. On the other hand, stands out, that the Tribunal would use as sources from the founder International Treaty of the International Tribunal for the Internet, to the

25 A complete list of arguments, reasons and details can to be found in our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

International Treaties related to the Internet, Electronic Commerce and Information Society.

20. Also, the Tribunal would use the Law chosen by the parties resulting from the application of an international agreement or terms of service of Web sites on the Internet, consistent with the Treaty of the International Tribunal to the Internet.
21. In the same vein, in a subsidiary and complementary way, the Tribunal would resort to international treaties in general, the International Customary Law, Principles of International Law, Principles of the Internet Law, the International Tribunal for the Internet, and the Doctrine of publicists and International academics of Internet Law, where applicable.
22. In the absence or inapplicability of all previous international sources, the domestic law of the jurisdictions involved, related to the Information Society, Internet, and Electronic Commerce, with primacy by the national law of the process of victim in question, and where the legislation is compatible with the purposes of the Treaty of the International Tribunal for the Internet, and the sources of international law.
23. For there to be an effective international judicial activity, the Tribunal shall be composed of a General Assembly, by a General Secretariat, by a Chamber of Prosecutors, by International Lawyers, by Diplomats in the service of the Tribunal, and by a Chamber of Judges.

Each of these bodies would be essential for the full implementation of the tasks related to the Tribunal.
24. At the General Assembly all States and International Organizations members have right to speak and vote. Moreover, this would be the appropriate forum for bringing, discussion and implementation of treaties defining International Law on the Internet and Electronic Commerce.
25. Have the Director General to manage the Registry of the Tribunal, would be the holder of the international relations of the Tribunal and shall establish relations with the countries, International Organizations and companies, as well

as enter into treaties on behalf and in the interest of the Tribunal. In addition, the General Secretariat takes care of the management, permanently, of the entire internal structure of the International Tribunal for the Internet, and the operation, communication and negotiation of future interests.

26. In addition to the required neutrality in the tasks of the Secretariat, the servers would be appointed by the Director General, through global selection process, ensuring the highest standards of efficiency, competence, impartiality, neutrality and integrity, and may be appointed to perform functions on any of the organs of the International Tribunal for the Internet.
27. With the same arguments explained above, would be the appointment of Judges, Prosecutors, Diplomats and International Lawyers of the Tribunal.
28. The Judge's Chamber, responsible for adjudicative task, would be divided into sub-chambers of Instruction, Specialized and General Chambers, and of Specialized and General Chambers of Resource.
29. In turn, Prosecutors must instruct the international investigations, submit and track complaints based on information about the Tribunal's jurisdiction practices. To this end, can gather additional information from States, corporations, individuals and other organizations as well as seeking receive written, scanned or oral testimony at the Tribunal headquarters or regional headquarters located in the participating countries, with criteria guided by prudence, neutrality and maximum efficiency.
30. The International Lawyers represent the authors or defendants in Tribunal lawsuits, where they do not have financial means to hire a lawyer.
31. With regard to the Diplomats of the Tribunal, these would be directed and appointed by the Director General, and shall represent the Tribunal's purposes, organize integration of conferences, meetings focused on multilateral negotiations to promote the Applicable Law to the Tribunal, actively participate in regular and extraordinary meetings, survey the international diplomatic positions the Tribunal should adopt and participate in the presentation of goals, proposals, strategies, and negotiations of interest of the International Tribunal for the Internet.

32. Another key point to the Tribunal, would be its Procedures, guided by judicial innovations, with adoption of all means and proper technological conditions for the Tribunal to exercise its operators working expeditious and effective internationally.
33. The procedural steps would be initiated by the International Investigation, going to the Presentation of Action and consequent International Contestation. In being necessary, additional evidence could be presented, seeking the cooperation of Internet companies, countries and International Organizations. Judgment and Decision would end the initial adjudication phase, and is possible to appeal once. Anyhow, using or not the appeal, the execution stage would end the action in Tribunal⁽²⁶⁾.
34. In order to make up to universally, the constitutive Treaty would be open for signature by all States and International Organizations on the planet.
35. With associative effect, the Treaty would be open to Internet companies and International Internet Commerce companies, seeking a regime of cooperation.
36. To the Judicial work, the English language would be the authentic language, ensuring the translation into Chinese, the Spanish, the Arabic, the Portuguese, the Japanese, the Russian, the German, the French, and the Malaysian language.
37. In respect to decisions on amendments or revisions of the founder Treaty of the Tribunal, or supervening texts that this should be part as attachments, shall be taken by a majority of two thirds of the States and International Organizations members present and voting.
38. All the locations of the Tribunal are expected to benefit by guaranteed privileges and immunities to the embassies of any sovereignty, and headquarters of International Organizations, and the servers, Judges, Prosecutors, Diplomats and International Lawyers. Similarly should be the treatment of technological

26 This working paper is based on our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3.

devices, including the Tribunal's communication networks and its agencies, which should receive similar treatment to those above, with absolute inviolability and immunity from jurisdiction.

39. Note that the founder Treaty of the International Tribunal for the Internet would not allow reservations to your text, and the Annexes Treaties.
40. For all the financial maintenance of the Tribunal, should help participating States through quotas. The Tribunal may, on occasion, to use the personal services, furniture and real estate, placed at their disposal, free of charge, by States Parties, other Organizations and companies with a view to collaboration with any of the organs of the Tribunal.
41. Finally, the founder Treaty of the International Tribunal for the Internet would take effect after the date of deposit of the twentieth instrument of ratification or accession with the Director General of the International Tribunal for the Internet.

3. CONCLUSION

For all that was idealized and proposed, which ultimately we must conclude that the multiple uses of the Internet have presented many challenges, judicial and legislative, that deserve the scientific and academic dedication.

The real incorporation of these challenges, which we seek to bring summarily along this working paper, presents the need for answers and solutions able to cope with the observed complexity of the Internet World.

That is what we humbly sought when outlining the contours of an innovative **International Tribunal for the Internet**⁽²⁷⁾.

27 A complete list of arguments, reasons and details can to be found in our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142>

BIBLIOGRAPHY

BOEHME-NEßLER, Volker. *CyberLaw. Lehrbuch zum Internet-recht*. München: Verlag C.H. Beck, 2001.

BÚRCA, Gráinne de. *The European Tribunal of Justice and the International Legal Order After Kadi*. Harvard International Law Journal, Volume 51, Number 1, Winter 2010.

CALLIESS, Galf-Peter. *Online Dispute Resolution: Consumer Redress in a Global Market Place*. German Law Journal, Volume 07, nº 08, 2006.

CASELLA, Paulo Borba, ACCIOLY, Hildebrando, NASCIMENTO E SILVA, G. E. do. *Manual de Direito Internacional Público*. São Paulo: Saraiva, 2008.

CASSESE, Sabino. *Regulation, Adjudication and Dispute Resolution Beyond the State*. Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008.

CASTELLS, Manuel. *A Era da Informação: Economia, Sociedade e Cultura. (O Poder da Identidade- Volume II)*. Lisboa: Fundação Calouste Gulbenkian, 2003.

CLAPHAM, Andrew. *The Role of the Individual in International Law*. The European Journal of International Law, Volume 21, Number 01, 2010.

DIZARD, Wilson. *Digital diplomacy: U.S. foreign policy in the information age*. Washington: Praeger, 2001.

DUTTON, Willian, HELSPER, Ellen, GERBER, Monica. *The Internet in Britain 2009*. Oxford: Oxford Internet Institute, 2009.

FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: <http://www.barnesandnoble.com/w/an-international-tribunal-for-the-internet-daniel-freire-e-almeida/1123118107?ean=9788584930142> or http://www.almedina.com.br/catalog/advanced_search_result.php?keywords=Daniel+Freire&x=14&y=3 .

FREIRE E ALMEIDA, Daniel. *Bioterrorism Act – A Nova Política Externa dos EUA e a Eleição Presidencial sob a Perspectiva Diplomática do Brasil*. In: SAVINO, Luis

María (Org.). *Las Elecciones de los Estados Unidos y El Impacto Global*. Buenos Aires: Fundación Centro de Estudios Americanos, 2004.

FREIRE E ALMEIDA, Daniel. *The Taxation of Electronic Commerce in the United States of America and in the European Union*. São Paulo: Almedina, 2016.

GREAT BRITAIN. *Government on the internet: progress in delivering information and services online*. London: The Stationery Office, 2007.

GRIFFIN, David, TREVORROW, Philippa, HALPIN, Edward. *Developments in e-government: a critical analysis*. Washington, DC: IOS Press, 2007.

HÖRNLE, Julia. *Cross-border Internet Dispute Resolution*. Cambridge: Cambridge University Press, 2009.

HOUSE OF COMMONS COMMITTEE OF PUBLIC ACCOUNTS. *Government on the Internet: Progress in delivering information and services online*. London: The Stationery Office Limited, Sixteenth Report of Session 2007–08, 2008.

HUNTINGTON, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster, 2003.

IGLEZAKIS, Ioannis. *The development of E-Governance and the issue of digital inclusion in Greece with particular regard to the constitutional right of e-participation*. Journal of Information, Law & Technology, 2008.

KASTO, Jalil. *New International Order and International Law After the Millennium*. London: International Law Series nº 07, 2002.

KLEINWÄCHTER, Wolfgang, DORIA, Avri. *Internet Governance Forum (IGF). The First Two Years*. Paris: UNESCO, 2010.

LEITE DE CAMPOS, Diogo. *O Direito em NÓS*. New York: Lawinter Review, Volume I, Issue 1, March 2010.

LEITE DE CAMPOS, Diogo. *Prefácio*. In: GOMES, Fabio Luiz. *Direito Internacional. Perspectivas Contemporâneas*. São Paulo: Saraiva, 2010.

LESSIG, Lawrence. *Code. Version 2.0*. New York: Basic Books, 2006.

LIMA PINHEIRO, Luís. *Direito Internacional Privado*. Coimbra: Almedina, Volume 1, 2008.

LIMA PINHEIRO, Luís. *O Direito aplicável aos Contratos Celebrados através da Internet*. In: PINHEIRO, Luís de Lima. *Estudos de Direito Internacional Privado*. Coimbra: Almedina, Volume II, 2009.

LORCA, Arnulf Becker. *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010.

MACHADO, Jónatas E. M. *Direito Internacional. Do Paradigma Clássico ao Pós-11 de Setembro*. Coimbra: Coimbra Ed., 2006.

MELLO, Celso D. de Albuquerque. *Curso de Direito Internacional Público*. Rio de Janeiro: Renovar, 2º Volume, 2004.

NORTON, Pedram. *Directgov: The Right Direction for E-government or a Missed Opportunity?* Journal of Information, Law & Technology, 2008.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Shaping Policies for the Future of the Internet Economy*. Paris: OECD publishing, nº 148, 2008.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Resolving E-commerce Disputes Online: Asking the Right Questions about ADR*. Paris: OECD publishing, nº 63, 2002.

OWADA, Hisashi. *The Rule of Law in a Globalizing World – An Asian Perspective*. Washington University Global Studies Law Review, Volume 7, Number 02, 2008.

PAVLICHEV, Alexei, GARSON, David. *Digital government: principles and best practices*. Hershey: Idea Group Publishing, 2004.

RABINOVICH-EINY, Orna. *Beyond Efficiency: The Transformation of Courts Through Technology*. UCLA Journal of Law & Technology, Volume 12, nº 01, 2008.

REUTERS, “Brazil judge orders WhatsApp blocked, affecting 100 million users”. Available at <http://www.reuters.com/article/us-facebook-brazil-whatsapp-idUSKCN0XT1KB>, 05.03.2016.

RÖBEN, Volker. *The Enforcement Authority of International Institutions*. In: GOLDMANN, Matthias VON BOGDANDY, Armin, WOLFRUM, Rüdiger, VON BERNSTORFF, Jochen, DANN, Philipp. *The Exercise of Public Authority by International Institutions: Advancing International Institutional Law*. Heidelberg: Springer, 2010.

ROBERTS, Paul. *Comparative Criminal Justice Goes Global*. Oxford Journal of Legal Studies, Volume 28, Number 02, 2008.

SALACUSE, Jeswald. *The Emerging Global Regime for Investment*. Harvard International Law Journal, Volume 51, Number 2, Summer 2010.

SCHOR, Miguel. *Mapping Comparative Judicial Review*. Washington University Global Studies Law Review, Volume 7, Number 02, 2008.

SIMMA, Bruno. *Universality of International Law from the Perspective of a Practitioner*. The European Journal of International Law, Volume 20, Number 02, 2009.

UERPMANN-WITZACK, Robert. *Principles of International Internet Law*. German Law Journal, Volume 11, n° 11, 2010.

VON BOGDANDY, Armin, DELLAVALLE, Sergio. *Universalism and Particularism as Paradigms of International Law*. New York: International Law and Justice Working Paper 2008/3.

WALD, Arnaldo. *Preface*. In: CHALHUB, Melhim Namem. *Trust*. Rio de Janeiro: Renovar, 2001.

WESTON, Burns, FALK, Richard, CHARLESWORTH, Hilary, STRAUSS, Andrew. *International Law and World Order*. St. Paul: Thomson/West, 2006.

WEBER, Rolf H. *Principles for governing the Internet, A comparative analysis*. Paris: United Nations Educational, Scientific and Cultural Organization, 2015.

ZITTRAIN, Jonathan. *The Future of the Internet – And How to Stop It*. London: Yale University Press, 2008.

CYBERLAW

by CIJIC

DIREITO À *INTERNET*

RIGHT TO INTERNET

CATARINA SARMENTO E CASTRO ¹

¹ Docente da Faculdade de Direito da Universidade de Coimbra; Juíza Conselheira do Tribunal Constitucional.

RESUMO

O presente texto estuda o Direito à *Internet*.

Defende-se que o uso das novas tecnologias tem vindo a representar o desenvolvimento dos direitos e liberdades. Exemplo dessa ampliação é o direito fundamental à *Internet*.

O Direito à *Internet* é um direito fundamental instrumental, traduzido num direito de acesso à *Internet*, que potencia e amplia o exercício de outros direitos e liberdades, incluindo direitos fundamentais, constitucionalmente reconhecidos, como a liberdade de expressão e de comunicação, o direito à informação administrativa, ou o direito de participação democrática.

Mas o Direito à *Internet* é, em si mesmo, um direito fundamental de conteúdo próprio, que se traduz, não apenas no direito de acesso à infraestrutura tecnológica, mas também de utilização das suas virtualidades de comunicação, de conhecimento, de participação e de interação, constituindo um direito à partilha e ao relacionamento digitais com outras pessoas e instituições.

Palavras-Chave: Direito à *Internet*; Direito da Informática; Direito de informação; Direito de participação eletrónica; Direito à partilha e ao relacionamento digitais; Direito a participar na sociedade virtual

ABSTRACT

This paper focuses on the right to Internet.

The use of new technology represents a development of rights and freedoms. An example of this enlargement is the fundamental right to Internet.

The right to access to Internet is an instrument to foster and enforce other individual rights and freedoms, including those established by the Constitution, like the freedom of expression and communication, the right to administrative information, or the right to a democratic participation.

The right to Internet is also a fundamental right with its own particular subject, which consists, not only on the right to access to the technological infrastructure, but also on the right to use its communication, knowledge, participation and interaction facilities, consisting on a right to share information and to relate digitally with other people and institutions.

Keywords: Right to Internet; Computer Law; Right to Information; Right to electronic participation; Right to share information and to relate digitally; Right to join the digital society.

INTRODUÇÃO

O ciberespaço - essa noção que a escrita de ficção científica de William Gibson, nomeadamente o seu romance *Neuromancer*, de 1984, ajudou a difundir⁽³⁾ - é muitas vezes encarado pelos juristas como uma zona que o Direito deve regular, por aí serem inovadoramente postos em causa direitos dos cidadãos há muito reconhecidos no mundo analógico, mas também por nele serem ameaçados direitos novos que o ambiente tecnológico proporciona.

Esse lugar, muito pouco físico e sobretudo virtual/digital, é, por exemplo, meio onde podem ocorrer violações aos direitos das pessoas por via digital, como o direito à autodeterminação sexual, incluindo as que se concretizam na pornografia infantil, o direito à honra ou o direito ao bom nome dos indivíduos, mas também onde pode ter lugar a incitação à violência e ao terrorismo, ou a emissão de mensagens racistas, assim como agressões à propriedade intelectual. Enquanto via de circulação de dados pessoais, e palco para a realização de tratamentos de dados que respeitam a cada um de nós, pode também propiciar consequências potencialmente nefastas para o direito à autodeterminação informativa, que os próprios mecanismos informáticos fizeram consagrar. Tais ameaças são exponenciadas, quer pelas transformações temporais e espaciais das tecnologias no tratamento de dados - pela rapidez do tratamento da informação, pela velocidade da sua circulação e pela quantidade e variedade de informação partilhada, pela sua possível instantaneidade e tendencial perpetuidade, e pelo alargamento do universo de destinatários e de emissores de informação - quer pelos diferentes serviços que a rede possibilita.

Neste trabalho, propomo-nos estudar o direito de aceder ao ciberespaço, entendido este, não como ambiente tecnológico que potencia novas formas de lesão de direitos, designadamente de direitos fundamentais ancorados na dignidade da pessoa

2 O presente texto teve origem na comunicação apresentada na *I Conferência Cibersegurança: perspectivas multidisciplinares*, organizada pelo Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito de Lisboa e pelo Instituto de Direito Brasileiro, realizada a 4 de janeiro de 2016, na Faculdade de Direito da Universidade de Lisboa.

3 GIBSON, William, *Neuromancer*, Ace Books, Nova Iorque, 1984.

humana, mas enquanto caminho e/ou lugar potenciador do exercício de direitos há muito reconhecidos no mundo real, incluindo direitos de personalidade e de cidadania, e, igualmente, capaz de suscitar a ampliação dos direitos reconhecidos aos cidadãos. Ao invés de estudar o direito que cada um de nós tem a ser protegido das ameaças que o uso das tecnologias digitais acarreta – designadamente a comunicação em rede -, propomo-nos sublinhar o direito de utilizar essas mesmas tecnologias, e a *Internet* em particular, enquanto novo direito⁽⁴⁾.

Esta perspetiva destaca, imediatamente, dois tipos de conexão que é possível surpreender entre o Direito e as novas tecnologias, incluindo a *Internet*.

Por um lado, uma relação em que representamos o Direito enquanto ferramenta que protege os indivíduos das agressões aos seus direitos, provocadas pela utilização das novas tecnologias, ou que lida com consequências do uso das redes chamando-se, assim, o Direito, enquanto Direito da informática, a regular os novos aspetos internos da informática, do seu uso e dos seus bens, transformando a informática em objeto do Direito, o que, por si só, já constituiria uma primeira superação da solução propugnada por John Barlow⁽⁵⁾ que, em 1996, na sua Declaração de independência do ciberespaço, propunha uma rede de redes livre do Direito.

Mas, por outro, é também uma relação em que se atribui à ordem jurídica a função de reconhecer os novos direitos que as tecnologias de informação e de comunicação fizeram emergir, atribuindo ao Direito da informática uma tarefa que vai além do mero papel de reação às ameaças digitais a bens jurídicos vários, para agora considerar os direitos resultantes das próprias interações informáticas.

4 Nos Estados Unidos da América, a decisão *Reno v. ACLU*, de 1997, do *Supreme Court*, apreciou a inconstitucionalidade de normas da *Communications Decency Act*, de 1996, de Bill Clinton, que pretendia combater o acesso pelas crianças à pornografia, considerando-as inconstitucionais, havendo demonstrando a tensão entre a liberdade da *Internet* e a liberdade de expressão, por um lado, e a necessidade de controlo, por outro. A decisão está disponível em <https://supreme.justia.com/cases/federal/us/521/844/case.html>. Sobre o assunto pode ler-se: SIMON, Glenn E., “Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors”, *The Journal of Criminal Law & Criminology*, Vol. 88, n.º 3, 1998, p. 1015 e ss., que pode ser consultado em: <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6967&context=jclc> (13 de dezembro de 2015).

5 Elemento da *Electronic Frontier Foundation*, que respondia à promulgação, pelo Presidente dos Estados Unidos da América, Bill Clinton, em 1996, da *Telecommunications Decency Act*. Defendeu uma conceção ciberlibertária de Internet sem donos, nem lei.

A estas duas perspectivas da conexão entre o Direito e a informática, ambas no âmbito do Direito da informática, pode juntar-se uma terceira, a que só muito lateralmente nos referiremos neste estudo – aquela em que a informática, a sua utilização, não é já objecto de regulação por parte do Direito, mas serve o Direito como seu instrumento – designadamente, para tratamento de informação jurídica, para celebração de contratos, para emissão de actos jurídicos, para publicitação de formas jurídicas de actuação – contribuindo de modo decisivo para a sua transformação. Afinal, se a “revolução da tecnologia de informação” tem “capacidade de penetração em todo o âmbito da actividade humana”, não deixou de modificar a própria actividade jurídica⁽⁶⁾.

Nas próximas páginas focaremos a nossa atenção no novo direito do cidadão cibernauta, direito reconhecido pela ordem jurídica, que dá mote a este trabalho.

6 As citações são de CASTELLS, Manuel, *La. Era de la Información, Economía, Sociedad y Cultura*, Alianza, Madrid, Vol. I, 1998.

I. O Direito à *Internet*

Um dos direitos cuja origem está necessariamente associada à evolução tecnológica é o que a doutrina tem abreviadamente denominado como Direito à *Internet*.

O Direito à *Internet* é, antes de mais, um direito de aceder a esse meio de comunicação universal, ou seja, de aceder aos suportes tecnológicos que tornam possível os serviços de comunicação disponíveis através da rede de redes. É um direito de utilização da infraestrutura tecnológica nascida nos anos 60, nos Estados Unidos, em plena Guerra fria, um direito de acesso à rede e aos equipamentos que propiciam esse acesso.

Mas a *Internet* não se resume ao seu aspecto tecnológico em sentido estrito, antes constituindo, igualmente, uma estrutura social, em que diferentes atores participam interagindo entre si, comunicando informação, trocando serviços, relacionando-se interactivamente em permanência.

Através dos serviços de comunicação que a rede propicia, é possível a divulgação de conteúdos (com o que isso significa em termos de interpenetração com a liberdade de expressão, como veremos), o acesso a conteúdos (por exemplo, à informação potenciadora de conhecimento utilizável para o desenvolvimento económico, nomeadamente aquele que se relaciona com a economia digital), o acesso à prestação de serviços eletrónicos (onde não pode deixar de se salientar o acesso, também, a serviços da Administração eletrónica), e a prestação destes mesmos serviços, assim como o estabelecimento de relações sociais na rede, aspecto absolutamente fundamental para que se possa compreender a verdadeira dimensão deste novo direito⁽⁷⁾.

Este direito de aceder à rede, mas também de utilizar os seus conteúdos, como os disponíveis na *World Wide Web*, de divulgar informações, de prestar e de aceder a serviços, e de por esse meio e nesse ambiente se relacionar com os outros, tem várias

7 "La tecnología de la información ha sido la herramienta indispensable para la puesta en práctica efectiva de los procesos de reestructuración socioeconómica. De importancia particular fue su papel al permitir el desarrollo de redes interconectadas como una forma expansiva y dinámica de organización de la actividad humana. Esta lógica de redes transforma todos los ámbitos de la vida social y económica". CASTELLS, Manuel, *La Era de la Información, Economía, Sociedad y Cultura*, Alianza, Vol. I, Madrid, 1998, p. 370.

cambiantes, ligadas a diferentes aspectos, muitos deles conexos com os direitos cujo gozo pleno surge actualmente associado ao acesso à rede.

Neste trabalho, salientaremos, em primeiro lugar, a *Internet* enquanto elemento determinante da revolução tecnológica que condiciona o exercício de vários outros direitos, já que estes nela, e através dela, em grande parte se realizam⁽⁸⁾. Esta estrutura, proporcionadora de conectividade permanente, simultaneamente impulsionadora e concretizadora da sociedade da informação e do conhecimento, é hoje espaço de realização privilegiado de outros direitos, e dinamizador das liberdades. O direito à *Internet* contribui para a concretização de outros direitos preexistentes.

De seguida, focar-nos-emos na *Internet* como ambiente criador de novos direitos. O mundo digital não se limitou a desmaterializar a realização de alguns direitos, que passaram a ser exercidos sob novas roupagens, e em ambiente digital, como criou novas relações que o Direito veio regular. É o caso do Direito à *Internet*.

8 Nesse sentido, por exemplo: LUCCHI, Nicola, “Internet Content Governance and Human Rights”, *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 16, n.º 4, 2014, p. 809 e ss., disponível em http://www.jetlaw.org/wp-content/uploads/2014/06/Lucchi_Final.pdf (2 de dezembro de 2015); TULLY, Stephen, “A Human Right to Access to the Internet? Problems and Prospects”, *Human Rights Law Review*, 2014, p. 175 e ss..

II. O Direito à *Internet* enquanto manifestação de outros direitos

O direito de acesso à rede é, para pedir emprestada uma expressão de Gomes Canotilho e de Vital Moreira, um “direito constitucional comunicativo” ⁽⁹⁾. Amplificador de direitos já reconhecidos, não é difícil encontrar exemplos que ilustram esta sua funcionalidade: a comunicação e interação, que o uso da *Internet* fomenta, alarga as vias de exercício da liberdade de comunicação e de expressão, do direito de acesso à informação, assim como à sua pesquisa e transmissão, o acesso ao conhecimento, no que isso significa no desenvolvimento da actividade económica, à educação ou à cultura, reforça a participação democrática, o acesso a serviços públicos, promove o desenvolvimento⁽¹⁰⁾.

1. O Direito à *Internet*, enquanto direito de utilização da rede e dos seus serviços, surge umbilicalmente ligado à liberdade de comunicação, à faculdade de utilização dos serviços de comunicação disponível em rede através dos quais o utilizador transmite e recebe informação. Esta especial plataforma de comunicação que é a rede possibilita a propagação de informação à escala mundial, fluxo intenso de informação que tem lugar em tempo real, e em que cada um dos participantes é simultaneamente emissor e receptor.

2. No exercício da sua liberdade de comunicação, a rede e a desmaterialização permitem ao utilizador, enquanto emissor, multiplicar os destinatários dos vários conteúdos e diversificar os modos de expressão. Por isso o Direito à *Internet* assume particular importância sendo hoje também indissociável do exercício da liberdade de expressão.

Mais do que fazer referência à tensão entre o exercício da liberdade de expressão através da rede e os direitos de outros cidadãos que podem por ela ser afetados – no seu direito à honra e ao bom nome, por exemplo - a reflexão que se pretende deixar é uma

9 Referindo-se aos “direitos constitucionais comunicativos” e suas funções veja-se: CANOTILHO, José Joaquim Gomes/MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. II, 4.ª Edição, 2010, Coimbra Editora, Coimbra, p. 823.

10 Como escreveu Lucchi: “The Internet has become an essential instrument and can now be viewed as a condition necessary for the proper enjoyment of a series of rights, including the rights to access information and to communicate”: LUCCHI, Nicola, “Internet Content Governance and Human Rights”, *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 16, n.º 4, 2014, p. 809 e ss., disponível em http://www.jetlaw.org/wp-content/uploads/2014/06/Lucchi_Final.pdf (2 de dezembro de 2015), p. 811.

outra, como se afirmou já⁽¹¹⁾: é a do uso das redes enquanto veículo ou espaço de comunicação que deve ser disciplinado por ser âmbito de realização de direitos – de que a liberdade de expressão, incluindo a liberdade de criação com ela conexas, é paradigma⁽¹²⁾. A *Internet* veio revolucionar a liberdade de expressão sobretudo pelas suas características de interactividade: ao contrário da imprensa escrita, ou da televisão e da rádio (sendo que estas últimas comungam com a *Internet*, por vezes, de uma certa instantaneidade), a *Internet* catapultou o utilizador para o papel de interlocutor direto do fazedor de informação e permite-lhe, até, o papel de ator na difusão informativa⁽¹³⁾. Espaço de expressão pública sem intermediação, e por isso, menos sujeito a qualquer filtro, a *Internet* amplifica o que decidimos tornar público, por decisão nossa – seja, designadamente, opinião, expressão artística, conhecimentos ou sentimentos.

Num ambiente em que a divulgação massificada de informação se assume como vertente essencial da liberdade de expressão, este mecanismo tecnológico começou por permitir contornar actos de censura dirigidos aos meios tradicionais de divulgação de informação, que esbarraram com a divulgação e o acesso globalizados à informação, sem intermediação, que a rede autoriza. No entanto, depressa alguns Estados desenvolveram atitudes conducentes ao bloqueio do acesso ou ao controlo e condicionamento da informação disponibilizada mediante mecanismos digitais, comportamento revelador de agressões a direitos fundamentais, como a liberdade de

11 Veja-se uma análise sob este prisma em ROQUES-BONNET, Marie-Charlotte, *Le Droit Peut-il Ignorer la Révolution Numérique?*, Michalon Éditions, Paris, 2010, Capítulo III, Secção I, I, A.

12 É muito interessante a recente posição do Tribunal Europeu dos Direitos do Homem a propósito da liberdade de expressão exercida através da rede. No Acórdão *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt v. Hungria*, de 2 de fevereiro de 2016, estando em causa o exercício da liberdade de expressão de um órgão regulador dos prestadores de serviços de conteúdos em linha (MTE) e de um portal de actualidades húngaro, de grande dimensão (*Index*) -, sendo que o primeiro disponibilizava, no seu sítio da *Internet*, espaço de comentário ao seus visitantes, que foi por estes utilizados para comentários ofensivos relativamente a pessoas colectivas visando as suas práticas comerciais, comentários que o segundo reproduziu -, o Tribunal considerou que MTE e *Index* protegeram suficientemente os visados, já que haviam disponibilizado formas de alerta para remoção de comentários ofensivos, haviam inscrito nas cláusulas gerais de utilização que a responsabilidade dos comentários seria de quem os colocasse *online* e não sua, tendo ainda em conta, como salienta a fundamentação, que estavam em causa pessoas colectivas, e que no momento da publicação estas estavam já a ser investigadas quantos aos factos descritos.

13 Disso mesmo nos dá conta o Relatório as Nações Unidas, de 2011, de que foi Relator Frank LaRue, disponível em <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/130/49/PDF/G1013049.pdf?OpenElement>. (consultado a 6 de dezembro de 2015). Também neste sentido, MARCON, João Paulo Falavinha, “O acesso à Internet como direito humano fundamental, perante as legislações internacional e brasileira”, *Mundorama*, 7 de março de 2013.

expressão ou o direito de acesso à informação⁽¹⁴⁾. É o caso do bloqueio do acesso pelos internautas aos resultados de pesquisas realizadas em motores de busca com base em palavras-chave específicas, ou à interrupção de serviços das redes sociais para evitar a difusão de informação, conducentes à concretização de censura política⁽¹⁵⁾.

3. Além de permitir a divulgação massificada de informação, o Direito à *Internet* é também um direito de acesso à informação, ao conteúdo da rede, por isso, direito a receber e a procurar informação, designadamente informação pública⁽¹⁶⁾, ou relativa ao exercício de específicos direitos de informação, de que é exemplo a informação ao consumidor⁽¹⁷⁾, a informação estatística⁽¹⁸⁾ ou a informação ambiental⁽¹⁹⁾. É um direito de informar, de se informar e de ser informado⁽²⁰⁾.

14 Veja-se o que diz, por exemplo, GOULART, Guilherme Damasio, “O Impacto das Novas Tecnologias nos Direitos Humanos e Fundamentais: o acesso à Internet e a Liberdade de Expressão”, *Revista Direitos Emergentes na Sociedade Global*, Vol. I, n.º 1, Janeiro-Junho 2012, p. 145 e ss. (p. 153), disponível em <http://ssrn.com/abstract=2156402> (consultado a 6 de dezembro de 2015).

15 Veja-se, no primeiro caso, o exemplo do braço de ferro levado a cabo pela *Google*, e, quanto ao segundo, a questão do bloqueio do *Twitter*, em 2009, ambos descritos no Relatório do (extinto) *Forum des Droits sur L'Internet*, La Documentation Française, 2009, p. 66 e 67, disponível em <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/104000464.pdf> (consultado a 6 de dezembro de 2015). A Declaração Conjunta, de 2010, do Relator Especial das Nações Unidas para a Liberdade de Opinião e de Expressão, do Representante da Organização para a Segurança e Cooperação na Europa para a Liberdade dos Meios de Comunicação, da Relatora Especial da Organização dos Estados Americanos para a Liberdade de Expressão e da Relatora Especial sobre a Liberdade de Expressão e Acesso à Informação da Comissão Africana de Direitos do Homem e dos Povos, sobre os desafios para a liberdade de expressão na próxima década, refere as questões mais preocupantes relativas à limitação ao acesso à *Internet* e meios de comunicação, nos pontos 9 (*Libertad de expresión en Internet*) e 10 (*acesso a tecnologias de información y comunicación*), disponível em <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=784&IID=2>. A 1 de junho de 2011, os mesmos protagonistas assinaram uma Declaração Conjunta específica sobre Liberdade de Expressão e Internet, disponível em <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2> (consultados a 6 de dezembro de 2015).

16 Especiais deveres de publicidade e transparência, e de prestação de acesso a arquivos e registos administrativos, obrigam as entidades públicas administrativas, para garantia do direito à informação administrativa, direito de natureza análoga aos direitos, liberdades e garantias, constitucionalmente consagrado no artigo 268.º da Constituição: no n.º 1, na vertente de direito à informação administrativa procedimental; no n.º 2, enquanto direito à informação administrativa não procedimental, direito que é, neste caso, de todos, independentemente da afirmação de um interesse legítimo.

17 Os direitos dos consumidores estão consagrados no artigo 60.º da CRP, no capítulo respeitante aos Direitos e deveres económicos, e incluem um direito à informação.

18 Sobre o assunto: CASTRO, Catarina Sarmento, “A Limitação do Segredo Estatístico: Segredo Estatístico Versus Publicidade”, a publicar em: *Indicadores Locais de Desenvolvimento Sustentável. O Caso de Estarreja* (Coord. Sara Moreno Pires, Alexandra Aragão, Teresa Fidélis, Irineu Mendes), Instituto Jurídico da Faculdade de Direito, 2016.

19 O acesso à informação sobre o ambiente está previsto na Directiva 2003/4/CE, transposta pela Lei n.º

19/2006, de 12 de Junho. A participação pública na elaboração de certos planos e programas relativos ao ambiente consta da Directiva 2003/35/CE, e a participação do público, entre outras, na Directiva relativas à Avaliação Ambiental Estratégica (Directiva 2001/42/CE), e na Directiva quadro da Água (Directiva 2000/60/EC), transpostas por diversos diplomas. Por outro lado, o desenvolvimento sustentável, a protecção do ambiente e dos recursos naturais são, como afirmámos já, tarefas fundamentais do Estado.

20 Entre nós, a liberdade de informação encontra-se protegida pelo artigo 37.º da Constituição.

4. Mediante o acesso à rede, designadamente por permitir a utilização da informação disponível na *World Wide Web*, garante-se o acesso ao conhecimento, traduzido no acesso à informação e ao conhecimento dela resultante, assim como ao desenvolvimento económico e social que estes potenciam. Um tal desenvolvimento económico resulta não apenas da utilização das informações disponíveis na rede em prol do desenvolvimento da atividade económica, resultando ela direta ou indiretamente de conteúdos digitais, mas advém, ainda, do genérico estabelecimento de relações comerciais em linha.

Este acesso ao conhecimento pode, ainda, ser encarado num sentido estrito, de acesso à educação e à cultura que a transmissão da informação, informaticamente memorizada e ampliada, de todos para todos, propicia. Pelo que o Direito à *Internet* é também um direito que facilita o exercício de direitos sociais como os consagrados no artigo 73.º da CRP (“Todos têm direito à educação e à cultura”), cuja concretização, na actual Sociedade de Informação e Conhecimento, passa pelo acesso às novas tecnologias e à rede das redes⁽²¹⁾.

5. O uso da *Internet* favorece igualmente o alargamento da participação democrática. Quer esta resulte de resposta reactiva a consultas que são eletronicamente provocadas, ou de participação eletrónica proactiva, ambas potenciadas pelo aumento da informação que chega ao cidadão, quer seja isoladamente exercida, ou colectivamente realizada, a participação eletrónica manifesta-se em diversas facetas⁽²²⁾.

A rede das redes contribui para uma maior consciencialização dos cidadãos para os problemas comuns e para o poder que cada um tem na sua resolução, mediante interação com as instituições públicas e com os atores políticos em geral, tornando-se palco de ativismo político. O desenvolvimento da *Internet* fomentou uma maior participação do cidadão na vida política, e nos assuntos públicos do país em geral, fosse por sua própria iniciativa, trocando interactivamente informações com quem o rodeia,

21 Estabelecendo expressamente esta conexão entre Sociedade de Informação, direito à cultura e direito de acesso à *Internet*, veja-se DIAZ REVORIO, Francisco Javier, “Tecnologías de la Información y de la Comunicación y Nuevas Dimensiones de los Derechos Fundamentales”, *Derechos, Libertades y Sociedad de la Información*, Centro de Investigaciones Jurídicas y Sociales, Facultad de Derecho y Ciencias Sociales UMNSH, México, , 2010, p. 21, disponível em https://www.researchgate.net/publication/271646314_Derechos_Libertades_y_Sociedad_de_la_Informacion (14 de dezembro de 2015).

22 Uma análise sobre o assunto pode ser encontrada em: AICHHOLZER, Georg/ ALLHUTTER, Doris, “Online Forms of Political Participation and Their Impact in Democracy”, *Manu:Script*, Junho 2011, disponível em http://epub.oeaw.ac.at/0xc1aa500e_0x00290b64.pdf (3 de dezembro de 2015).

manifestando-se mediante o uso de redes sociais, ou de *blogs* de opinião, em defesa dos seus próprios projectos, fosse a solicitação das instituições públicas, designadamente através da participação em sondagens eletrónicas, de *chats* em direto, ou mediante colaboração em iniciativas que permitem obter do cidadão o *feedback* necessário sobre políticas prosseguidas e a prosseguir⁽²³⁾.

Por outro lado, candidatos ou eleitos passam também a fazer campanha, a debater e a expressar-se em linha, assim se permitindo a comunicação pluridireccional de todos com todos, dentro ou fora do período eleitoral⁽²⁴⁾. A *Internet* aproxima a política das pessoas e as pessoas da política, fortalece o seu poder e torna-as mais iguais na sua capacidade de influenciar os agentes políticos.

Nalguns países, as comunicações eletrónicas em rede simplificam o exercício de outros direitos políticos individuais ou coletivos, como o direito de petição⁽²⁵⁾, noutros tornam até possível o exercício do direito fundamental de sufrágio, mediante recurso ao voto eletrónico⁽²⁶⁾. A relativização espacial a que a rede conduz possibilita também um maior envolvimento democrático dos cidadãos residentes no estrangeiro, o mesmo ocorrendo relativamente à participação na política europeia.

Em suma, a rede torna possível a concretização das várias valências da democracia eletrónica (campanhas eleitorais eletrónicas, voto eletrónico, petições eletrónicas, sondagens eletrónicas, difusão e debate de ideias por via eletrónica, fiscalização eletrónica democrática da actividade política...).

23 A Constituição da República Portuguesa consagra, no artigo 48.º, um direito à participação na vida pública.

24 MANUEL CASTELLS, “Democracy in the Age of Internet”, disponível em http://lull.cat/IMAGES_175/transfer06-not01.pdf (2 de janeiro de 2016), p. 96 e ss.; MANUEL CASTELLS, “Communication, Power and Counter-power in the Network Society”, *International Journal of Communication*, n.º 1, 2007, p. 238 e ss., MANUEL CASTELLS, “A Sociedade em Rede: do Conhecimento à Política”, *A Sociedade em Rede*, Imprensa Nacional – Casa da Moeda, p. 17 e ss..

25 Entre nós com dignidade constitucional (artigo 52.º, n.º 1, da CRP).

26 Situação hoje possível, por exemplo, no Brasil (veja-se, para maior desenvolvimento, as explicações constantes de <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica>, acedido em dezembro de 2015). Ainda assim, o voto não é, no caso brasileiro, um “voto em mobilidade”, realizado pela *Internet*, antes implicando a deslocação a mesas de voto eletrónicas onde é disponibilizada uma urna eletrónica. O “voto em mobilidade” acontece, por exemplo, na Estónia (o *I-voting* encontra-se descrito em <http://www.vvk.ee/voting-methods-in-estonia/>, consultado em 7 de dezembro de 2015). Entre nós, nas autárquicas de 97 e de 2001, bem como nas europeias de 2004 e nas legislativas de 2005, foram realizadas algumas experiências piloto, que não contavam para os resultados oficiais. Veja-se, para maior detalhe, a informação constante da página da UMIC: http://www.umic.pt/index.php?option=com_content&task=view&id=44&Itemid=112 (15 de dezembro de 2015).

Ao mesmo tempo, o Direito à *Internet* pode ser instrumento de concretização da liberdade de associação, e, em especial, do direito de reunião ou de manifestação constitucionalmente consagrados, nomeadamente pelo efeito de mobilização não intermediada que podem desencadear, associados à facilidade de comunicação e de transmissão de informação⁽²⁷⁾. São hoje muito diversificados os exemplos de movimentos sociais espontâneos iniciados e/ou alimentados na *Internet*, através de redes sociais e *blogs*, que se estenderam ao espaço público, desde, entre nós, o movimento que deu origem à manifestação de 15 de Setembro de 2014, sob o lema “Que se lixe a Troika”, ou, em Espanha, as “Mareas Ciudadanas” ou o movimento “15M”, até à “Primavera Árabe”, cujos participantes, com recurso à *Internet*, contornaram o embargo noticioso sobre os acontecimentos. Muitos destes movimentos, “redes de indignação e esperança”, na nomenclatura de Castells, usam a rede como mecanismo de “autocomunicação de massas”, que “va de muchos a muchos com interactividad”⁽²⁸⁾, transformando a rede em origem e amplificação de outras redes⁽²⁹⁾. O acesso à *Internet* e às novas tecnologias desempenha aqui um papel determinante no exercício do direito que o cidadão tem de se reunir e de se manifestar.

6. O Direito de utilização da rede é hoje, também, essencial para o acesso aos mais variados serviços administrativos fornecidos *online*. A informática – e aqui falamos já da informática jurídica – permite, atualmente, o desenvolvimento de uma atuação jurídico-administrativa digital. O Parlamento Europeu reconheceu, na Recomendação relativa ao reforço da segurança e liberdades fundamentais da *Internet*, a necessidade da regulação jurídica dos meios técnicos que permitem ao cidadão aceder aos serviços administrativos electrónicos⁽³⁰⁾.

27 Previstos no artigo 45.º da CRP.

28 CASTELLS, Manuel, “El Poder en la era de las redes sociales”, *Nexos*, septiembre 2012, disponível em www.nexos.com.mx (consultado a 15 de Dezembro de 2015).

29 CASTELLS, Manuel, *La Era de la Información. Economía, Cultura y Sociedad – La Sociedad Red*, Volume 1, 3.ª Edição, 2005. Mais recentemente: *Redes de Indignación y Esperanza: Los Movimientos Sociales en la Era de Internet*, 2ª Edição, Alianza Editorial, Madrid, 2015.

30 O Considerando B, da Recomendação do Parlamento Europeu, de 26 de março de 2009, estabelece: “considérant que les gouvernements ainsi que les organisations et institutions d’intérêt public doivent prévoir un cadre réglementaire adapté et les moyens techniques appropriés pour permettre aux citoyens de participer activement et efficacement aux procédures administratives grâce à des applications du gouvernement électronique”. A Recomendação está disponível em <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2009-0194+0+DOC+PDF+V0//FR> (consultado a 15 de dezembro de 2015).

Estas diferentes formas de atividade administrativa digital vêm sendo juridicamente reconhecidas em diversas ordens jurídicas como a espanhola, a alemã, a italiana ou, mais recentemente, a portuguesa. Por exemplo, o Código de Administração Digital italiano estabelece um estatuto de cidadania digital. Sem o qualificar expressamente como tal, entre nós, o novo Código de Procedimento Administrativo, no artigo 14.º, consagrou também um *eDireito* ao relacionamento do cidadão com a Administração Pública pela via digital, ou um direito ao uso das tecnologias no relacionamento com a Administração⁽³¹⁾. Um tal direito contribui, por exemplo, para melhorar o acesso dos cidadãos a prestações sociais, algumas constituindo prestações relativas a verdadeiros fundamentais, ou para melhorar o acesso à informação administrativa, a que faremos referência no próximo ponto.

7. A disponibilização e o acesso à informação em rede contribui para a transparência da Administração Pública e da atividade política, facilitando, não apenas o conhecimento da actividade desenvolvida, como também o controlo do seu exercício pelo cidadão.

No primeiro caso, assume especial importância o acesso à informação detida pela Administração Pública, acumulada no desempenho das suas funções, que pode ser, em certas circunstâncias, reutilizada. A informação sobre o acesso à Administração e serviços prestados, bem como as análises à qualidade dos serviços, são igualmente relevantes. Especialmente significativo é, contudo, o papel de divulgação da rede relativamente a informação que permite controlar a legalidade e o mérito da actividade administrativa.

Neste caso, ao lado da informação libertada pelos actores políticos, para divulgação de ideias, tem especial relevo a informação disponibilizada na rede pelos organismos de fiscalização, bem como pelos cidadãos em geral e pelos *media* tradicionais, para efeitos de controlo. Nesta vertente, o uso da *Internet* também contribui para a realização da democracia eletrónica que acima mencionámos.

31 “Os órgãos e serviços da Administração Pública devem utilizar meios eletrónicos no desempenho da sua atividade, de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados” (n.º 1), e que “Os serviços devem disponibilizar meios eletrónicos de relacionamento com a Administração Pública e divulgá-los de forma adequada, de modo a que os interessados os possam utilizar no exercício dos seus direitos e interesses legalmente protegidos, designadamente para formular as suas pretensões, obter e prestar informações, realizar consultas, apresentar alegações, efetuar pagamentos e impugnar atos administrativos” (n.º 4).

8. Reconhecido no artigo 22.º, n.º 1, da Carta Africana de Direitos do Homem e dos Povos, em 1981⁽³²⁾, e pela Declaração do Direito ao Desenvolvimento, aprovada pela Resolução n.º 41/128, da Assembleia Geral das Nações Unidas, em 1986, o direito ao desenvolvimento depende, também ele, do acesso às novas tecnologias, incluindo o acesso à *Internet*. O uso da rede permite diminuir a distância entre os diferentes Estados, desde logo pelo desenvolvimento cultural e educacional que facilita e pelo desenvolvimento económico que potencia⁽³³⁾.

9. Por fim, e atendendo ao que atrás se escreveu, é incontornável que se reconheça que o direito à *Internet* deve, actualmente, ser considerado como contribuindo para o livre desenvolvimento da personalidade⁽³⁴⁾. Há hoje toda uma geração que nunca viveu sem estar permanentemente conectado em rede⁽³⁵⁾. E mesmo os que conheceram outra realidade dependem hoje, em grande medida, quer da realização propiciada pelo relacionamento interpessoal em rede, quer de uma leitura da realidade construída com base em informações *online*. Como adiante veremos, o livre desenvolvimento da personalidade está intimamente ligado àquilo que de singular tem o Direito à *Internet*: o direito de integrar a sociedade digital.

Em suma, o Direito à *Internet* é, numa das suas vertentes, um direito funcionalizado à garantia ou exercício pleno de vários outros direitos, que prolonga, entre os quais se contam diversos direitos fundamentais.

32 “All peoples shall have the right to their economic, social and cultural development with due regard to their freedom and identity and in the equal enjoyment of the common heritage of mankind”.

33 Referindo a *Internet* como potenciando o desenvolvimento económico, veja-se o relatório das Nações Unidas sobre liberdade de expressão, de 2011: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, p. 16, acedido em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, consultado a 3 de janeiro de 2016.

34 Entre os direitos, liberdades e garantias pessoais a Constituição Portuguesa consagra expressamente um direito ao desenvolvimento da personalidade (artigo 26.º, n.º 1).

35 Como refere Castells, é a permanente conectividade que contribui decisivamente para a modificação do modelo social de comunicação: CASTELLS, Manuel, “Democracy in the Age of the Internet”, p. 96 e ss. (99), disponível em http://lull.cat/IMAGES_175/transfer06-not01.pdf (consultado a 2 de janeiro de 2016).

III. O Direito à *Internet* na sua especificidade

1. Do que ficou dito resulta que a utilização da *Internet* é indispensável ao exercício de direitos, nomeadamente, de direitos fundamentais.

O direito à *Internet* aprofunda o exercício da cidadania, agora eletrónica⁽³⁶⁾, facilita o exercício e fruição de direitos pelos administrados, suporta ou facilita a realização de direitos como a liberdade de comunicação, a liberdade de expressão, de informação ou de acesso à informação e ao conhecimento, fomentando a liberdade de comunicar, de fazer circular, e de partilhar informação. É um direito amplificador do acesso a direitos já reconhecidos.

2. Mas o Direito à *Internet*, no contexto atual da sociedade de informação, de conhecimento e de relacionamento em rede, assume um conteúdo que não se confunde com o mero suporte a outros direitos, alguns dos quais com dignidade constitucional. Hoje, na nova estrutura social em rede, tudo é informação e comunicação⁽³⁷⁾. As nossas actuações e interacções, sociais ou outras, em grande parte exteriorizadas na rede, baseiam-se no uso que fazemos da informação de que dispomos. Assim, o Direito à *Internet* traduz, igualmente, um direito de se relacionar (no sentido de estabelecer relações humanas) por meios eletrónicos. Vittorio Frosini referiu-se-lhe como sendo “il diritto di partecipazione alla società virtuale, che è stata generata dall’avvento degli elaboratori elettronici nella società tecnologica”⁽³⁸⁾.

A rede possibilita a reorganização das relações sociais, de maior cooperação e troca de informação, e fortalece os vínculos sociais, enquanto sistema tecno-social: infraestrutura tecnológica global, a *Internet* é também infraestrutura social, humana, de comunicação, de cooperação, de inter-relação e de troca de conhecimentos. A sociedade em rede é uma sociedade hipersocial⁽³⁹⁾.

36 A Estónia reclama ser pioneira na ideia de país sem fronteiras físicas, sendo o primeiro país do mundo a oferecer eResidência a qualquer cidadão que, sem ali residir fisicamente, pode, por exemplo, gerir electronicamente uma empresa e pagar os correspondentes impostos. Veja-se a descrição do programa em <https://e-estonia.com/e-residents/about/> (consultado a 17 de dezembro de 2015).

37 CASTELLS, Manuel, “Globalización, Sociedad y Política en la Era de la Información”, *Bitacora*, n.º 4, 2000, p. 42 e ss. (p. 43).

38 FROSINI, Vittorio, “L’Orizzonte Giuridico dell’Internet”, *Diritto dell’Informazione e dell’Informatica*, n.º 271, 2002, p. 275.

39 Como afirmou CASTELLS, Manuel, *A Sociedade em Rede: do Conhecimento à Política*, Imprensa-Nacional Casa da Moeda, 2005, p. 23.

3. Aceder, hoje, à *Internet*, é exercer o direito a integrar a sociedade digital, nela se relacionando com o outro - interagindo e participando digitalmente, como forma de concretização do seu direito ao livre desenvolvimento da personalidade e à felicidade que daí resulta⁽⁴⁰⁾ -, e com o Estado – designadamente, no exercício do seu direito ao uso das novas tecnologias nas relações com a Administração Pública. Estas valências de interação digital são, actualmente, elementos indispensáveis à vida e dignidade dos indivíduos numa sociedade democrática.

Assim, sendo embora um direito instrumental relativamente a outros direitos, o Direito à *Internet* goza, ainda, de autonomia lógico-jurídica própria, sendo possível invocá-lo em juízo, sem necessidade de associar o seu eventual desrespeito à violação de outros direitos como a liberdade de expressão⁽⁴¹⁾.

40 Escrevendo, ainda antes do advento da *Internet*, sobre o direito à felicidade e a influência que sobre esta exerce a utilização do computador: FROSINI, Vittorio, “Human Rights in the Computer Age”, *Informatica e Diritto*, Vol. XVII, 1.^a Série, n.º 1-3, 1989, p. 7 e ss., disponível em http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1989_01_07-13_Frosini.pdf (3 de janeiro de 2016). O autor afirmava, por exemplo: “The right to happiness increases in intensity with the participation of other people”.

41 Neste sentido, BADOCCO, Francesca, “Reflessioni sul Diritto d’accesso a Internet nell’ambito del Diritto dell’Unione Europea”, *Informatica e Diritto*, Vol. XVIII, n.º 1, 2009, p. 153 e ss., disponível em http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD_2009_01_Badocco.pdf (2 de janeiro de 2016).

IV. O acesso universal à rede e a *digital divide*

No contexto do conteúdo que vimos delimitando ao Direito à *Internet*, a garantia de um acesso universal à rede é condição essencial para evitar a discriminação social, política e democrática que a barreira digital inflige⁽⁴²⁾. Por exemplo, para que a liberdade de expressão na plataforma privilegiada que é a *Internet*, o acesso a serviços públicos eletrônicos, o acesso a informação *online*, ou a participação política em rede, não constituam privilégios reservados às elites - seja por razões económicas (que impossibilitam a aquisição de equipamentos ou do próprio acesso), por razões sociais (como as derivadas da separação geracional, por razões de limitação da acessibilidade, ou relacionadas com o nível de escolaridade), geográficas (associadas à cobertura de rede) ou políticas -, é indispensável que todos possam aceder à rede sem distinção. A garantia da universalidade do acesso torna importante a cobertura de rede alargada a todas as regiões geográficas, o acesso generalizado aos equipamentos, nomeadamente mediante acesso em espaços públicos, ou com o apoio à aquisição de equipamentos pessoais, assim como assume cada vez maior importância o tipo de acesso à rede (fazendo diferença a largura de banda e a velocidade, o acesso por *wifi*, ou, hoje, a possibilidade de ter acesso móvel, assim como o preço do acesso, *etc.*)⁽⁴³⁾. Tendo em conta a fundamentalidade do Direito à *Internet* em si mesmo, bem como o seu papel relativamente ao exercício pleno de outros direitos fundamentais⁽⁴⁴⁾ é importante que se reconheça caber ao Estado a promoção do acesso universal à rede.

42 Neste mesmo sentido prescrevia a Recomendação do Parlamento Europeu, relativa ao reforço da segurança e liberdades fundamentais da Internet, que em pode ser encontrada em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//FR#ref_1_9 (parágrafo 1 B das recomendações, consultado a 3 de janeiro de 2016). Recomendava-se que se estabelecesse como princípio que as instituições são responsáveis por participar no desenvolvimento do acesso à rede e seus conteúdos, devendo lutar contra o analfabetismo informático e a exclusão democrática eletrónica. Veja-se, também o Relatório das Nações Unidas sobre liberdade de expressão, de 2011: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, p. 16, acedido em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, consultado a 3 de janeiro de 2016.

43 Veja-se a análise profunda a que procede, sobre a realidade francesa, no ponto “II – La fracture numérique: premier défi à relever”, ROQUES-BONNET, Marie-Charlotte, *Le Droit Peut-il Ignorer la Révolution Numérique?*, Michalon Éditions, Paris, 2010.

44 Neste duplo sentido, por exemplo, DÍAZ REVORIO, Francisco Javier, “Tecnologías de la Información y la Comunicación y Nuevas Dimensiones de los Derechos Fundamentales”, *Derechos, Libertades y Sociedad de la Información*, 2010, p. 21.

V.O direito à *Internet* como direito fundamental

1. Embora entre nós pouco estudado, o Direito à *Internet* é, actualmente, considerado por alguma doutrina como um direito fundamental, encontrando-se autores que assim o defendem (mais abundantemente na doutrina de espanhola⁽⁴⁵⁾, italiana⁽⁴⁶⁾, francesa⁽⁴⁷⁾ e brasileira⁽⁴⁸⁾⁽⁴⁹⁾. Uns, derivando-o do texto constitucional, de forma indirecta, já que dele dependeria o exercício pleno de outros direitos fundamentais, em relação aos quais seria instrumental⁽⁵⁰⁾, ou de forma directa, quando no texto da Lei fundamental se encontre autonomamente estabelecido; outros autores, defendendo a necessidade de adaptação dos textos constitucionais para o receber, enquanto direito autónomo, valendo-se, em abono da sua posição, do reconhecimento judicial da fundamentalidade deste direito, já ocorrido nalgumas ordens jurídicas, ou da sua qualificação como direito fundamental em instituições e organismos internacionais. Outros autores, sustentam,

45 Por exemplo, DÍAZ PINTOS, G, “En favor de un Derecho Fundamental de Acceso a la Red”, *Persona y Derecho*, Vol. 45, 2001, p. 323 e ss. (337), disponível em <http://dadun.unav.edu/handle/10171/14366> (2 de janeiro de 2016); ou, em castelhano, mas um autor mexicano, DÍAZ REVORIO, Francisco Javier, “Tecnologías de la Información y la Comunicación y Nuevas Dimensiones de los Derechos Fundamentales”, *Derechos, Libertades y Sociedad de la Información*, 2010, p. 9 e ss..

46 FROSINI, Vittorio, “L’Orizzonte Giuridico dell’Internet”, *Diritto dell’Informazione e dell’Informatica*, n.º 271, 2002, p.275; FROSINI, Tommaso Edoardo, “Il Diritto Costituzionale di Accesso a Internet”, *Rivista Telemática Giuridica dell’Associazione Italiana dei Costituzionalisti*, n.º1, 2011, p. 1 e ss.; Idem, “Nuevas Tencologias y Constitucionalismo”, *Revista Derecho del Estado*, n.º 15, dezembro 2003, p. 29 e ss.. Defendendo que o direito de acesso à Internet não é um direito fundamental, mas somente um direito de acesso que é condição necessária para a realização de direitos fundamentais como a liberdade de expressão e de comunicação: LUCCHI, Nicola, “Internet Content Governance and Human Rights”, *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 16, n.º 4, 2014, p. 809 e ss., disponível em http://www.jetlaw.org/wp-content/uploads/2014/06/Lucchi_Final.pdf (2 de dezembro de 2015), p. 809 e ss..

47 MARINO, Laure, “Le Droit d’Accès à l’Internet, Nouveau Droit Fondamental”, *Rec. Dalloz*, 2009, p. 2045; ROQUES-BONNET, Marie-Charlotte, *Le Droit Peut-il Ignorer la Révolution Numérique?*, Éditions Michalon, Paris, 2010.

48 Entre outros, GOULART, Guilherme Damasio, “O Impacto das Novas Tecnologias nos Direitos Humanos e Fundamentais: o acesso à Internet e a Liberdade de Expressão”, *Revista Direitos Emergentes na Sociedade Global*, Vol. I, n.º 1, Janeiro-Junho 2012, p. 145 e ss. (p. 153), disponível em <http://ssrn.com/abstract=2156402>.

49 E outros como, por exemplo, BEST, Michael L., “Can Internet be a Human Right?”, p. 23 e ss., disponível em <http://www.du.edu/korbel/hrhw/volumes/2004/best-2004.pdf> (6 de Dezembro de 2015).

50 Embora outros autores defendam, inversamente, que o facto de a *Internet* ser instrumento para o exercício de direitos fundamentais (“the Internet has become an essential tool for the proper enjoyment of a series of rights – including the right to access knowledge and information and the right to communicate”), isso não transforma o acesso ou a utilização da *Internet* num direito fundamental: LUCCHI, Nicola, “Internet Content Governance and Human Rights”, *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 16, n.º 4, 2014, p. 809 e ss., disponível em http://www.jetlaw.org/wp-content/uploads/2014/06/Lucchi_Final.pdf (2 de dezembro de 2015). O autor considera, pelo contrário, que é a liberdade de expressão que inclui a garantia de acesso à *Internet* (p. 854). Nesse mesmo sentido, assim interpretando a decisão HADOPI, do *Conseil Constitutionnel*, como integrando o direito de acesso à *Internet* no âmbito da liberdade de expressão e de comunicação, RIDARD, Basile, “La Protection Constitutionnelle du Droit d’Accès à l’Internet”, *Congrès Mondial de l’AIDC*, dezembro de 2010, disponível em: <http://www.juridicas.unam.mx/wccl/ponencias/3/64.pdf> (p. 3; p. 5 e ss.; consultado a 19 de dezembro de 2015).

ainda, a necessidade da realização de um *check-up* à Constituição, para aferir da capacidade do seu texto de suportar os novos desafios gerados pelas novas tecnologias⁽⁵¹⁾.

Na jurisprudência também é possível encontrar esta caracterização variada. Merecem destaque a decisão “Hadopi” (n.º 2009-580, de 10 de junho⁽⁵²⁾), do *Conseil Constitutionnel* francês, que, em 2009, pronunciando-se sobre a sanção de suspensão do acesso à Internet determinada por uma autoridade administrativa (HADOPI) prevista na Lei, reconheceu que o direito a aceder aos serviços de comunicação, quando estava em causa o acesso à Internet, é fundamental ao exercício da liberdade de expressão, de comunicação e de participação política⁽⁵³⁾. Assim, o acesso à Internet foi considerado uma componente essencial à liberdade de expressão e comunicação e à participação na vida democrática, reconhecendo-se que um direito de acesso a Internet é uma decorrência da consagração constitucional destes outros direitos⁽⁵⁴⁾.

Mais tarde, uma decisão do Supremo Tribunal da Costa Rica, de 30 de julho de 2010, veio afirmar existir um direito de acesso à Internet, considerando-o um verdadeiro direito fundamental, que teria sido posto em causa pelo atraso na abertura do mercado das telecomunicações⁽⁵⁵⁾. Um tal direito facilitaria o exercício de outros

51 Entre nós, em artigo recente, Raquel Alexandra Brízida Castro, “Constituição e Ciberespaço: argumentos para um «direito constitucional do inimigo»?”, *Cyberlaw*, n.º 1, janeiro 2016, disponível em http://www.cijic.org/wp-content/uploads/2016/01/CONSTITUI---O-E-CIBERESPA---O_ARGUMENTOS-PARA-UM---DIREITO-CONSTITUCIONAL-DO-INIMIGO---.pdf. (consultado a 3 de janeiro de 2016).

52 Que pode ser acedida em <http://www.conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html> (30 de dezembro de 2015).

53 O considerando 12 estabelecia «qu’aux termes de l’article 11 de la Déclaration des droits de l’homme et du citoyen de 1789 : “La libre communication des pensées et des opinions est un des droits les plus précieux de l’homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l’abus de cette liberté dans les cas déterminés par la loi”; qu’en l’état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu’à l’importance prise par ces services pour la participation à la vie démocratique et l’expression des idées et des opinions, ce droit implique la liberté d’accéder à ces services.».

54 Uma análise da decisão do *Conseil Constitutionnel* pode ser encontrada em ROQUES-BONNET, Marie-Charlotte, *Le Droit Peut-il Ignorer la Révolution Numérique?*, Michalon Éditions, Paris, 2010, Capítulo III, Secção I, I, A.

55 Nela pode ler-se o seguinte: “debe decirse que el avance en los últimos veinte años en materia de tecnologías de la información y comunicación (TIC’s) ha revolucionado el entorno social del ser humano. Sin temor a equívocos, puede afirmarse que estas tecnologías han impactado el modo en que el ser humano se comunica, facilitando la conexión entre personas e instituciones a nivel mundial y eliminando las barreras de espacio y tiempo. En este momento, el acceso a estas tecnologías se convierte en un instrumento básico para facilitar el ejercicio de derechos fundamentales como la participación democrática (democracia electrónica) y el control ciudadano, la educación, la libertad de expresión y pensamiento, el acceso a la información y los servicios públicos en línea, el derecho a relacionarse con los poderes públicos por medios electrónicos y la transparencia administrativa, entre otros. Incluso, se ha afirmado el carácter de derecho fundamental que reviste el acceso a estas tecnologías, concretamente,

direitos e liberdades fundamentais como o direito de participação democrática, o direito à educação, a liberdade de expressão, o direito de acesso à informação e à transparência da actuação administrativa, o direito de aceder eletronicamente aos serviços administrativos e de se relacionar com os poderes públicos, entre outros.

Embora não tendo afirmando expressamente um autónomo Direito à *Internet*, deve igualmente lembrar-se a Decisão do Supremo Tribunal do Estados Unidos da América *Reno v. American Civil Liberties Union (ACLU)*, sobre a constitucionalidade de normas da *Communications Decency Act* de 1996 que pretendiam combater o acesso pelas crianças à pornografia na Internet, e a ligação que nela se estabeleceu entre a fruição da liberdade de expressão e o acesso à rede⁽⁵⁶⁾.

O Tribunal Europeu dos Direitos do Homem, na Decisão Ahmet Yildirim contra a Turquia, de 18 de dezembro de 2012 - em que estava em causa o bloqueio total e sem limitação temporal do acesso ao *Google Sites*, domínio pertencente a *Google Inc.*, que facilita a criação de sítios *web*, um dos quais albergava conteúdos que um tribunal turco considerou atentar contra a memória de Atatürk, havendo o bloqueio afectado, colateralmente, todos os outros sítios da Internet aí albergados -, também considerou que o direito de aceder à *Internet* é uma componente essencial da liberdade de expressão⁽⁵⁷⁾.

Para além dos Tribunais, outras instituições se pronunciaram sobre o direito de aceder à *Internet*. Por exemplo, a Comissão Europeia, em 2009, deu visibilidade à

el derecho de acceso a la Internet o red de redes. (...) En este contexto de la sociedad de la información o del conocimiento, se impone a los poderes públicos, en beneficio de los administrados, promover y garantizar, en forma universal, el acceso a estas nuevas tecnologías. Partiendo de lo expuesto, concluye este Tribunal Constitucional que el retardo verificado en la apertura del mercado de las telecomunicaciones ha quebrantado no solo el derecho consagrado en el artículo 41 de la Constitución Política sino que, además, ha incidido en el ejercicio y disfrute de otros derechos fundamentales como la libertad de elección de los consumidores consagrada en el artículo 46, párrafo in fine, constitucional, el derecho de acceso a las nuevas tecnologías de la información, el derecho a la igualdad y la erradicación de la brecha digital (info-exclusión) –artículo 33 constitucional-, el derecho de acceder a la internet por la interfase que elija el consumidor o usuario y la libertad empresarial y de comercio. A decisão pode ser consultada em http://200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_texto_sentencia.asp?nValor2=483874&tem1=013141¶m7=0&lResultado=3&nValor1=1&strTipM=T&strLib=LIB. (consultado a 19 de dezembro de 2015)

56 Decisão *Reno v. ACLU*, de 1997, que pode ser encontrada em <https://supreme.justia.com/cases/federal/us/521/844/case.html> (consultada a 18 de dezembro de 2015). Uma outra decisão foi também importante: *Denver Area Educational Telecommunications Consortium, Inc v. FCC*, de 1996.

57 A decisão, de 18 de dezembro de 2012, encontra-se em [http://hudoc.echr.coe.int/eng?i=001-115401#{\"itemid\":\[\"001-115401\"\]}](http://hudoc.echr.coe.int/eng?i=001-115401#{\) (consultada a 19 de dezembro de 2015).

necessidade de alfabetização digital, na Recomendação 2009/625/CE, de 20 de agosto. E o Parlamento Europeu, na já mencionada Recomendação relativa ao reforço da segurança e liberdades fundamentais da Internet⁽⁵⁸⁾, afirmou a importância do direito cidadão de participar na Sociedade de Informação, e da relevância do acesso à *Internet*, que o Direito deve garantir, para a plena realização de vários direitos fundamentais.

No Conselho da Europa, através da Recomendação CM/Rec (2011) 8, de 21 de setembro de 2011, o Comité de Ministros recomendou aos Estados a protecção e a promoção da universalidade, da integridade e da abertura da *Internet*, enquanto condição para garantir a liberdade de expressão e o acesso à informação. Antes disto, já em 2005, o Comité de Ministros, numa Declaração sobre a Sociedade de Informação (CM (2005) 56 final, de 13 de maio) reconheceu que o acesso limitado ou a inexistência de acesso às tecnologias de informação e comunicação pode privar os indivíduos da capacidade de exercício livre dos seus direitos fundamentais.

Por seu lado, as Nações Unidas no seu Relatório sobre a liberdade de expressão, de 2011⁽⁵⁹⁾, embora não defendendo a existência de um novo e autónomo direito, consideraram a importância do acesso à *Internet* como catalisador do gozo da liberdade de expressão, da busca e partilha de informação, mas também da realização de outros Direitos do Homem, assim como para o progresso da sociedade em geral. O Relatório sublinhou o relevo do acesso universal à rede no combate à *digital divide*.

Seguindo esta perspectiva, o Conselho de Direitos Humanos das Nações Unidas, reconhecendo a importância da utilização das novas tecnologias, veio a aprovar, em 2012, uma Recomendação sobre a Promoção, Protecção e Exercício dos

58 A Recomendação do Parlamento Europeu, de 26 de março de 2009, pode ser encontrada em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//FR#ref_1_9 (consultada a 19 de dezembro de 2015). O Parlamento recomenda ao Conselho que estabeleça um acesso à Internet sem reservas e seguro, devendo, designadamente: “reconnaître qu'Internet peut être une possibilité extraordinaire de renforcer la citoyenneté active et que, à cet égard, **l'accès aux réseaux et aux contenus est l'un des éléments-clé**; recommander que cette question continue à être développée en posant comme principe que **chacun a le droit de participer à la société de l'information** et que les institutions et les acteurs à tous les niveaux ont pour responsabilité générale de participer à ce développement, luttant ainsi contre les deux nouveaux défis de l'analphabétisme informatique et de l'exclusion démocratique à l'ère électronique;” (sublinhado nosso), consultada a 3 de janeiro de 2016.

59 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, p. 16 e ss., acedido em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, consultado a 3 de janeiro de 2016.

Direitos do Homem na Internet.⁽⁶⁰⁾ Afirmando que os direitos reconhecidos às pessoas no mundo analógico devem também ser reconhecidos em linha, nomeadamente, a liberdade de expressão, recomendou que todos os Estados promovessem e facilitassem o acesso à *Internet*.

Ainda o Relator Especial das Nações Unidas para a Liberdade de Opinião e de Expressão, mas agora também com o Representante da Organização para a Segurança e Cooperação na Europa para a Liberdade dos Meios de Comunicação, a Relatora Especial da Organização dos Estados Americanos para a Liberdade de Expressão e a Relatora Especial sobre a Liberdade de Expressão e Acesso à Informação da Comissão Africana de Direitos do Homem e dos Povos, a 1 de junho de 2011, assinaram uma Declaração Conjunta específica sobre Liberdade de Expressão e *Internet*, na qual afirmam: “Los Estados tienen la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión. El acceso a Internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres”⁽⁶¹⁾.

Aos poucos, a legislação dos vários estados vai reconhecendo o papel essencial do acesso à *Internet*. A ideia fundamental é a do acesso universal e de qualidade, traduzindo preocupações de largura de banda e preço razoável.

Assim, por exemplo, em Portugal ou em Espanha, o acesso à *Internet* é já considerado um serviço universal, à semelhança com o que sucede com outros serviços fundamentais como o fornecimento de água, de energia elétrica, os serviços postais, a recolha e tratamento de águas residuais, a gestão de resíduos sólidos urbanos, o fornecimento de gás e natural e de gases de petróleo liquefeitos⁽⁶²⁾. É também o caso da Estónia que, em 2000, passou a considerar o acesso à *Internet* como um serviço universal. Igualmente na Finlândia, em 2010, o acesso à banda larga foi considerado um direito essencial⁽⁶³⁾. Por sua vez, a Carta de Direitos Fundamentais da União

60 Documento A/HRC/20/L.13, de 29 de junho de 2012.

61 Disponível em <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2> (consultado a 21 de dezembro de 2015).

62 A Lei n.º 23/96, de 26 de julho, modificada, nomeadamente, pela Lei n.º 12/2008, de 26 de fevereiro, que lhe aditou, entre outras normas, a que passou a incluir os serviços de comunicação eletrónica, criou mecanismos destinados a proteger os utentes destes serviços essenciais.

63 Na Finlândia consagrou-se legalmente o direito de acesso à *Internet*, havendo o Governo definido que o acesso à *Internet* através de uma ligação de alta qualidade e a preços razoáveis é um direito essencial.

Europeia, no artigo 36.o, consagra expressamente o acesso a serviços de interesse económico geral⁽⁶⁴⁾.

No Brasil, o *Marco Jurídico da Internet*, aprovado pela Lei 12 965, de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da *Internet*, prescreve, no artigo 7.º, em que define os direitos do usuário, que o acesso à *Internet* é essencial ao exercício da cidadania⁽⁶⁵⁾.

Para além das provisões legais sobre o Direito à *Internet*, existem Constituições que, neste âmbito, consagram direitos fundamentais autónomos.

Em 2008, a Constituição do Equador, no artigo 16.º, veio garantir a todas as pessoas, singulares ou colectivas, o direito de acesso universal a todas as tecnologias de informação e de comunicação.

Na Grécia, o artigo 5.º-A, depois de consagrar um direito à informação, estabeleceu que todos têm direito a participar na Sociedade de Informação, constituindo obrigação do Estado promover o acesso, a produção, a troca e a difusão electrónica da informação⁽⁶⁶⁾.

O 2.º parágrafo do artigo 30.º da Constituição da República do Paraguai, já em 1992, estabelecia que a lei deve assegurar, em igualdade de oportunidades, o livre acesso à utilização do espectro eletromagnético, bem como aos instrumentos de acumulação e elaboração de informação pública⁽⁶⁷⁾.

64 Considerando que a Carta "eleva a direito fundamental o direito a serviços públicos de interesse económico geral", veja-se CANOTILHO, José Joaquim Gomes, *Direito Constitucional e Teoria da Constituição*, 7.a Edição, Almedina, Coimbra, 2003, p. 344. Em sentido contrário: SILVA, João Nuno Calvão da, "Comentário ao artigo 36.o da Carta dos Direitos Fundamentais da União Europeia", in SILVA, Alessandra/CANOTILHO, Mariana, *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, Coimbra, 2013, p. 436 e ss. (p. 445).

65 O Marco Jurídico da Internet pode ser encontrado em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm (consultado a 2 de janeiro de 2016).

66 Na revisão de 2001, deu-se, igualmente, a consagração de um direito à protecção de dados pessoais (artigo 9.º).

67 Mais precisamente: "La ley asegurará, en igualdad de oportunidades, el libre acceso al aprovechamiento del espectro electromagnético, así como al de los instrumentos electrónicos de acumulación y procesamiento de información pública, sin más límites que los impuestos por las regulaciones internacionales y las normas técnicas. Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución".

E, em Itália, tem lugar uma interessante discussão em torno de propostas de revisão constitucional com o intuito de inserir um novo artigo que consagre um direito de aceder à *Internet*. A proposta inicial foi apresentada por Stefano Rodotà que defendeu que “a Internet promove uma lógica constitucional nova”, apresentando uma alteração para inserção de um artigo 21bis⁽⁶⁸⁾. Mais recentemente, outras propostas se lhe seguiram, no sentido de inserir um tal direito num artigo 34bis, que poria ênfase na conexão em rede: este direito asseguraria o prolongamento dos modos de realização da personalidade humana e dos demais direitos exercidos em rede, devendo, segundo os proponentes, ser considerado um direito social⁽⁶⁹⁾.

Independentemente do reconhecimento expresso de um direito de acesso à *Internet* na legislação, ou enquanto direito fundamental nas normas constitucionais dos Estados, é inegável que este direito é, actualmente, considerado, pelo menos, um direito instrumental para o exercício de outros direitos fundamentais, com especial destaque para a liberdade de expressão e de comunicação. Como refere o mencionado Acórdão do TEDH, de 2012, é possível concluir que do conjunto de garantias genericamente estabelecidas para protecção da liberdade de expressão se pode extrair que é reconhecido um direito de acesso à Internet sem entraves (ponto 31). O que também resulta, claramente, do Acórdão do *Conseil Constitutionnel* francês acima referido, por exemplo.

2. Será possível defender a existência, na ordem jurídica portuguesa, de um direito fundamental de acesso à rede e de utilização das suas virtualidades de comunicação, de procura e difusão de informação, de conhecimento, de participação e de interação? Encontrará este direito guarida constitucional na ordem jurídica portuguesa?

Esta questão encontra resposta no artigo 35.º, da CRP, com a epígrafe “utilização da informática”, que, no seu n.º 6, consagra que “a todos é garantido livre acesso às redes informáticas de uso público”. É a expressão mais evidente da

68 O novo direito (que se seguiria ao artigo 21 relativo à liberdade de expressão) estabeleceria o seguinte: “*Tutti hanno eguale diritto di accedere alla Rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale*”. RODOTÀ, Stefano, “Un articolo 21bis per Internet”, disponível em: <http://archivio.articolo21.org/2183/notizia/un-articolo21bis-per-internet-.html>. (consultado a 21 de dezembro de 2015).

69 O texto, proposto está disponível em: <http://www.art34bis.it/la-nostra-proposta/>: “*Tutti hanno eguale diritto di accedere alla rete Internet, in modo neutrale, in condizione di parità e con modalità tecnologicamente adeguate. (consultado a 19 de dezembro de 2015). La Repubblica promuove le condizioni che rendano effettivo l’accesso alla rete Internet come luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale*”.

consagração constitucional de um autónomo Direito à *Internet*, enquanto direito fundamental incluído no catálogo dos direitos, liberdades e garantias, que implica, antes de tudo o resto, um direito de aceder à rede⁽⁷⁰⁾.

Mas, como resulta do que ficou dito, em nossa opinião, este direito fundamental à *Internet* não consiste apenas num direito de acesso aos meios tecnológicos, às infraestruturas, um direito de aceder aos serviços de comunicação e aos serviços prestados eletronicamente, nomeadamente aos serviços públicos, sendo, ainda, um direito de obter da rede informação e de nela criar e divulgar conteúdos, devendo igualmente ser considerado um direito a participar na rede relacionando-se socialmente, partilhando opiniões, mobilizando e construindo coletivamente opções nas mais diferentes áreas de atuação social. É um direito de comunicação, de participação, de inclusão, de interação. Naquela que deve ser uma compreensão aberta da norma disposta no n.º 6 do artigo 35.º, o livre acesso à rede, constitucionalmente previsto, abrange o direito de interagir em rede, de partilhar socialmente, de inegável fundamentalidade. Esta forma de interação integra, hoje, um certo tipo de concepção de vida e de estruturação de relacionamento, para muitos, indispensável a uma existência digna.

Pioneira na consagração de direitos dos cidadãos em face dos tratamentos de dados (então) mecanográficos (de que a utilização de mecanismos associados aos cartões perfurados foram exemplo), concedendo proteção desde a sua versão original em 1976, a Constituição Portuguesa soube adaptar-se à evolução tecnológica e desde a revisão constitucional de 1997 prevê este direito fundamental de acesso à rede.

70 Existem outras posições na nossa doutrina: Gomes Canotilho e Vital Moreira sustentam que esta “garantia de acesso às redes informáticas de uso público” “é, em rigor, uma nova dimensão da liberdade de expressão. O acesso à rede é uma espécie de pré-requisito (*pre-commitment*) da própria liberdade de expressão via *Internet*”: CANOTILHO, José Joaquim Gomes/MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. II, 4.ª Edição, 2010, Coimbra Editora, Coimbra, p. 557. Já Vieira de Andrade insere as garantias relativas à utilização da informática, incluindo o disposto no n.º 6 do artigo 35.º, da CRP, na categoria das garantias, dos direitos, liberdades e garantias, autonomizáveis enquanto posições jurídicas subjectivas. Considerá-las garantias significa que lhes atribui um papel secundário, que não acompanhamos, já que, para o autor, as garantias seriam, ou “direitos-garantias”, já que teriam função instrumental para protecção de outros direitos, que seriam os “direitos-direitos”, posições primárias cujo objecto imediato seria um bem específico da pessoa, ou “direitos-liberdades”, protegendo uma esfera de autodeterminação de comportamento. ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 5.ª Edição, Almedina, Coimbra, 2012, p. 114 e ss..

Daqui resulta que, no caso português, o impacto das novas tecnologias manifestou-se desde muito cedo no texto constitucional, poupando-nos, relativamente ao direito fundamental de acesso à rede, à eventual necessidade, também defensável, de fazer derivar um tal direito, por interpretação, do texto de outros preceitos constitucionais (mediante a delimitação do âmbito de protecção de outros direitos fundamentais⁽⁷¹⁾), diferentemente do que sucede noutras ordens jurídicas, ou com outros direitos associados ao desenvolvimento de novas tecnologias.

71 Modalidade de abertura explicada, por exemplo, por ALEXANDRINO, José de Melo, *A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa*, Vol. II, Almedina, Coimbra, 2006, p. 374 e ss..

VI. Conclusão

A nota final que gostávamos de sublinhar, fazendo uso das palavras de Tommaso Frosini, é a de que, apesar dos desafios, o uso das tecnologias tem vindo a representar um desenvolvimento dos direitos e liberdades, de que o Direito à *Internet* é exemplo paradigmático⁽⁷²⁾.

A importância deste direito é hoje manifesta, desde logo, pelo facto de o Direito à *Internet* constituir instrumento fundamental para a realização de outros direitos, nomeadamente de direitos fundamentais.

É certo que os direitos fundamentais conservam a mesma dignidade quer sejam exercidos digital ou analogicamente. Mas, com o tempo, com a progressiva massificação dos mecanismos tecnológicos, a sua realização tende cada vez mais a assumir formato digital, pelo que o acesso à rede adquire uma importância determinante.

A evolução tecnológica dita que a *Internet* seja, crescentemente, o meio ou o lugar do exercício de velhos e de novos direitos.

Ao mesmo tempo, como vimos, a rede será, também, lugar cada vez mais privilegiado para as interferências nos direitos e liberdades fundamentais, como o direito à autodeterminação informativa ou como a liberdade de expressão são exemplo, seja em virtude de agressões por parte do próprio Estado, seja por parte de outros cidadãos.

Ao lado da característica de suporte à realização de outros direitos, que faz com que a negação do acesso à *Internet* se possa traduzir na violação desses outros direitos, o Direito à *Internet* assume-se, também, com um conteúdo próprio, de direito de acesso e de direito à partilha e ao relacionamento digitais.

Em qualquer dos casos, um tal direito fundamental obrigará o Estado a assegurar as condições necessárias que garantam o acesso universal à rede, enquanto direito a prestações para promover o acesso e fruição do direito, ou seja, direito a uma acção positiva do Estado, seja ela normativa ou fáctica. E, enquanto direito de defesa, impedi-

72 FROSINI, Tommaso Edoardo, “Il Diritto Costituzionale di Accesso a Internet”, *Rivista Telemática Giuridica dell’Associazione Italiana dei Costituzionalisti*, n.º1, 2011, p. 1 e ss..

lo-á (salvo em situações devidamente justificadas) de adotar medidas que ponham em causa o exercício do Direito à *Internet*, como a criação de barreiras eletrónicas que evitem o acesso à rede, ou o acesso a informação dela constante (dever de abstenção), impondo, igualmente, ao Estado, prestações positivas, instrumentais, de protecção do Direito à *Internet* face a terceiros.

O Direito à *Internet* é, na sua especificidade de acesso à rede, um direito da categoria dos direitos, liberdades e garantias, previsto no artigo 35.º, n.º 6, da Constituição, que, simultaneamente, é condição de exercício de outros direitos, liberdades e garantias. É-o, também, na sua vertente de direito de interação digital, resultante do livre acesso à rede.

CYBERLAW

by CIJIC

THE IMPORTANCE OF A FREE AND OPEN INTERNET

A IMPORTÂNCIA DA INTERNET LIVRE E ABERTA

NUNO M. GARCIA ¹

¹Universidade da Beira Interior, Departamento de Informática e Instituto de Telecomunicações, UBI, Covilhã, Portugal.

Universidade Lusófona de Humanidades e Tecnologias, Lisboa, Portugal.

Correio eletrónico: ngarcia@di.ubi.pt

ABSTRACT

The concept for a Free and Open Internet seems so generic that apparently is consensual. Yet, there are commercial policies that seem to undermine the exercise of freedom that the Internet has provided since its creation. This paper presents the concepts of Free and Open Internet and of Net Neutrality, discussing the principles on which these are founded, and arguing that not having a Free and Open Internet may compromise the prosecution of some Human Rights. Finally, this paper identifies usual practices in the telecommunications market that seem to undermine a Free and Open Internet, and suggests three lines of action to not only correct these practices, but also to increase the level of participation of Portuguese users in the multi-stakeholder Internet governance model.

Keywords: Free and Open Internet, Zero Rating, Data Caps, Human Rights.

RESUMO

O conceito de Internet Livre e Aberta parece tão genérico que aparentemente é consensual. No entanto, há práticas que parecem limitar o exercício de liberdade que desde a sua concepção caracterizou a Internet. Este artigo apresenta os conceitos de Internet Livre e Aberta e de *Net Neutrality*, discute os princípios em que esta assenta, e argumenta que a não-existência de uma Internet Livre e Aberta pode comprometer a prossecução de alguns dos Direitos Humanos. Finalmente, identifica práticas correntes no mercado das telecomunicações que parecem prejudicar uma Internet Livre e Aberta, e sugere três linhas de acção para não só corrigir estas práticas, mas também para aumentar o nível de participação dos utilizadores portugueses no modelo *Multistakeholder* de governação da Internet.

Palavras-chave: Internet Livre e Aberta, *Zero rating*, limites de dados, direitos humanos.

1. INTRODUÇÃO

Recentemente, Vinton G. Cerf publicou um artigo no New York Times no qual defendia que o acesso à Internet⁽²⁾ não é um Direito Humano (Vinton Cerf, 2012). O seu argumento, que subscrevemos, é o de que há apenas um conjunto de valores e garantias que merecem a classificação de Direito Humano, ou até de Direito Civil, e que nenhuma tecnologia, por muito avançada que possa ser, merece a distinção de ser considerada um Direito Humano. A reflexão de Cerf é interessante não apenas por ser feita por um dos maiores pioneiros da Internet, mas porquanto, feita em 2012, vinha em contraciclo com um relatório de 2011 das Nações Unidas que afirmava que impedir o acesso à Internet constitui uma violação dos Direitos Humanos e uma violação do Direito Internacional (Kravets, 2011). No entanto, e se considerarmos que em muitos pontos do globo, é precisamente a ferramenta Internet que garante o acesso à Educação e à Informação, temos que concluir que também estes relatores das Nações Unidas merecem a nossa concordância. Aliás, argumentando que a Internet é o suporte do acesso a vários direitos básicos, o sítio da Internet “*A Human Right*” vem defendendo o acesso livre e gratuito para todos, com o moto “Como será o mundo quando todos os humanos estiverem conectados?” (Grammatis, 2010). E apenas para adicionar um outro internauta famoso defensor da mesma linha, embora eventualmente com mais interesses comerciais que Vint Cerf e motivado certamente também por esses interesses comerciais (“Internet.org,” n.d.), Mark Zuckerberg afirma também que o acesso à Internet é um Direito Humano (Rampton, 2015).

A questão do acesso à Internet e a questão da defesa dos Direitos Humanos nesta área, levam-nos a outras considerações mais amplas, desde logo, a que é basilar para o funcionamento de toda a Internet: como é que será possível sustentar o modelo de negócio da Internet no futuro? É que se a Internet não for financeira e politicamente sustentável, sucumbirá. Kevin Kelly, numa brilhante comunicação apresentada num evento TED (Kelly, 2007), dizia que o modelo de negócio inicial da *Web* era um exercício de utopia porque, na realidade, a *Web* trouxe-nos uma quantidade cronologicamente inigualável em termos de quantidade de informação (mas também de qualidade) a um preço virtualmente nulo. E no entanto ela move-se, *i.e.*, apesar da

2 “Internet” é um nome de uma plataforma e, portanto, deve ser escrito com a primeira letra em maiúscula. Pelo contrário, a palavra “internet” foi em tempos usada para designar o conjunto de redes de computadores interligadas, tendo o conceito entretanto ficado obsoleto.

aparente utopia, a Internet e os seus serviços, a *Web*, existem e provavelmente existirão no futuro com um modelo muito semelhante ao que temos hoje.

Entre os actores que têm interesses na Internet estão, desde logo, as empresas de fornecimento de acesso, em inglês, os *Internet Service Providers* ou ISP. Os ISP são empresas cujo modelo de negócio consiste no aluguer ao cliente do tempo para utilização das infraestruturas que os ISP fizeram instalar no terreno⁽³⁾, como por exemplo, as fibras ópticas ou as antenas de acesso da rede de telemóveis. Os ISP queixam-se frequentemente que estes são investimentos muito elevados e que precisam de um aumento no volume de negócios (Helena Garrido, Alexandra Machado, 2015). Admitindo como certo que os investimentos na infraestrutura são elevados, não apenas inicialmente mas também na sua manutenção, é também certo que os ISP que detêm a infraestrutura, repetidamente têm apresentado resultados positivos para o seu exercício, *e.g.* (Sara Ribeiro, 2016).

Certamente seguindo melhores práticas de gestão, a procura de novas fontes de receita não abranda e recentemente, alguns ISP têm tentado criar um serviço *Premium* no qual os seus clientes acedem mais rapidamente aos dados, obviamente, pagando para isso a correspondente contrapartida (Brodkin, 2014). E mais, os ISP estão disponíveis para receber quer dos clientes que querem um serviço mais rápido, quer dos fornecedores de conteúdos que querem usar da vantagem comercial de disponibilizar um serviço mais rápido para aumentar a sua base de clientes. À primeira vista, não há nada de estranho com esta proposta de negócio, excepto que do ponto de vista tecnológico, esta aceleração da transmissão de conteúdos é um engano, já que na realidade não há forma de acelerar o fluxo de acesso para um cliente ou para um conteúdo ou um servidor de um fornecedor de conteúdos sem ser à custa da degradação da velocidade de transmissão dos outros fluxos dos outros clientes e/ou dos outros fornecedores. Comparativamente, seria como permitir que numa autoestrada de quatro faixas, duas delas estivessem reservadas para quem pagasse portagens *premium*, e obviamente, as outras duas faixas seriam prejudicadas porque todos os outros condutores, que anteriormente circulavam nas quatro faixas, agora teriam que circular apenas em duas, sendo para ambas o caminho exactamente igual. Com esta estratégia

3 Há outros ISP que não detendo infraestruturas físicas fazem negócio alugando estas estruturas e revendendo aos clientes finais, e na prática, identificam-se vários níveis de ISP, habitualmente identificados como *Tier 1*, *Tier 2*, *etc.*.

comercial, os ISP acabaram por introduzir um problema adicional na questão do acesso à Internet, que é o da qualidade do acesso à Internet e o da igualdade de acesso à Internet. Percebendo uma ameaça ao paradigma de uma plataforma tecnológica essencial para a sociedade como a conhecemos hoje, a comunidade que se debruça sobre as políticas de governação da Internet respondeu instantaneamente com a iniciativa Internet Livre e Aberta.

Este artigo debruça-se sobre dois dos problemas que hoje ameaçam o modelo de uma Internet Livre e Aberta e apresentando o que são os conceitos base de uma Internet Livre e Aberta, argumenta que também em Portugal há exemplos que, na nossa opinião, contrariam estes conceitos.

Escolhemos organizar este artigo da seguinte forma: a primeira secção inclui esta algo longa introdução, onde se fez uma revisão superficial dos conceitos fundamentais, e se ancorou o problema de uma Internet não livre e não aberta numa potencial violação de Direitos Humanos; a secção dois apresenta uma definição do que é a Internet Livre e Aberta e lista alguns dos seus mais fortes apoiantes; a secção três apresenta o caso de alguns operadores portugueses que nos parece contrariam alguns dos princípios apresentados. Finalmente, a secção quatro apresenta as conclusões e sugere linhas de acção para o futuro.

2. INTERNET LIVRE E ABERTA E A NEUTRALIDADE DA REDE

O conceito de Internet Livre e Aberta está bem descrito em duas iniciativas endossadas, a primeira pela empresa Google (Google Inc., 2015), e a segunda pelo Presidente dos Estados Unidos da América (EUA) (Barack Obama, 2014)⁽⁴⁾, e pode ser resumizada como segue.

A Internet Livre e Aberta é anunciada como sendo:

- Um pilar essencial para uma economia digital vibrante e inovadora;
- Uma forma de aproximar comunidades, exercer direitos e aumentar a democratização dos estados; e é
- Suportada pelo conceito de *Network Neutrality* (Wu, 2003).

Além disso, uma Internet Livre e Aberta, trazendo consigo a promessa do acesso rápido, livre e igualitário aos conteúdos que são produzidos, constitui o garante físico para o exercício de um conjunto de direitos a que arbitrariamente designaremos de Direitos Digitais.

Quando os pioneiros da Internet, de entre os quais Cerf tem lugar de destaque (Kathy Pretz, 2014), definiram os protocolos de comunicação e transmissão de dados que todos usamos, previram logo no princípio um modo de criar transmissões prioritárias, usando o campo *Type of Service* do cabeçalho do pacote IPv4 (*Internet Protocol version 4*). No entanto, e como este campo é definível na aplicação de origem, a menos que haja uma política de priorização de tráfego muito estrita, o seu conteúdo é normalmente visto como não-confiável, o mesmo se dizendo do campo equivalente no IPv6 (*Internet Protocol version 6*), o campo *Traffic Class*. Ainda assim, a priorização de tráfego é uma realidade nas nossas redes, sendo o exemplo mais comum a priorização do tráfego de voz sobre o tráfego *Web*, porque, *e.g.*, um segundo de atraso num pacote de voz pode ser crítico para a qualidade de serviço percebida numa chamada telefónica, mas um segundo a mais a carregar uma página *Web* é muitas vezes imperceptível. No entanto, e apesar de os protocolos preverem formas de hierarquização de prioridade para o tráfego de rede, na realidade o tráfego tem na sua

4 Apesar da inversão cronológica das referências apresentadas, é certo que o ainda Senador Barack Obama já tinha em 2007 alertado para a necessidade de uma Internet Livre e Aberta, e que a acção da Google só foi corporizada como forma de fazer frente a uma eventual posição desfavorável da FCC.

base uma natureza muito anárquica, sendo cada pacote processado, genericamente, apenas em função do estado de disponibilidade dos recursos, *i.e.*, um pacote pode ter sucesso na transmissão ou perder-se, não em função da sua origem ou destino, da empresa que o gerou ou da empresa para onde se destina, nem sequer do seu conteúdo, mas sim, porque o equipamento de rede que está encarregue de o encaminhar tem ou não recursos disponíveis para realizar essa tarefa. E isto é também algo que constitui a implementação do que é a neutralidade da rede, um conjunto de equipamentos, infraestruturas e protocolos que funcionam de forma maioritariamente autónoma e automática, que tratam cada pacote na medida das suas capacidades e recursos.

A neutralidade da rede é defendida por importantes organismos, como por exemplo a *Federal Communications Commision* (FCC) dos EUA (Federal Communications Commission, 2011), que apesar de independente foi largamente influenciada por uma posição forte do Presidente dos EUA e de um movimento amplo de bases, quer de empresas quer de indivíduos.

Na União Europeia (UE), a questão da Internet Livre e Aberta foi objecto de um amplo conjunto de recomendações e de acordos, incluindo o desenvolvimento da política de desenvolvimento do Mercado Único Digital. Talvez o momento político público mais significativo de todos tenha sido a declaração assinada em Istambul em 2014 pela Vice-Presidente da Comissão Europeia e Comissária Europeia para a Agenda Digital na altura, Neelie Kroes, e por alguns membros do Parlamento Europeu, onde se defendem seis princípios (European Commission, 2016; European Commission, 2014):

- Continuação da expansão global do acesso à Internet;
- Continuação da manutenção da Internet como um recurso global, aberta e comum, e de acesso não discriminado ao conhecimento;
- Aumento da transparência e da responsabilidade no modelo de governação “*multistakeholder*” da Internet;
- Rejeição da ideia de “internets” controladas por estados;
- Um mandato estável e continuado para a continuação do *Internet Governance* Fórum, dotado de recursos adequados; e,

- O reconhecimento de que as liberdades fundamentais e os direitos humanos não são negociáveis e devem ser protegidos *online*.

Este conjunto de recomendações daria para um outro artigo sobre as motivações e as intenções da Comissão Europeia e do Parlamento Europeu. Contextualizando, esta declaração surge na altura em que o governo dos EUA estava a fazer transitar as funções de gestão da IANA para o ICANN, e no Brasil tinha-se realizado a iniciativa NETMundial, seguida depois pelo Reino Unido e pelo *World Economic Forum*. Algumas das recomendações desta declaração parecem ter destinatários claros, como a da recomendação da rejeição de “internets” controladas por estados, ou a da chamada ao aumento da transparência na governação da Internet, enquanto outras são mais genéricas e destinam-se a reiterar a posição da UE sobre as questões base da Internet Livre e Aberta.

Aliás, no documento que sumariza as ligações para a iniciativa *Digital Single Market* da UE (European Commission, 2016), é claramente dito que uma Internet Aberta e Livre se baseia sobre quatro princípios, que são:

- Liberdade de escolha,
- Transparência,
- Qualidade de Serviço, e,
- E-Privacidade (privacidade no domínio da Internet).

Também nesse ano a FCC regulou o mercado de forma a que nenhum ISP ou nenhum produtor de conteúdos possa priorizar tráfego de uma qualquer origem sobre o restante tráfego, *i.e.*, e em concreto, a neutralidade da rede assenta sobre três princípios:

- Não bloqueio,
- Não estrangulamento,
- Não priorização paga.

Adicionalmente, Obama tinha pedido ainda à FCC que incluísse um quarto pilar que resultasse no aumento da transparência na forma como se processa o intercâmbio

de tráfego em todos os pontos da rede (Barack Obama, 2014), nos locais reconhecidos como *Internet Exchange Points* ou *Peering*, i.e., quando um ISP se liga a outros ISP, as ligações entre eles devem gozar do mesmo nível de prioridade e sempre que possível, com larguras de banda e velocidades de transmissão semelhantes, pois seria pouco ético que, por exemplo, o Operador X se ligasse ao Operador Y a uma velocidade de 100 Mb/s⁽⁵⁾ e, no mesmo local físico, se ligasse ao Operador Z a uma velocidade de 10 Mb/s, supondo que estes três operadores estão ao mesmo nível de transporte de tráfego de rede e têm idênticas capacidades de transmissão de dados.

Detalhemos um pouco o que são os três pilares da neutralidade da rede, uma vez que isso será importante para o caso que iremos apresentar na secção 3. Assume-se que o leitor compreende que na Internet, e por via da forma como os algoritmos e protocolos de transmissão e de encaminhamento de pacotes dentro da rede foram definidos, a transmissão de pacotes entre duas máquinas faz-se usando o princípio de melhor esforço (*best effort*), i.e., numa transmissão de dados sobre a Internet, não há, *a priori*, nenhuma garantia de que todos os pacotes de dados que contêm a informação a ser transmitida chegam sem atrasos, sem perdas e até na mesma ordem em que foram transmitidos para o computador de destino. No entanto, alguns destes protocolos incluem mecanismos que permitem ao computador de origem e de destino negociar uma forma eficiente e segura de transmitir os vários pacotes de dados.

- NÃO BLOQUEIO

O não bloqueio determina que um operador não poderá bloquear o acesso a um sítio da Internet, desde que legítimo, seja ele qual for. Isto garante que qualquer produtor de conteúdos na Internet tem exactamente o mesmo tratamento, quer seja um produtor de conteúdos mundialmente reconhecido como por exemplo, o Youtube⁽⁶⁾, quer seja um produtor de conteúdos nacional, como por exemplo, o Sapo⁽⁷⁾. Esta igualdade de tratamento entre todos os produtores legítimos de conteúdos é um princípio essencial da Internet e ajudará a seguir a definir outros dois pilares da Internet Livre e Aberta.

5 Mb/s = Mega bits por segundo. Para transmissões de dados este valor é percebido como um milhão de bits por segundo.

6 <http://www.youtube.com>

7 <http://www.sapo.pt>

- NÃO ESTRANGULAMENTO

O não estrangulamento refere-se a que um operador não poderá estrangular o tráfego de um determinado tipo ou de um determinado produtor de conteúdos para poder alocar maior largura de banda a outros tipos de tráfego ou a outros produtores de conteúdos. Em concreto, isto diz que um operador não poderá atrasar artificialmente o tráfego do, por exemplo, Vimeo⁽⁸⁾, para que o tráfego do, por exemplo, Youtube, tenha maior probabilidade de transmissão sem perdas.

- NÃO PRIORITIZAÇÃO PAGA

Finalmente, a não priorização paga consiste em garantir que nenhum operador implementa políticas que impliquem que um dado conteúdo é tratado de forma diferente por não pagar um serviço de “prioritização”. As aspas usadas no termo priorização, novamente, recordam que nas redes, um serviço só pode receber tratamento diferenciado positivamente, se outros serviços receberem tratamento diferenciado negativamente. Uma analogia interessante e que se pode usar neste caso pode ser encontrada no processo de abordagem para um avião. Habitualmente, os clientes *premium* das classes executivas têm o privilégio de poder entrar primeiro para o avião. No entanto, enquanto isso acontece, os passageiros das classes turísticas esperam porque o pessoal de terra está ocupado a verificar os passes de embarque e porque o acesso ao avião faz-se, neste exemplo, apenas por uma manga. Logo, o tratamento diferenciado positivo que uns recebem resulta à custa do tratamento diferenciado negativo que é fornecido aos outros. Uma forma de dar tratamento diferenciado sem degradação da qualidade de serviço para nenhuma das classes de bilhetes seria ter uma manga de abordagem dedicada a cada classe, com pessoal de terra dedicado também a cada manga, ou seja, a equalização do tratamento na abordagem far-se-ia à custa da maior afectação de recursos, algo que, abandonando a analogia e regressando às redes, é também possível, mas impraticável pelos custos que isso acarretaria.

⁸ <https://vimeo.com>

3. LIMITAÇÕES À INTERNET LIVRE E ABERTA EM PORTUGAL

No entanto, além destes três princípios, há outros dois que decorrem directamente dos anteriores, e são eles o limite de dados e o *Zero Rating*, melhor detalhados a seguir.

- LIMITES DE DADOS (*DATA CAPS*)

Um problema adicional que não é habitualmente associado às preocupações de uma Internet Livre e Aberta assente numa rede neutra, é a questão dos limites de tráfego. No entanto, é nossa opinião que esta prática é frequentemente detrimental para o paradigma da Internet Livre e Aberta, e em seguida apresentamos as razões que nos levam a esta posição.

Habitualmente, e particularmente nos tarifários de redes móveis mas não só, os operadores impõem um limite quanto ao número de bytes que podem ser transmitidos de e para o terminal móvel, *e.g.*, um telemóvel ou entre uma localização do cliente e o seu ISP. Apenas a título de exemplo, e apenas também porque este operador é o líder de mercado em Portugal nos últimos anos (Inês F. Alves, 2015; PORDATA, 2014) e os líderes de mercado, sabe-se, tendem a influenciar o comportamento de todo os actores nesse mercado, os tarifários móveis pós-pagos “*unlimited*” (MEO, 2016b) prevêem um limite no volume de transmissão de dados que vai dos 500MB⁽⁹⁾ aos 30 GB. Internacionalmente, outros operadores móveis de referência aplicam este tipo de políticas que, ao cobrarem ao utilizador um valor adicional pela transmissão de dados acima do frequentemente magro limite contratualizado, vão assim contribuir de forma real para o aumento da sua facturação.

A origem da imposição deste limite está ligada ao argumento de que é assim que o operador assegura aquilo que se designa por Política de Utilização Responsável (*fair use*), *i.e.*, o utilizador fica limitado no volume de dados mensais que pode transmitir porque isso é uma forma de autorregulação contra o uso abusivo dos recursos da rede, garantindo que nenhum utilizador monopoliza os recursos do operador que têm que ser partilhados por todos os utilizadores.

9 MB = Mega Byte, habitualmente interpretado como sendo 1024 Bytes, aproximadamente 1.000.000 Bytes; GB = Giga Byte, habitualmente interpretado como sendo 1024 Bytes, aproximadamente 1.000.000.000 Bytes.

No caso do operador que é líder de mercado em Portugal, a política de utilização responsável está descrita em particular, e por exemplo, nos pontos D 1 a 3 do Anexo 1 do contrato de subscrição dos serviços M4O, no item “CONDIÇÕES ESPECÍFICAS DO SERVIÇO DE DADOS – INTERNET NO TELEMÓVEL, BANDA LARGA MÓVEL E ACESSO À INTERNET WI-FI DA MEO – SERVIÇOS DE COMUNICAÇÕES E MULTIMÉDIA S.A.” (MEO, 2016a), mas também no ponto 8 do item “CONDIÇÕES ESPECÍFICAS DE PRESTAÇÃO DO SERVIÇO DE ACESSO À INTERNET EM BANDA LARGA DA MEO - SERVIÇOS DE COMUNICAÇÕES E MULTIMÉDIA, S.A.”⁽¹⁰⁾.

A limitação da quantidade de bytes transmitidos entre o cliente e o ISP é conhecida como *data caps*, e apesar do argumento aparentemente louvável de promoção de utilização responsável, esta limitação não parece no entanto ser sustentada por razões tecnológicas (Brodkin, 2016; Fight for the Future, n.d.). Recentemente surgiu até um excerto de um documento supostamente oficial e interno, onde um operador dos EUA parece sugerir que a razão da implementação da limitação no volume de dados transmitido não está relacionada com a necessidade de controlo de congestão da sua rede (desconhecido, 2015; Mills, 2015).

Aliás, o provável discurso deste ISP americano é sustentado por razões de natureza tecnológica, *i.e.*, há um argumento adicional que sugere que a imposição de limites à comunicação de dados em terminais móveis não está de facto relacionado com a autorregulação de utilização responsável dos recursos partilhados do operador, mas antes com a procura talvez ilegítima de lucro adicional, e que é este: na realidade, é muito mais eficiente para o operador monitorizar em contínuo uma eventual utilização irresponsável por parte dos seus utilizadores do que fazê-lo num período que dura um mês. Isto é, a eventual utilização irresponsável de um utilizador é melhor controlada e monitorizada em permanência, uma vez que, por exemplo, um ataque para negação de serviço, pode causar interrupções no fornecimento de serviços de voz e de dados a todo um segmento de rede, o que é de todo impensável. Acresce que os operadores implementam na realidade este tipo de monitorização, primeiramente por razões de segurança da rede, mas também porque, sendo os terminais móveis, é preciso prever, prover e alocar recursos suficientes para, numa dada zona geográfica, não correr o risco

10 As maiúsculas decorrem do título das secções nos documentos citados.

de sobrecarregar tanto a rede que ela deixe de funcionar. Acima dizia-se que a implementação de limites de transmissão de dados é talvez ilegítima (provavelmente não ilegal, e já debatemos porquê) se motivada por razões que não têm a ver com a solidez e funcionalidade da infraestrutura partilhada, por uma razão que é melhor demonstrável recorrendo, novamente, a uma analogia. Consideremos a forma anterior de disseminação de conhecimento, e os seus suportes, tais como os livros, as revistas, as bibliotecas, e se quisermos, até o contacto com sábios e professores em contextos de aprendizagem formal ou não. Consideremos agora que, para um conjunto de pessoas, com pouco poder financeiro, determinamos que essas pessoas só podem ter acesso a um número limitado pequeno de livros, ou a um número limitado pequeno de contacto em escolas. Consideremos ainda que, além disso, limitamos também o número de interacções com outras pessoas, o número de tarefas que podem fazer, e o número de horas de acesso a conteúdos recreativos. Sem mais argumentos, o mínimo que se pode dizer é que esta limitação compromete o exercício de alguns direitos humanos básicos dessas pessoas. E assim seria, se não regressássemos ao argumento de Cerf, o de que a tecnologia em si não é um direito. Mais, uma qualquer pessoa que esteja limitada no uso dos seus direitos digitais, para dizer isto de alguma forma, não está intrinsecamente impedida de ainda assim usufruir as prerrogativas que lhe são concedidas pela Declaração Universal dos Direitos do Homem, porquanto há outros métodos, outras formas, outras estratégias para aprender e para se recrear, desde logo, as que eram usadas antes de 1990, e ainda o são agora.

Não obstante, a limitação do número de bytes transmitidos imposta por um operador a um cliente, aplicada aparentemente seguindo um argumento de natureza mercantil, deixa um incómodo ético que urge estudar. Não o faremos aqui, mas ousamos deixar uma pista que pode ser útil. E novamente recorremos a outra analogia. Civilizacionalmente, antes dos livros, o saber era essencialmente transmitido de forma oral, de mestres para aprendizes, sendo os termos “mestre” e “aprendiz” aqui usados na sua forma funcional. No entanto, a humanidade reconheceu, de forma gradual, lenta mas virtualmente unânime⁽¹¹⁾, que o acesso generalizado ao conhecimento dos livros constituía uma mais-valia para todos. Para isso contribuíram um conjunto de tecnologias, desde logo a primeira, a escrita, e mais tarde, a imprensa. Ora estamos

11 Recorde-se aqui a recente galardeada com o Prémio Nobel para a Paz 2015, Malala Yusef, cuja vida foi colocada em risco por, precisamente, ousar querer ir à escola, sendo mulher.

precisamente, hoje, num ponto semelhante: não é que esta nova tecnologia resolva problemas que antes não tivessem sido solucionados, é que esta tecnologia, como antes o foram os livros, permite uma maior, melhor, mais rápida e mais ampla disseminação do conhecimento, e o reconhecimento do papel da Internet socorrendo-nos de anteriores tecnologias que permitiram a expansão do conhecimento humano, como por exemplo, a escrita, a imprensa, a comunicação à distância, dizíamos, esse reconhecimento tem que levar-nos à conclusão que limitar o acesso à Internet é equivalente a, historicamente, limitar o acesso aos livros, ou até às histórias contadas pelos seniores à aldeia, à volta da fogueira comunitária.

Nesta linha de razão, sendo certo que o exercício de direitos fundamentais não é cerceado pela limitação dos direitos digitais, é certo que acto de limitar o acesso à Internet produz uma imagem que não é agradável à luz dos valores da cultura humanista que promovemos, sobretudo porque, como referimos, a razão subjacente não parece ser a da imposição técnica para a promoção do Uso Responsável dos recursos.

Recorde-se a este propósito que em tempos, houve vários operadores em Portugal que distinguiam entre “tráfego nacional” e “tráfego internacional”, impondo limites distintos para um e para outro, e cobrando tarifas distintas para um e para outro (Fátima Caçador, 2001). Esta prática, felizmente, não resistiu nem às tensões do mercado, nem ao tempo.

Finalmente, e para concluir este ponto, põe-se uma questão que é frequentemente esquecida, e que é a questão do aferimento dos instrumentos de medida. Noutras realidades, os produtos que consumimos e que estão sujeitos a uma taxa ou preço de consumo, são-no porque os instrumentos de medida se encontram normalizados, vistoriados e regularmente aferidos, e porque quer o comprador quer o vendedor têm acesso ao seu estado em todo o tempo da medição. Em concreto referimo-nos aos contadores de energia eléctrica, da água, dos combustíveis que compramos nas estações de serviço, nas balanças dos mercados, por exemplo.

Mas, e os contadores de bytes, zelosamente instalados e mantidos nos ISP e nos operadores de comunicações móveis, quem os controla, quem os afere, quem os normalizou? Que tipo de tráfego medem? Medem apenas tráfego do cliente ou também medem tráfego de controlo e gestão entre o ISP e os dispositivos que estão em casa do cliente?

É legítimo cobrar um quilo de bytes, quando a balança que os pesa não está regulamentada, nem regulada, nem aferida? Eis a eventual ilegalidade anteriormente referida. Excepcionalmente, permita-se-nos relatar um caso pessoal, ocorrido com alguém próximo do autor deste artigo, há muitos anos atrás. Nessa altura, um ISP que ainda opera no nosso mercado apresentou uma factura na qual tentava cobrar um adicional pelo número de bytes transmitidos acima do limite contratado. Alegava o ISP que o consumidor tinha gasto 1.003.000.000 Bytes, isto é, 3.000.000 Bytes acima do limite de 1GB que estava contratualizado. O consumidor prontamente reclamou porque é sabido que $1 \text{ KB} = 1024 \text{ B}$, $1 \text{ MB} = 1024 \times 1024 \text{ B} = 1.048.576 \text{ B}$, e $1 \text{ GB} = 1 \text{ KB} \times 1 \text{ KB} \times 1 \text{ KB}$, isto é, $1 \text{ GB} = 1.073.741.824 \text{ B}$, e portanto, se era verdade que tinham sido transmitidos os 1.003.000.000 Bytes, isto estava ainda abaixo do limite do 1GB contratualizado. Este, entre outros argumentos, convenceu o ISP e a cobrança foi feita sem o valor adicional. Na realidade este é apenas um dos argumentos que podem ser usados para questionar a lisura das medições feitas pelos operadores. A questão da base numérica dos múltiplos do Byte, sendo habitualmente de base 2 para as medições de quantidades de Bytes, mas de base 10 para as medições das velocidades de transmissão, introduz uma ambiguidade que só pode ser usada em favor do consumidor. Numa numeração de base 2, $1 \text{ KB} = 2^{10} \text{ Bytes}$ ($1 \text{ KB} = 1024 \text{ B}$), mas numa numeração de base 10 (mais usada para medir velocidades de transmissão de dados), $1 \text{ KB/s} = 10^3 \text{ B/s}$ ($1 \text{ KB/s} = 1000 \text{ B/s}$).

O outro argumento é sobretudo usável em redes não cabladas, como as redes de telemóveis, uma vez que aqui o meio de comunicação *wireless* é partilhado por todos os terminais, o que quer dizer que, uma comunicação numa célula que esteja sobrecarregada terá muito mais *overhead* do que uma comunicação numa célula pouco carregada. E se esta situação de carga não pode ser imputada ao consumidor, porque não é o consumidor que determina qual o patamar de carga que uma célula de comunicações deve suportar sem degradar a comunicação, é no entanto o consumidor que acaba por pagar este *overhead*. Passe-se então a explicar o que é o *overhead* das comunicações neste contexto.

Numa transmissão de dados, por exemplo, um utilizador tenta fazer a abertura de uma página *Web* que está num servidor num sítio qualquer. Admita-se que esta transmissão de dados não consiste apenas no transporte dos caracteres que compõem a página *web*, mais as suas imagens, mais as suas formatações e programação do

comportamento da página, mas ainda, esta transmissão tem implícitos os pacotes de dados de controlo da transmissão, que incluem desde logo o *Three-Way-Handshake* e os pacotes de confirmação e gestão da transmissão do protocolo TCP (Clark, Jacobson, Romkey, & Salwen, 1989). Ora acontece que, quanto mais ruidosa ou sobrecarregada forem a rede e os recursos da rede, mais frequentes são estes pacotes, ou seja, numa rede pouco carregada, o rácio entre o número de pacotes de controlo e o número de pacotes de dados é muito menor do que numa rede sobrecarregada; no limite, numa rede muito sobrecarregada, o utilizador ou o *software* do *browser*, por exemplo, podem abortar a abertura da página. A experiência de tentar descarregar uma página *web* numa rede sobrecarregada ou com pouco sinal não é uma experiência rara: há alturas em que a rede, apesar de funcionar, pura e simplesmente não está funcional, e o utilizador, eventualmente, desiste de carregar a página que queria ver. No entanto, apesar do insucesso da acção, apesar de este não ser imputável ao utilizador, este pedido e os dados eventualmente transmitidos contaram para o seu limite de tráfego. E os pedidos de retransmissão, gerados e causados por uma rede subdimensionada, contam também para o seu limite de tráfego.

No nosso ponto de vista, a imposição de limites de tráfego em redes móveis e em redes domésticas é um entrave ao aumento do grau de digitalização que se pretende trazer para a sociedade, e como tal, a forma de garantia do Uso Responsável deveria ser implementada de outra forma mais transparente que não envolva o controlo do número de bytes recebidos e transmitidos. E apesar de este não ser um problema que esteja directamente relacionado com o paradigma de uma Internet Livre e Aberta, é algo que limita a sua completa prossecução.

- APLICAÇÕES COM TRÁFEGO LIVRE (ZERO RATING)

Outra das técnicas de marketing é o chamado “*Zero Rating*”, que consiste em isentar da contagem para o limite contratado de tráfego os bytes que são gerados por uma dada aplicação. Este conceito, presente por exemplo nos tarifários WTF da operadora NOS (NOS S.A., 2016) ou nos YORN da operadora Vodafone (Vodafone S.A., 2016) mas noutros também, é uma violação do princípio da não-discriminação da Internet Aberta e Livre, e tem efeitos secundários perversos.

Apesar do princípio da não discriminação não estar explícito nos três princípios base que anteriormente foram enunciados, a saber, o não-bloqueio, o não-

estrangulamento e a não priorização paga, o princípio da não discriminação acresce aos anteriores e decorre directamente do princípio da não priorização paga, porque a isenção da contagem do tráfego de aplicações específicas, de um fabricante específico, configura um favorecimento a esse fabricante, dado que os utilizadores desse operador, se sentirão compelidos a usar essa aplicação em detrimento de outras que, sendo do mesmo tipo e tendo funcionalidades semelhantes, por não beneficiarem desta isenção, representam um custo adicional para o utilizador. É portanto, uma configuração ligeiramente diferente do princípio da não priorização paga, só que em vez de essa priorização ser feita quanto ao preço a cobrar pelo aumento da velocidade do serviço, a priorização é feita directamente sobre a disponibilidade do serviço, *i.e.*, o utilizador que pague tem acesso livre a todas as aplicações, o utilizador que não pague tem acesso livre apenas às aplicações escolhidas pelo operador.

Mais, esta isenção faz ainda menos sentido em países altamente inovadores como, por exemplo, Portugal. Suponhamos que uma empresa nacional cria uma aplicação do tipo “Snapchat” e que pretende que ela ganhe uma massa crítica de utilizadores. Ora, jamais a concorrência entre essa nova aplicação e o “Snapchat” será justa e equilibrada em Portugal, porque os operadores nacionais decidiram dar “Zero Rating” à aplicação “Snapchat” mas não à aplicação nacional. Recorrendo novamente a uma analogia com uma biblioteca, a definição de políticas de “Zero Rating”, recorde-se, anunciadas como uma grande vantagem comercial pelos diferentes operadores, seria o equivalente a dizer que, numa dada rede de bibliotecas, os livros do autor X ou da editora Y podem ser consultados sem qualquer limite em termos de número ou de tempo, mas os livros de todos os outros autores, esses estão sujeitos a limites de consulta.

Para concluir este ponto, o “Zero Rating” além de violar o princípio da não priorização paga, na sua versão de não-discriminação, é prejudicial para a inovação dos pequenos fabricantes, dos pequenos programadores, e das pequenas economias, uma vez que favorece os grandes actores, das grandes economias mundiais. Este é um dos pontos em que os diferentes reguladores poderiam e deveriam ter uma acção mais activa (com perdão para a eventual redundância), dentro do contexto das suas funções e competências.

Complementarmente, acresce-se que a diferenciação do tráfego a facturar ao cliente cai também numa situação de eventual ilegitimidade, *i.e.*, a identificação de se o tráfego tem origem na aplicação X (que está isenta de limites) ou na aplicação Y (cujo tráfego deve ser taxado), esta diferenciação é feita por sistemas que também escapam ao controlo do utilizador e do regulador, configurando mais uma vez uma situação opaca, não regulada, não regulamentada, e não supervisionada de medição e facturação que, pode argumentar-se, está sujeita à discricionariedade do vendedor do serviço.

4. CONCLUSÕES

Neste documento apresentaram-se os conceitos de Internet Livre e Aberta e de *Net Neutrality*, identificando quais os mais importantes actores institucionais para a defesa destes princípios, e quais os contextos e conceitos que configuram a existência de uma rede livre e aberta, argumentando que a não-existência de uma Internet Livre e Aberta pode comprometer a prossecução de alguns dos Direitos Humanos, considerando uma sociedade cada vez mais focada na digitalização do conhecimento, e fundamentando esta opinião também em analogias com o mundo da informação com substrato de carbono.

Além dos quatro princípios base enunciados pelo principal regulador americano, a saber, o não-bloqueio, o não-estrangulamento e a não-prioritização paga, e a não discriminação, identificámos duas práticas habituais não só em Portugal mas também noutras partes do mundo que configuram um potencial incumprimento destes princípios, em concreto, falámos do *Zero Rating* e do *Data Caps*, argumentando que em ambos o consumidor poderá ser facturado por um serviço sobre o qual não tem forma de aferir da justeza dos instrumentos de medição, uma vez que estes estão apenas e exclusivamente no domínio do fornecedor.

Finalmente, cabe aqui concluir apontando caminhos futuros.

Decorre dos argumentos que antes apresentámos que somos favoráveis a uma Internet Livre e Aberta, sem limitações ao consumo medido no volume de bytes transmitidos, mas ainda assim, advogando que os ISP implementem mecanismos de controlo e promoção de políticas de utilização responsável junto dos seus utilizadores. Concluindo que os limites de transmissão de dados são profundamente prejudiciais para a prossecução dos objectivos de aumento e melhoria do grau de digitalização da sociedade, *i.e.*, são detrimenais para o usufruto dos nossos Direitos Digitais individuais e colectivos, estamos conscientes de que uma utilização responsável por parte de todos os utilizadores é uma condição fundamental para garantir a operação e a funcionalidade da infraestrutura de comunicações e da Internet, mas também certos de que todos os ISP implementam mecanismos que lhes dão métricas de identificação de não-conformidades nos perfis de utilização dos seus utilizadores, em tempo real, e que, portanto, é possível e desejável que estas políticas de utilização responsável sejam

promovidas de uma forma que não implique a diferenciação dos utilizadores com base no seu poder económico.

É ainda opinião do autor que a implementação de estratégias comerciais que favorecem umas aplicações sobre outras, implementando o que se designa por *Zero Rating*, é igualmente uma ofensa aos princípios que definem uma Internet Livre e Aberta, com especial gravidade no caso português, dado que nestes casos concretos, o favorecimento de grandes plataformas internacionais não permite um nível de concorrência equilibrado para os inovadores em Portugal, enviesando de forma real as oportunidades de inovação.

Além destas limitações, a Internet Livre e Aberta é ameaçada também por uma miríade de outros problemas, que vão dos políticos aos tecnológicos, passando pelos problemas sociológicos. Desde logo, e por exemplo, os actores que acima identificámos como tendo tido um aporte positivo na defesa de uma Internet Livre e Aberta num dado momento da história, vieram depois mais tarde a ter outras atitudes que envergonham a face de paladinos da Liberdade com que se quiseram fazer reconhecer, por exemplo advogando à necessidade de limitar o grau de cifragem das mensagens que circulam na rede (Murillo Roncolato, 2015).

Outro dos problemas não abordados neste artigo é o da fragilidade do sistema de governação Internet, assente num modelo *multistakeholder* ancorado no Internet Corporation for Assigned Names and Numbers (ICANN), uma empresa com sede no estado da Califórnia que gere as bases de dados de nomes e números dos sítios da Internet. O ICANN tem várias sub-organizações, uma das quais é o Non-Commercial Users Constituency (NCUC, n.d.), um grupo do Generic Name Supporting Organization (GNSO, n.d.). O NCUC e o GNSO são grupos compostos por indivíduos e organizações com fim não comercial, e a sua actividade consiste na discussão e aconselhamento ao ICANN sobre problemas concretos que influenciam os utilizadores da Internet.

Os ISP e os operadores de telecomunicações desempenham um papel fundamental na disseminação da tecnologia e da utilização da Internet, mas como é óbvio, os seus legítimos interesses nem sempre coincidem com os interesses da sociedade em geral e dos seus clientes em particular. No entanto, e talvez por isso mesmo, há muito espaço para melhoria e não aproveitar estas oportunidades seria injustificável.

Terminamos este artigo com três sugestões:

1ª Seria útil que o regulador nacional e os reguladores europeus estudassem o impacto que as políticas de *Data Caps* e *Zero Rating* tem na prossecução dos objectivos nacionais e europeus para a promoção dos Direitos Digitais dos cidadãos e da economia e para a iniciativa de Mercado Único Digital;

2º Seria útil que os operadores tomassem a iniciativa de implementar verdadeiros mecanismos de promoção da utilização responsável da Internet e deixassem de implementar limites à transmissão de dados como os conhecemos hoje; mais, os termos contratuais que hoje impõem aos seus clientes não são impedimento a que mudem estas práticas. Provavelmente, isto é até uma oportunidade de mercado, já que muitos utilizadores estariam disponíveis para, mediante o pagamento de uma pequena quantia, não terem limite no volume de dados transmitidos;

3º Por fim, sugerimos que cada um de nós se envolva na Non-Commercial Users Constituency. Neste momento há muito poucos elementos inscritos representando Portugal, e este é um fórum privilegiado para a discussão dos problemas da Internet global. É só seguir o *link* que está nas referências.

5. BIBLIOGRAFIA E REFERÊNCIAS

Barack Obama. (2014, September 24). Net Neutrality, President Obama's Plan for a Free and Open Internet. Retrieved April 27, 2016, from <https://www.whitehouse.gov/embeds/footer>

Brodkin, J. (2014, July 16). Verizon claims common carrier rules would require Web services to pay ISPs. Retrieved April 27, 2016, from <http://arstechnica.com/tech-policy/2014/07/verizon-claims-common-carrier-rules-would-require-web-services-to-pay-isp/>

Brodkin, J. (2016, June 3). Data caps are a business decision—not a network necessity, Frontier says. Retrieved June 6, 2016, from <http://arstechnica.com/business/2016/06/ex-verizon-customers-wont-face-data-coverage-charges-with-frontier/>

Clark, D. D., Jacobson, V., Romkey, J., & Salwen, H. (1989). An analysis of TCP processing overhead. *Communications Magazine, IEEE*, 27(6), 23–29.

desconhecido. (2015). Suposto documento oficial de um operador norte-americano. Retrieved April 28, 2016, from <http://i.imgur.com/quf68FC.jpg>

European Comission. (2016). Open Internet - Digital Single Market - European Commission. Retrieved June 2, 2016, from <https://ec.europa.eu/digital-single-market/en/open-internet>

European Commission. (2014). European Commission - PRESS RELEASES - Press release - Fighting for a free and open internet. Retrieved June 2, 2016, from http://europa.eu/rapid/press-release_STATEMENT-14-272_en.htm

Fátima Caçador. (2001, January 14). Limites de tráfego no ADSL da Telepac em vigor a partir de Janeiro (alterada). Retrieved June 2, 2016, from http://tek.sapo.pt/noticias/internet/artigo/limites_de_trafego_no_adsl_da_telepac_em_vigor_a_partir_de_janeiro_alterada-878046tek.html

Federal Communications Commission. (2011, January 12). Open Internet. Retrieved April 28, 2016, from <https://www.fcc.gov/general/open-internet>

Fight for the Future. (n.d.). Sneak Attack on Net Neutrality. Retrieved April 28, 2016, from <https://www.battleforthenet.com>

GNSO. (n.d.). Non-Commercial Users | Generic Names Supporting Organization. Retrieved June 3, 2016, from <http://gnso.icann.org/en/about/stakeholders-constituencies/ncsg/ncuc>

Google Inc. (2015). Um mundo livre e aberto depende de uma Web livre e aberta. | Google. Retrieved April 27, 2016, from <https://www.google.com/takeaction/>

Grammatis, K. (2010). A Human Right: Everyone Connected. Retrieved April 26, 2016, from <http://ahumanright.org>

Helena Garrido, Alexandra Machado. (2015, January 29). Telecomunicações O futuro: A prazo, os consumidores terão de pagar a qualidade das redes. Retrieved May 29, 2016, from http://www.jornaldenegocios.pt/negocios_iniciativas/detalhe/telecomunicacoes_o_futuro_a_prazo_os_consumidores_terao_de_pagar_a_qualidade_das_redes.html

Inês F. Alves. (2015, June 11). Meo mantém liderança nas comunicações móveis e Nos aumenta quota de mercado. Retrieved April 28, 2016, from http://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/servicos_moveis_meo_mantem_a_lideranca_mas_nos_aumenta_quota_de_mercado.html

Internet.org. (n.d.). Retrieved May 29, 2016, from <https://info.internet.org/en/>

Kathy Pretz. (2014). The Fathers of the Internet - IEEE - The Institute. Retrieved April 28, 2016, from <http://theinstitute.ieee.org/people/achievements/the-fathers-of-the-internet>

Kelly, K. (2007). *The next 5,000 days of the web*. Retrieved from https://www.ted.com/talks/kevin_kelly_on_the_next_5_000_days_of_the_web

Kravets, D. (2011, June 3). U.N. Report Declares Internet Access a Human Right. Retrieved April 26, 2016, from <http://www.wired.com/2011/06/internet-a-human-right/>

MEO. (2016a). Condições Específicas do Serviço de Dados – Internet no Telemóvel, Banda Larga Móvel e Acesso à Internet Wi-Fi da MEO – Serviços de Comunicações e

Multimédia S.A., Modelo C./1001328. Retrieved from <http://conteudos.meo.pt/meo/Documentos/Contratos-Adesao/Contratos-Adesao-servico-M4O-Mod-C1001328.pdf>

MEO. (2016b). MEO - Televisão, Internet, Telefone e Telemóvel. Retrieved April 28, 2016, from <https://www.meo.pt/>

Mills, C. (2015). Comcast Will Cap More People's Data Because of "Fairness." Retrieved April 28, 2016, from <http://gizmodo.com/comcast-will-cap-more-peoples-data-because-of-fairness-1740913276>

Murillo Roncolato. (2015, January 13). Primeiro-ministro britânico quer banir WhatsApp e Snapchat - Link. Retrieved June 3, 2016, from <http://link.estadao.com.br/noticias/geral,primeiro-ministro-britanico-quer-banir-whatsapp-e-snapchat,10000029832>

NCUC. (n.d.). NonCommercial Users Constituency | Advocating noncommercial interests at ICANN, which governs and sets policies for domain names you use every day. Retrieved from <http://www.ncuc.org/>

NOS S.A. (2016). WTF – Tá-se tudo a passar. Retrieved June 2, 2016, from <http://www.wtf.pt>

PORDATA. (2014). PORDATA - Quota de mercado do operador líder em telecomunicações móveis na Europa. Retrieved April 28, 2016, from <http://www.pordata.pt/Europa/Quota+de+mercado+do+operador+l%C3%ADder+em+telecomunica%C3%A7%C3%B5es+m%C3%B3veis-1502>

Rampton, J. (2015, October 23). Is Internet Access a Human Right? Mark Zuckerberg Thinks So. Retrieved April 26, 2016, from <https://www.entrepreneur.com/article/251942>

Sara Ribeiro. (2016, January 3). Lucros da Nos sobem 10,7% em 2015. Retrieved May 29, 2016, from http://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/lucros_da_nos_sobem107_em_2015.html

Vinton Cerf. (2012). Internet Access Is Not a Human Right - The New York Times. Retrieved April 26, 2016, from http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=0

Vodafone S.A. (2016). Yorn És Tu. Retrieved June 2, 2016, from <http://www.yorn.net/YORN/tarifario/yorn-x/>

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 2, 141.



**A PARTILHA DE RECURSOS PARA O TRANSPORTE DE DADOS E
A SUA RELAÇÃO COM A PRIVACIDADE NAS REDES EUROPEIAS
DE ENERGIA**

**RESOURCE SHARING FOR DATA TRANSPORT AND THE
RELATION WITH PRIVACY IN EUROPEAN ENERGY NETWORKS**

ELLEN M. WESSELINGH ¹

¹ The author lectures at The Hague University of Applied Sciences, faculty of Technology, Innovation & Society, program Mechanical Engineering. She can be contacted at E.M.Wesselingh@hhs.nl. This article was written as a result of the OPSCHALER project, iDEEGO (TSE) OPSCHALER: Open Platform for Smart data in Combination with Holistic Analysis Leading to Energy Reduction - Program: iDEEGO Innovation Durable Energy and Energy reduction Built Environment of TKI-EBGO, Program line: 4. Energy Control Systems and services for energy savings and optimised energy use at building and area level, Grant Giver: Top consortium Knowledge and Innovation - Energy reduction in the Built Environment (TKI-EBGO).

RESUMO

Nas últimas décadas, o mercado único da UE tem procurado moldar-se ao mundo digital, ainda que a Comissão Europeia procure, de forma mais ambiciosa, um cada vez maior nível de harmonização. Destacaríamos, neste introito e com influência directa sobre o digital, as transições operadas no mercado da energia eléctrica, de geração, distribuição e transporte. Ante o surgimento do prosumidor (produtor-consumidor) na geração de energia eléctrica, cada vez mais as redes de distribuição e de transporte de energia eléctrica exigirão mais e mais dados para equilibrarem o fluxo de energia das respectivas redes. Este procedimento abrirá o caminho para a partilha de dados através de redes eléctricas. Neste conspecto, que implicações materiais suscitará em termos de privacidade?¹

Palavras-Chave: Mercado Único da UE; Protecção de Dados; Distribuição de Energia; Partilha de recursos físicos; redes de dados

¹ Translation of the summary thanks to Nuno Teixeira Castro.

ABSTRACT

The single EU market with regard to the digital world has been shaped in the past decades, but the European Commission is even more ambitious with regard to the level of unity that it strives for. Another development that has taken place recently, that influences the digital world, is the transition of the electrical energy generation, distribution and transport market. With the emergence of the prosumer (producer-consumer) in the generation of electrical energy, electrical distribution and transport networks now require more and more data to balance the energy in their networks. This opens the road to sharing of data over electrical networks. What are the implications with regard to privacy?

Keywords: EU Single Market; Data Protection; Energy Distribution; Physical Resource sharing; Data networks

1. INTRODUCTION

The European Commission (EC) strives for a further integration of the market for data services [1], and is also investigating cost efficient ways for a more climate-friendly economy [2] but faces the problem of legislation that is not fully harmonised across Europe [3]. Part of the envisioned single market space is Directive 2014/61/EU that enables physical resource sharing for data transport across energy networks: a sort of net neutrality for the energy distribution industry [4].

The new General Data Protection Regulation 2016/679 (full harmonisation) that is expected to enter into force 2018 [5] is being made from a different perspective than the previous legislation from 1995 that was a directive (minimum harmonisation to which the Member States could make additions). For this reason, the European Commission and Parliament have worked on full harmonisation by way of Regulation 2016/679 setting out a general EU framework for data protection [5].

How does this new regulation that has just been published, influence the way energy network operators have to manage their networks? Will the proposed legislation change the entire energy industry and the way the market works? Those are questions yet to be answered. This article focuses on the electricity distribution networks as a starting point for the discussion.

2. CHARACTERISTICS AND REGULATION OF DATA IN ELECTRICAL ENERGY NETWORKS

It is important to realise that electricity cannot be easily stored in great quantities, and this poses a problem for the electrical distribution grid. In the past, electricity generation was done in large power plants and could, therefore, be carefully planned and controlled by single entities. Solar and wind energy are, on the other hand, less predictable. Another development is the recent emergence of many more stakeholders in the energy production chain, now that households can produce their own energy with the use of solar panels or wind turbines.

This means that more data on actual production capacity and actual energy use must be available at any moment to the energy network operator. The network operator needs this data to balance the network, preventing energy shortage or surplus. Shortages lead to possible damage with the customer who may be unexpectedly confronted with a black-out. Surplus leads to inefficiency and thus extra cost for either the energy supplier or the network operator.

Each entity connected to the energy grid is responsible for its own individual balancing of energy consumption and production, but households and small enterprises typically outsource this responsibility to the supplier [2]. Hence the supplier needs the energy consumption and production data to fulfil its responsibility. The data is transported over the electrical grid using Power Line Communications (PLC). The so-called Smart (electricity) Meters that are installed in the home today send the data of the domestic energy consumption to the energy supplier.

This data contains information that can be traced back to natural persons and it is therefore considered to be personal data subject to Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data [6], and its successor Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [7]. Further, Directive 2016/680 on the use of personal data for criminal investigation was issued in conjunction with the regulation [8]. The focus of this article is on the regulation, because it has a big impact on the energy sector.

Other recent regulation with impact on the energy sector is Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks, which imposes obligations on utilities companies in the public sector (of which electricity networks are one) to cooperate with the telecommunications sector on measures to reduce cost

of deploying high-speed electronic communication networks. If they do not agree on issues, national regulators may decide on a resolution which is binding to the parties (preamble 19, 23, and articles 3(5), 4(6), 5(4) and 6(4)) [4] [9]. Under this directive, sharing of public sector physical infrastructure will commence on January 1st, 2017.

The Directive 2014/61/EU aims to enable the sharing of public sector physical infrastructure (preamble 4 and article 1(1)) and thus, reduce the cost for civil engineering works (preamble 7 and article 1(2)) by lifting regulatory differences that prevent cooperation across utilities (preamble 10 and 24, article 3(1) and 3(2)). The Directive 2014/61/EU lays down minimum rights and obligations for cross-sector coordination (preamble 11). One of the obligations for public sector bodies is to facilitate the use of utilities such as physical networks for the provision of electricity by new electronic communications network operators (preamble 13 and article 4(2)).

The provision of access should be under fair and reasonable terms (preamble 14 and article 3(2)), and according to the technological neutrality principle (preamble 15 and 29). In the directive there are security concerns explicitly mentioned as for example where sharing the infrastructure jeopardizes the network integrity and security (preamble 16, 17, articles 4(1) and 6(1)). The premises may be visited in an on-site survey (article 4(5)), which means that the provider of the physical infrastructure may have to adapt its on-site procedures to accommodate other parties entering the premises. Given the fact that most companies work with contractors at their sites, that should not be a major issue.

Critical national infrastructure may be exempt from the obligation to sharing of physical infrastructure (articles 4(7) and 6(5)), but it is likely that the bar for denomination of critical infrastructure will be set high.

Further complicating factor in the Directive 2014/61/EU is the fact that by allowing third parties telecommunications access to their critical infrastructure the electricity networks providers become subject to the set directives governing the telecommunications sector (directives 2002/19, 2002/20, 2002/21, and 2002/22) (preamble 12 and article 1(4)). In the past the different industry sectors (media, telecommunications, energy infrastructure) were relatively set apart, each with their own set of regulation (for example the telecommunications directives 2002/19, 2002/20, 2002/21 and 2002/22). The Directive 2014/61/EU provides a further step in blurring the lines and further integration of industry sectors.

In the past, integration of sectors was at times troublesome. In the Netherlands, the national telecommunications provider Royal Dutch KPN was unwilling to open up its network to mobile phone providers. After a number of conflicts on the interpretation of reasonable and fair conditions the market now appears to have settled. Cable companies providing radio and television over their own networks have opened up their networks to competitors since 2000, but apparently not wholeheartedly [10].

3. KEY PERSONAL DATA PROTECTION ISSUES FOR NETWORK OPERATORS

The reform of the data protection legislation in the EU started in January 2012, when the European Commission proposed a comprehensive reform. After four years of discussion, on 4 May 2016, the official texts of Regulation 2016/679 and the Directive 2016/680 have been published in the EU Official Journal in all the official languages. The Regulation entered into force on 24 May 2016, and it is applicable from 25 May 2018. The Directive 2016/680 entered into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018 [11] [12].

This reform of EU data protection has some very far-reaching consequences for all those companies that process personal data, and as such for the energy sector. Two trends could be identified: the first is the big data trend, in which more and more personal data becomes available for analysis and use. The second trend is the data protection trend, in which stricter regulation on the processing of all this personal data, with the option of serious penalties in case of data protection breaches. The data protection trend is elaborated in the regulation, which introduces a number of new rights and severe penalties if these rights are infringed upon.

The new data protection regulation builds on the principles of Privacy-by-design. These principles were developed by the Canadian privacy protection officer Ann Cavoukian, and they consist of seven principles. Summarised, the principles are [13] [14]:

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default Setting
- Privacy Embedded into Design
- Full Functionality — Positive-Sum
- End-to-End Security — Full Lifecycle Protection
- Visible and Transparent
- Respect for User Privacy — User-Centric

These principles can be found in Regulation 2016/679 as the explicit consent requirement (preamble 32 and 42, articles 6(1)(a) and 7), the transparency requirement (preamble 39, 58, 60, 63, and articles 5(1), 12, 13, and 15), the preventative technical

requirements on systems (preamble 67), the data portability right contributing to full functionality (preamble 68 and article 20). The full lifecycle protection principle can be found in the many requirements on the processing security and transfer of personal data (for example preamble 73 or 75 and article 32). Data protection by default and the technical implementation obligations to establish this default are explicitly mentioned in preamble 78, and article 25.

One key newly created obligation for data processors is the data breach notification obligation (preamble 73 and articles 33 and 34). While Regulation 2016/679 aims to give data processors more freedom and responsibility to process the data as they see fit, it also aims for more legal and practical certainty for all stakeholders, including the natural persons it aims to protect, by placing the responsibility and liability on the data processor (preamble 74 and article 28(4)). In the political process of designing the legislation, the data breach notification obligation has been transformed into data protection impact assessments and (implicit) data breach impact assessment (preamble 84, 90, 91 and articles 35 and 33(3)(c)) [7] [15]. The data breach notification obligation is implemented as a general notification obligation to the regulatory authorities (preamble 85 and article 33) and a notification obligation to the data subject in case of serious risk of damage (preamble 86 and article 34).

Newly created rights for individuals are the data portability right, and the ‘right to be forgotten’ for customers of data services (preamble 59, 65, 66 and articles 13(2)(b) and 17). Further, EU rules must be much stricter applied when processing personal data abroad, reducing opportunities for alternative safe harbour regimes (preamble 101-108, articles 28(3)(a) and 44 – 46) [5] [7]. The data portability right means that the energy sector must cooperate on some sort of data standard in order to be able to efficiently implement the new obligation.

The right to be forgotten will probably not have a major impact on the energy sector, as it applies to erasure of data for which there is no longer a purpose, especially applicable to online publications, which is not a core business at the moment. Energy companies should already have policies in place to deal with data erasure of customers that no longer use their services. However, future developments of merging sectors may create a different situation in this regard.

The stricter rules on offshoring of data processing have the potential for impact on the sector depending on the business model for the processing of data that is used. However, the regulation does encourage groups of undertakings by providing for approved binding corporate rules (preamble 110, article 47). Whether Regulation 2016/679 will indeed cause problems for

companies making use of the cloud services of major US cloud providers, for example, remains to be seen. In recent years, some of these providers anticipated Regulation 2016/679 and moved part of their operations to EU Member States in order to comply with the EU data protection legislation. It remains to be seen to what extent this solution passes the bar that Regulation 2016/679 has set. In that regard, the legal certainty that the regulation aims to establish will have to be effectuated in the future.

Infringement of Regulation 2016/679 can have serious consequences, with the regulatory body being enabled to impose an administrative fine of up to 10 million Euro, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year (article 83(4)). In cases of a lack of baseline security and compliance, these fines may be up to 20 million Euro or 4% of the total worldwide annual turnover of the preceding financial year (article 83(5) and (6)). The wording of these articles seems to indicate that other entities than corporations can be fined, such as natural persons performing the data breach, which is confirmed by preamble 148.

In this discussion, it is important to highlight the broad nature of what the European Commission defines as personal data: any information relating to an individual, be it that individual's private, professional or public life. This may encompass anything from a name, a photo, an email address, bank details, posts on social networking websites, medical records, a computer's or smart phone's IP address [5] [7]. This broad definition means that any service provider will be denoted a data processor under the regulation as soon as the service provider processes only the tiniest bits of data about individually recognisable customers.

4. CONSEQUENCES & CONCLUSIONS

The new data protection Regulation 2016/679 will have impact on the energy sector, a sector that is in the process of a transition towards durable energy production, which requires much more data in the energy production and distribution chain. Part of the data contains personal data, which is subject to strict regulation in the EU. First of all this means that the collection of data shall be done such that no unnecessary data collection takes place. What was never collected cannot be leaked, after all. This is in line with the privacy as the default setting and embedded into the design, as explicated in preamble 39 and articles 5(1)(a) and 25(2) of the EU data protection Regulation 2016/679.

Where it cannot be avoided to collect certain personal data, the principle of data minimisation requires this data must be aggregated or pseudonomised as soon as possible by the data processor (articles 5(1)(c) and 32(1)(a)). For example the Smart Meter data is collected over a defined period of time and aggregated before it is sent. The aggregation can be done, because the system does not need real-time data for the balancing purposes. A time period of 15 – 20 minutes is adequate for most purposes. Further aggregation on for example 6 digit postal code nearest to the home provides further data protection. However, with more and more information coming online, for example through social media, this may not prove to be adequate to prevent the leaking of personal data in the future.

Directive 2014/61/EU, which provides for sharing of the physical infrastructure of the energy sector further complicates the data management, because adequate security measures will have to be taken to ensure adequate separation of the data streams of the different data network providers that share the physical infrastructure. For each instance in its physical infrastructure the owner will have to assess the impact of sharing of that facility. This will require some sort of risk assessment in which not only network integrity must be addressed, but also the data protection.

While the trend of resource sharing does offer efficiency opportunities, it also poses significant challenges for the subjects of the new legislation who have to implement it. Companies not traditionally involved in network operations will have to adapt to this new reality. It is likely that this will cause growing pains with regard to security and data protection. It would be advisable for national regulators to carefully monitor this process in order to prevent frequent large data breaches.

5. BIBLIOGRAPHY

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a thriving data-driven economy*, Brussels, 2.7.2014, COM(2014) 442 final, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6210
2. Smart Grid Task Force (2015), Expert Group 3 (Regulatory Recommendations for Smart Grids Deployment), *Regulatory Recommendations for the Deployment of Flexibility*, <http://ec.europa.eu/energy/sites/ener/files/documents/EG3%20Final%20-%20January%202015.pdf>
3. EY (2013), *Mapping power and utilities regulation in Europe*, EYG no. DX0201, <http://www.ey.com/GL/en/Industries/Power---Utilities/Mapping-power-and-utilities-regulation-in-Europe>
4. Directive 2014/61/EU of the European Parliament and the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0061&from=GA>
5. Article 29 Data Protection Working Party, *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)*, 2.2.2016, 442/16/EN, WP 236, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:PDF>
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>
8. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

9. Smart Grid Task Force (2015), *Regulatory Recommendations for the Deployment of Flexibility*, EG3 Report (p.57), <http://ec.europa.eu/energy/sites/ener/files/documents/EG3%20Final%20-%20January%202015.pdf>
10. Peggy Valcke (2004). *Digitale diversiteit: Convergentie van Media-, Telecommunicatie- en Mededingingsrecht*, Larcier (p. 32)
11. European Commission, *Protection of personal data*, <http://ec.europa.eu/justice/data-protection/> (visited May 2016)
12. European Commission - Press Release, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, Brussels, 25.1.2012, IP/12/46, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
13. E.M. Wesselingh, P. van Willigenburg, H. Stokman (2015), *DCCPP = Privacy by Design. Direct Current Communications & Privacy Protocol (DCCPP) Proposed for a Privacy Protective DC Smart Grid*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671170
14. E.M. Wesselingh, P. van Willigenburg, H. Stokman (2015), *Proposal for a Transparent Sustainable Energy Market* (Poster), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2622930
15. Article 29 Data Protection Working Party, Work programme 2016 – 2018, 2.2.2016, 417/16/EN, WP235, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp235_en.pdf

CYBERLAW

by CIJIC

A CIBEREDUCAÇÃO E A CIBERSEGURANÇA

CYBEREDUCATION AND CYBERSECURITY

SALOMÉ DE JESUS VIEIRA ¹

E

FERNANDO JORGE RIBEIRO CORREIA ²

1 Aspirante Salomé de Jesus Vieira. Correio electrónico: salome.jesus.vieira@marinha.pt

2 Capitão-de-fragata Fernando Jorge Ribeiro Correia. Correio electrónico: ribeiro.correia@marinha.pt

ABSTRACT

The role of Information Technology (IT) in contemporary societies is predominant. The emergence of the Internet and the popularization of its use has changed the paradigm of corporate operation.

Industrial societies have turned into information societies, where knowledge and information are valued and have a key role. The Internet, primarily regarded as an absolute space of freedom that allowed access and sharing data instantly from anywhere in the world, is now seen as a factor of insecurity.

Cyberspace is susceptible to new forms of threat as crime in the virtual world. Cyber-attacks threaten citizens' privacy and freedom, undermine state sovereignty and may also disclose information that threatens national security.

The Information Security doesn't only depend upon available technology, but how the users use that technology to manage the information. Knowledge about how the technology works and how information is processed allows risk reduction and increase Information Security level, i.e., cybereducation is required to reach a security culture.

This work discusses the challenges that cyberspace brings us and maps the Cyberspace Security National Strategy with European Union follow the path of Cyberspace Information Security culture.

Keywords: cybersecurity, cybereducation, security culture, education model, Portugal.

RESUMO

O papel das Tecnologias de Informação (TI) nas sociedades atuais é preponderante. O aparecimento da Internet e a vulgarização do seu uso veio alterar o paradigma do modo de funcionamento das sociedades.

As sociedades industriais transformaram-se em sociedades da informação, onde o conhecimento e a informação são valorizados e têm um papel fulcral. A Internet, primeiramente considerada como um espaço de liberdade absoluta e que possibilitava o acesso e compartilhamento de dados instantaneamente e a partir de qualquer ponto do globo, é hoje vista como um fator de insegurança.

O ciberespaço está suscetível a novas formas de ameaça sobre a forma de crime no mundo virtual. Os ciberataques colocam em risco a privacidade e liberdade dos cidadãos, põem em causa a soberania do Estado e podem, ainda, divulgar informação que ameace a segurança nacional.

A Segurança da Informação não depende apenas da tecnologia disponível, mas essencialmente, a forma como os utilizadores empregam essa mesma tecnologia para gerir a informação. O conhecimento sobre o funcionamento da tecnologia e como a informação é processada permite reduzir os riscos e aumentar o nível de Segurança da Informação, ou seja, são necessárias acções cibereducação que conduzem a uma cultura de segurança.

O presente trabalho discute os desafios que o ciberespaço nos coloca e mapeia a Estratégia Nacional de Segurança do Ciberespaço a fim de se caminhar para uma cultura de segurança da informação no ciberespaço.

Palavras-chave: cibersegurança, cibereducação, cultura de segurança, modelo de formação, Portugal.

1. INTRODUÇÃO

O conhecimento humano surge da necessidade permanente de entender o mundo que nos rodeia. Trata-se de uma ferramenta fundamental que o Homem utiliza não só para a sua sobrevivência, mas também para se relacionar com o seu semelhante.

A necessidade e a dúvida são os fatores impulsionadores do desenvolvimento das capacidades do ser humano e as inovações tecnológicas sempre acompanharam a evolução humana e foram desenvolvidas com o objetivo de facilitar e aprimorar as atividades necessárias para a subsistência do homem.” (Efing, 2012, p. 23).

Atualmente vivemos na “Era da Informação”, e qualquer tentativa de definição da sociedade da informação^(1) em que nos inserimos, mostra-se redutora. A sua complexidade e amplitude é tal que podemos definir características, mas não dar uma definição concreta de sociedade da informação.

A expressão “sociedade da informação” realça o papel da informação na sociedade, por vezes também designada por “sociedade do conhecimento”, na medida em que o conhecimento é gerado a partir da informação. Esta inversão de paradigma veio relativizar o espaço e o tempo, uma vez que as novas tecnologias, como a Internet, permitem o acesso e a partilha de dados a partir de casa instantaneamente.

Cada vez mais, a nossa vida profissional, pessoal e social depende da tecnologia. Já não há uma distinção clara entre a casa e o local de trabalho. As diferentes dimensões da nossa vida estão correlacionadas. Contudo, o preço a pagar pela globalização e inovações tecnológicas é o fim da envolvente estruturada, organizada e facilmente previsível em que nos encontrávamos.

A Internet assume-se como “uma dimensão de comunicação livre”, é “um símbolo de liberdade e de capacidade para dominar o tempo e o espaço” (Wolton, 1999, p. 92), pela sua acessibilidade, universalidade e por conduzir o processo de globalização.

Contudo, apesar do seu papel fundamental, a Internet também compreende riscos, nomeadamente para a segurança e defesa nacionais. Apesar de numa primeira análise se

1 Um dos primeiros autores a referir o conceito de Sociedade da Informação foi o economista Fritz Machlup, no seu livro publicado em 1962, *The Production and Distribution of Knowledge in the United States*. Contudo, o desenvolvimento do conceito deve-se a Peter Drucker que, em 1966, no seu livro *The Age of Discontinuity*, fala pela primeira vez numa sociedade pós industrial em que o poder da economia assenta num novo bem precioso: a informação. (Crawford, 1983, pp. 380-385)

considerar a Internet como um espaço por excelência de liberdade absoluta e sem fronteiras, a realidade porém, leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar” (Martins, 2012).

Assim, constata-se que temos uma necessidade emergente de educar os cidadãos para uma melhor utilização das novas tecnologias, uma vez que a chave para a prosperidade futura e para os modos de vida qualitativamente diferentes está na aprendizagem dos processos de manipulação, transmissão, armazenamento e obtenção de informação (Lyon, 1992, p. 1).

O ciberespaço é um assunto cada vez mais relevante, tanto a nível nacional como internacional. Somos confrontados com todas as suas capacidades, assim como com os aspetos positivos e negativos que resultam da sua utilização. Contudo, o conhecimento sobre o seu real funcionamento, bem como as suas vulnerabilidades e sujeições, dificilmente serão mapeadas por completo.

É necessário confrontar os desafios que o ciberespaço nos coloca com a capacidade de resposta desenvolvida, uma vez que a necessidade de cibersegurança é hoje mais importante que uma defesa bélica eficaz.

Novas formas de ameaça surgiram com a evolução tecnológica, mudando a dimensão do teatro de operações, do espaço físico para o ciberespaço, onde nos confrontamos com um inimigo que se tornou invisível perante os nossos olhos (Martins, 2012).

Os ciberataques põem em risco a privacidade e liberdade dos cidadãos, ameaçam a segurança nacional e até mesmo a soberania do Estado. Torna-se cada vez mais imperativa a necessidade de proteger a informação, uma vez que esta já não se encontra armazenada num espaço singular e preciso, mas sim no ciberespaço.

No ciberespaço, o controlo de acesso à informação torna-se mais difícil, podendo esta ser utilizada de forma abusiva, por indivíduos mal-intencionados, para servir interesses ilegítimos e afrontar os direitos, liberdade e segurança dos cidadãos.

De acordo com o Special Eurobarometer 404 – Cyber Security Report², as perdas devido a cibercrimes representam biliões de euros por ano, e estima-se que existem mais de 150.000 vírus e outros tipos de *malware* em circulação e aproximadamente um milhão de pessoas vítimas de cibercrime por dia. Os resultados apresentados no relatório indicam que 28% dos utilizadores da Internet na UE não está confiante da sua capacidade para usar serviços como *online banking* ou comprar bens *online*. Contudo, 70% afirmam estar razoavelmente ou muito confiantes, valores estes muito semelhantes aos obtidos no Special Eurobarometer 390³, pesquisa efetuada em 2012.

Foi ainda apurado que 10% dos utilizadores sofreu fraude *online*, 6% foram alvo de roubo de identidade, 12% não conseguiram aceder a serviços *online* devido a ciberataques, 12% dos utilizadores tiveram a sua conta pessoal acedida de forma indevida (*hacker*), 7% foi vítima de fraude bancária *online* e 14% afirma ter encontrado, acidentalmente, material que promove o ódio racial e extremismo religioso.

Posto isto, e tendo como ponto de partida este panorama, considera-se essencial colaborar para a consciencialização e ação política no que respeita à cibersegurança. Ao Estado reconhece-se a capacidade última de proteger os seus cidadãos, e para isso é necessário fazer frente a estas ameaças que são uma constante diária. A cibereducação é uma competência que deve ser leccionada na atividade formativa de cada cidadão e é da responsabilidade do Estado incluir este tema nos programas de formação.

O presente trabalho encontra-se dividido em cinco secções. Na primeira secção é feito um enquadramento do tema. Na secção seguinte é apresentado um mapa de conceitos, onde são incluídos alguns tópicos que ajudam a enquadrar o tema do trabalho. Na terceira secção é abordado de forma sucinta o tema da partilha de informação nas redes sociais. O tema da cibereducação é apresentado na secção quatro. Finalmente, as conclusões são apresentadas na secção cinco.

2 Relatório elaborado por *TNS Opinion & Social*, a pedido da *European Commission, Directorate-General Home Affairs*, composto pelos resultados de uma pesquisa feita aos 27 países que constituem a UE e à Croácia, entre maio e junho de 2013. Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (consultado a 09/11/15).

3 Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (consultado a 09/11/15).

2. MAPA DE CONCEITOS

2.1 SEGURANÇA

O termo segurança abrange diversas aceções. Em linhas gerais, pode-se afirmar que este conceito deriva do latim *securitas*, que se refere à qualidade daquilo que é seguro, ou seja, aquilo que está protegido de quaisquer perigos, danos ou riscos. Quando se diz que algo é seguro, significa que é algo estável e indubitável. A segurança é uma certeza, mas também uma necessidade.

2.2 SEGURANÇA DO INDIVÍDUO

Segundo o artigo 27º n.º1 da Constituição da República Portuguesa (CRP): “Todos têm direito à liberdade e à segurança”. Contudo, só é possível beneficiar de liberdade e segurança num ambiente de justiça, como previsto no artigo 28º da Declaração Universal dos Direitos do Homem, de 10 de Dezembro de 1948: “Toda a pessoa tem direito a que reine, no plano social e no plano internacional, uma ordem capaz de tornar plenamente efetivos os direitos e as liberdades enunciados na presente Declaração”.

O conceito de “segurança humana” ou segurança do indivíduo surgiu nos anos 1990 e veio alargar a noção tradicional de segurança, antes centrada na segurança dos Estados. Passou-se a atribuir mais valor ao próprio indivíduo.

A segurança do indivíduo visa proteger os indivíduos contra ameaças, criminalidade, violações dos direitos humanos, invasão de privacidade e ameaça à reserva de intimidade. Aponta ainda para ameaças como a fome, doença, pobreza, violação sexual, imigração, desemprego e tráfico de pessoas.

Em suma, todos têm direito à segurança, ao reconhecimento dos direitos fundamentais e de viver em liberdade e com dignidade.

2.3 CIBERESPAÇO

Ciberespaço pode ser definido como um “ambiente virtual onde se agrupam e relacionam utilizadores, linhas de comunicação, *sites*, fóruns, serviços de Internet e outras redes” (Gobierno de España, 2011, p. 43).

De acordo com a Dicionário Editora da Língua Portuguesa, ciberespaço é definido como um “espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações”.

No atual mundo globalizado, o ciberespaço é visto como um espaço virtual, “que a par dos tradicionais domínios da interação humana como a terra, o mar, o ar e o espaço, é o meio onde se desenvolvem as atividades económicas, produtivas e sociais das nações mais desenvolvidas”. (IDN, 2013, p. 9)

“O ciberespaço é assim um ambiente em si mesmo, onde se deve ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-los, como os fatores humanos, uma vez que são estes que caracterizam os utilizadores deste ambiente” (IDN, 2013, pp. 9-10).

2.4 CIBERAMEAÇAS

Ameaças que surgem na sequência da utilização massiva das TI ligadas em rede e que podem afetar infraestruturas críticas para o equilíbrio funcional da sociedade, assim como o sistema político internacional. Como exemplos de Ciberameaças existe o *hacking*, o *hacktivismo*, o ciberterrorismo e a ciberespionagem.

O termo *hacking* refere-se a ações realizadas com recurso a ferramentas de *software* e *hardware* para exploração de vulnerabilidades dos sistemas informáticos com o objetivo de aumentar o nível de acesso ou controlo sobre os mesmos.

Hacktivismo é a ação conduzida por indivíduos ou grupos que utilizam meios informáticos e “veem a Internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem” (Santos, 2011, p. 27). A ideologia defendida pode ter motivações distintas, desde políticas a religiosas, mas o objetivo final é comum: chamar a atenção da opinião pública para determinado assunto.

O ciberterrorismo consiste no uso das TI para ameaçar e realizar ataques políticos deliberados com grande impacto nos sistemas de redes de computadores e infraestruturas críticas. Promove o medo e o terror, “é um novo tipo de atividade criminal, (...) que materializa a convergência do ciberespaço com o terrorismo” (Santos & Bessa, 2008) que desencadeia determinadas ações políticas.

Ciberespionagem é caracterizada pela exploração de vulnerabilidades encontradas em *sites* para ter acesso a informação sensível. “É perpetrada por estados que procuram adquirir conhecimento e recolher informações, que lhe podem conceder uma vantagem estratégica sobre terceiros” (Pereira, 2012). A ciberespionagem é motivada pela vantagem competitiva sobre Estados ou ainda por benefícios financeiros provenientes da venda de informação roubada.

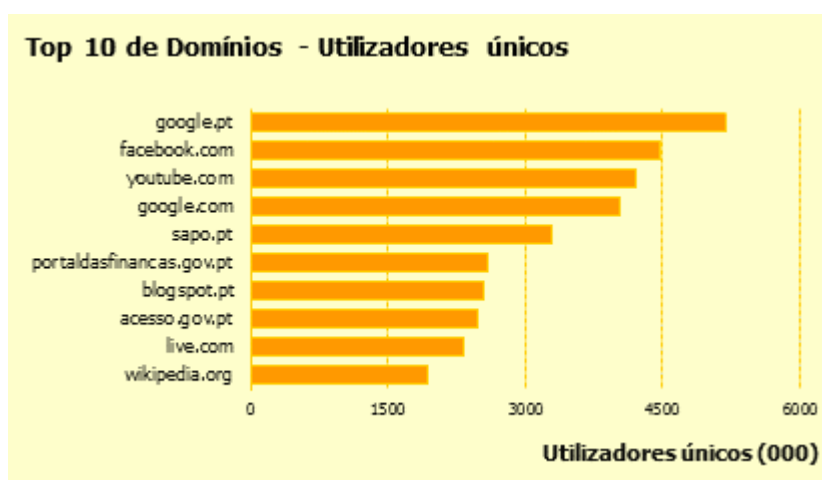
3.PARTILHA DE INFORMAÇÃO E AS REDES SOCIAIS

A utilização massiva das TI tem transformado a sociedade. Atualmente, a Internet é uma ferramenta que permite ao utilizador efetuar múltiplas tarefas. Não só é uma ferramenta de trabalho, mas também de diversão, indispensável a qualquer indivíduo.

Existem riscos associados à utilização da Internet, nomeadamente das redes sociais, dos quais é necessário ter conhecimento, estar alerta, agir em conformidade e, sobretudo, em segurança.

Segundo uma notícia do Público, publicada em Novembro de 2014, os Portugueses usam mais as redes sociais do que a média europeia.⁴ Cerca de “70% dos utilizadores de Internet em Portugal usavam no ano passado [2013] redes sociais, significativamente acima dos 57% que eram a média dos 28 Estados-membros”.

Em adição, conforme dados obtidos em 2016 e mostrados na Figura 1, é possível constatar que o motor de pesquisa do Google é a rede social eleita pelos utilizadores, estando em segundo lugar no Top 10 dos Domínios utilizados.



Fonte: Marktest, Netpanel meter

Figura 1 - Top 10 Domínios em milhares de utilizadores únicos de Abril de 2016

A navegação dos Portugueses na Internet é distribuída, essencialmente, em torno do Google, Facebook e YouTube. O Facebook, que é hoje a rede social com mais adesão.

⁴ Disponível em: <http://www.publico.pt/tecnologia/noticia/portugal-acima-da-media-da-ue-no-acesso-a-redes-sociais-online-1675356> Consultado a: 19/11/2015.

Em 2009 era notícia por ter ultrapassado o número de utilizadores do Hi5, que chegou a atingir os 3,2 milhões em Portugal.

O gigante da informação, a Google, oferece os seus serviços ao mais comum dos utilizadores quase sem custos directos. Esta é a percepção que cada um tem quando acede aos serviços como o Gmail, Google Maps, Google+, Hangouts, ou o Drive. Porém o acesso a estes serviços trás custos indirectos bastantes elevados para cada um: a informação pessoal que é disponibilizada quando viajamos, quem são os nossos amigos, que tipo de pesquisas fazemos, que informação guardamos na nuvem. Claro que todos nós podemos consultar o que disponibilizamos ao Google⁵ e visualizar a quantidade de informação de cada um de nós torna público, porém sem termos consciência do que estamos a fazer.

A questão que se coloca, e que se tem vindo a tornar cada vez mais imperativa é de que forma se pode proteger os utilizadores dos perigos associados à utilização das redes sociais, e dos restantes domínios da Internet, quando estes, que reivindicaram pela criação de leis de proteção de dados pessoais estão hoje a publicar de livre e espontânea vontade os seus próprios dados nos perfis das redes sociais.

Os dados publicados voluntariamente pelos utilizadores das redes sociais vão deixando um rasto e são passíveis de se criar uma identidade digital acessível a qualquer outro utilizador. Há uma inconsciência generalizada, e uma despreocupação global com este assunto.

Os utilizadores expõem-se demasiado, revelando informações privadas e dados pessoais verdadeiros, o que pode acarretar consequências como roubos de identidade, assédios por parte de desconhecidos, raptos e violações.

Não há um conhecimento dos riscos associados e muito menos uma noção, ainda que básica, do que implica navegar na Internet. Os riscos atuais são bastantes e se não se educar os utilizadores para a cibersegurança estes não serão minimizados.

É nesta sequência que se compreende a necessidade emergente da cibereducação, isto é, consciencializar e educar os cidadãos para a importância da cibersegurança. Saber utilizar um computador não finda com o saber manuseá-lo e utilizar Internet não é tão

⁵ <http://history.google.com>

simples como apenas aceder e navegar em *sites*. A gestão da informação, pessoal ou da organização, é um tema emergente que todas as entidades que manuseiam informação devem saber como fazer. Conhecer os mecanismos, políticas e procedimentos de segurança pode não ser suficiente. É necessário também ter conhecimento sobre como a tecnologia funciona.

4. CIBEREDUCAÇÃO EM PORTUGAL

A cibereducação, para muitos utilizadores de Tecnologias de Informação e Comunicação (TIC), é o conhecimento estritamente necessário para o desempenho das suas funções numa organização. A cibereducação é considerada como sendo a aprendizagem da utilização de ferramentas e aplicações. Porém, a cibereducação não é apenas saber utilizar ferramentas de escritório, ou navegar na Internet, é também saber como gerir o que de mais-valia todos temos, a informação.

A troca e partilha de dados em rede são feitas em diferentes níveis de um sistema de comunicações. De uma forma simplificada, podemos considerar quatro níveis de interação da informação: o nível geográfico, o nível tecnológico, o nível lógico e o nível interface do utilizador.

O nível geográfico representa a localização física dos sistemas de informação e comunicação, bem como onde, estão localizados os sistemas de armazenamento e processamento de dados. O funcionamento de cada um destes sistemas é regulamentado por leis cuja aplicabilidade é regional. O conhecimento legal é uma parte da cibereducação e é da responsabilidade de todos, principalmente de quem tem capacidade de decisão.

O nível tecnológico abrange os sistemas de comunicação, de processamento e armazenamento de dados. Este nível, maioritariamente, é considerado pelos utilizadores, como sendo da responsabilidade dos administradores de sistemas e dos técnicos de informática. O conhecimento tecnológico requerido para se actuar neste nível deve ser adequado às funções que cada um desempenha. Porém, todos os utilizadores de sistemas de informação usam tecnologia para aceder à Internet. O modo como os nossos dispositivos interagem com os sistemas de comunicação depende da tecnologia que está disponível em cada local. Compreender as diferenças de acesso à rede através de um acesso sem fios (Wifi aberto ou cifrado, ligação de dados), ou de um acesso por cabo, é essencial para se perceber que tipo de informação pode ser acedido com segurança.

O nível lógico está relacionado com os processos de formatação de dados, com os protocolos de comunicação entre sistemas, com os algoritmos usados no processamento da informação. Este nível pode ser bastante complexo para a maioria dos utilizadores dos sistemas de informação. No entanto, os protocolos usados nos processos de comunicação

podem ser do tipo binário ou de texto, pode ser cifrados ou abertos. Os protocolos binários são aqueles que, olhando para um cabeçalho, compreender o seu significado implica decodificar o que cada bit ou grupos de bits representam. Carecem de ferramentas próprias para o efeito. Os protocolos de texto são todos aqueles que enviam mensagens de controlo em texto que pode ser lido e interpretado por um humano. Conhecer como funcionam estes protocolos pode ser a diferença entre olharmos para um *mail* que tem um grafismo e um formato expectável, mas o seu conteúdo tem outro significado. Um protocolo com cifra significa que os dados dados que são trocados entre sistemas não são compreensíveis caso não se conheça a chave de cifra. Mas existem diversos tipos de cifra. O que significa em termos de segurança uma cifra de 128bits, ou uma cifra de 256bits? Qual o nível de segurança que é expectável quando se usa *Secure Hyper Text Transfer Protocol* (HTTPS)? Onde é que está a segurança do HTTPS? Com estas questões não se pretende que o utilizador conheça em detalhe o funcionamento dos protocolos, mas sim, saber as diferenças entre protocolos e que informação pode transferir com segurança entre sistemas.

O nível interface do utilizador abrange todos os atores que usam os sistemas de informação. Um utilizador deve conhecer as políticas de segurança que estão em vigor na sua organização, deve conhecer as fragilidades e vulnerabilidades da rede onde que está a aceder, deve saber quais as consequências que podem advir da partilha de informação, deve compreender quais as capacidade de segurança disponíveis na sua interface com a rede – dispositivo de comunicações fixo ou móvel. O utilizador executa múltiplas e complexas de troca de informação com outros níveis do ambiente de informação, onde, as suas ligações variam ao longo do tempo. Neste contexto, a segurança da informação está dependente do conhecimento que o utilizador tem do ambiente onde está inserido, e não apenas da segurança física do seu equipamento ou da segurança lógica das aplicações que usa.

O conhecimento necessário para se poder compreender as relações que existem entre estas quatro camadas deve ser publico, e disponibilizado pelos organismos públicos e privados que têm responsabilidade nesta matéria.

Em Portugal, têm-se observado uma crescente preocupação sobre a segurança da informação na Internet. Este facto pode ser verificado pelo número de seminários e conferências que tem sido realizados nos últimos anos. Entidades como a Associação para

as Comunicações, Eletrónica, Informações e Sistemas de Informação (AFCEA Portugal), o Centro Nacional de Cibersegurança (CNCS), o Centro de Investigação Jurídica do Ciberespaço (CIJIC), entre outras, têm contribuído para a divulgação de temas relacionados com a segurança da informação. Porém, esta capacidade de atuação deve ser considerada com um complemento e atualização de conhecimento adquirido.

A base para se efetuar uma partilha de informação com segurança deve ter origem em matérias lecionadas durante o percurso académico de qualquer utilizador, adaptadas aos diferentes níveis de ensino. No ensino básico e secundário temos os adolescentes e jovens, grandes consumidores de novas tecnologias, que devem conhecer as vulnerabilidades dos sistemas que eles usam e como se podem proteger. As ações de formação do nível utilizador e do nível lógico devem estar direcionadas para a realidade que eles têm dos sistemas de informação e para perceção que têm de segurança. Deve ser aplicado o conceito de política de utilização aceitável, ensinando quais os limites que podem ser alcançados garantindo a segurança da informação que partilham.

No ensino superior temos homens e mulheres que estão a adquirir conhecimentos para ingressar no grupo da população ativa. São formados com competências necessárias para entrarem no mercado de trabalho, de acordo com a vocação de cada um. Matérias como a Gestão da Informação, a Segurança da Informação e a Gestão da Segurança da Informação devem fazer parte de todos os cursos do ensino superior, independentemente de os cursos não terem uma vertente tecnológica ou de gestão. Em alguma fase da atividade profissional, qualquer utilizador vai ter que usar sistemas de informação e ser responsável pela gestão de conteúdos. A profundidade das matérias associadas aos quatro níveis de interação da informação deve estar adaptada a cada curso, ou seja, não se pretende que um advogado substitua um engenheiro, ou vice-versa, mas o engenheiro tem que ter conhecimento legal sobre a utilização dos sistemas de comunicação e da informação, e o advogado deve compreender os processos de armazenamento e processamento da informação em rede, p.ex.

5. CONCLUSÕES

Este trabalho teve como objectivo enquadrar os temas da cibersegurança e do ciberespaço, e apresentar uma plataforma que permita identificar necessidades que levem à implementação do conceito de cibereducação a todos os utilizadores da Internet.

A segurança da informação no ciberespaço não deve ser interpretada como, um conjunto de políticas e procedimentos que são da responsabilidade das pessoas e organismos que administram os sistemas de comunicações, processamento e armazenamento de dados. A segurança da informação é da responsabilidade de todos os utilizadores de sistemas de comunicação em rede. O mapa de conceitos apresentado identifica alguns temas que se enquadram na actividade de qualquer utilizador que aceda a serviços em rede.

Quando é realizada uma pesquisa na Internet, em *sites* de redes sociais, como o Facebook, Instagram, Youtube, entre outros, a quantidade de informação pessoal que os utilizadores destes serviços disponibilizam de forma aberta é uma consequência da falta de conhecimento do que estão a fazer, ou seja, é falta de cibereducação. Este facto pode ser observado na criança que utiliza o *smartphone* dos pais e descarrega qualquer tipo de aplicação, no adolescente ou jovem que quer ser popular entre os amigos e disponibiliza conteúdos pessoais, no adulto que quer mostrar que a sua vida não é monótona e que tem mais actividade social que os seus amigos.

Uma política de utilização aceitável para acesso a serviços em rede permite minimizar os riscos de segurança da informação. Deve ser do conhecimento de todos os utilizadores. Cada utilizador deve conhecer os procedimentos e mecanismos de segurança que estão associados à política de utilização aceitável e compreender as consequências que o desrespeito por estas regras podem trazer para cada um e para a organização.

A cibereducação é uma matéria que deve estar presente no percurso académico de qualquer pessoa, desde o ensino básico. A cibereducação deve ser continuada com acções de actualização durante a vida profissional de cada um.

6.BIBLIOGRAFIA

EFING, António Carlos e FREITAS, Cinthia Obladen de Almendra (2012), ***Direito e Questões Tecnológicas Aplicados no Desenvolvimento Social (Vol.2)***, 1ª ed., Curitiba, Juruá Editora.

Gobierno de España (2011), *Estrategia Española de Seguridad: Una responsabilidad de todos*, Madrid.

IDN (2013), *Estratégia da Informação e Segurança no Ciberespaço (caderno nº12)*, Instituto de Defesa nacional. Disponível em pdf em http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

LYON, David (1992), ***A Sociedade da Informação. Questões e Ilusões***, Oeiras, Celta Editora.

MARTINS, Marco (2012), “Ciberespaço: Uma nova realidade para a Segurança Nacional”, Cibersegurança. Caderno N.º133 IDN, Lisboa, pp.32-49.

PEREIRA, Júlio (2012), Cibersegurança – O Papel do Sistema de Informações da República Portuguesa, Lisboa, Diário de Bordo.

SANTOS, Lino (2011), *Contributos para uma melhor governança da cibersegurança em Portugal*, Lisboa, Tese de Mestrado, Faculdade de Direito da Universidade Nova de Lisboa. Disponível em http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF

SANTOS, Paulo e Bessa, Ricardo e Pimentel, Carlos (2008), ***Cyberwar – O Fenómeno, as Tecnologias e os Atores***.

WOLTON, Dominique (1999), ***E depois da Internet?*** Algés, Difel.



**CIBERESPAÇO, ENTIDADES ADMINISTRATIVAS
INDEPENDENTES E DIREITOS FUNDAMENTAIS**

**CYBERSPACE, ADMINISTRATIVE INDEPENDENT ENTITIES
AND FUNDAMENTAL RIGHTS**

MARIANA MELO EGÍDIO ¹

¹ Assistente Convidada da Faculdade de Direito da Universidade de Lisboa. Investigadora Associada do Centro de Investigação em Direito Público (CIDP). Doutoranda em Ciências Jurídico-Políticas na Faculdade de Direito da Universidade de Lisboa. Contacto: marianameloevidio@fd.ulisboa.pt. O presente texto corresponde à intervenção proferida no painel “Cibersegurança e liberdades de expressão”, no âmbito da conferência “Cibersegurança: perspectivas multidisciplinares”, ocorrida a 04 de Janeiro de 2016, na Faculdade de Direito da Universidade de Lisboa, com algumas alterações.

ABSTRACT

Independent administrative entities were firstly created with the purpose of regulating the exercise of certain fundamental rights, seeking also to protect these rights in sensitive areas.

It turns out, however, that the performance of these entities will itself in parallel affect the fundamental rights of those regulated by them, which can consequently lead to constitutional problems.

It should be noted that these entities can exercise not only regulatory but also sanctioning powers, as well as para-jurisdictional functions, which can lead to a concentration of powers likely to call into question the very principle of the separation of powers.

Considering that article 37 of the Portuguese Constitution comprises as well a right to freedom of expression in cyberspace, the conduct of administrative bodies that affect this right (*e.g.* through mechanisms of notice and take down) can be seen as a fundamental rights' restriction, which must follow the constitutional controls applied to such interventions.

Keywords: Independent administrative agencies; administrative encroachment on fundamental rights; freedom of speech; notice and takedown;; proportionality principle

RESUMO

As entidades administrativas independentes foram primeiramente criadas com o intuito de regular o exercício de determinados direitos fundamentais, procurando também salvaguardar o exercício destes direitos em sectores sensíveis e, conseqüentemente, proteger os direitos fundamentais dos cidadãos.

Sucede que, paralelamente a estes propósitos, a actuação destas entidades vai, ela própria, contender com os direitos fundamentais dos regulados e colocar, conseqüentemente, problemas de constitucionalidade. Lembre-se que estas entidades podem concentrar em si poderes regulatórios e sancionatórios, nos termos dos seus estatutos, exercendo também funções para-jurisdicionais, o que conduz a uma concentração de poderes – de natureza normativa, executiva e (para) jurisdicional – susceptível de por em causa o próprio princípio da separação de poderes.

Atendendo à interpretação do artigo 37.º da Constituição como compreendendo também um direito à liberdade de expressão no ciberespaço, a actuação de entidades administrativas que contenda com este direito (v.g. através de mecanismos de *notice and takedown*) pode configurar uma restrição de direitos fundamentais, que terá de ser enquadrada no âmbito dos controlos constitucionais a este tipo de intervenções.

Palavras-chave: Entidades administrativas independentes; intervenções administrativas; liberdade de expressão; *notice and take down*; princípio da proporcionalidade

I. INTRODUÇÃO

1. Apenas recentemente se iniciou o estudo da relação entre o *ciberespaço*, as *entidades administrativas independentes* e o exercício de *direitos fundamentais*, tema que ainda carece de maior aprofundamento, tendo em conta os múltiplos aspectos relevantes do mesmo no quadro de uma sociedade da informação⁽²⁾ e do risco⁽³⁾.

Na verdade, o estudo das relações entre Direito e ciberespaço⁽⁴⁾ pode ser feito de uma pluralidade de perspectivas, tendo em conta, também, a multiplicidade de problemas suscitados pela Internet: pensemos, por exemplo, na prática de ciberterrorismo ou de outros crimes informáticos; no uso de redes sociais para difamação e insultos e consequente responsabilização dos autores e/ou dos *hosts*; na responsabilidade adveniente da celebração de contratos através da Internet; nos problemas colocados pela perda do direito à privacidade adveniente da utilização das mesmas redes ou casos como o denominado *facejacking*⁽⁵⁾. Os problemas que se colocam são inúmeros e muitos deles começam, só agora, a ser resolvidos⁽⁶⁾, após o fim de algum cepticismo por parte da comunidade jurídica sobre a susceptibilidade de os mesmos poderem, sequer, ser discutidos⁽⁷⁾.

2 Ou talvez mais correctamente “sociedade informacional”, cfr. MANUEL CASTELLS, *The Internet galaxy: reflections on the Internet, business, and Society*, Oxford, Oxford University Press, 2001, já que em todas as sociedades ao longo da História, a informação teria desempenhado, à sua maneira, um papel relevante.

3 A expressão “sociedade do risco” deriva, como é sabido, da obra de ULRICH BECK, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Suhrkamp, Frankfurt, 1986.

4 Uma das primeiras aparições do termo foi na obra de ficção científica *Neuromancer* de WILLIAM GIBSON, na qual o mesmo vem definido nos seguintes termos “Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding”, WILLIAM GIBSON, *Neuromancer*, New York, Ace Books, 1984, p. 69.

5 Para o enunciado de algumas destas questões, cfr. ALEXANDRE SOUSA PINHEIRO, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, pp. 224-244.

6 O estudo da ligação entre o Direito e o ciberespaço já ocorre desde a década de noventa. Porém, muitas das questões que têm vindo a ser colocadas não encontraram, ainda, resposta. Falamos de questões como “o que tem o Direito a ver com o ciberespaço?”, “Existe um Direito do Ciberespaço? Nos mesmos termos em que se pode falar de outros ramos do Direito?”, “O ciberespaço é um sítio que tem um sistema jurídico como o de Portugal ou Espanha?”, “O ciberespaço pode ser regulado/é susceptível de regulação?”, “Quem pode e como pode regular o ciberespaço?”, questões essas recolhidas e adaptadas de LILIAN EDWARDS/CHARLOTTE WAELDE, “Introduction”, *Law & the Internet: regulating cyberspace* / LILIAN EDWARDS/CHARLOTTE WAELDE, Oxford, Hart Publishing, 1998, pp. 5-11, p. 5.

7 “Se as comunidades virtuais são o caminho do futuro, que regime legal as deve regular? Podem os advogados encontrar um caminho para conceber sistemas jurídicos virtuais, aplicáveis a ciber-nações que podem ou não corresponder aos estados-nação do mundo de hoje? Como pode o direito ser feito numa comunidade tal como a Internet, na qual falha completamente um soberano do tipo que Austin

Ora, de entre esta multiplicidade de perspectivas, aquela que nos interessará no presente texto corresponde à perspectiva *constitucional* do tema⁽⁸⁾, nomeadamente atendendo às vinculações que decorrem da Constituição para a intervenção de autoridades administrativas independentes na regulação do ciberespaço, nomeadamente ao efeito que têm nos direitos fundamentais dos destinatários da actividade de regulação exercida⁽⁹⁾.

2. Quanto ao conceito de *direitos fundamentais* (mais especificamente de direitos, liberdades e garantias) embora estejamos a pensar nos direitos contemplados no catálogo da Constituição portuguesa, atendendo ao surgimento de uma “revolução informática”, poder-se-á falar mesmo falar de uma “digitalização dos direitos fundamentais”⁽¹⁰⁾, que importa não só o surgimento de direitos novos ou de novas interpretações de direitos clássicos (como o surgimento de um direito à

havia proposto como essencial para a criação do Direito, ou mesmo a regra de reconhecimento adorada por H. L. A. Hart? O que substituiria os parlamentos e tribunais de tal comunidade? Poderiam os destinatários virtuais dessa comunidade incluir não só as pessoas singulares e colectivas com as quais os advogados estão familiarizados, mas também as identidades (*personae*) virtuais frequentemente adoptadas por utilizadores mais frequentes e *role-players* virtuais, que podem diferir em nome, sexo e raça da pessoa correspondente àquele indivíduo no mundo real?.

Estas são questões especulativas e exóticas, especialmente para advogados. Porém, há uma necessidade de começar a perguntar, senão a responder, a essas questões”, LILIAN EDWARDS/CHARLOTTE WAELDE, “Introduction”, *Law & the Internet: regulating cyberspace*, *op. cit.*, pp. 10-11.

8 O facto de a Internet ser uma realidade por natureza extra-territorial não significa um afastamento da aplicação das normas da Constituição quando as entidades actuem no espaço de aplicação da mesma, ainda que no ciberespaço. Cfr. PAUL SCHIFF BERMAN, “Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to ‘Private’ Regulation”, *University of Colorado Law Review*, Vol. 71, No. 4, May 2000, pp. 1263-1310, particularmente p. 1289 e ss.

9 Veja-se ALEXANDRE SOUSA PINHEIRO, *op. cit.*, p. 231, mencionando o acórdão *Reno v. ACLU* (1997) do *Supreme Court* norte-americano, no qual foi decidido que duas disposições do *Communications Decency Act* de 1996 violavam a Constituição norte-americana. Como sintetiza o autor, “ao fazê-lo admitiu, porém, que a Administração dispunha de competência para operar regulamentarmente no ciberespaço”. Numa perspectiva diferente, PEDRO GONÇALVES, “Regulação Administrativa da Internet”, *Revista de Direito Público da Economia*, Nº 1 (Janeiro-Março 2003), pp. 177-199, posteriormente republicado sobre o título “Disciplina administrativa da internet”, *Direito da sociedade da informação*, volume V, Coimbra, Coimbra Editora, 2004, pp. 215-236, salientando, p. 177, que «ao invés do que se verifica em muitas esferas sujeitas a regulação, no mundo da internet não é simples a tarefa de identificar com rigor as áreas de intervenção, regulação administrativa pública (...) a dificuldade está, aí sim, em perceber a existência e os contornos de uma “regulação administrativa pública da internet”. Como expõe o autor, p. 178, «existe uma regulação administrativa pública da internet, impondo-se o direito administrativo como disciplina reguladora de certos aspectos da actuação de “actores privados” que actuam por “delegação” de autoridades públicas.» Cfr. ainda o estudo «Regulação pública de conteúdos na internet em Portugal : contributo para a compreensão da designada “solução provisória de litígios” pela Administração Pública no âmbito do Decreto-Lei nº 7/2004, de 7 de Janeiro», *Direito da sociedade da informação*, volume VII, Coimbra, Coimbra Editora, 2008, pp. 107-128.

10 GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7.ª edição, Coimbra, Almedina, 2003, pp. 514-515.

autodeterminação informativa), mas também uma necessidade de ler a Constituição atendendo à nova realidade do ciberespaço⁽¹¹⁾.

O Tribunal Constitucional já se pronunciou em alguns acórdãos, aliás, sobre temáticas ligadas ao ciberespaço. Assim, no acórdão n.º 640/2013, de 2 de outubro de 2013, Processo n.º 998/13⁽¹²⁾ - embora tenha decidido pela inutilidade superveniente do recurso interposto- estava em causa uma deliberação da Comissão Nacional de Eleições, a qual, invocando o artigo 7.º da Lei n.º 71/78, de 25 de dezembro (Lei da CNE), ordenou a remoção imediata de um comunicado eleitoral do *sítio oficial* da Câmara Municipal do Porto na Internet. O acto impugnado foi praticado no exercício dos poderes da CNE enquanto órgão de administração eleitoral, previstos nos artigos 5.º, n.º 1, al. d) e 7.º da Lei n.º 71/78, de 27 de dezembro, procurando impedir a prática de actos por entidades públicas que favoreçam ou prejudiquem uma candidatura em detrimento ou vantagem de outra. Saliente-se, pois, a restrição aqui operada por uma entidade administrativa em direitos fundamentais das entidades sujeitas à supervisão dessa mesma entidade, tendo o direito em causa sido exercido, precisamente, no ciberespaço.

Veja-se também o acórdão n.º 241/2002,⁽¹³⁾ Processo n.º 444/01, de 29 de maio de 2002, no qual o Tribunal “em ordem a apreciar o objecto do presente recurso”, decidiu “fazer um comentário, necessariamente breve, sobre as tecnologias da informação (telecomunicações) em geral e, em particular, sobre a Internet”. Nesse acórdão analisou o surgimento da Internet e seu desenvolvimento, bem como a evolução do direito das telecomunicações em Portugal. O acórdão em causa incidia

11 Cfr. LUÍSA NETO, “Informação e liberdade de expressão na Internet e a violação de direitos fundamentais: um conflito de (im)possível resolução”, *Informação e liberdade de expressão na Internet e a violação de direitos fundamentais: comentários em meios de comunicação online*, Gabinete Cibercrime da Procuradoria-Geral da República (coord.), Lisboa, Imprensa Nacional-Casa da Moeda, 2014, pp. 29-48, pp. 31-32, “Assim, se a protecção da individualidade da pessoa em contexto cibernético deve ser a continuidade da protecção garantida pelo Estado na realidade *offline*, a imaterialidade convoca todavia desafios acrescidos. Trata-se pois de saber se é ainda possível a utilização dos “odres velhos” para conter e disciplinar o “vinho novo” da Internet, em especial quanto à susceptibilidade de aplicação da dogmática comum da responsabilidade civil e penal e da protecção dos direitos fundamentais à realidade fáctica da Internet. (...) Fundamentalmente, a discussão da responsabilização pela expressão e informação digital *online* – *rectius*, pela respetiva possível ilícita violação- encontra escolhos na imensidão da informação disponível, não filtrada, constantemente actualizada e virtualmente impossível de apagar”.

12 Consultado em <http://www.tribunalconstitucional.pt/tc/acordaos/20130640.html>

13 Consultado em <http://www.tribunalconstitucional.pt/tc/acordaos/20020241.html>

sobre a questão da confidencialidade e sigilo das comunicações electrónicas, conferindo-lhes tutela constitucional, por aplicação do artigo 34.º da Constituição⁽¹⁴⁾.

Tendo em conta o âmbito do painel onde proferi a intervenção agora reduzida a escrito (*Cibersegurança e liberdades de expressão*), a análise centrar-se-á numa breve síntese do impacto que a intervenção por parte de algumas entidades administrativas independentes tem nos direitos fundamentais dos regulados, particularmente nos direitos de liberdade de expressão e de informação, constitucionalmente protegidos no artigo 37.º da Constituição⁽¹⁵⁾.

3. Se pensarmos no caso do bloqueio do *WhatsApp* no Brasil ou, no contexto português, do memorando celebrado entre a IGAC (Inspeção Geral das Actividades Culturais e o MAPiNET (Movimento Cívico Anti-Pirataria na Net), entre outras entidades, ou o bloqueio de *sites* de jogos *online* efectuado pelo Turismo de Portugal, I.P., a que voltaremos no texto, facilmente se compreende a pertinência e actualidade do tema⁽¹⁶⁾.

14 Acabando por “julgar inconstitucional a norma ínsita no artigo 519.º, n.º 3, alínea b), do Código de Processo Civil quando interpretada no sentido de que, em processo laboral, podem ser pedidas, por despacho judicial, aos operadores de telecomunicações informações relativas aos dados de tráfego e à facturação detalhada de linha telefónica instalada na morada de uma parte, sem que enerve de nulidade a prova obtida com a utilização dos documentos que veiculam aquelas informações, por infracção ao disposto nos artigos 26.º n.º 1 e 34.º n.os 1 e 4 da Constituição”.

15 Cfr. ANA PROENÇA COELHO, “Entre o dever de colaborar e o direito de não se autoinculpar: O caso da supervisão do ICP-ANACOM”, *Revista Concorrência & Regulação*, n.º 11 e 12, Julho/Dezembro 2002, pp. 429-466, p. 436, “a referida prerrogativa [solicitar informações e documentos] das autoridades reguladoras é do prévio conhecimento de todos os regulados e a sua vigência deverá ser interpretada como uma verdadeira condição para o exercício de determinada actividade regulada por parte de um privado, tendo em conta o interesse geral no regular e eficiente funcionamento dos mercados, tal como previsto no artigo 61.º, n.º 1, da Constituição da República Portuguesa (CRP). Com efeito, muitas das actividades sujeitas a regulação revestem carácter reservado, na medida em que, devido à sua relevância, complexidade e exigência, o respectivo exercício depende de autorização prévia – autorização essa geralmente concedida pela própria entidade reguladora sectorial -, circunstância de onde se pode retirar que as pessoas (singulares e colectivas) sujeitas à regulação conhecem, à partida, as regras a que estão sujeitas, nomeadamente no que concerne ao dever de colaborar com a respectiva autoridade reguladora”. A restrição da análise, tendo em conta o âmbito do painel, apenas ao direito à liberdade de expressão, implica que não se considerem outras situações que configuram também intervenções de entidades administrativas em direitos fundamentais, como a que ocorre por parte da CNPD, nos termos do artigo 22.º, n.º 3, alínea b) da lei n.º 67/98, de 26 de Outubro (Lei da protecção de dados pessoais) : A CNPD dispõe “De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português”.

16 Ainda que não esteja sempre aí em causa, é certo, apenas a intervenção de entidades administrativas.

II. ENTIDADES ADMINISTRATIVAS INDEPENDENTES: APROXIMAÇÃO A UM CONCEITO

4. Como é sabido, a revisão constitucional de 1997 consagrou, no artigo 267.º, n.º 3, a possibilidade de a lei criar entidades administrativas independentes, no contexto de um Estado regulador⁽¹⁷⁾. A administração independente⁽¹⁸⁾ corresponde ao exercício da função administrativa prosseguida por entidades não integradas na administração directa do Estado, com ausência de orientação⁽¹⁹⁾ e de tutela estrutural, mas sem poderem ser assimiladas a um caso de administração autónoma⁽²⁰⁾.

As entidades administrativas independentes foram primeiramente criadas para intervir em áreas como a dos direitos fundamentais e direitos de natureza análoga⁽²¹⁾. Mas mais recentemente, sobretudo após os fenómenos de liberalizações e privatizações, passaram a ser também intervenientes nos domínios da economia e das finanças⁽²²⁾.

17 Entre outros, GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, op. cit., p. 352 e PEDRO GONÇALVES, “Direito Administrativo da Regulação”, *Estudos em Homenagem ao Professor Doutor Marcello Caetano (no Centenário do seu Nascimento)*, volume II, Coimbra, Coimbra Editora, 2006, pp. 535-573.

18 GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, op. cit., p. 567.

19 A administração independente é caracterizada por VITAL MOREIRA, *Administração Autónoma e Associações Públicas*, Coimbra, Coimbra Editora, 1997, p. 127 como “a Administração *infra-estadual* prosseguida por instâncias administrativas não integradas na Administração directa do Estado e livres da orientação e da tutela estadual, sem todavia corresponderem à auto-determinação de quaisquer interesses organizados”.

20 Cfr. DIOGO FREITAS DO AMARAL, *Curso de Direito Administrativo*, com a colaboração de LUÍS FÁBRICA, JORGE PEREIRA DA SILVA e TIAGO MACIEIRINHA, volume I, 4.ª edição, Coimbra, Almedina, 2015, p. 245 e ss, especificamente p. 269 e ss, que a propósito dos serviços independentes e de vocação geral, aborda o surgimento da administração independente, que escapa à tripartição clássica entre administração directa, indirecta e autónoma, Ao lado dos *órgãos administrativos independentes*, coloca as *entidades administrativas independentes com funções de regulação*, cfr. p. 276 e ss, agregando-as sob o nome “entidades administrativas independentes”. Na definição de MARIA CELESTE CARDONA, *Contributo para o Conceito e Natureza das Entidades Administrativas Independentes*, dissertação de doutoramento policopiada apresentada à Faculdade de Direito da Universidade de Lisboa, 2014, p. 24, “as entidades administrativas independentes que se inserem na Administração Pública na modalidade de administração independente são pessoas colectivas de direito público dotadas de personalidade jurídica pública, encarregadas por lei de prosseguir o interesse público concreto nelas estabelecido, devem a sua institucionalização ao princípio do pluralismo da organização administrativa e exercem as suas actividades/competências ao abrigo e com observância estrita do princípio da unidade de acção da administração pública”.

21 Sobre o papel de defesa dos direitos fundamentais visado por estas entidades, cfr. DIOGO FREITAS DO AMARAL, *Curso de Direito Administrativo*, op. cit., pp. 270-271. Mas, como assinala o autor, na p. 277, mesmo as entidades que não visam em primeira linha a protecção dos direitos fundamentais podem, na sua actividade, contender com estes.

22 Cfr. MARIA CELESTE CARDONA, op. cit., p. 36 e p. 967 “As entidades administrativas independentes operam em duas áreas: a) A área da garantia, promoção e protecção de direitos fundamentais e; b) A área que integra a actividade económica e financeira”, não podendo, pois, agrupar-se todas debaixo do mesmo estatuto.

Distinguindo entre i) entidades que operam no domínio dos direitos fundamentais e dos direitos eleitorais e ii) entidades que operam nos sectores da economia, comunicações, energia e concorrência e ainda entre

Sob esta designação, poderão agrupar-se, assim, entidades com origens distintas. Seguindo uma recente classificação^(23), poder-se-á distinguir entre *autoridades públicas independentes* e *entidades administrativas independentes*, atendendo ao seu modo de criação:

- a) Entidades criadas com fundamento directo em preceito constitucional;
- b) Entidades criadas ao abrigo e com fundamento directo em estatuto constitucional;
- c) Entidades criadas para o exercício de missões de promoção e de garantia de direitos fundamentais e de natureza análoga previstos na Constituição;
- d) Entidades criadas ao abrigo do disposto no n.º 3 do artigo 267.º da Constituição, para a prossecução de atribuições/incumbências do Estado previstas na Constituição.

Neste entendimento, todas as entidades criadas com fundamento em preceito expresso ou com estatuto constitucional, como é o caso, entre outros, da Entidade Reguladora para a Comunicação Social (ERC) e do Banco de Portugal, devem ser qualificadas como *Autoridades Públicas Independentes*, e, nessa medida, equiparadas aos demais órgãos de soberania previstos na Constituição”⁽²⁴⁾.

São, em suma, entidades que se caracterizam por uma independência *orgânica, funcional e social* ⁽²⁵⁾, e com especial interesse, caracterizadas pela ausência de ordens, instruções ou directivas, controlo de mérito e obrigação de prestação de contas face ao

i) entidades criadas com fundamento em preceito expresso da Constituição (ERC, Provedor de Justiça, CSM e CSMP, Banco de Portugal), ii) entidades criadas por lei com fundamento no seu estatuto constitucional, iii) entidades criadas para exercer missões de garantia de direitos fundamentais (CNE, CADA, Comissão Nacional Objectivação de Consciência, CNECV, CNPD, Entidade Reguladora da Saúde), iv) entidades com consagração constitucional criadas para a garantia/prossecução de incumbências/atribuições do Estado consagradas na Constituição, cfr. MARIA CELESTE CARDONA, *op. cit.*, pp. 951-952, nomeadamente p. 983, “Torna-se, assim, possível proceder à distinção entre estas entidades administrativas com funções de regulação e as entidades administrativas independentes que operam na área dos direitos fundamentais que, com fundamento nos seus estatutos de independência orgânica e funcional, não são parte da Administração Pública e não estão, por isso, subordinadas ao princípio da unidade de acção”.

23 Cfr. MARIA CELESTE CARDONA, *op. cit.*, pp. 43-44.

24 Cfr. MARIA CELESTE CARDONA, *op. cit.*, pp. 45-46. «Para além da ERC e do Banco de Portugal, também o Provedor de Justiça, os Conselhos Superiores da Magistratura e do Ministério Público devem ter-se como entidades “fora” da Administração Pública dotadas de regime e estatutos de natureza constitucional respectivamente nos domínios dos direitos fundamentais e do direito comunitário, devendo assim ser qualificadas como Entidades Públicas Independentes de estatuto constitucional».

25 GOMES CANOTILHO, *op. cit.*, p. 576.

Governo⁽²⁶⁾. São pois *entidades administrativas*, por um lado, e *independentes*, por outro, tendo a doutrina vindo a identificar critérios mais ou menos consensuais para a classificação das mesmas, nomeadamente:

- i) o desenvolvimento de actividades públicas predominantemente administrativas;
- ii) a ausência de poderes de hierarquia, superintendência ou tutela dos órgãos do poder político sobre a autoridade independente, embora a ausência de tutela deva ser entendida mitigadamente;
- iii) a existência de garantias de inamovibilidade e irresponsabilidade para os membros dos órgãos de direcção e a insusceptibilidade de dissolução dos órgãos de direcção por autoridades do poder político;
- iv) designação dos titulares dos órgãos de direcção através de um largo assentimento representativo ou, em alternativa, mediante a intervenção de órgãos distintos;
- v) se a autoridade exerce competências administrativas de regulação ou disciplina sobre um determinado sector, a maioria legal dos seus membros não deve pertencer ou ser designada pelo sector que é objecto da regulação⁽²⁷⁾, concluindo pela sua qualificação como entidades híbridas, “semi-independentes”⁽²⁸⁾.

5. A entrada em vigor, em 2013, da Lei n.º 67/2013, de 28 de agosto, (Lei-Quadro das Entidades Administrativas Independentes com Funções de Regulação da Actividade

26 *Ibidem*.

27 CARLOS BLANCO DE MORAIS, “O estatuto híbrido das entidades reguladoras da economia”, *Estudos em Homenagem ao Prof. Doutor Jorge Miranda*, volume IV, Coimbra Editora, 2012, pp. 183-217, pp. 202-203.

28 *Idem*, p. 208, “Autoridades administrativas independentes são órgãos do Estado ou pessoas colectivas públicas de carácter institucional que a lei incumbe da prossecução de fins do Estado, para o que lhes confia o exercício da função administrativa, com outorga de competências de administração activa, mas cujos dirigentes beneficiam de um regime de independência orgânica e funcional, perante órgãos de soberania”. Cfr. JOSÉ LUCAS CARDOSO, “Autoridade Administrativa Independente”, *Enciclopédia da Constituição Portuguesa*, coordenação de JORGE BACELAR GOUVEIA/FRANCISCO PEREIRA COUTINHO, Lisboa, Quid Juris, 2013, pp. 52-54, p. 52, identificando como características a independência das mesmas face aos órgãos de soberania, o exercício de funções administrativas e a natureza de administração activa (p. 53).

Económica dos Sectores Privado, Público e Cooperativo⁽²⁹⁾) poderia trazer alguma clareza quanto à identificação das características do também já denominado “quarto poder”. Sucedo que, como decorre do artigo 3.º, n.º 3:

«Para efeitos do disposto no n.º 1, são reconhecidas como entidades reguladoras as seguintes entidades actualmente existentes:

a) Instituto de Seguros de Portugal;

b) Comissão do Mercado de Valores Mobiliários;

c) Autoridade da Concorrência;

d) Entidade Reguladora dos Serviços Energéticos;

e) Autoridade Nacional de Comunicações (ICP - ANACOM) que será objeto de red denominação nos termos do artigo seguinte;

f) Instituto Nacional de Aviação Civil, I. P. (INAC, I. P.), que será objeto de red denominação nos termos do artigo seguinte;

g) Instituto da Mobilidade e dos Transportes, I. P. (IMT, I. P.), nas suas atribuições em matéria de regulação, de promoção e defesa da concorrência no âmbito dos transportes terrestres, fluviais e marítimos, que será objeto de reestruturação nos termos do artigo seguinte;

h) Entidade Reguladora dos Serviços de Águas e Resíduos;

i) Entidade Reguladora da Saúde.

4 - A lei-quadro em anexo à presente lei não se aplica ao Banco de Portugal e à Entidade Reguladora para a Comunicação Social, que se regem por legislação própria», exclusão reiterada no artigo 2.º, n.º 3, da Lei-Quadro⁽³⁰⁾.

29 Para uma síntese da génese da Lei-Quadro, entre outros, TÂNIA CARDOSO SIMÕES, “Entidades reguladoras: Um ano de Lei-Quadro”, *Concorrência & Regulação*, Ano V, Número 17, Janeiro/Março 2014, pp. 239-269. Na senda da evolução que culminou na referida lei. Cfr., ainda, VITAL MOREIRA/FERNANDA MAÇÃS, *Autoridades Reguladoras Independentes, Estudo e Projecto de Lei-Quadro*, Coimbra, Coimbra Editora, 2003.

30 Sublinhados nossos.

Note-se, portanto, que o mencionado diploma não visa cobrir toda a realidade das denominadas entidades administrativas independentes, centrando-se apenas nas entidades com funções de regulação da actividade económica (como decorre, aliás, do seu título). Contudo, ainda que tendo em conta a referida restrição do seu âmbito de aplicação e, consequentemente, a sua inaplicabilidade à primeira categoria de entidades administrativas atrás traçada, convém atender à definição constante do artigo 3.º da Lei-Quadro, o qual vem definir no n.º 1 as entidades reguladoras como “as pessoas colectivas de direito público, com a natureza de entidades administrativas independentes, com atribuições em matéria de regulação da actividade económica, de defesa dos serviços de interesse geral, de protecção dos direitos e interesses dos consumidores e de promoção e defesa da concorrência dos sectores privado, público, cooperativo e social”, dispondo no n.º 2 que, «*“Por forma a prosseguirem as suas atribuições com independência, as entidades reguladoras devem observar os requisitos seguintes:*

- a) Dispor de autonomia administrativa e financeira;*
- b) Dispor de autonomia de gestão;*
- c) Possuir independência orgânica, funcional e técnica;*
- d) Possuir órgãos, serviços, pessoal e património próprio;*
- e) Ter poderes de regulação, de regulamentação, de supervisão, de fiscalização e de sanção de infrações;*
- f) Garantir a protecção dos direitos e interesses dos consumidores”».*

6. Muitas das referidas entidades – e particularmente as que interessam para o presente texto, ainda que não abrangidas pela Lei-Quadro – foram criadas com o intuito de

regular o exercício de direitos fundamentais⁽³¹⁾ (pense-se na ERC⁽³²⁾ ou na CNPD), procurando salvaguardar o exercício destes direitos⁽³³⁾ em sectores sensíveis, num ambiente de liberdade e concorrência, mas também proteger os direitos fundamentais dos cidadãos, nas manifestações de boa administração, informação e transparência⁽³⁴⁾. Na medida em que as entidades em causa operem no domínio dos direitos fundamentais podem ser qualificadas como “entidades independentes com grau de liberdade de acção forte”⁽³⁵⁾, porquanto sobre estas não pode ser exercido qualquer poder de orientação ou controlo de mérito.

Contudo - e no que especialmente nos interessa - a sua actuação destas entidades poderá, ela própria, contender com direitos fundamentais dos regulados e colocar, consequentemente, problemas de constitucionalidade⁽³⁶⁾. Lembre-se que estas entidades podem concentrar em si poderes regulatórios e sancionatórios, nos termos dos seus estatutos, exercendo funções quase para-jurisdicionais⁽³⁷⁾, levando a uma

31 *Ibidem*. Cfr. JOSÉ LUCAS CARDOSO, *op. cit.*, p. 53, referindo que adoptam a natureza de órgãos da pessoa colectiva Estado a generalidade das autoridades incumbidas da protecção dos direitos fundamentais, apresentando a ERC como um caso distinto, de pessoa colectiva de tipo institucional. Cfr. também MARIA CELESTE CARDONA, *op. cit.*, p. 46-47. “Em resultado dessa análise, consideramos que a nossa ordem jurídica comporta entidades administrativas independentes com vocação de protecção de direitos fundamentais que, por isso, assumem *graus de independência* na sua acção, mais *intensos e menos limitados* do que as restantes entidades administrativas independentes que operam e detêm competências de promoção do mercado. Nesse sentido consideramos a Comissão Nacional de Eleições, a Comissão de Acesso aos Documentos Administrativos, a Comissão Nacional de Protecção de Dados, como Entidades Administrativas Independentes”.

32 Sobre a ERC e o seus poderes, cfr. MARIA CELESTE CARDONA, *op. cit.*, pp. 630-637.

33 Sobre a caracterização das entidades administrativas independentes como forma de efectivação dos direitos fundamentais dos cidadãos, tornando-se a Administração “guardiã da juridicidade”, cfr. PAULO OTERO, *O Poder de Substituição em Direito Administrativo- Enquadramento dogmático-constitucional*, volume II, Lisboa, Lex, 1995, p. 575 e ss. Note-se, novamente, contudo, que nem todas as entidades administrativas independentes visam estritamente salvaguardar direitos fundamentais, havendo outras que se ocupam, primeiramente, da regulação da economia (neste sentido, em síntese, JOSÉ LUCAS CARDOSO, *Autoridades Administrativas Independentes e Constituição*, Coimbra, Coimbra Editora, 2002, p. 540).

34 Cfr. GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, volume II, 4.ª edição revista, Coimbra, Coimbra Editora, 2010, p. 810, anotação ao artigo 267.º, de forma mais rápida, eficiente e flexível do que com recurso a outras figuras; Cfr. ainda MARIA CELESTE CARDONA, *op. cit.*, p. 958.

35 Cfr. MARIA CELESTE CARDONA, *op. cit.*, p. 951. Sobre as competências respeitantes ao exercício da administração activa por parte destas entidades, cfr. BLANCO DE MORAIS, *op. cit.*, p. 210.

36 No sentido de que «as decisões tomadas por estas “autoridades” têm força para proceder à restrição do exercício de um direito fundamental constitucionalmente consagrado» (falando a propósito do que designa como “entidades criadas com fundamento em princípios constitucionais de garantia e protecção de direitos fundamentais de natureza análoga”), MARIA CELESTE CARDONA, *op. cit.*, p. 962. «O intérprete não se pode alhear da fonte normativa que o legislador no exercício da sua função soberana escolhe para proceder à criação de uma entidade que, por força das competências que lhe são cometidas, dispõe do poder de “restringir” direitos, liberdades e garantias», *op. cit.*, p. 962.

37 Entre outros, ANA PROENÇA COELHO, *op. cit.*, p. 434, “a fim de poderem desenvolver a sua actividade e realizar o seu fim último- exercer a regulação sectorial-, estas entidades foram genericamente dotadas de três tipos de poderes públicos: de ordem normativa, de cariz executivo e de natureza sancionatória

concentração de poderes (de natureza normativa, executiva e para jurisdicional), susceptível de por em causa o próprio princípio da separação de poderes⁽³⁸⁾ - ainda que essa concentração de poderes seja intencional e a forma mais adequada para cumprir o fim das mencionadas entidades⁽³⁹⁾.

Tal implica que a actuação destas entidades não pode, obviamente, estar imune a controlo jurisdicional⁽⁴⁰⁾, fazendo surgir um novo domínio de estudo – o Direito Sancionatório das Entidades Reguladoras, na fronteira entre o Direito Penal e o Direito Administrativo⁽⁴¹⁾.

(parajudicial). Sucintamente pode afirmar-se que os poderes de ordem normativa consistem na competência das entidades reguladoras para elaborarem regulamentos com carácter geral e abstracto aplicáveis ao respectivo sector de actividade ou às matérias reguladas. Já os poderes executivos exprimem-se nas acções de supervisão desenvolvidas pelas autoridades reguladoras autónomas, no âmbito das quais estas entidades investigam e inspecionam o comportamento e a actividade dos seus regulados, *podendo mesmo emitir ordens destinadas a impor-lhes determinados comportamentos*. Por fim, os poderes parajudiciais relacionam-se com as competências sancionatórias no âmbito das contraordenações previstas em cada um dos sectores e matérias regulados, concedendo-se às autoridades reguladoras a missão de verificarem, em concreto, se os agentes económicos cumprem as normas legais e regulamentares em vigor e, consequentemente, de aplicarem coimas e/ou sanções acessórias aos seus autores” ainda que conclua, p. 435, que “o poder sancionatório das autoridades reguladoras não pode ser equiparado ao poder judicial, enquanto poder autónomo e independente, mas antes entendido como uma vertente da supervisão que se consubstancia na garantia da sua própria eficácia”.

38 Salientando que as grandes questões em torno da constitucionalidade da criação de entidades administrativas independentes giram em torno do princípio democrático, do princípio da separação de poderes, JOSÉ LUCAS CARDOSO, *Autoridades Administrativas Independentes e Constituição*, *op. cit.*, pp. 194-196, nomeadamente p. 195 «Acerca dos princípios mencionados, coloca-se a questão da criação de estruturas organizatórias cujos titulares não são legitimados pelo voto dos cidadãos e que simultaneamente beneficiam de um regime de tendencial imunidade aos clássicos mecanismos de controlo político. No que concerne ao segundo daqueles princípios, a doutrina alerta para a verosímil alteração do equilíbrio institucional estabelecido pela Constituição, por um lado, na medida em que a criação de “autoridades administrativas independentes” implica por regra que algumas competências de que eram titulares os órgãos de soberania, ou órgãos deles dependentes, sejam afectadas a novos centros de poder e, por outro lado, porque a concentração de competências subsumíveis a diferentes funções de Estado na mesma instituição pode originar uma situação de exercício do poder sem o controlo do correlativo e necessário contra-poder».

Especificamente quanto aos poderes sancionatórios da ERC, MIGUEL PRATA ROQUE, “Os poderes sancionatórios da ERC- Entidade Reguladora para a Comunicação Social”, MARIA FERNANDA PALMA/AUGUSTO SILVA DIAS/PAULO DE SOUSA MENDES (coord.), *Direito Sancionatório das Autoridades Reguladoras*, Coimbra, Coimbra Editora, 2009, pp. 367-442.

39 Cfr. ANA PROENÇA COELHO, *op. cit.*, p. 438.

40 Cfr. GOMES CANOTILHO, *op. cit.*, p. 568, “A intervenção destas entidades administrativas independentes não posterga o direito de recurso para os tribunais, nos termos gerais, pois só assim se não descaracteriza o esquema jurisdicional de controlo constitucionalmente plasmado”. Cfr. ainda ANA PROENÇA COELHO, *op. cit.*, p. 438, “as autoridades reguladoras exercem os poderes que lhes foram confiados de acordo com o princípio da legalidade, sendo independentes na sua actuação (...) e que os actos que praticam são sujeitos ao escrutínio judicial (seja dos tribunais comuns- em matéria sancionatória- , seja dos tribunais administrativos – no caso de impugnação dos actos que revistam esta natureza”.

41 Sobre o tema, MIGUEL PRATA ROQUE, “O Direito Sancionatório Público enquanto bissectriz (imperfeita) entre o direito penal e o direito administrativo – a pretexto de alguma jurisprudência constitucional”, *Revista Concorrência & Regulação*, ano IV, n.º 14/15, Abril/Setembro de 2013, pp. 105-

7. Sem poder entrar, no âmbito deste texto, nesse domínio, importa salientar que ao lado das sanções de tipo financeiro, disciplinar e contra-ordenacional existem as chamadas “sanções administrativas *stricto sensu*”⁽⁴²⁾, «quando ocorre uma restrição de um “*direito subjectivo*” ou a imposição de um “*ónus*” ou “*encargo*” a um particular, por decisão unilateral da administração pública, com intuito sancionatório – ou seja, predominantemente destinada à imposição de um sacrifício, como consequência de um incumprimento do conteúdo preceptivo de um comando normativo”⁽⁴³⁾.

Em nota de rodapé refere Miguel Prata Roque⁽⁴⁴⁾, «a mero título exemplificativo, refira-se – pela sua impressividade – o regime sancionatório previsto na Lei do Jogo (aprovada pelo Decreto-Lei n.º 422/89, de 2 de dezembro, de acordo com a redacção que lhe foi conferida pelo Decreto-Lei n.º 114/2011, de 30 de novembro), que, logo no seu artigo 118.º, n.º 1, distingue e autonomiza expressamente a “*responsabilidade administrativa*” (prevista nos artigos 119.º a 137.º daquele diploma), que se aplica apenas às pessoas colectivas privadas que exercem funções de concessionários do jogo, e a “*responsabilidade contra-ordenacional*” (prevista nos artigos 138.º a 150.º), que se aplica aos funcionários e frequentadores daqueles estabelecimentos concessionados de jogo. Entre essas “*sanções administrativas*”, podem destacar-se: i) a rescisão ou suspensão da execução dos contratos de concessão (artigos 119.º e 120.º); ii) a imposição de sanções pecuniárias pelo incumprimento de normas prescritivas de condutas (artigos 121.º a 130.º). Trata-se, por conseguinte, de verdadeiras “*sanções administrativas ‘stricto sensu’*”, manifesta e expressamente autonomizadas das “*sanções contra-ordenacionais*” que, portanto devem estrita obediência às normas procedimentais e aos princípios gerais de Direito Administrativo.” Voltaremos no texto às sanções aplicáveis no âmbito do jogo (*online*), tendo em conta um caso recentemente verificado em Portugal de bloqueio de um destes sites.

173 e ainda MARIA FERNANDA PALMA/AUGUSTO SILVA DIAS/PAULO DE SOUSA MENDES (co1ord.), *Direito Sancionatório das Autoridades Reguladoras*, Coimbra, Coimbra Editora, 2009.

42 MIGUEL PRATA ROQUE, “O Direito Sancionatório Público (...)”, *op. cit.*, p. 117. Cfr. MARIA CELESTE CARDONA, *op. cit.*, p. 809, identificando, no espectro das actuações integradas na função administrativa, as “actividades de comando e de controlo, com cariz policial e ordenador (administração de ordenação e sancionatória)”.

43 Não curando já do exercício de poderes regulamentares e jurisdicionais por parte destas entidades.

44 MIGUEL PRATA ROQUE, *op. cit.*, p. 117, nota de rodapé 55.

Tirando eventualmente o artigo 34.º, n.º 2⁽⁴⁵⁾, são os artigos 40.º a 44.º da Lei-Quadro que parecem referir-se a procedimentos de intervenção administrativa em direitos fundamentais, que se reconduzem a fixação de tarifas e sanção de infracções e adopção das medidas necessárias (cfr. nomeadamente alíneas c) e d) do n.º 3 do artigo 40.º).

45 “As entidades reguladoras podem ainda cobrar, nos termos dos respectivos estatutos, taxas ou tarifas às empresas e outras entidades destinatárias da actividade da entidade reguladora e dos serviços prestados por esta, com excepção das situações a que se refere o n.º 4 do artigo 40.º”.

III. INTERVENÇÃO ADMINISTRATIVA NO EXERCÍCIO DA LIBERDADE DE EXPRESSÃO NO CIBERESPAÇO

8. Como já foi assinalado, o artigo 37.º da Constituição deve ser lido da forma mais ampla possível, implicando aí também o exercício da liberdade de expressão através da Internet, no ciberespaço⁽⁴⁶⁾. Este aspecto (a inclusão no âmbito de protecção da liberdade de expressão também do exercício da mesma no ciberespaço), não é, contudo, praticamente focado pela doutrina portuguesa, salvo honrosas excepções⁽⁴⁷⁾.

Pelo contrário, a análise da Primeira Emenda à Constituição dos Estados Unidos da América e a sua ligação com o ciberespaço já originou variados estudos. Mark Tushnet, por exemplo, veio indagar sobre a aplicabilidade da Primeira Emenda à Internet – realidade obviamente aí não contemplada aquando da sua inserção em 1791 no Bill of Rights. Naquilo que é denominado como *First Amendment Internet exceptionalism* (Excepção da Internet da Primeira Emenda), indaga se as características tecnológicas da Internet – bem como de outras tecnologias do século XXI – justificam uma diferenciação na regulação da disseminação da informação face àquela feita por referência à imprensa, rádio ou televisão⁽⁴⁸⁾. No ordenamento brasileiro e tendo em conta o Marco Civil da Internet, (Lei n.º 12.965, de 23 de abril de 2014), a inclusão no direito à liberdade de expressão também do exercício da mesma no ciberespaço é unânime⁽⁴⁹⁾.

46 Cfr. GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, volume II, *op. cit.*, p. 572, “Além da protecção do conteúdo, o programa normativo do preceito alarga-se à protecção dos meios de expressão (palavra, imagem ou qualquer outro meio). A abertura constitucional - «qualquer outro meio»- permite incluir sem dificuldades as novas formas de expressão como «blogs», «chats», «protestos electrónicos» e os vários estilos (satíricos, irónicos, agressivos, retóricos, etc)”.

47 Veja-se a menção feita na nota de rodapé anterior, bem como JOSÉ DE MELO ALEXANDRINO, anotação ao artigo 37.º, JORGE MIRANDA/RUI MEDEIROS, *Constituição Portuguesa Anotada*, Tomo I, 2.ª edição, Coimbra, Coimbra Editora, 2010, “os meios de comunicação podem ser: (...) (ii) meios de *acesso condicionado e de utilização livre* (como a rádio e televisão pela internet, a própria Internet, o correio electrónico, o *chat*, o telemóvel, o fax, o telefone, o telégrafo e meios de comunicação similares”, salientando ainda, quanto ao contexto em que surgem, os meios de comunicação directa, os de comunicação de massas e aqueles com suporte nas novas tecnologias de informação.

48 MARK TUSHNET, “Internet Exceptionalism: An Overview from General Constitutional Law”, 56 *Wm. & Mary Law Rev.* 2015, <http://scholarship.law.wm.edu/wmlr/vol56/iss4/15>, pp. 1637-1672. Cfr. ainda SETH F. KRAIMER, “Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of The Weakest Link”, *University of Pennsylvania Law Review*, Vol 155, 2006, pp. 11-101 “the rise of the Internet has changed the First Amendment drama, for governments confront technical and political obstacles to sanctioning either speakers or listeners in cyberspace”.

49 Cfr. MARCOS WACHOWICZ, apresentação, *Direito Autoral & Marco Civil da Internet*, MARCOS WACHOWICZ (org.), Curitiba, Gedai Publicações, 2015, p. 6, “o Marco Civil da Internet visa principalmente assegurar a liberdade de expressão e de informação, tudo para garantir a construção de espaços democráticos na Sociedade Informacional. Assim é que o Marco Civil da Internet, ao prever

3), sendo inegável que, independentemente de não haver uma cláusula de limites expressos, o referido direito tem em todo o caso de ser harmonizado e sujeito a operações de ponderação com outros bens constitucionais⁽⁵²⁾, por exemplo quando coloque em causa os bens tutelados no artigo 26.º, n.º 1, da Constituição, ou o segredo de justiça (20.º, n.º 3). Como refere José Eduardo Figueiredo Dias⁽⁵³⁾, «A resolução dos conflitos e colisões entre direitos fundamentais é muitas vezes feita pelo próprio legislador. Tal será mesmo uma exigência constitucional, no caso dos direitos sujeitos à reserva de lei restritiva. No entanto, as dificuldades são inúmeras, uma vez que não se pode ter a pretensão de prever todos os hipotéticos conflitos entre direitos fundamentais através da via geral e abstracta (típica dos actos legislativos). Nesta linha, torna-se imprescindível que os juízos de ponderação e de eventual prevalência de um direito em relação a outro não sejam apenas efectuados ao nível legislativo, exigindo a intervenção do juiz e dos outros aplicadores concretos da Constituição. Daí que, se são de saudar as tentativas de diversas leis administrativas em fazer a articulação e a composição entre o direito à informação e à protecção da intimidade da vida privada - casos do CPA, da LADA e da LPDP -, a verdade é que o problema nunca será assim definitivamente resolvido. A lei terá de se limitar a densificar os parâmetros constitucionais, mas as tarefas de harmonização de direitos, da sua ponderação e a tentativa de conseguir a sua concordância prática, bem como a eventual opção por um dos direitos em detrimento do outro (quando a composição não for possível) só poderá ser feita ao nível do caso concreto. Como afirma RODERICK BAGSHAW a propósito do direito à privacidade, quando em conflito com outros interesses (designadamente a liberdade de expressão e de imprensa, a que poderemos acrescentar o próprio direito à informação), “insistir numa resolução perfeita ao nível teórico antes de passar ao nível prático seria utópico”»⁽⁵⁴⁾.

A propósito da liberdade de expressão, convém também não esquecer as limitações decorrentes do Direito Internacional e recebidas no ordenamento jurídico

que o meio de comunicação seja a internet, a liberdade de expressão e informação não é absoluta, encontrando restrições nos termos do art.º 18.º, CRP, e na concordância que possa ser necessário estabelecer em caso de conflito com outros direitos de igual dignidade constitucional”.

52 Cfr. GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, volume II, *op. cit.*, p. 574.

53 JOSÉ EDUARDO FIGUEIREDO DIAS, “Direito à informação, protecção da intimidade e autoridades administrativas independentes”, *Estudos em Homenagem ao Prof. Doutor Rogério Soares*, Coimbra, Coimbra Editora, 2001, pp. 615-653, nomeadamente pp. 638-639.

54 Sublinhados nossos.

português: pense-se, nomeadamente, no artigo 10.º, n.º 2, da Convenção Europeia dos Direitos do Homem, que dispõe que “O exercício desta liberdades, porquanto implica deveres e responsabilidades, pode ser submetido a certas formalidades, condições, restrições ou sanções, previstas pela lei, que constituam providências necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a protecção da saúde ou da moral, a protecção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial”⁵⁵, bem como os considerandos (9) e (10) da Directiva 2000/31/CE, do Parlamento Europeu e do Conselho de 08/06/00, “relativa a determinados aspectos jurídicos dos serviços da sociedade de informação, em particular do comércio electrónico no mercado interno”, que lançam importantes pistas às considerações que faremos de seguida, relativas ao plano jurídico interno:

“ (9) A livre circulação dos serviços da sociedade da informação pode em muitos casos constituir um reflexo específico, no direito comunitário, de um princípio mais geral, *designadamente o da liberdade de expressão, consagrado no n.º 1 do artigo 10.º da Convenção para a protecção dos Direitos do Homem e das liberdades fundamentais, ratificada por todos os Estados-Membros*. Por esta razão, as directivas que cobrem a prestação de serviços da sociedade da informação devem assegurar que essa actividade possa ser empreendida livremente, à luz daquele preceito, apenas se subordinando às restrições fixadas no n.º 2 daquele artigo e no n.º 1 do artigo 46.º do Tratado. *A presente directiva não tem por objectivo afectar as normas e princípios nacionais fundamentais respeitantes à liberdade de expressão.*

⁵⁵ Chama-se a atenção, a este propósito, para o recente caso *Delfi AS v. Estonia* (2015) ECtHR 64659/09, de 16 de junho de 2015, onde, por 15 votos a favor e 2 contra, a maioria decidiu que considerar o *site* de notícias estoniano *Delfi* responsável por comentários difamatórios anónimos publicados *online* por leitores, mesmo tendo estes sido removidos após pedido, não consubstanciava uma violação do artigo 10.º da Convenção Europeia dos Direitos do Homem (liberdade de expressão), no que já tem sido apelidada de “decisão inesperada”, que “vai contra a Directiva sobre comércio electrónico” e que “dramaticamente retirou a Internet do espectro da liberdade de expressão- conforme veiculado em <http://arstechnica.co.uk/tech-policy/2015/06/shock-european-court-decision-websites-are-liable-for-users-comments/>”. Embora o acórdão não tenha efeito directo, pode vir a influenciar outras decisões judiciais no espaço europeu. O Tribunal entendeu que a natureza extremista dos comentários (configurando um discurso de ódio), o facto de serem publicados num *site* de notícias profissional, bem como as “medidas insuficientes” levadas a cabo pela *Delfi* para dissuadir com os comentários e a baixa probabilidade de os autores dos comentários serem responsabilizados, justificavam que fosse o *site* a ser responsabilizado.

(10) De acordo com o *princípio da proporcionalidade*, as medidas previstas na presente directiva limitam-se ao mínimo estritamente necessário para alcançar o objectivo do correcto funcionamento do mercado interno. Sempre que seja necessário intervir a nível comunitário, e a fim de garantir a existência de um espaço efectivamente isento de fronteiras internas no que diz respeito ao comércio electrónico, a presente directiva deve assegurar um alto nível de protecção dos objectivos de interesse geral, em especial a protecção dos menores e da dignidade humana, a defesa do consumidor e a protecção da saúde pública. Nos termos do artigo 152.º do Tratado, a protecção da saúde é uma componente essencial das outras políticas da Comunidade”.

9. O que parece evidente, à luz da formulação constitucional, é a proibição de censura, nos termos do n.º 2 do artigo. Ora, este conceito de *censura*, tendo em conta o surgimento de novas realidades provenientes da Internet e ciberespaço, implica a necessidade de ampliar o próprio conceito de “censura”⁽⁵⁶⁾, aí contemplando também intervenções na liberdade de expressão, mesmo que praticadas por entidades administrativas, logo, não sendo “restrições a direitos fundamentais” no sentido estrito do artigo 18.º, n.º 2⁽⁵⁷⁾.

E é neste ponto que gostaria de me focar sumariamente, tomando em especial atenção o mecanismo conhecido como “*notice and take down*” e o papel, entre outros, do ICP- ANACOM, enquanto autoridade administrativa independente⁽⁵⁸⁾.

10. A mencionada Directiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de

56 Cfr. RAQUEL ALEXANDRA BRÍZIDA CASTRO, “Constituição e ciberespaço: argumentos para um “Direito Constitucional do Inimigo”?”, *Cyberlaw by CIJIC*, Número 1, Janeiro 2016, pp. 204-243, p. 231.

57 Não nos interessa, por outro lado, a situação em que a intervenção é decretada por um tribunal, porquanto nesse caso, como é evidente, a intervenção é praticada pela função jurisdicional e não administrativa. Veja-se por exemplo o caso do *blog* Póvoa Online, cujo encerramento foi decretado por sentença judicial, tendo a mesma considerado que a maior parte do *blog* consistia em artigos de opinião, criticando o presidente e vice-presidente da Câmara em várias facetas, também como “cidadãos, pais, familiares e amigos”, não estando em causa, pois, “uma crítica construtiva, baseada em factos provados, concretos e objectivos, mas com o objectivo de difundir, junto do público, de forma gratuita, a ideia de que os requerente são corruptos e corruptíveis” (informação obtida em <https://lugardeconhecimento.wordpress.com/2008/06/30/blogue-povoa-online-encerrado/>).

58 Questiona LUÍSA NETO, *op. cit.*, p. 33, “Sendo os blogues actualmente dos principais meios de exercício do direito fundamental à liberdade de expressão, até que ponto é legítimo fazer impender sobre o fornecedor de serviço de armazenagem de blogues (por ex., o *blogger*) a obrigação imediata de retirar ou impossibilitar, por si mesmo, sem ordem de nenhum tribunal ou entidade administrativa competente, o acesso a esse determinado conteúdo?”. Contudo, como se verá, poderá, eventualmente, estar em causa uma ordem decretada por uma entidade administrativa, o que, seguindo o raciocínio admitido pela autora, seria, nesse caso, argumento a favor da legitimidade da entidade.

informação, em especial do comércio electrónico, tem como objectivos principais evitar que as legislações nacionais divirjam de forma a perturbar o funcionamento do mercado interno e fixa as bases que facilitam o recurso a acordos voluntários que estabelecem mecanismos céleres e fiáveis para a retirada ou bloqueio do acesso a conteúdos ilícitos.

Os artigos 12.º a 14.º da Directiva estabelecem diferentes tipos de responsabilidades consoante se tratem de serviços de transmissão e acesso de dados, de *caching* (armazenamento automático e provisório de dados) e de *hosting* (alojamento de dados), definindo os pressupostos que configuram a dita responsabilidade e as suas isenções.

O mecanismo previsto no artigo 14.º da Directiva denomina-se, como já referido, *notice and take down*. Com o objectivo de eliminar conteúdo ilegal da Internet, desresponsabiliza os servidores caso eles removam expeditamente ou impeçam o acesso aos conteúdos ilícitos, após terem conhecimento da ilicitude dos mesmos. Contudo, estando em causa, na colocação do conteúdo, uma manifestação do direito à liberdade de expressão do utilizador- pense-se num comentário racista, violento ou na colocação de conteúdos relacionados com pedofilia- a ordem de eliminação do conteúdo irá, necessariamente, implicar uma restrição a esse direito fundamental.

O artigo 14.º da Directiva não impõe, contudo, a criação de um procedimento específico em cada Estado membro, embora isso fosse benéfico para os objectivos comuns da União, como foi concluído após consulta pública em 2010 e, nomeadamente, face à contestação a este tipo de medidas, por causa do *chilling effect* que podem ter no exercício da liberdade de expressão⁽⁵⁹⁾.

11. Ora, a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, foi transposta para a ordem jurídica nacional pelo Decreto-Lei n.º 7/2004, de 07 de janeiro, entretanto alterado pelo Decreto-Lei n.º 62/2009, de 10 de março e pela Lei n.º 46/2012, de 29 de agosto.

Como decorre da exposição de motivos do Decreto-Lei n.º 7/2004 (nomeadamente do seu ponto 3), um dos grandes objectivos do mesmo “consiste em determinar o regime de responsabilidade dos prestadores intermediários de serviços.

59 Cfr. SETH F. KREIMER, “Censorship By Proxy (...)”, *op. cit.*, pp. 11-101.

Mais precisamente, visa-se estabelecer as condições de irresponsabilidade destes prestadores face à eventual ilicitude das mensagens que disponibilizam. Há que partir da declaração da ausência de um dever geral de vigilância do prestador intermediário de serviços sobre as informações que transmite ou armazena ou a que faculta o acesso. Procede-se também ao enunciado dos deveres comuns a todos os prestadores intermediários de serviços”, como resulta das disposições da Directiva atrás citadas. “Segue-se o traçado do regime de responsabilidade específico das actividades que a própria directiva enuncia: simples transporte, armazenagem intermediária [*coaching*] e armazenagem principal. Aproveitou-se a oportunidade para prever já a situação dos prestadores intermediários de serviços de associação de conteúdos (como os instrumentos de busca e as hiperconexões), que é assimilada à dos prestadores de serviços de armazenagem principal. Introduce-se um esquema de resolução provisória de litígios que surjam quanto à licitude de conteúdos disponíveis em rede, dada a extrema urgência que pode haver numa composição *prima facie*. Confia-se essa função à entidade de supervisão respectiva, sem prejuízo da solução definitiva do litígio, que só poderá ser judicial.”

Dispõe-se ainda (ponto 8) que “muitas funções atribuídas a entidades públicas aconselham a previsão de entidades de supervisão. Quando a competência não couber a entidades especiais, funciona uma entidade de supervisão central: essa função é desempenhada pelo ICP-ANACOM⁽⁶⁰⁾. As entidades de supervisão têm funções no domínio da instrução dos processos contra-ordenacionais, que se prevêem, e da aplicação das coimas respectivas”.

Saliente-se ainda o artigo 7.º e 8.º do diploma, que evidenciam a possibilidade, genérica, de medidas restritivas por parte das entidades competentes, e com maior interesse, o artigo 13.º.

«Artigo 7.º - Medidas restritivas

1 - Podem ser adotadas medidas, incluindo providências concretas contra um prestador de serviços, restritivas à circulação de um determinado serviço da sociedade

60 Sobre o ICP-ANACOM e suas competências, MARIA CELESTE CARDONA, *op. cit.*, pp. 696-711 e, com mais detalhe, pp. 737-745, dividindo as suas competências em regulatórias (de protecção de direitos dos utentes), de supervisão e fiscalização, sancionatórias, competências regulamentares e competências de cooperação interna e internacional. Cfr. também ANA PROENÇA COELHO, *op. cit.*, p. 439 e ss.

da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente:

b) A saúde pública;

c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais;

d) Os consumidores, incluindo os investidores.

2 - A adoção deve ser precedida:

a) Da solicitação ao Estado membro de origem do prestador do serviço que ponha cobro à situação;

b) Caso este o não tenha feito, ou as medidas que tome se revelem inadequadas, da notificação à Comissão e ao Estado membro de origem da intenção de adotar as medidas restritivas.

3 - O disposto no número anterior não prejudica a realização de diligências judiciais, incluindo a instrução e demais actos praticados no âmbito de uma investigação criminal ou de um ilícito de mera ordenação social.

4 - As medidas adotadas devem ser proporcionais aos objetivos a tutelar.

Artigo 8.º - Actuação em caso de urgência

Em caso de urgência, as entidades competentes, incluindo os tribunais, podem tomar medidas restritivas não precedidas das notificações à Comissão e aos outros Estados membros de origem previstas no artigo anterior.”»

Já o artigo 13.º do referido diploma, relativo aos deveres comuns dos prestadores intermediários dos serviços, estabelece que “cabe aos prestadores intermediários de serviços a obrigação para com as entidades competentes:

a) De informar de imediato quando tiverem conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam;

b) De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem;

c) De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação;

d) De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido”⁽⁶¹⁾.

Salientam-se de seguida ainda alguns artigos e passagens mais importantes do Decreto Lei n.º 7/2004 (sublinhados nossos): «”Artigo 14.º - *Simples transporte*

1 - O prestador intermediário de serviços que prossiga apenas a actividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas.

2 - A irresponsabilidade mantém-se ainda que o prestador realize a armazenagem meramente tecnológica das informações no decurso do processo de transmissão, exclusivamente para as finalidades de transmissão e durante o tempo necessário para esta.

Artigo 15.º - *Armazenagem intermediária*

1 - O prestador intermediário de serviços de transmissão de comunicações em rede que não tenha intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários e respeite as condições de acesso à informação é isento de toda a responsabilidade pela armazenagem temporária e automática, exclusivamente para tornar mais eficaz e económica a transmissão posterior a nova solicitação de destinatários do serviço.

2 - Passa, porém, a aplicar-se o regime comum de responsabilidade se o prestador não proceder segundo as regras usuais do sector:

a) Na actualização da informação;

61 Sublinhados nossos.

b) No uso da tecnologia, aproveitando-a para obter dados sobre a utilização da informação.

3 - As regras comuns passam também a ser aplicáveis se chegar ao conhecimento do prestador que a informação foi retirada da fonte originária ou o acesso tornado impossível ou ainda que um tribunal ou entidade administrativa com competência sobre o prestador que está na origem da informação ordenou essa remoção ou impossibilidade de acesso com exequibilidade imediata e o prestador não a retirar ou impossibilitar imediatamente o acesso.

Artigo 16.º - Armazenagem principal

1 - O prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento de actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação.

2 - Há responsabilidade civil sempre que, perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação.

3 - Aplicam-se as regras comuns de responsabilidade sempre que o destinatário do serviço actuar subordinado ao prestador ou for por ele controlado.

(...)

Artigo 18.º- Solução provisória de litígios

1 - Nos casos contemplados nos artigos 16.º e 17.º, o prestador intermediário de serviços, se a ilicitude não for manifesta, não é obrigado a remover o conteúdo contestado ou a impossibilitar o acesso à informação só pelo facto de um interessado arguir uma violação.

2 - Nos casos previstos no número anterior, qualquer interessado pode recorrer à entidade de supervisão respectiva, que deve dar uma solução provisória em quarenta e oito horas e logo a comunica electronicamente aos intervenientes.

3 - Quem tiver interesse jurídico na manutenção daquele conteúdo em linha pode nos mesmos termos recorrer à entidade de supervisão contra uma decisão do

prestador de remover ou impossibilitar o acesso a esse conteúdo, para obter a solução provisória do litígio.

4 - O procedimento perante a entidade de supervisão será especialmente regulamentado.

5 - A entidade de supervisão pode a qualquer tempo alterar a composição provisória do litígio estabelecida.

6 - Qualquer que venha a ser a decisão, nenhuma responsabilidade recai sobre a entidade de supervisão e tão-pouco recai sobre o prestador intermediário de serviços por ter ou não retirado o conteúdo ou impossibilitado o acesso a mera solicitação, quando não for manifesto se há ou não ilicitude.

7 - A solução definitiva do litígio é realizada nos termos e pelas vias comuns.

8 - O recurso a estes meios não prejudica a utilização pelos interessados, mesmo simultânea, dos meios judiciais comuns.

(...)Artigo 36.º - Atribuições e competência

1 - As entidades de supervisão funcionam como organismos de referência para os contactos que se estabeleçam no seu domínio, fornecendo, quando requeridas, informações aos destinatários, aos prestadores de serviços e ao público em geral.

2 - Cabe às entidades de supervisão, além das atribuições gerais já assinaladas e das que lhes forem especificamente atribuídas:

a) Adotar as medidas restritivas previstas nos artigos 7.º e 8.º;

b) Elaborar regulamentos e dar instruções sobre práticas a ser seguidas para cumprimento do disposto no presente diploma;

c) Fiscalizar o cumprimento do preceituado sobre o comércio electrónico;

d) Instaurar e instruir processos contra-ordenacionais e, bem assim, aplicar as sanções previstas;

e) Determinar a suspensão da actividade dos prestadores de serviços em face de graves irregularidades e por razões de urgência.

3 - A entidade de supervisão central tem competência em todas as matérias que a lei atribua a um órgão administrativo sem mais especificação e nas que lhe forem particularmente cometidas.

4 - Cabe designadamente à entidade de supervisão central, além das atribuições gerais já assinaladas, quando não couberem a outro órgão:

a) Publicitar em rede os códigos de conduta mais significativos de que tenha conhecimento;

b) Publicitar outras informações, nomeadamente decisões judiciais neste domínio;

c) Promover as comunicações à Comissão Europeia e ao Estado membro de origem previstas no artigo 9.º;

d) Em geral, desempenhar a função de entidade permanente de contacto com os outros Estados membros e com a Comissão Europeia, sem prejuízo das competências que forem atribuídas a entidades sectoriais de supervisão.”»

Como já salientado por Raquel Brízida Castro⁽⁶²⁾, podemos concluir que existem casos de *notice and takedown* no ordenamento jurídico-nacional, praticados por entidades

62 RAQUEL BRÍZIDA CASTRO, *op. cit.*, pp. 204-243, p. 232 “Atente-se, por exemplo, no regime português do *notice and take down*, que habilita dois órgãos administrativos reguladores, com natureza de entidades administrativas independentes, a procederem a uma verdadeira censura material de informações difundidas por meios de comunicação social *online*, que contenham dados que estas entidades considerem sensíveis e como tal insuscetíveis de serem divulgados, por violarem ou poderem violar o direito à reserva da intimidade da vida privada ou a segurança pública. Serão tais procedimentos subsumíveis ao conceito de censura, em termos constitucionalmente *ilícitos*?” e nota de rodapé 17 na mesma página “Veja-se o caso do *notice and take down* obrigatório:

a) No caso da CNPD (Comissão Nacional de Proteção de Dados), o artigo 20.º, número 1, alínea b) do Decreto-Lei n.º 67/98, o sujeito pode solicitar à CNPD que bloqueie ou mande destruir dados pessoais recolhidos ou divulgados;

b) No caso da ERC, de acordo com o artigo 24.º, número 3, alínea e), dos seus Estatutos, o sujeito pode solicitar a restrição da circulação de serviços da sociedade da informação que contenham conteúdos submetidos a tratamento editorial e que, “lesem ou ameacem gravemente” os valores previstos no artigo 7.º, número 1, do Decreto-Lei n.º 7/2004, de 7 de janeiro. O artigo 7.º refere-se às medidas restritivas que podem ser adotadas contra um prestador de serviços “na medida em que possa lesar ou ameaçar gravemente: b) Saúde pública; c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais; d) Os consumidores, incluindo os investidores. Este Decreto-lei foi aprovado no uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de maio, e transpõe para a ordem jurídica nacional a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio

administrativas independentes fortes (ERC), mas também por entidades administrativas independentes com funções de regulação (ICP-ANACOM)⁽⁶³⁾. Com efeito, nos termos do Decreto-Lei n.º 7/2004, especificamente do seu artigo 35.^o(64) e 36.^o, n.º 1, resulta que as autoridades que poderão impor o bloqueio ou a remoção de conteúdos do ciberespaço são as entidades de supervisão específica ou, caso não existam, o ICP-ANACOM.

12. No Decreto-Lei n.º 7/2004, a existência de um procedimento de *notice and takedown* retira-se da conjugação dos artigos atrás mencionados – sem prejuízo da necessária articulação com as normas estatutárias das entidades reguladores competentes consoante a matéria.

Como expõe Pedro Gonçalves⁽⁶⁵⁾, o artigo 18.^o prevê uma situação de “solução provisória de litígios” em que a entidade administrativa na verdade não actua enquanto juiz do litígio, mas no âmbito de uma “missão pública de polícia”⁽⁶⁶⁾, num “sistema

eletrónico, no mercado interno”. Cfr. também RAQUEL BRÍZIDA CASTRO, *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa, p. 219 “Cumprir, em conformidade com o exposto, aquilatar se, apesar as novas tecnologias: i) esta é uma forma de o Estado, através dessas autoridades administrativas, interferir materialmente nos conteúdos expressivos, sujeitos a tratamento editorial, objeto de *notice and take down* e se, mesmo assim: ii) este procedimento constitui um meio adequado, indispensável e proporcional de garantir a proteção dos bens eventualmente colidentes, os quais beneficiam de igual respaldo constitucional, expresso ou implícito”.

63 Cfr. MARIA CELESTE CARDONA, *op. cit.*, p. 741, “O ICP pode praticar diversos tipos de actos sancionatórios, aplicar multas contratuais, sanções no âmbito de processos contra-ordenacionais, sanções de natureza administrativa e sanções pecuniárias compulsórias”.

64 Artigo 35.^o

Entidade de supervisão central

1 - É instituída uma entidade de supervisão central com atribuições em todos os domínios regulados pelo presente diploma, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade.

2 - As funções de entidade de supervisão central serão exercidas pela ICP - Autoridade Nacional de Comunicações (ICP-ANACOM).

65 PEDRO GONÇALVES, “Regulação Pública de Conteúdos na Internet”, *op. cit.*, pp. 111-112, “Assim, a diferenças entre as duas situações (artigos 15.^o/3, por um lado, e 16.^o e 17.^o, por outro) cifra-se no facto de, na primeira, o prestador de serviços (de “caching”) ser confrontado com o conhecimento de que um determinado conteúdo que transmite e armazena foi retirado pelo seu autor, por sua própria iniciativa ou na sequência de um acto público (*administrativo* ou *judicial*) de carácter impositivo. Neste cenário, o prestador intermediário não tem de efectuar qualquer ponderação sobre o carácter ilícito da informação em causa. Actuando mecanicamente, limita-se a (dever) retirar todas as consequências de uma decisão tomada a montante.

Diferentemente, na segunda situação, o prestador intermediário de serviço (de “hosting” ou de associação de conteúdos) é confrontado com a alegação, feita por um terceiro, de que transmite e armazena uma informação ilícita; não há agora qualquer decisão prévia de remoção ou de impedimento de acesso a essa informação. Na posição de “middleman”, o prestador intermediário é convidado ou instado (por um terceiro) a remover ou impedir o acesso a uma informação posta em rede pelo seu contratante. Nos termos da lei, para se eximir de qualquer responsabilidade, deve actuar em conformidade com o pedido que lhe é dirigido se a ilicitude da informação em causa é manifesta”.

66 Cfr. PEDRO GONÇALVES, *op. cit.*, p. 113.

político-administrativo de controlo de conteúdos”⁽⁶⁷⁾, enquadrando Portugal - ao lado da Alemanha e Espanha- nos países em que a lei atribui directamente a uma autoridade administrativa a competência para exercer funções de polícia e controlo de conteúdos no ciberespaço, podendo determinar a remoção e o bloqueio de acesso a conteúdos ilícitos⁽⁶⁸⁾.

Independentemente da classificação que se faça do tipo de intervenção em causa, certo é que a mesma, restringindo direitos fundamentais, nomeadamente o direito à liberdade de expressão, deve encontrar-se sujeita ao princípio da proporcionalidade⁽⁶⁹⁾- seja entendendo que a mesma se enquadra no artigo 18.º, n.º 2, da Constituição, seja enquanto decorrência do artigo 266.º, n.º 3, da Constituição, já que o princípio da proporcionalidade vincula, como é sabido, toda a actividade da Administração Pública.

13. Tendo em conta as críticas que se podem traçar em torno do artigo 14.º da Directiva (lentidão da retirada dos conteúdos ilícitos, desrespeito por direitos fundamentais), a Comissão iniciou, em Junho de 2012, um procedimento de consulta pública relativamente ao tratamento de conteúdos ilegais na Internet (*public consultation on “procedures for notifying and acting on illegal content hosted by online intermediaries”*)⁽⁷⁰⁾. Durante esse procedimento, mais uma vez se fizeram sentir críticas em torno da fraca salvaguarda dos direitos fundamentais dos utilizadores (particularmente da liberdade de expressão) no procedimento de *notice and take down*⁽⁷¹⁾.

67 *Idem*, p. 116.

68 *Ibidem*.

69 LUÍSA NETO, *op. cit.*, p. 34, “Seja como for, a questão deve ser vista à luz da evidência de que a eventual restrição – e/ou mero condicionamento- de direitos, liberdades e garantias, como os que ao caso subjazem, não pode deixar de acolher os critérios de legitimidade constitucionalmente previstos na lei fundamental portuguesa, que acompanha nesta matéria aliás os principais documentos internacionais atinentes à matéria.

RAQUEL BRÍZIDA CASTRO, “Constituição e ciberespaço (...)”, *op. cit.*, p. 227, “tal como a rigidez constitucional, o imperativo de proteção dos direitos, liberdades e garantias mantém-se, através da sua aplicabilidade directa, reserva de lei ou exigência de reserva de densificação total, assim como as novas tecnologias não os isenta de ponderações, para resolver limitações e restrições, como todos os outros. Esse deve ser o princípio”.

70 Mais informações em http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm

71 Os resultados podem ser consultados em http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet/summary-of-responses_en.pdf

Tendo em conta os resultados obtidos, a Comissão entendeu desenvolver um novo regime dos procedimentos em causa, lançando um novo procedimento de consulta dedicado apenas ao *notice and take down*.

Em 2013, a Comissão apresentou, aliás, um documento de trabalho intitulado *E-commerce Action plan 2012-2015 – State of play 2013*⁽⁷²⁾, onde refere que “on the basis of the information obtained through these consultations and other information, the Commission services are working on an impact assessment on notice-and-action procedure”, tendo já surgido vozes no sentido de estar em preparação uma eventual Directiva apenas referente ao *notice and takedown*. Contudo, não foi possível obter mais informação sobre o desenvolvimento da matéria.

14. Gostaríamos de terminar esta análise com a chamada de atenção para alguns casos recentes – já enunciados no início do texto- e que demonstram o impacto da intervenção de autoridades (ainda que no primeiro caso de fonte jurisdicional) sobre o exercício de direitos fundamentais no ciberespaço, nomeadamente da liberdade de expressão:

De acordo com a notícia constante de http://rr.sapo.pt/noticia/53204/juiz_bloqueia_whatsapp_a_100_milhoes_de_brasileiros, a justiça brasileira ordenou o bloqueio do *WhatsApp* em Maio de 2016, tendo como objectivo entregar às autoridades informação sobre um grupo de traficantes de droga, sendo esta a segunda vez em cinco meses que a justiça brasileira ordena o bloqueio da aplicação (note-se, bloqueio para todos os seus – muitos – utilizadores). Já no ano passado um tribunal, que pretendia obter informações sobre um grupo de criminosos, perante a recusa do *Whatsapp* em fornecer as referidas informações decretou o bloqueio da aplicação por 48 h, baseado no Marco Civil da Internet. Contudo, durante a tarde um outro juiz, em São Paulo, levantou o mesmo bloqueio, argumentando ser desrazoável afectar milhões de utilizadores por causa da conduta da empresa, convertendo antes o bloqueio numa sanção pecuniária.

Já em Portugal e com maior interesse para a presente temática, a Inspeção Geral das Actividades Culturais, serviço da Administração direta do Estado, na sequência de um memorando assinado em Agosto entre a IGAC, a Direcção-Geral do Consumidor, a APRITEL (Associação dos Operadores de Telecomunicações) e o

72 Disponível em http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf

MAPiNET (Movimento Cívico Anti-Pirataria na Net), e ainda várias associações do sector⁽⁷³⁾, pretende simplificar o bloqueio de *sites* com conteúdo pirata, baseado em eventual incumprimento de regras respeitantes a direitos de autor (fundado no artigo 2, n.º 2, al. b), do Decreto-Regulamentar n.º 43/2012, de 25 de maio, conjugado com o disposto no Decreto-lei n.º 7/2004 de 7 de janeiro, com as suas alterações⁽⁷⁴⁾. Assim, com base num acordo, o bloqueio passará a ser feito com intervenção do MAPiNET, no que representa um “acordo de auto-regulação relativo à protecção do direito de autor e dos direitos conexos em ambiente digital”.

De acordo com a notícia presente na página do MAPiNET, <http://www.mapinet.org/site/index.php/artigos-noticias/25-assinado-um-acordo-que-simplifica-o-bloqueio-de-sites>, «A operacionalização vai ser feita pela MAPiNET - Movimento Cívico Antipirataria na Internet, que conta entregar dois blocos de 50 *sites* com conteúdos pirata por mês ao IGAC⁽⁷⁵⁾, que por sua vez envia o ofício aos operadores para que os endereços Web (DNS) sejam bloqueados, passando a ser exibida aos utilizadores a mensagem de “site indisponível” ou “site não encontrado” quando tentarem aceder a um URL bloqueado».

O critério base para que os *sites* sejam bloqueados é a identificação de, pelo menos, 500 conteúdos ilegais, ou de dois terços do repositório com obras piratas⁽⁷⁶⁾. Recolhida a prova, o MAPiNET encaminha a denúncia para a IGAC, que tem a responsabilidade de a confirmar e, caso se justifique, fazer chegar uma notificação junto dos operadores de comunicações⁽⁷⁷⁾. Cabe a estes garantir o bloqueio dos *sites* piratas denunciados, passando a ser exibida aos utilizadores a mensagem de “site indisponível” ou “site não encontrado” quando tentarem aceder ao respectivo URL.

Desde a data da assinatura do Memorando do Entendimento, terão sido bloqueados pelos operadores de telecomunicações 330 *sites* que alegadamente partilhavam conteúdos ilegais⁽⁷⁸⁾. Um dos bloqueios em causa (*site* Ultimate Music) levou a críticas de que a informação que a IGAC está a receber do MAPiNET é criada

73 Memorando disponível em <https://paulasimoesblog.files.wordpress.com/2015/09/memorando.pdf>

74 Cfr. considerando 3 do Memorando e Cláusula 3.ª do mesmo.

75 Nos termos da cláusula 5.ª, n.º 3, do Memorando.

76 Cfr. cláusula 5.ª, n.º 4, do Memorando.

77 Cfr. cláusula 6.ª do Memorando.

78 Conforme informação constante de <http://fevip.org/site/noticias/>, veiculada por Paulo Santos, Diretor Executivo da FEVIP, Associação Portuguesa de Defesa de Obras Audiovisuais.

pelo próprio MAPiNET e de que os documentos que eventualmente poderiam ser usados como prova (a localização exacta das obras; a defesa da pessoa que está a ser acusada) não estão a chegar à IGAC⁽⁷⁹⁾. De acordo com esta informação “Mesmo não tendo provas ou evidências entregues pelo MAPiNET, a IGAC também não está, ela própria, a analisar os pedidos de bloqueio: se o fizesse nunca teria bloqueado o *site* Ultimate Music, uma vez que este *site* não disponibiliza obras, nem dá acesso ilegítimo a obras disponibilizadas por terceiros. Acresce a este argumento, que poucos dias depois de se saber do bloqueio do Ultimate Music, veio a público o bloqueio de um outro *site* cujo domínio nem sequer estava registado, ou seja, a IGAC mandou bloquear um *site*, que não existia (entretanto o site foi registado por alguém e mais recentemente foi desbloqueado em pelo menos alguns ISPs)”⁽⁸⁰⁾.

Entretanto, também recentemente o bloqueio de um *site* de jogos (o *Carbon Games*) com base no Decreto-Lei n.º 66/2015 (Regime Jurídico dos Jogos e Apostas *Online*) – que permite a suspensão do exercício da actividade de jogos e apostas *online* pelo Serviço de Regulação e Inspeção de Jogos, integrado no Turismo de Portugal (cfr. ainda artigo 3.º, n.º 2, alínea p) do Decreto-Lei n.º 129/2012, de 22 de junho, republicado em anexo ao Decreto-Lei n.º 66/2015 e artigo 19.º, n.º 1, determinando que “o Turismo de Portugal, I.P., no âmbito da sua atividade de controlo, inspeção e regulação da exploração e prática dos jogos de base territorial e dos jogos e apostas *online*, exercida através da comissão de jogos e do Serviço de Regulação e Inspeção de Jogos, detém poderes e prerrogativas de autoridade pública administrativa e de entidade de regulação”) - já foi qualificado como um “erro” pela própria entidade⁽⁸¹⁾.

Como resulta, aliás, da pergunta n.º 443/XIII, de 22 de janeiro de 2016, formulada pelo Bloco de Esquerda ao Ministro da Cultura, “o problema de fundo mantém-se: é possível o bloqueamento indiscriminado de *sites* por ordem administrativa sem qualquer controlo judicial e, neste caso, sem sequer ser notificada a

79 Ver, entre outros, <https://revolucaodosbytes.pt/novo-site-legitimo-bloqueado-e-sujeito-a-duplo-pagamento/> e <https://revolucaodosbytes.pt/igac-e-mapinet-nao-cumprem-o-memorando-de-entendimento/>. Mais críticas em <https://paulasimoesblog.wordpress.com/2016/01/21/update-turismo-de-portugal-bloqueou-carbon-games/>

80 Segundo <https://paulasimoesblog.wordpress.com/2016/03/10/igac-e-mapinet-nao-cumprem-memorando-de-entendimento/>

81 <http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626e4a6c635639775a584a6e6457353059584d7657456c4a535339775a7a51304d79313461576c704c5445756347526d&fich=pg443-xiii-1.pdf&Inline=true>

entidade alvo do bloqueio, nem haver nenhuma possibilidade da entidade alvo do bloqueio poder reclamar”⁽⁸²⁾.

15. Os casos avançados, nomeadamente o último, permitem defender que também a intervenção restritiva de um direito fundamental praticada pela Administração, neste caso no ciberespaço, para além de sujeita ao princípio da proporcionalidade e apenas justificável se procurar a concordância prática com outros bens constitucionalmente protegidos, tenha de ser feita com base em lei prévia, que defina os denominadores mínimos necessários à actuação da entidade administrativa, só assim respeitando exigências de determinabilidade⁽⁸³⁾, sob pena de inconstitucionalidade.

82 Veja-se que a resposta, disponível em <http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626e4a6c635639775a584a6e6457353059584d7657456c4a53533977636a51304d79313461576c704c544574595335775a47593d&fich=pr443-xiii-1-a.pdf&Inline=true>, na qual vem distinguir o que resulta do Memorando de Entendimento, sujeito à tutela do Ministério da Cultura, e o que resulta do Decreto-Lei, sujeito à tutela do Ministério da Economia e fora do âmbito do referido memorando. Contudo, a resposta afigura-se também relevante pelas considerações que faz sobre o Memorando e objectivos do mesmo.

83 Cfr. JORGE REIS NOVAIS, *Os princípios constitucionais estruturantes da República Portuguesa*, Coimbra, Coimbra Editora, 2004, pp. 191-194.

CYBERLAW

by CIJIC

CYBERLAW

by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Do we have one real perception of the true degree of technological intrusiveness into the lives of citizens?

At this «Cyberlaw by CIJIC», 2nd edition, we intend to bring to one legal and technological debate some of the most worrying questions related with the weakness of the traditional concepts of public law. Take, for example, old problems where, alleged, threats to state security compress ordinary individual freedoms. Cyberspace currently dominates daily life. Where can we find the protection of the legal-subjective positions of individuals in it?

Traditional juridical and legal programs will lose all effectiveness, sliding into nominal, if the rule of law gives up to respond to the daily problems of netizens.

We all face new legal dimensions. In face of the ineluctable conclusion that the Internet is a global resource, which we dare say, incompatible, par excellence, with the old concept of territorial sovereignty of State, which scientific criteria need to be included in the construction of a dogmatic approach to the regulation of cyberspace? Furthermore, can it be regulated? Which - if any - new international, worldwide, legal solutions we must strive for?»



FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa