Instituto de Referência em Internet e Sociedade

Jurisdição e internet

Estudo sobre mecanismos de bloqueio e fragmentação da rede

IRIS
Instituto de Referência em Internet e Sociedade

Instituto de Referência em Internet e Sociedade

Jurisdição e internet

Estudo sobre mecanismos de bloqueio e fragmentação da rede

Coordenação
Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos

Autores
Laila Damascena Antunes
Matheus Rosa
Pedro Vilela

Projeto gráfico
André Oliveira e Lucca Falbo

Capa
Freepik

Diagramação
André Oliveira

Produção Editorial
Instituto de Referência em Internet e Sociedade

Revisão
Lucas Costa dos Anjos

Finalização
André Oliveira

Como citar em ABNT
ANTUNES, Laila Damascena; ROSA, Matheus; VILELA, Pedro. **Jurisdição e internet**: Estudo sobre mecanismos de bloqueio e fragmentação da rede. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: http://bit.ly/2PjUqYT. Acesso em: DD mmm. AAAA

SUMÁRIO

1. Considerações iniciais[1]

O modelo westfaliano de Estado-nação, baseado na soberania territorial, contrasta com o modelo da internet, fundamentado na descentralização, na abertura, na colaboração e nos movimentos transfronteiriços - ou que ocorrem no ciberespaço. Por terem naturezas e pressupostos tão diversos, a conexão entre Estado e internet é complexa. A internet é estruturada especialmente por linguagem computacional (código) e infraestrutura física (computadores, cabos e satélites, entre outros). O Estado, por sua vez, organiza e controla seu território e uma população por meio de uma constituição, leis, instituições e costumes. Conectar geografia e ciberespaço, então, é uma tarefa complexa, em plena construção e mudança nos tempos atuais[2]. Um dos primeiros visionários e entusiastas da internet proferiu em seu manifesto de independência do ciberespaço:

> Governos do Mundo Industrial, vocês gigantes cansados de carne e aço, eu venho do Ciberespaço, o novo lar da Mente. Em nome do futuro, peço-lhes do passado para nos deixar em paz. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nos reunimos.[3]

Os poderes soberanos, contudo, adentram a internet e vão mais além de suas fronteiras informacionais. Existem diversas razões pelas quais um Estado, uma entidade pública ou privada podem querer relativizar a natureza transfronteiriça e universal da internet, especialmente pelo recurso a mecanismos técnicos e desenvolvimento de tecnologias e saberes com essa finalidade. Como tecnologia originalmente criada para ignorar a existência de fronteiras nacionais, a internet foi responsável por uma revolução na comunicação transnacional, mas também acarretou uma série de consequências jurídicas e riscos diversos para usuários, governos e empresas.

A dificuldade em se adjudicar conflitos transnacionais originados na internet fez com que governos e empresas buscassem prevenir o surgimento desses litígios. Ao longo dos anos, novas tecnologias possibilitaram mecanismos que simulassem e adulterassem fronteiras geográficas, identificando ou reposicionando a origem de usuários no espaço global, para então restringir seu pleno acesso a sites, conteúdos ou serviços e reproduzir no ambiente da internet as divisões políticas do mundo offline.

Cada vez mais, o fenômeno, conhecido como 'balcanização da internet', preocupa acadêmicos e ativistas da sociedade civil que temem que a fragmentação da rede acabe com seu potencial democrático, colaborativo, catalisador da inovação e do acesso à informação.

Este estudo analisa casos em que a natureza transnacional originária da internet foi alterada para atender a demandas políticas, culturais, econômicas e/ou jurídicas.

1 Trabalho de pesquisa elaborado sob a coordenação de Fabrício B. Pasquot Polido e Lucas Costa dos Anjos, no âmbito do Instituto de Referência em Internet e Sociedade - IRIS e do Grupo de Estudos Internacionais de Internet, Inovação e Propriedade Intelectual - GNet, da Universidade Federal de Minas Gerais. Contribuíram como autores para este trabalho os pesquisadores Laila Damascena Antunes, Matheus Rosa e Pedro Vilela.

2 Ver LESSIG, Lawrence. Code: Version 2.0. Nova Iorque: Basic Books, 2006. Disponível em: <https://goo.gl/kUcPRA>. Acesso em 09 de fevereiro de 2017.

3 Tradução livre de: *"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather"*. BARLOW, John Perry. A Declaration of the Independence of Cyberspace. 1996. Disponível em: <https://goo.gl/kocxlM>. Acesso em 09 de fevereiro de 2017.

Em seguida, explicam-se brevemente os mecanismos técnicos utilizados por governos e empresas para efetuar essa fragmentação. Por fim, discutir-se-ão teorias e princípios sobre a natureza transnacional da rede, seu impacto sobre a sociedade contemporânea e as possíveis consequências de sua distorção. Ressalta-se que a fragmentação aqui discutida é a de natureza técnica, não sendo do escopo deste trabalho as discussões sobre fragmentação social e/ou cultural causadas pela internet.

2. Por que falar-se em balcanização da internet?

O processo de fragmentação da internet por mecanismos técnicos e jurídicos tem sido chamado de "balcanização" da internet. O termo faz referência à fragmentação política dos Estados do Sul da Europa, em razões de diferenças étnicas, religiosas e culturais, após o fim do domínio estrangeiro sobre a região[4]. O fenômeno se caracteriza quando programas governamentais de censura, interesses comerciais, preocupações com cibersegurança e outras mudanças dinâmicas no ecossistema da internet acabam por retalhar a rede global em diversas versões regionais. Essa retaliação ameaça a comunicação universal, a inovação e a prosperidade econômica trazida pela internet como inicialmente estruturada.[5]

A fragmentação da rede é considerada uma das maiores ameaças à internet como a conhecemos, e a importância de seu caráter universal é reconhecida por diversos estudiosos do tema[6] [7]. Todavia, parece fadada a se concretizar, já que governos e agentes de elevado poder econômico implementam medidas técnicas que favorecem seus interesses. Diferenças de lei aplicável também são citadas entre as principais razões pelas quais governos adotam mecanismos de fragmentação da internet. Analisaremos alguns casos e contextos onde diferentes meios técnicos foram utilizados para fragmentar a internet, criando versões idiossincráticas da rede em diferentes jurisdições.

a. Grande Muralha de Fogo da China

O termo "*Great Firewall of China*" tem origem na década de 1990 e foi cunhado para se referir a uma série de práticas e regulações restritivas por parte do governo chinês sobre a internet[8]. Com o intuito de controlar conteúdo, comunicação e até mesmo de favorecer empreendimentos locais, o governo chinês buscou, por meio de uma combinação de diferentes métodos, policiar provedores de conteúdo e conexão, consumidores individuais, sites e aplicativos estrangeiros.[9]

O sistema chinês de filtragem baseia-se, principalmente, na filtragem de uma enorme lista de endereços de IP considerados inapropriados ou sensíveis pelo governo.

4 ALVES, Sergio, Jr. The Internet Balkanization Discourse Backfires, *SSRN Electronic Journal*. Disponível em: <https://goo.gl/pQpLF6>. Acesso em 17 de fevereiro de 2017. p. 1-2.

5 HILL, Jonah Force. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs*. 2012 p. 49-58.

6 CLARK, Liat, BERNERS-LEE, Tim. Wired. We need to re-decentralise the web. Disponível em: <https://goo.gl/txGONw>. Acesso em 10 de fevereiro de 2017.

7 MARKOFF, John. New York Times. Viewing Where the Internet Goes. Disponível em: <https://goo.gl/js8Gp4>. Acesso em 10 de fevereiro de 2017.

8 BARME, Jeremie e YE, Sange. Wired. *The Great Firewall of China*. Disponível em: <https://goo.gl/P5zF0l>. Acesso em 05 de fevereiro de 2017.

9 LEE, Jyh-An e LIU, Ching-Yi, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China (March 7, 2012). *Minnesota Journal of Law, Science, and Technology,* Vol. 13, No. 1, 2012. Disponível em: <https://goo.gl/R6ZJ6Z>. Acesso em 05 de fevereiro de 2017. p. 127.

A lista é fornecida aos provedores de backbone[10] [11], especificamente à China Telecom, que são responsáveis pela espinha dorsal da infraestrutura da rede ('backbone') e pelas conexões internacionais da internet no país. Esses provedores são obrigados a instalar aparatos específicos que identificam a origem de pacotes de dados e os descartam quando originários de um endereço vetado[12].

A lista de conteúdos vetados varia enormemente, contudo há certa predominância de assuntos de natureza política entre os selecionados. São frequentemente bloqueados sites que hospedam informações associadas à independência de Taiwan e Tibet, aos direitos humanos, ao movimento Falung Gong e outras ameaças ao Partido Comunista[13]. São bloqueados sites como The New York Times, the Economist, Anistia Internacional, BBC entre outros[14] [15]. O caso de gigantes da tecnologia da informação, como Google e Facebook, também é amplamente estudado. Devido às dificuldades por parte do governo chinês em regular essas empresas e à resistência delas de agir conforme os interesses do Estado chinês, o Partido Comunista optou por restringir completamente seu acesso[16].

Durante sua curta estadia na China, por exemplo, a Google foi obrigada a remover resultados de busca relacionados aos conteúdo supracitados, como o massacre de Tiananmen e o movimento de independência do Tibet. Pressões políticas, tanto do governo chinês, quanto americano, e a própria política da empresa fizeram com que a empresa se retirasse do país e passasse a ser permanentemente bloqueada[17].

O resultado é uma internet na China considerada fundamentalmente diferente da internet do resto do mundo: ela é comparada, com frequência, ao ecossistema de uma laguna isolada do resto do oceano, em que versões chinesas análogas substituem aplicativos acessados por usuários do resto do mundo[18].

b. Localização de dados, *data centers* brasileiros e a *'Euro Cloud'*

Em oposição à tendência de livre fluxo de dados transfronteiriços, estão os regramentos sobrea localização de dados, que podem ser entendidos como "esforços a nível nacional ou regional para regular o fluxo de dados transfronteiriços ou criar incentivos para localizar o processamento e o armazenamento de dados".[19] Assim como

10 Segundo a *Nota conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações*, de maio de 1995: *"A Internet é organizada na forma de espinhas dorsais* [ou, no termo original,] *backbones, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade"*. COMITÊ GESTOR DA INTERNET NO BRASIL. *Nota conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações* (maio de 1995). Disponível em: <https://goo.gl/xlHXDB>. Acesso em 03 de março de 2017.

11 De acordo com Marcel Leonardi: "*O backbone, ou "espinha dorsal", representa o nível máximo de hierarquia de uma rede de computadores. Consiste nas estruturas físicas pelas quais trafega a quase totalidade dos dados transmitidos através da Internet, e é usualmente composto de múltiplos cabos de fibra ótica de alta velocidade*". LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. *Op.cit*.

12 FARIS, Robert, VILLENEUVE, Nart, Measuring Global Internet Filtering. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press, 2008. p. 5-27

13 LEE e LIU,Forbidden City Enclosed by the Great Firewall, *Op. cit.* , p. 127

14 *Idem*. p. 131

15 Para uma lista completa, acessar: <https://goo.gl/oYFhjc>.

16 LEE, Jyh-An, LIU, Ching-Yi, LI, Weiping, Searching for Internet Freedom in China: A Case Study on Google's China Experience. *Cardozo Arts & Entertainment Law Journal*, Vol. 31, No. 2, 2013. Disponível em: <https://goo.gl/oRGuKB>. Acesso em 07 de fevereiro de 2017, p. 409.

17 *Idem*. p. 416

18 MOZUR, Paul. Chinese Tech Firms Forced to Choose Market: Home or Everywhere Else, *New York Times.* Disponível em: <https://goo.gl/UMoEn8>. Acesso 10 de fevereiro de 2017.

19 Tradução livre de: "[...] *efforts at the national or regional level to regulate the flow of data across borders or to create incentives to*

a utilização de mecanismos de filtragem pelo governo chinês, a localização forçada de dados tem sido apontada como uma ameaça à integridade da internet que contribui para sua balcanização. Restrições quanto à localização de dados já foram propostas por diversos países, dentre os quais se destacam Alemanha, Rússia e Brasil, particularmente motivados por pressões públicas de combate à vigilância cibernética transfronteiriça e à espionagem de dados praticada por governos estrangeiros e empresas transnacionais.

Essas restrições ocorrem no âmbito territorial e podem ser caracterizadas em cinco grandes modalidades: *i.* restrição do processamento de dados por entidades dentro de determinada jurisdição; *ii.* requerimento de que dados sejam armazenados "localmente" (dentro de determinado território); *iii.* mudanças na arquitetura da rede e uso de roteamento de dados para mantê-los dentro de um espaço territorial, como espécie de 'confinamento informacional' ; *iv.* políticas discriminatórias que permitem a implementação dessas restrições apenas por certas organizações, com o critério de origem/nacionalidade; e *v.* restrições ao movimento transfronteiriço de algumas categorias de dados[20].

Notadamente, o tipo *(ii)*, armazenamento local de dados, foi amplamente debatido durante a elaboração do Marco Civil da Internet no Brasil. Por fim, as previsões de implantação de *data centers* em território nacional não avançaram para o texto final[21]. No entanto, essa prática, a título de exemplo, pode ser observada atualmente em uso na Rússia, sendo o recente caso de bloqueio do site *LinkedIn* o exemplo mais significativo das consequências das regras russas de localização[22].

Percebe-se, ademais, que o tipo *(v)*, restrições de movimento transfronteiriço, também é aplicado no âmbito da União Europeia, a partir dos modelos estabelecidos pela antiga Diretiva 95/46/CE[23] e atualmente no Regulamento 2016/679, denominado Regulamento Geral sobre a Proteção de Dados[24]. Ele se refere à limitação da transmissão de dados de cidadãos europeus a países não-membros da União, exceto àqueles que oferecem um reconhecido nível de proteção adequada ao tratamento de dados pessoais. Exemplo notório de acordo julgado insuficiente ocorreu no caso *Safe Harbour*, em decisão da Corte de Justiça da União Europeia de 2015, que invalidou o acordo que permitia a transmissão de dados por/para empresas dos Estados Unidos.[25]

localize data processing and storage". KUNER, Christopher. Data Nationalism and its Discontents. *Emory Law Journal Online*, v. 64, p. 2089, 2015. Disponível em: <https://goo.gl/VxMkfp>. Acesso em: 07 de fevereiro de 2017.

20 Sobre isso, ver DRAKE, William J. e CERF, Vinton G. e KLEINWÄCHTER, Wolfgang. Internet Fragmentation: An Overview. *Future of the Internet Initiative White Paper*. World Economic Forum, p. 41, 2016. Disponível em: <https://goo.gl/wTlV1e>. Acesso em 27 de janeiro de 2017.

21 BRAGA, Juliana. Governo não vai insistir em data center no país, diz Dilma no Facebook. *G1 Globo.com*, 24 Abr 2014. Disponível em: <https://goo.gl/PRMG69>. Acesso em 07 de fevereiro de 2017.

22 Rússia inicia bloqueio ao LinkedIn após decisão judicial. *Folha de S. Paulo*, 17 Nov 2016. Disponível em: <https://goo.gl/SDKPZX>. Acesso em 7 de fevereiro de 2017. Em junho de 2016, o parlamento russo aprovou as mudanças da Lei Federal sobre Informação, Tecnologias de Informação e Proteção da Informação de 2006 (Federal Law On Information, Informational Technologies and the Protection of Information of 2006), atingindo justamente os provedores de acesso de provedores de conteúdos, considerados "communications service providers ("CSP") e "facilitators of information dissemination on the Internet" ("FIDI"), nos termos da lei. Em novembro de 2017 entra em vigor os bloqueios a ferramentas de navegação anônima e VPNs (virtual private networks). Ver LEXOLOGY, New Russian Legislation on Massive Telecoms Surveillance, 12 de julho de 2016. Disponível em: <https://goo.gl/fHNZuV>, acesso em 18 de setembro de 2017.

23 UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Diário Oficial da União Europeia*, L 281, de 23 de Novembro de 1995, p. 31–50. Disponível em: <https://goo.gl/GKm9dD>. Acesso em 07 de fevereiro de 2017.

24 UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Diário Oficial da União Europeia*, L 119, de 04 de maio de 2016, p. 1–88. Disponível em: <https://goo.gl/tzzWf8>. Acesso em 07 de fevereiro de 2017.

25 CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Schrems v Data Protection Commissioner (C-362/14) (Request for a preliminary ruling from the High Court (Ireland)). Judgment of the Court (Grand Chamber), 6 Out 2015. *Digital reports (Court Reports - general)*. Disponível em: <https://goo.gl/bYDdaS>. Acesso em 07 de fevereiro de 2017.

Analisaremos dois casos distintos, em que a localização de dados foi discutida: a proposta alemã para um serviço de nuvem europeu e a tentativa de inclusão de obrigação de localização de *data centers* em território nacional no Marco Civil da Internet brasileiro.

Os casos alemão e brasileiro surgiram como reação às revelações de Edward Snowden acerca dos programas de vigilância em massa por parte do governo americano, que incluíam provas de que a Agência de Segurança Nacional espionava diretamente as comunicações da Chanceler Angela Merkel e da Presidente Dilma Rousseff.[26] Em resposta, o governo alemão promoveu em parceria com o governo brasileiro a conferência NETMundial, uma nova plataforma de debates para a governança da internet. O maior esforço, entretanto, diz respeito às diretrizes para desenvolvimento de infraestrutura da internet para a União Europeia propostas por Angela Merkel, além da inclusão de uma cláusula no Marco Civil da Internet que obrigasse empresas de internet que tratassem dados no Brasil a armazená-los em *data centers* no solo brasileiro. A criação de uma nova conexão de cabos submarinos entre Brasil e Europa, de forma que o tráfego entre as regiões não precisasse passar pelos Estados Unidos, também foi proposta e se encontra em fase de construção.[27]

A proposta legislativa acerca da instalação de *data centers* no Brasil foi abandonada após reações negativas de especialistas, que afirmaram ser a medida ineficaz e possivelmente prejudicial à internet no Brasil.[28] A presença da norma no projeto de lei do Marco Civil da Internet também era um dos maiores entraves a sua aprovação.

A proposta alemã envolvia o desenvolvimento de infraestrutura informacional que permitisse aos cidadãos europeus optar por serviços que armazenassem seus dados dentro da União Europeia e, portanto, estivessem sujeitos à legislação de privacidade do continente. Legisladores alemães enxergavam a proeminência de empresas americanas na coleta e tratamento de dados como uma ameaça à proteção da privacidade dos cidadãos europeus.[29] A proposta foi coloquialmente chamada de 'Euro Cloud' e não recebeu muita atenção posterior e, até a data de publicação deste trabalho, não alcançou nenhum avanço significativo.[30]

c. A 'internet halal' e outros casos de 'intranets nacionais'

Esforços por parte de governos para criar barreiras rígidas ao tráfego de informações vindas do estrangeiro têm se tornado comuns. Um dos casos mais notáveis é a iniciativa por parte do governo teocrático do Irã para criar a "internet halal". *Halal* é uma palavra árabe que significa 'permissível' [31] e é geralmente usada para se referir à dieta permitida pelo Corão. O termo foi adotado então para se referir à *intranet* composta apenas por conteúdo considerado legítimo pelo governo da República Islâmica.[32]

26 MACASKILL, Ewan, DANCE, Gabriel. The Guardian. NSA Files: Decoded. 1 Nov 2013. Disponível em: <https://goo.gl/YoVhD1>. Acesso em 07 de fevereiro de 2017.

27 RT News. *Brazil-Europe undersea cable to hide web traffic from US Snooping*. 26 Fev 2016. Disponível em: <https://goo.gl/05oopm>. Acesso em 07 de fevereiro de 2017.

28 BARABAS, Emily. CDT. Brazil's "Internet Bill of Rights" regains momentum in Congress. 27 Mar 2017. Disponível em: <https://goo.gl/ZwbjDJ>. Acesso em 07 de fevereiro de 2017.

29 The Register. '*European IT Airbus could lead to competition concerns*'. Disponível em: <https://goo.gl/3bKEqa>. Acesso em 13 de fevereiro de 2017.

30 BRANDON, Jonathan. Merkel, Kroes' proposition for EU Cloud "aren't contradictory" , says EC. Telecoms.com. 17 Fev 2014. Disponível em: <https://goo.gl/En5gVO>. Acesso em 17 de fevereiro de 2017.

31 '*What is Halal*'. Disponível em: <https://goo.gl/9cvdeR>. Acesso em 17 de fevereiro de 2017.

32 BEITER, Katie. 'Iran introduces Halal Internet'. *The Medialine*. Disponível em: <https://goo.gl/obxtVs>. Acesso em 17 de fevereiro de 2017.

A proposta funciona mais como uma *intranet* do que como a internet: uma rede privada controlada por uma organização. *Intranets* são comuns em ambientes de trabalho como corporações ou universidades. Por meio de mecanismos diversos, seus gerenciadores podem escolher que tipo de conteúdo estará disponível. É válido ressaltar que a intranet tem apenas uma conexão limitada com a internet ou, em alguns casos, não possui qualquer contato com a rede mundial de computadores.

O caso iraniano é notável, pois sua justificativa não se baseia em questões puramente jurídicas: o governo iraniano teme infiltração da cultura ocidental por meio da internet. Desde a Revolução Islâmica, em 1979, o país tem se posicionado de forma antagônica ao Ocidente e suas instituições. A experiência iraniana pode servir de inspiração para iniciativas por parte de outros Estados que frequentemente vivenciam choques culturais catalisados pela internet. Diferenças culturais, principalmente em relação a questões de discurso, estão entre as principais forças motrizes da fragmentação da internet [33].

Outros países que desenvolveram *intranets* nacionais, cujo conteúdo é limitado e o acesso à internet, restrito, incluem Cuba,[34] Myanmar[35] e Coréia do Norte. Neste último Estado, o número de websites acessíveis se limita a 28,[36] a maioria dos quais se restringe a conteúdo favorável ao governo.

3. Mecanismos de bloqueio

Para entender a possibilidade de implementação de mecanismos de partilhamento do espaço da internet de acordo com fronteiras territoriais, primeiro é fundamental compreender o funcionamento básico da camada lógica sobre a qual a internet se sustenta.

A internet, como a conhecemos hoje, utiliza do protocolo TCP/IP[37] para encaminhar pacotes de dados de ponta a ponta. Toda a comunicação feita pela internet utiliza esses pacotes, seja para visualizar uma página de texto, para trocar mensagens instantâneas ou para realizar uma videoconferência.

Na infraestrutura da rede, há um tipo específico de computador chamado roteador, cujo trabalho é servir de ponto de encontro, ou "nó", de diferentes conexões (sejam elas cabos de fibra ótica, redes wireless ou antenas de rádio), para então direcionar corretamente os pacotes que por ele passam. A escolha de encapsular todos os pacotes sob um mesmo protocolo (IP) é um dos maiores trunfos da internet, pois permite que diferentes redes, em diferentes estruturas, possam se comunicar livremente.

Os roteadores identificam os computadores destinatários e remetentes a partir de seus endereços IP, que são "estampados" nos pacotes de dados. A partir daí, podem conduzir apropriadamente o tráfego de dados pela rede. Uma analogia comum é a que compara os roteadores de uma rede aos correios e carteiros e os pacotes de dados, às cartas e pacotes. Os correios recebem uma carta ou pacote de um remetente e seus

33 CHANDER, Anupam, LE, Uyen, 'Data Nationalism'. *Emory Law Journal*, Vol. 64, No. 3, 2015. Disponível em: <https://goo.gl/vdZ5nC>. Acesso em 17 de fevereiro de 2017, p. 678-679.
34 PRESS, Larry, The state of the Internet in Cuba, 2011. Disponível em: <https://goo.gl/fQzQJj>. Acesso em 17 de fevereiro de 2017.
35 RHOADS, Christopher, FASSIHI, Farnaz. 'Iran vows to unplug Internet'. *Wall Street Journal*. 2011. Disponível em: <https://goo.gl/Za6UIq>. Acesso em 17 de fevereiro de 2017.
36 ASHER, Sara. 'What the North Korean Internet Really Look Like', *BBC News*. 2016. Disponível em: <https://goo.gl/ptc0c9>. Acesso em 17 de fevereiro de 2017.
37 Do inglês "Transmission Control Protocol/Internet Protocol" ou "Protocolo de Controle de Transmissão/Protocolo de Internet"

carteiros utilizam da infraestrutura física da cidade para se locomover e entregar a carta.

a. Filtragem de conteúdo e acesso

A filtragem de conteúdo e acesso é um dos principais mecanismos adotados por provedores de acesso e conteúdo, por exigência governamental, ou por opção própria.

O objetivo do uso de mecanismos de filtragem varia enormemente de acordo com a natureza da organização envolvida. Governos geralmente exigem a implementação de mecanismos de filtragem como forma de prevenir atos ilícitos ou de punição desses atos. Empresas o fazem como forma de observar normas de Direito nacional ou como forma de evitar serem chamadas para responder em jurisdições inesperadas. Até mesmo usuários podem optar por usar mecanismos de filtragem com a finalidade de escapar de conteúdos indesejados ou de proteger sua privacidade.

Os mecanismos utilizados também variam muito de acordo com a capacidade técnica ou coercitiva de quem os executa, bem como a eficácia mínima deles exigida. Quaisquer que sejam os meios para filtragem escolhidos, dificilmente terão plena eficiência e uma certa taxa de erros estará sempre presente, podendo até mesmo acarretar efeitos colaterais inesperados ou indesejados. A filtragem pode ser encoberta ou evidente para terceiros.

É importante considerar também que qualquer filtragem deve vir acompanhada de uma base de dados precisa a respeito da informação, destino, origem ou conteúdo que deve ser filtrado. Construir e manter essa base de dados atualizada já exige, por si só, um esforço significativo, na medida em que o volume de informações que permitirão a filtragem pode ser vasto (conforme a amplitude do que se deseja filtrar) e em constante mudança. Os métodos de filtragem aqui abordados levarão em conta um recorte definido dos recursos necessários para a filtragem. Utilizando-se da analogia do carteiro, para que este possa impedir o envio ou recebimento de uma carta, precisará primeiro saber quais endereços estão vetados ou que tipo de pacote não deve ser entregue.

A seguir, são explorados os principais mecanismos de filtragem ou bloqueio utilizados na atualidade[38].

b. Filtragem por localização geográfica

Os filtros de localização geográfica (*geolocation filtering*) são utilizados por provedores de conteúdo que desejam restringir seu site a uma determinada região. Normalmente, a filtragem ocorre por país, podendo, em situações mais complexas, filtrar por cidades ou áreas internas de seu território. Atualmente, há diferentes tecnologias de geolocalização, como geoidentificação - geralmente para adicionar locais a fotos e vídeos - e geobloqueio - empregado usualmente para bloquear conteúdo em diferentes locais. Este estudo não busca analisar a fundo as nuances de cada uma dessas tecnologias, mas sim entender o funcionamento de tecnologias de localização e seu impacto na fragmentação da rede.

A escolha pela localização encontra fundamento, frequentemente, na melhor experiência do usuário, sendo o serviço ou produto projetado para sua localização. Em

38 Os termos filtragem e bloqueio são empregados intercambiavelmente neste trabalho, já que assim também são usados na literatura.

consequência, altera-se, por exemplo, o idioma em que o site é mostrado, muitas vezes com o redirecionamento a um site local (e.g., os sites www.google.com e www.google.com.br).

Devido aos filtros de localização geográfica, sites como o de streaming *Netflix*, por exemplo, disponibilizam catálogos de filmes e séries diferentes para cada país. É devido aos filtros que *Spotify, Apple Music* e *Google Play Music* podem disponibilizar músicas específicas para os usuários de diferentes países. Os aplicativos disponíveis na *App Store* e na *Play Store* também variam de acordo com o país onde se faz a conexão de internet.

Dessa forma, a melhor experiência do usuário é regularmente empregada como prática que permite também a filtragem do conteúdo acessível ao usuário em razão de sua posição geográfica, até porque alguns dos direitos de exibição e reprodução audiovisual dessas obras variam territorialmente, de acordo com as leis de cada país. A filtragem de conteúdo pode ter diversos fundamentos legais: propriedade intelectual, proteção ao consumidor, difamação, censura atrelada a políticas especiais contra discursos de ódio, como divulgação do nazismo, entre outras.

Estando em amplo desenvolvimento no Direito, é importante ressaltar que:

> [...] é difícil saber se as normas fortalecerão ou enfraquecerão a influência regulatória das tecnologias de geolocalização. A sociedade ainda não tomou suficientemente partido para que existam normas claras em relação à sua utilização. No entanto, talvez se possa presumir que a maioria dos usuários irá reagir negativamente à discriminação baseada na localização.[39]

Todavia, iniciativas já podem ser observadas, notadamente a proposta de regulamento acerca do "geobloqueio e outras formas de discriminação baseadas na nacionalidade dos clientes, no local de residência ou no local de estabelecimento no mercado interno"[40], cujo projeto foi aprovado pela Comissão Europeia e pelo Conselho da União Europeia, ao final de novembro de 2016, seguindo para discussão no Parlamento Europeu.[41]

Quanto às tecnologias em si, existem técnicas de geolocalização denominadas sofisticadas e não-sofisticadas. As sofisticadas podem ser classificadas como do cliente ou do servidor. Uma tecnologia de geolocalização do lado do cliente é localizada em seu computador ou dispositivo *wireless*, geralmente empregando o Sistema de Posicionamento Global (GPS, na sigla em inglês) ou pela triangulação das torres de rede próximas. Pelo lado do servidor, traduz-se o número IP por uma localização geográfica.[42] Essas tecnologias alcançam alto grau de precisão.[43]

39 Tradução livre de "[...] *it is difficult to know whether norms will strengthen or weaken the regulatory influence of geo-location technologies. Society has not yet sufficiently clearly taken sides for there to be any clear norms in relation to their use. Nevertheless, it can perhaps be assumed that the majority of users will react negatively to discrimination based on location.*" SVANTESSON, Dan Jerker B. *Private International Law and the Internet.* 3. ed. Holanda: Kluwer Law International, p. 543, 2016.

40 Tradução livre de "(...) geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market". UNIÃO EUROPEIA. Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. Disponível em: <https://goo.gl/u9oh0a>. Acesso em 12 de fevereiro de 2017.

41 CONSELHO DA UNIÃO EUROPEIA. Geo-blocking: Council agrees to remove barriers to e-commerce. Disponível em: <https://goo.gl/FGv0jV>. Acesso em 12 de fevereiro de 2017.

42 Discute-se mais sobre a filtragem pelo endereço IP nos tópicos abaixo.

43 SVANTESSON, Dan Jerker B. *Op.cit.*, p. 523-526.

As tecnologias não-sofisticadas, por outro lado, não proporcionam alta precisão, sendo geralmente compostas por informações trocadas entre um computador e um website ou um servidor que hospeda o website. São exemplos dessas informações as configurações de linguagem, de hora/fuso horário, e de localização, que podem ser requeridas por certos sistemas.[44]

Por depender da aplicação de outros mecanismos de bloqueio, a filtragem por localização geográfica não é em si uma ferramenta de bloqueio, mas um facilitador para o bloqueio, usualmente de conteúdo, em diferentes locais.

c. Filtragem por cabeçalho TCP/IP

Um pacote sob o protocolo TCP/IP consiste de um cabeçalho seguido pelos dados que carrega. Esse cabeçalho contém o IP dos computadores de origem e de destino daquele pacote, i.e., quem o enviou e para quem o enviou.

Para impedir que determinado conteúdo seja acessado, ou que dados de qualquer natureza trafeguem entre duas pontas, o roteador pode ser programado para descartar quaisquer pacotes vindos de ou destinados a um determinado endereço IP. Um bloqueio baseado apenas no IP fará com que qualquer serviço hospedado naquele endereço se torne indisponível para a rede.[45]

Note-se que um site pode ter vários nomes de domínio, mas geralmente estará sediado em apenas um endereço de IP. A filtragem por cabeçalho bloqueará o acesso de usuários a todos os nomes de domínio atribuídos àquele IP.

Uma filtragem mais precisa pode ser feita por meio da filtragem das *portas*, que também estão no cabeçalho. As *portas* diferenciam serviços em um mesmo IP e é comum que diferentes tipos de aplicações usem portas específicas. Para bloquear apenas tráfego na web, por exemplo, pode-se bloquear a porta 80, enquanto a porta 25 é geralmente utilizada para serviços de e-mail SMTP.

Embora não tenhamos acesso às decisões que ordenaram o bloqueio do *WhatsApp* no Brasil, por correrem em sigilo, é provável que o método utilizado pelos provedores de acesso e de *backbone* para impedir o uso do aplicativo por usuários brasileiros tenha envolvido algum nível de filtragem por cabeçalho de TCP/IP.

A filtragem por TCP/IP deve ser conduzida por meio de um provedor de acesso, o que pode resultar em efeitos colaterais indesejados. Constantemente, um provedor de *backbone* atua internacionalmente e uma decisão que obrigue-o a filtrar pacotes de dados de e/ou para um certo número de IP pode ter consequências sobre outras jurisdições. Esse também foi o caso do bloqueio do *WhatsApp* no Brasil, que, em 2015, foi sentido em diversos outros países da América Latina, também servidos por um provedor em comum.[46]

Novamente utilizando da analogia dos correios, a filtragem por cabeçalho é como se ao carteiro fosse entregue uma "lista negra" de endereços impedidos e, no momento da entrega, descartasse apenas cartas e pacotes cujo endereço de origem ou

44 *Idem*, p. 541-542.

45 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering.. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press, 2008. p. 59

46 TUDO CELULAR. *Argentina, Chile e outros países são afetados pelo bloqueio do WhatsApp.* 17 de dezembro de 2015. Disponível em: <https://goo.gl/XuFrgw>. Acesso 17 de fevereiro de 2017.

destino estivessem nessa lista negra, sem lhe interessar o que está dentro de um pacote ou o que está escrito na carta.

A filtragem por endereço de IP pode ser contornada por usuários com algum conhecimento técnico por meio de Redes Virtuais Privadas (VPNs), que direta ou indiretamente funcionam como um intermediário adicional na comunicação entre usuário e site ou aplicação bloqueado. No uso da VPN, um usuário primeiro se conecta a outra rede, geralmente estrangeira, para então se conectar ao site ou aplicação desejada. O provedor encarregado de conduzir a filtragem receberá pacotes endereçados para ou originários do endereço de IP da VPN e não do site/aplicação que deveria bloquear, sendo incapaz, portanto, de saber se o pacote veio ou vai para um dos endereços que deve filtrar. A quantidade de VPNs disponível para o usuário comum é enorme e seu uso não é ilícito, fazendo com que a simples adição do IP da VPN ao rol de endereços vetados seja desproporcional ou mesmo inviável.

d. Filtragem por conteúdo de pacotes

A filtragem cega de qualquer pacote vindo de ou destinado a um determinado endereço é geralmente considerada uma medida excessiva. São raras as situações em que bloquear completamente o tráfego de um site ou aplicação é ideal ou proporcional no combate ao ato ilícito que se deseja sancionar.[47]

Uma espécie de filtragem mais precisa é a filtragem por conteúdo dos pacotes. Além de examinar o cabeçalho para descobrir de onde veio e para onde vai o pacote, um nódulo da rede pode também inspecionar o conteúdo do pacote e a partir de uma configuração pré-definida de conteúdos indesejados, impedir seu trânsito. A filtragem por conteúdo exige infraestrutura mais sofisticada, uma vez que roteadores convencionais não são originalmente programados para fazer essa inspeção.

Uma das formas de filtragem por conteúdo é conhecida como *Deep Packet Inspection* e é utilizada principalmente por governos para vigilância e/ou censura das atividades de seus cidadãos, por meio de sua própria infraestrutura, ou fazendo uso de empresas de segurança. A Agência Nacional de Segurança (NSA, na sigla em inglês) dos Estados Unidos, que se tornou notória após as revelações de Edward Snowden, em 2013, faz uso de *Deep Packet Inspection* para analisar o conteúdo de todo tipo de pacotes que trafegam por aplicações e provedores nos Estados Unidos[48]. Outros governos, como o chinês, também deliberadamente bloqueiam certos pacotes baseados em seu conteúdo por razões políticas e econômicas: a conhecida 'Grande Muralha de Fogo da China', que impede que provedores de conteúdo comuns no Ocidente, como *Google e Facebook*, sejam normalmente inacessíveis em seu território[49].

A filtragem por conteúdo é alvo de críticas duríssimas e é considerada uma violação do direito à privacidade e ao princípio da neutralidade da rede, e que o sigilo dos pacotes de dados que trafegam pela internet não devem ser violados.[50] O Marco Civil da internet proíbe o *Deep Packet Inspection* com a finalidade de filtragem de conteú-

47 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering, *Op. cit.* p. 59

48 DPACKET.ORG. *Deep Security: DISA Beefs up security with Deep Packet Inspection of IP Transmissions.* 30 Out 2008. Disponível em: <https://goo.gl/WjoHYy>. Acesso 05 de fevereiro 2017.

49 EIGN, Ben e EINHORN, Bruce. *The Great Firewall of China.* Business Week. 12 Jan 2006. Disponível em: <https://goo.gl/uoD194>. Acesso 05 de fevereiro 2017.

50 FUCHS, Cristian. Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society. *The Privacy & Security Research Paper Series*, Issue # 1 Uppsala, Centre for Science, Society & Citizenship. 2013.

do sem ordem judicial prévia em seu artigo 7º, incisos III e IV.[51] A inspeção de pacotes para filtragem de conteúdo também contraria princípios do decálogo do Comitê Gestor da internet no Brasil, que, em seus princípios I e VI, prima pela privacidade do usuário e pela manutenção da neutralidade da rede.[52] A Declaração de Princípios de Genebra da Cúpula Mundial para a Sociedade da Informação também reitera a privacidade nas comunicações privadas como um princípio importante para a governança da internet, contribuindo assim para a rejeição da inspeção de pacotes na maioria dos casos.

Deep Packet Inspection e outros tipos de filtragem de conteúdo nem sempre são utilizados a fim de vigilância ou censura. Em alguns casos, podem ser utilizados de forma mais ou menos anonimizada para gerenciamento de tráfego legítimo e *Quality of Service*[53].

e. Rejeição de DNS

Grande parte das comunicações na internet faz uso do Sistema de Nomes de Domínio (DNS, na sigla em inglês) em vez de apenas endereços de IP, especialmente a navegação comum por websites. Por isso, uma forma de se bloquear o acesso a determinados sites ou conteúdos é intervindo no sistema de DNS dos provedores de acesso.[54]

Simplificadamente, quando um usuário digita em seu navegador o endereço URL de um site (e.g. www.google.com), seu computador primeiro envia uma pergunta ao servidor de DNS de seu provedor de acesso (ou outro que o próprio usuário tenha configurado manualmente). O servidor de DNS então verifica qual o número de IP associado àquele URL e o retorna para o usuário, que pode se comunicar diretamente com o site ou aplicação por meio do número de IP.

Assim, é possível que o provedor de acesso filtre a navegação do usuário nesta fase de resolução, retornando ao usuário um número de IP inválido toda vez que certos URLs sejam solicitados. Essa forma de filtragem é relativamente fácil de ser burlada, pois basta que o usuário configure seu computador para acessar um servidor de DNS diferente do padrão utilizado pelo provedor para que volte a navegar normalmente. O servidor DNS da Google, por exemplo, é amplamente utilizado.

Um dos julgados de maior repercussão mundial no que diz respeito a mecanismo de filtragem por DNS é, sem dúvida, o proveniente do caso LICRA v. Yahoo!, de 2000[55]. Com a decisão de um tribunal francês, o Yahoo! foi proibido de anunciar leilões de produtos de memorabilia nazista, vez que tal prática é proibida por lei na França, apesar da alegação de que esses leilões ocorreriam em jurisdição dos Estados Unidos da América, já que os servidores se encontravam em território norte-americano. Todavia, os leilões eram abertos a participantes de qualquer país.

Outra alegação mantida pelo Yahoo! argumentou pela incapacidade técnica de cumprimento do bloqueio, ao que a corte francesa respondeu com a convocação de

51 BRASIL. *Lei nª 12965, 23 de Abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://goo.gl/t93wcy>. Acesso em 05 de Fevereiro de 2017.

52 O decálogo do CGI estabelece em seu princípio primeiro: "*O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.', em seu princípio sexto 'Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento*".

53 O quality of service será explicado posteriormente no tópico 4.

54 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering, *Op. cit.* p. 61

55 FRANÇA. Tribunal de grande instance. *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA v. Yahoo!).*

experts, para que opinassem sobre os mecanismos mais adequados. O método apontado foi o de bloqueio por DNS, que permitiria identificar os usuários franceses. Em vez de protocolar recurso na França, o Yahoo! Inc. ajuizou uma ação nos Estados Unidos, alegando que a decisão da justiça francesa não era válida no território norte-americano por violar a Primeira Emenda da Constituição, que garante o direito à liberdade de expressão. Em decisão da corte superior não revertida pela Suprema Corte, a justiça dos Estados Unidos não firmou jurisdição sobre as partes francesas, e o caso teve forte repercussão contra o Yahoo!.

Outro caso de significativa importância ocorreu em outubro de 2016, quando um ataque distribuído de negação de serviço (*Distributed Denial of Service* - DDoS, na sigla em inglês) atingiu a empresa norte-americana Dyn, impactando o sistema de DNS. Como resultado, milhões de pessoas não obtiveram acesso a vários websites como Twitter, Spotify, Netflix e PayPal, já que o sistema da empresa foi sobrecarregado por pedidos de acesso.[56] Nota-se, por último, que não se sabe ao certo quem e o que motivou o ataque, mas resta o ataque efetuado sobre um serviço basilar da internet pelo provedor de DNS.

4. Neutralidade de rede

Quando se fala em governança da internet, um importante tópico está sempre presente nas discussões: a neutralidade da rede. Trata-se de um princípio que surgiu no início do século XXI, e tem como um de seus principais teóricos o acadêmico norte-americano Tim Wu, professor da Columbia Law School. Segundo o *The Net Neutrality Compendium*:

> A Neutralidade da Rede prescreve que o tráfego de dados na Internet deve ser tratado de maneira não discriminatória, para que os usuários da mesma possam escolher livremente o conteúdo, os aplicativos, os serviços e os dispositivos utilizados, sem ser influenciados por uma disponibilização discriminatória do tráfico de dados na Rede[57].

Segundo os defensores da neutralidade da rede, esse princípio é responsável por fazer com que a internet continue sendo uma rede com arquitetura aberta, em que usuários podem consumir, produzir e compartilhar todo tipo de conteúdo entre eles. A neutralidade da rede preserva, desse modo, a integridade da internet.

Há pelo menos três formas de discriminar um conteúdo ou aplicação na internet: bloqueando, reduzindo sua velocidade ou cobrando preços diferentes de acesso. Para ilustrar essa situação, imagine um país que não protege a neutralidade da rede. Nele, empresas provedoras de acesso têm permissão para fornecer planos de internet com acesso a sites específicos, semelhante ao que ocorre nos canais fechados de televisão, em que usuários compram pacotes com acesso apenas à canais de esportes, de filmes, de culinária ou de notícias, por exemplo. Uma provedora de acesso poderia oferecer um pacote de internet mais barato com acesso aos principais sites do mundo. Porém, sites

56 Esse caso demonstrou ademais as falhas de segurança atualmente exploráveis no chamado "internet of things" ou internet das coisas, que integra objetos como portas, relógios, máquinas de café, etc., à rede. Ver HILTON, Scott. *Dyn Analysis Summary Of Friday October 21 Attack*. Disponível em: <https://goo.gl/jpUjkS>. Acesso em 09 de fevereiro de 2017.

57 Tradução livre de: "*Network neutrality prescribes that Internet traffic shall be treated in a non-discriminatory fashion so that Internet users can freely choose online content, applications, services and devices without being influenced by discriminatory delivery of Internet traffic*". BELLI, Luca; FILIPPI, Primavera De. *The Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*. P. 3. 1ª ed. Suíça: Springer, 2016.

de empresas nascentes na internet, as startups, ou conteúdos relacionados à disseminação de cultura poderiam ficar em um pacote mais caro, o que prejudicaria as jovens empresas, além de impedir o acesso à educação. Além disso, nesse país, o governo teria autoridade para bloquear qualquer tipo de conteúdo que julgasse indesejável para o acesso de sua população.

Existem aqueles que defendem que a neutralidade é prejudicial ao consumidor e à internet. Eles alegam que a neutralidade da rede impede que consumidores escolham e comprem acesso apenas aos sites que de fato desejam, sendo obrigados a pagar por acesso a tipos de conteúdo que raramente, senão nunca, consomem. Somado a isso, os que são contrários à neutralidade da rede alegam que esse princípio prejudica a internet, pois a rede mundial de computadores não possui estrutura para fornecer acesso ilimitado aos seus 3 bilhões de usuários. Caso não exista discriminação de conteúdo, a mesma poderá, em um futuro próximo, entrar em colapso.

Devido às polêmicas intrínsecas ao tema, a neutralidade da rede é alvo de frequente debates nos países que buscam legalizá-la. Países latino-americanos são considerados referência em matéria de governança da internet e proteção ao princípio da neutralidade da rede. Brasil (Marco Civil da Internet - Lei 12.965)[58], Chile (Lei Geral de Telecomunicações - Lei 18.168)[59] e Argentina (Lei Argentina Digital - Ley 27.078)[60] foram pioneiros na proteção desse princípio.

Nos Estados Unidos, a neutralidade da rede é alvo de frequentes debates entre as grandes corporações associadas à internet e setores da sociedade civil. A Comissão Federal de Comunicação Norte Americana (FCC) se posiciona a favor da neutralidade da rede, tendo aprovado, em fevereiro de 2015, T*he FCC's Open Internet Rules*, isto é, As Regras da FCC para Internet Aberta. Esse regulamento apresenta importantes disposições, impedindo o bloqueio, a discriminação e a priorização de conteúdos.

De acordo com *The FCC's Open Internet Rules*, os provedores de acesso não podem bloquear o acesso a conteúdo legal, a aplicativos, a serviços ou a dispositivos que não sejam considerados prejudiciais. Os provedores de acesso não podem prejudicar ou degradar o tráfego legal da internet com base em conteúdo, aplicativos, serviços ou dispositivos não prejudiciais. E os provedores de banda larga não podem favorecer algum tráfego lícito da internet em detrimento de outros tráfegos legais em troca de qualquer tipo de consideração. Entretanto, o Congresso Norte-Americano ainda não legislou acer-

58 "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] IV - preservação e garantia da neutralidade de rede". BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://goo.gl/C7KI9J>. Acesso em 6 de fevereiro de 2017.

59 "Artigo 24 I.- Para a proteção dos direitos dos usuários da internet, o Ministério, por meio da Subsecretaria, sancionará as infrações às obrigações legais ou regulamentos associados à implantação, operação e funcionamento da neutralidade da rede que impeçam, dificultem ou, de qualquer forma, ameacem o desenvolvimento ou o legítimo exercício dos direitos que dela derivam, em que incorram tanto os concessionários de serviço público de telecomunicações que prestam serviço a provedores de acesso a internet, como também estes últimos, em conformidade com o disposto no procedimento contemplado no artigo 28 bis da Lei Nº 18.168, Geral de Telecomunicações." Tradução livre de: "*Artículo 24 I.- Para la protección de los derechos de los usuarios de Internet, el Ministerio, por medio de la Subsecretaria, sancionará las infracciones a las obligaciones legales o reglamentarias asociadas a la implementación, operación y funcionamiento de la neutralidad de red que impidan, dificulten o de cualquier forma amenacen su desarrollo o el legítimo ejercicio de los derechos que de ella derivan, en que incurran tanto los concesionarios de servicio público de telecomunicaciones que presten servicio a proveedores de acceso a Internet como también éstos últimos, de conformidad a lo dispuesto en el procedimiento contemplado en el artículo 28 bis de la Ley N° 18.168, General de Telecomunicaciones.*" CHILE. *Ley 18.168.* Ley General de Telecomunicaciones. Disponível em: <https://goo.gl/ZaDRFY>. Acesso em 06 de fevereiro de 2017.

60 "ARTIGO 56. – Neutralidade da rede. É garantido para cada usuário o direito de acessar, utilizar, enviar, receber ou oferecer qualquer conteúdo, aplicação, serviço ou protocolo através da Internet, sem qualquer restrição, discriminação, distinção, bloqueio, interferência, entorpecimento ou degradação." Tradução livre de: "*ARTÍCULO 56. — Neutralidad de red. Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.*"ARGENTINA. *Ley 27.078.* Ley Argentina Digital. Disponível em: <https://goo.gl/qGzigf>. Acesso em 10 de fevereiro de 2017.

ca do tema, fazendo com que o *The FCC's Open Internet Rules* não tenha eficácia de lei.[61]

Na Europa, em 2015, o Parlamento Europeu aprovou o Regulamento (UE) 2015/2120, que estabelece medidas respeitantes ao acesso à internet aberta[62]. Em seu ponto (1):

> O presente regulamento tem por objetivo estabelecer regras comuns para garantir o tratamento equitativo e não discriminatório do tráfego na prestação de serviços de acesso à Internet e os direitos dos utilizadores finais relacionados com essa prestação. O presente regulamento visa proteger os utilizadores finais e garantir, simultaneamente, o funcionamento contínuo do ecossistema da Internet como motor de inovação. As reformas introduzidas no domínio da itinerância deverão incutir nos utilizadores finais a confiança necessária para permanecerem conectados quando viajarem na União e, com o tempo, deverão impulsionar a convergência dos preços e de outras condições na União[63].

Já em 30 de agosto de 2016, o Organismo de Reguladores Europeus das Comunicações Eletrônicas (BEREC)[64] publicou as Linhas de Orientação às Autoridades Reguladoras Nacionais (ARN)[65], uma diretiva[66] que estabelece regras a serem seguidas para implementação da neutralidade da rede no continente. A Diretiva impõem limitação rígidas à prática do *zero-rating*, além de proibir o gerenciamento de tráfego, exceto quando há necessidade do Quality of Service.[67]

Sendo contra ou a favor desse conceito, é inegável a importância da neutralidade de rede como ferramenta na luta pela manutenção da integridade da internet. Caso esse princípio seja respeitado, Estado e empresas provedoras de acesso não poderão discriminar conteúdo com base em critérios políticos e/ou econômicos.

Para entender o impacto de programas e aplicativos no contexto do fracionamento ou fragmentação do espaço da internet, levando em consideração o princípio da neutralidade da rede, as análises do aplicativo Free Basics e das práticas conhecidas como *zero-rating* e *quality of service* são fundamentais.

61 FEDERAL COMMUNICATIONS COMMISSION. *Open Internet.* Disponível em: <https://goo.gl/sRHoNZ>. Acesso em 06 de fevereiro de 2017.

62 Parlamento Europeu aprova neutralidade da rede e extingue roaming entre países do bloco. *O Globo*, Amsterdã, 03 de abril de 2014. Disponível em: <https://goo.gl/KZOSQD>. Acesso em 10 de fevereiro de 2017.

63 UNIÃO EUROPEIA. Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) nº 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União. P. 1. Jornal Oficial da União Europeia L 310/1, de 26 de novembro de 2015. Disponível em: <https://goo.gl/xloHrF>. Acesso em 10 de fevereiro de 2017.

64 O BEREC é uma agência da União Europeia (UE) que presta serviços de apoio administrativo e profissional ao Organismo de Reguladores Europeus das Comunicações Eletrónicas. O BEREC vela pela aplicação uniforme da legislação relevante da UE, a fim de garantir o correto funcionamento mercado único das comunicações eletrónicas da UE. UNIÃO EUROPEIA. *Gabinete do Organismo de Reguladores Europeus das Comunicações Eletrónicas.* Disponível em: <https://goo.gl/KHwM0p>. Acesso em 10 de fevereiro de 2017.

65 BEREC. *Comunicado de imprensa: O BEREC publica Linhas de Orientação sobre neutralidade de rede (net neutrality)*, de 30 de agosto de 2016. Disponível em: <https://goo.gl/gPL2bb>. Acesso em 10 de fevereiro de 2017.

66 Uma «diretiva» é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo. UNIÃO EUROPEIA. *Regulamentos, diretivas e outros atos legislativos. Disponível em:* <https://goo.gl/WEfbXI>. Acesso em 10 de fevereiro de 2017.

67 BEREC. *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.* Disponível em: <https://goo.gl/jwjwhI>. Acesso em 10 de fevereiro de 2017.

a. Free Basics

O *Free Basics*, inicialmente denominado de *Internet.org*, é um projeto desenvolvido pela rede social Facebook em parceria com as empresas Samsung, Ericsson, MediaTek, Opera Software, Nokia and Qualcomm, que surgiu no ano de 2013. Segundo o site:

> O Free Basics by Facebook fornece às pessoas acesso a serviços úteis em seus celulares, em mercados nos quais o acesso à Internet pode ser mais caro. Os sites estão disponíveis gratuitamente sem cobranças de dados e incluem conteúdo como notícias, empregos, saúde, educação e informações locais. Ao apresentar às pessoas os benefícios da Internet por meio desses sites, esperamos incluir mais pessoas online e ajudar a melhorar suas vidas.[68]

Esse projeto foi desenvolvido com o objetivo de fornecer acesso gratuito à internet para as populações mais carentes do planeta. Para isso, além da infraestrutura usual necessária para acessar a rede mundial de computadores (por exemplo, a fibra ótica), drones também estão sendo utilizados para alcançar as regiões mais inacessíveis.[69] Para utilizar a internet por meio do programa, é fundamental que os usuários possuam um aparelho com wi-fi para baixar o aplicativo Free Basics. Esse aplicativo possui um navegador de internet, com acesso a sites selecionados pelo Facebook e por empresas parceiras.

O modo como o Free Basics funciona polarizou as discussões entre acadêmicos, setores da sociedade civil e governos. Os que discordam do programa alegam que ele fere gravemente o princípio da neutralidade da rede, já que, ao fornecer acesso apenas a sites previamente selecionados, está fragmentando o espaço virtual. Além disso, o Free Basics poderia tanto alienar os novos usuários, já que os mesmos teriam uma visão "parcial" da internet, quanto utilizar os dados dos usuários de forma ilimitada. Entretanto, os que concordam com o programa argumentam que ele evidencia preocupação com setores marginalizados da sociedade, já que pessoas em situação de miséria só poderiam acessar a internet por meio do Free Basics. Somado a isso, seus defensores alegam que o programa funciona como um incentivo, demonstrando os benefícios da internet para aqueles que não estão inclusos no meio virtual.

Até o presente momento, o Free Basics está presente em mais de cinquenta e três países, divididos entre África, América Latina (o Facebook planeja trazer para o Brasil em um futuro próximo[70]), Ásia e Oriente Médio. Entretanto, governos da Índia[71] e do Egito,[72] que inicialmente permitiram o aplicativo em seus territórios, proibiram a utilização do mesmo no ano de 2016.

68 *Free Basics by Facebook*. Disponível em: <https://goo.gl/bcPVMz>. Acesso em 10 de fevereiro de 2017.
69 Mark Zuckerberg anuncia drones para Free Basics. *Soluciones Telcel*, 26 de fevereiro de 2016. Disponível em: <https://goo.gl/QOJ08j>. Acesso em 10 de fevereiro de 2017.
70 Facebook está preparando lançamento do Free Basics no Brasil. *Canaltech*, 14 de abril de 2016. Disponível: <https://goo.gl/vRT9ff>. Acesso em 10 de fevereiro de 2017.
71 GARATTONI, B. Índia proíbe novo serviço do Facebook; veja por que. *Super Interessante*, 22 de fevereiro de 2016. Disponível em: <https://goo.gl/gJwDKY>. Acesso em 10 de fevereiro de 2017.
72 Programa de internet gratuito é proibido no Egito. *O Globo*, Cairo, 30 de dezembro de 2015. Disponível em: <https://goo.gl/xSBTrB>. Acesso em 10 de fevereiro de 2017.

b. Zero-rating

A prática do *zero-rating* também pode ser considerada uma ameaça à integridade da internet. Segundo o BEREC:

> Zero-rating é quando um ISP [provedor de acesso à internet] aplica um preço zero ao tráfego de dados associado a um aplicativo ou classe particular de aplicativos (e os dados não contam para qualquer limite de dados no serviço de acesso à Internet)[73].

Para exemplificar essa prática, imagine uma empresa provedora de acesso à internet, que fornece, por exemplo, acesso grátis ao aplicativo de mensagens WhatsApp, mas cobra pelo acesso aos aplicativos semelhantes concorrentes, como Telegram ou WeChat. Essa situação, além de representar concorrência desleal, também fragmenta a internet, ao induzir o usuário a utilizar determinado aplicativo somente por este não cobrar da franquia de internet.

Na América Latina, Brasil, Argentina e Chile destacam-se na luta para coibir o *zero-rating*. No Brasil, o Decreto nº 8.771, em seus artigos 9º e 10, apresenta disposições que proíbem expressamente essa prática[74]. Já a Argentina (Lei Argentina Digital)[75] e o Chile (Lei Geral de Telecomunicações)[76] proíbem, de forma indireta o zero-rating.

---

73 Tradução livre de: "'*Zero-rating' is when an ISP applies a price of zero to the data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service).*" BEREC. *What is zero-rating?* Disponível em: <https://goo.gl/4MAvqd>. Acesso em 13 de fevereiro de 2017.

74 "Art. 9º Ficam vedadas condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que: I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País; II - priorizem pacotes de dados em razão de arranjos comerciais; ou III - privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico. Art. 10. As ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória". BRASIL. *Decreto Nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <https://goo.gl/5Dikve>. Acesso em 13 de fevereiro de 2017.

75 "ARTIGO 57. - *Neutralidade da rede. Proibições.* Os prestadores de Serviços de TIC [Tecnologia da informação e conteúdo] não poderão: a) Bloquear, interferir, discriminar, entorpecer, degradar ou restringir a utilização, envio, recebimento, oferecimento ou acesso a qualquer conteúdo, aplicação, serviço ou protocolo, salvo ordem judicial ou expressa solicitação do usuário". Tradução livre de: "ARTÍCULO 57. - *Neutralidad de red. Prohibiciones*. Los prestadores de Servicios de TIC no podrán: a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario." ARGENTINA. *Ley 27.078*. Ley Argentina Digital. Disponível em: <https://goo.gl/qGzigf>. Acesso em 10 de fevereiro de 2017.

76 "Artigo 24 H.- Às concessionárias de serviços público de telecomunicações que prestam serviço aos provedores de acesso a Internet e também estes últimos; entendida como tal, toda pessoa natural ou jurídica que preste serviços comerciais de conectividade entre os usuários ou as suas redes e da Internet: a) Não podem arbitrariamente bloquear, interferir, discriminar, impedir ou restringir o direito de qualquer usuário da Internet para utilizar, enviar, receber ou oferecer qualquer conteúdo, aplicação ou serviço legal através da Internet, assim como qualquer outro tipo de atividade ou uso legal realizado através da rede. A este respeito, deverão oferecer a cada usuário um serviço de acesso a Internet ou de conectividade ao provedor de acesso à Internet, segundo corresponda, que não distinga arbitrariamente conteúdos, aplicações ou serviços, baseados na fonte de origem ou propriedade destes, havendo em conta as distintas configurações de conexão a Internet segundo o contrato vigente com os usuários." Tradução livre de: "*Artículo 24 H.- Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos; entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet: a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios*". CHILE. *Ley 18.168.* Ley General de Telecomunicaciones. Disponível em: <https://goo.gl/ZaDRFY>. Acesso em 06 de fevereiro de 2017.

Além dos países latino-americanos, Índia e Europa têm trabalhado para proibir o *zero-rating*. O país asiático proibiu, por meio de sua agência de telecomunicações (*Telecom Regulatory Authority of India*), a discriminação tarifária com base em conteúdos acessados pelos usuários[77]. No continente europeu, o BEREC apresentou, em suas Linhas de Orientação publicadas no ano de 2016, diretivas que restringem a prática do zero-rating[78]. Entretanto, o documento permite interpretações diversas ao argumentar que há diferentes tipos de *zero-rating*, devendo as autoridades nacionais avaliar se ele mesmo prejudica o consumidor e o ecossistema de inovação da internet.[79]

É importante salientar, por fim, que o zero-rating não se confunde com o *quality of service*. O primeiro diz respeito a uma discriminação tarifária entre aplicativos semelhantes, ao passo que o segundo diz respeito a uma discriminação de dados entre aplicativos de classes distintas.

c. Quality of service

O *quality of service*, ou *qualidade de serviço*, é uma forma de discriminação de dados utilizada por provedores de acesso. O *qualidade de serviço* discrimina dados de pacotes com conteúdos diferentes, em benefício do melhor funcionamento da internet para o usuário.

Imagine a hipótese em que um usuário está assistindo um filme na Netflix em sua Smart TV e outro usuário, da mesma residência (portanto, mesmo IP), está enviando e-mail utilizando seu celular. Considerando essa situação, o filme deve ter uma prioridade sobre o e-mail, pois um atraso de dez ou doze segundos no recebimento deste não é algo ruim para o usuário, já que um e-mail não é uma mensagem com caráter de urgência. Entretanto, um atraso de dez ou doze segundos na reprodução do filme é algo que certamente irá frustrar o usuário.

Provedores de acesso priorizam os dados do filme em benefício dos dados do e-mail, para que haja um serviço com maior qualidade. Essa prática não é considerada ruim, já que mantém o bom funcionamento da internet.

No Brasil, o Marco Civil da Internet (Lei 12.965)[80] e o Decreto Nº 8.771[81] preocu-

77 SANTOS, Vinicius W.O. Como a Índia baniu o zero rating. *Observatório da Internet no Brasil,* 11 de fevereiro de 2016. Disponível em: <https://goo.gl/Go1wBE>. Acesso em 13 de fevereiro de 2017.

78 "Uma oferta de zero rating onde todas as aplicações são bloqueadas (ou têm velocidade reduzida) quando atingido o limite de dados com exceção da aplicação em zero rating infringe o Artigo 3(3) primeiro (e terceiro) sub parágrafos (ver parágrafo 55)". Tradução livre de: "41. *A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe Article 3(3) first (and third) subparagraph (see paragraph 55)*". BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. P. 11. Disponível em: <https://goo.gl/jwjwhI>. Acesso em 10 de fevereiro de 2017.

79 BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. p. 11-12. Disponível em: <https://goo.gl/jwjwhI>. Acesso em 10 de fevereiro de 2017.

80 Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de: I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações. BRASIL. *Lei 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://goo.gl/C7KI9J>. Acesso em 16 de fevereiro de 2017.

81 Art. 4º A discriminação ou a degradação de tráfego são medidas excepcionais, na medida em que somente poderão decorrer de requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações ou da priorização de serviços de emergência, sendo necessário o cumprimento de todos os requisitos dispostos no art. 9º, § 2º, da Lei nº 12.965, de 2014. BRASIL. *Decreto Nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <https://goo.gl/5Dikve>. Acesso em 16 de fevereiro de 2017.

param-se em não proibir o *quality of service*. É importante salientar que a lei brasileira entende o *quality of service* como uma prática de exceção, ou seja, para situações excepcionais, em que exista tráfego intenso na rede. Entretanto, a tendência, para o futuro, é que esta prática seja utilizada com maior frequência, pois 50% das residências brasileiras já possuem acesso à internet[82]. Com maior número de usuários com integrados à rede mundial de computadores no país, faz-se essencial práticas que otimizem a navegação, além de necessárias melhorias na estrutura física da internet.

5. Internet e Estados

Assim como não há governo global, também não existe um tribunal internacional para a internet, dedicado a resolver controvérsias advindas da rede, ou uma convenção a respeito da governança da internet. A resolução pacífica de controvérsias que têm natureza nas relações da internet apresenta, pois, grandes desafios aos Estados. Em busca de soluções, muitas vezes são empregados métodos alternativos de resolução de conflitos, ou mecanismos extrajudiciais.[83] Quando acionado o Poder Judiciário, percebe-se que novas regras são criadas, especiais ao contexto online. Ainda assim, também é comum a reformulação de normas que, ainda que precedentes às novas tecnologias, podem ser transplantadas, caso averiguado que são adequadas - geralmente, essas normas tratam de situações jurídicas que existem tanto no mundo offline quanto no online, como e.g. um contrato de compra e venda.

Para mais, uma das principais características da internet é a sua interoperabilidade, nomeadamente as funções estruturais que permitem a conectividade e operabilidade de redes e aparelhos distintos. Essa característica, porém, não pode ser considerada resultante dos esforços de Estados. Ainda que os países de fato estabeleçam regras e princípios para a regulação da internet, a interoperatividade é aspecto estrutural e fundamental para a funcionalidade na internet. Em qualquer lugar do mundo, protocolos como TCP/IP ou padrões como HTML, por exemplo, funcionam da mesma forma, garantindo interconectividade e padronização aos usuários e mantenedores da rede. A ausência de interoperatividade, portanto, leva à ausência de interconectividade, que, em seu turno, afeta a capacidade de criar conexões de variados tipos - conexões que são responsáveis por fazer a internet funcionar como tal.

A noção de interoperabilidade jurídica desponta como um possível meio para solucionar conflitos da rede e harmonizar os regimes jurídicos em diferentes territórios nacionais, evitando assim maior fragmentação da internet. O termo tem origem recente em face da expansão da internet e dos desafios que esta impõe aos ordenamentos jurídicos. Representa, contudo, uma ideia antiga: a da cooperação entre diferentes jurisdições, tornando as regras jurídicas mais harmônicas a fim de facilitar a comunicação a nível global, estimular inovação e reduzir custos em operações transfronteiriças.[84]

No âmbito procedimental, interoperabilidade jurídica pode ser desenvolvida com o emprego de participação multisetorial (*multi-stakeholder participation*) e aumento da transparência pública. Outro modo de alcançar a interoperabilidade se dá por meio

82 GOMES, Helton Simões. Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE. *G1*, São Paulo, 06 de abril de 2016. Disponível em: <https://goo.gl/SZZpcJ>. Acesso em 16 de fevereiro de 2017.

83 BYGRAVE, Lee A. e MICHAELSEN, Terje. Governors of internet. *In*: BYGRAVE, L. A.; BING, J. (eds.). *Internet Governance*: *Infrastructure and Institutions.* Oxford: Oxford University Press, 2009, p. 92–93.

84 WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. *Global Commission on Internet Governance,* Paper Series: No. 4, Dez 2014, p. 5-6. Disponível em: <https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf>. Acesso em: 27/01/2017.

do Direito Internacional Privado, que estipula regras sobre conflitos de leis - ou seja, qual a lei aplicável ao caso concreto. Todavia, as regras providas pelo Direito Internacional Privado não indicam a resposta ao caso - a solução almejada pelas partes - mas apenas apontam a lei aplicável, consistindo, então, de influência indireta na interoperabilidade jurídica.[85]

Quanto ao âmbito material, pode-se citar a Diretiva 2000/31/EC, que trata sobre o comércio eletrônico no mercado único digital europeu.[86] Outro exemplo de documento que harmoniza regras materiais é a Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, do Conselho da Europa.[87] No resto do mundo, a interoperabilidade jurídica ainda se apresenta incipiente em matéria de internet, mas é possível mencionar a União Internacional de Telecomunicações (UIT), a *Internet Engineering Task Force* e a *World Wide Web Consortium* como importantes centros de harmonização e padronização de regras.[88]

De maneira geral, Estados podem agir causando fragmentação da internet de diversas maneiras, que foram exploradas ao longo deste estudo. Seus motivos são ainda mais diversos e podem até mesmo estar fundamentados em segurança e interesse nacional, que frequentemente representam razões pelas quais Estados podem agir sem transparência pública. Sendo assim, a implantação de mecanismos de bloqueio pode passar despercebida à população em geral - mesmo em face do direito fundamental à liberdade de expressão, assentado em diversos tratados internacionais e constituições nacionais, mais notadamente o artigo 19 da Declaração Universal dos Direitos Humanos.[89]

De resto, percebe-se que a criação de "fronteiras" na internet surgiu primeiro de forma *bottom-up*,[90] já que partiu da iniciativa de usuários em busca de melhor experiência, baseada na localização geográfica. No entanto, os países passaram a exercer, de maneira *top-down*,[91] influência sobre o controle das comunicações com o exterior.[92] Assim, a tendência recente tem sido o aumento de limites territoriais na internet, o que importa no perigo de fragmentação da rede.

6. Considerações Finais

O controle da internet ganhou importância proporcional a sua expansão e adquiriu novos contextos no mundo globalizado. Neste trabalho, abordamos as principais formas de bloqueio empregadas na atualidade, que são colocadas em prática por autoridades governamentais, entidades privadas ou pessoas físicas com distintas finalidades. Para entender essas formas de bloqueio e o crescente ciberativismo contrários

85 WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. *Op.cit.*, p. 6.

86 UNIÃO EUROPEIA. *Diretiva 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 informação, em especial do comércio eletrônico, no mercado interno (Directiva sobre o comércio eletrônico). *Jornal Oficial das Comunidades Europeias*, L 178, 17 de Julho de 2000, p. 1–16. Disponível em: <https://goo.gl/4NWod4> . Acesso em: 11/02/2017.

87 CONSELHO DA EUROPA. *Convenção sobre o Cibercrime*. Budapeste, Nov 2001.

88 WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation.*Op.cit.*, p. 7-8.

89 "Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e idéias por qualquer meio de expressão." ONU. *Declaração Universal dos Direitos Humanos.* Disponível em: <https://goo.gl/ooOzZR>. Acesso em: 19/02/2017.

90 De maneira geral, entende-se por *bottom-up* os processos ou mecanismos que partes dos níveis inferiores para atingir os mais superiores, por exemplo, como em uma iniciativa de determinada população que apresenta proposta aos governantes.

91 Simplificadamente, *top-down* detém o sentido inverso de *bottom-up*, ou seja, diz respeito a práticas que partem dos níveis mais altos e sofisticados, como governos e organizações internacionais.

92 GOLDSMITH, Jack e WU, Tim. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press, 2006, p. 49-50.

a elas, a análise do conceito de neutralidade da rede, assim como feita neste trabalho, é fundamental. Além disso, procuramos entender o uso de tecnologias de geolocalização, que cresce abruptamente, seja em razão da melhor personalização da experiência do usuário, tornando o conteúdo mais adaptado ao seu local de acesso, seja em decorrência de tentativas de controlar o conteúdo presente na internet.

Paralelamente ao desenvolvimento da internet, os ordenamentos jurídicos esforçam-se para regular o uso das novas tecnologias. A adoção de mecanismos razoáveis e proporcionais, que respeitam os direitos humanos e as características essenciais da rede, particularmente no que tange aos riscos de sua fragmentação, é imperativa para o funcionamento regular e a expansão da internet no mundo. Afinal, o Direito busca proteger contra casos excepcionais, mas o deve fazer sem generalizar as soluções para além da incidência que o justifique. Isto é, não se deve trivializar práticas abusivas.

Além do ciberativismo contra a fragmentação da internet e do desenvolvimento dos ordenamentos jurídicos de cada Estado, surgem os grupos que desejam moldar a internet à sua vontade. Esses grupos, normalmente ligados a multinacionais provedoras de acesso e conteúdo, procuram, por meio da fragmentação da internet, maximizar seus lucros e influência junto a cada usuário. Comumente, essa maximização do lucro está associada a serviços deficientes. Portanto, é necessário que todos os setores que integram a internet entendam minimamente sobre seu funcionamento, para que possam defender seus próprios interesses e lutar pelos seus direitos.

7. Referências

a. Livros, artigos e teses

BELLI, Luca; DE FILIPPI, Primavera De. *The Net Neutrality Compendium*: Human Rights, Free Competition and the Future of the Internet. 1ª ed. Suíça: Springer, 2016.

BYGRAVE, Lee A. e MICHAELSEN, Terje. Governors of internet. In: BYGRAVE, L. A.; BING, J. (eds.). *Internet Governance: Infrastructure and Institutions*. Oxford: Oxford University Press, 2009.

GOLDSMITH, Jack e WU, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford: Oxford University Press, 2006.

LESSIG, Lawrence. Code v2.0. Nova Iorque: Basic Books, 2006.

SVANTESSON, Dan Jerker B. *Private International Law and the Internet.* 3ª ed. Holanda: Kluwer Law International, 2016.

ALVES, Sergio, Jr., The Internet Balkanization Discourse Backfires, SSRN Electronic Journal. Disponível em: <https://ssrn.com/abstract=2498753> Acesso em 17/02/2017.

FARIS, Robert, VILLENEUVE, Nart, Measuring Global Internet Filtering. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering,* Cambridge: MIT Press, 2008

HILL, Jonah Force. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs*. 2012

LEE, Jyh-An e LIU, Ching-Yi, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science, and Technology*, Vol. 13, No. 1, 2012.

LEE, Jyh-An, LIU, Ching-Yi, LI, Weiping, Searching for Internet Freedom in China: A Case Study on Google's China Experience. *Cardozo Arts & Entertainment Law Journal*, Vol. 31, No. 2, 2013. Disponível em: <https://ssrn.com/abstract=2243205> Acesso em 07/02/2017.

LEONARDI, Marcel. Controle de conteúdos na Internet: filtros, censura, bloqueio e tutela. In: *Âmbito Jurídico*, Rio Grande, XII, n. 67, ago 2009. Disponível em: <https://goo.gl/rndS2V>. Acesso em 30 de janeiro 2017.

MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering.. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press, 2008.

WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. *Global Commission on Internet Governance*, Paper Series: No. 4, Dez 2014. Disponível em: <https://goo.gl/QAT6RT>. Acesso em: 27/01/2017.

b. Legislação e outros materiais de referência

ARGENTINA. *Ley 27.078.* Ley Argentina Digital. Disponível em: <https://goo.gl/qGzigf>. Acesso em 10 de fevereiro de 2017.

BEREC. *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.* Disponível em: <https://goo.gl/jwjwhI>. Acesso em 10 de fevereiro de 2017.

_____. *Comunicado de imprensa: O BEREC publica Linhas de Orientação sobre neutralidade de rede (net neutrality)*, de 30 de agosto de 2016. Disponível em: <https://goo.gl/gPL2bb>. Acesso em 10 de fevereiro de 2017.

_____. *What is zero-rating?* Disponível em: <https://goo.gl/4MAvqd>. Acesso em 13 de fevereiro de 2017.

_____. *Decreto Nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e

proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <https://goo.gl/5Dikve>. Acesso em 13 de fevereiro de 2017.

_____. *Lei 12.965, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://goo.gl/C7KI9J>. Acesso em 6 de fevereiro de 2017.

CHILE. *Ley 18.168.* Ley General de Telecomunicaciones. Disponível em: <https://goo.gl/ZaDRFY>. Acesso em 06 de fevereiro de 2017.

CONSELHO DA EUROPA. *Convenção sobre o Cibercrime.* Budapeste, Nov 2001.

CONSELHO DA UNIÃO EUROPEIA. *Geo-blocking: Council agrees to remove barriers to e-commerce.* Disponível em: <https://goo.gl/FGv0jV>. Acesso em: 12/02/2017.

Facebook está preparando lançamento do Free Basics no Brasil. *Canaltech*, 14 de abril de 2016. Disponível: <https://goo.gl/vRT9ff>. Acesso em 10 de fevereiro de 2017.

Federal Communications Commission. Open Internet. Disponível em: <https://goo.gl/sRHoNZ>. Acesso em 06 de fevereiro de 2017.

Free Basics by Facebook. Disponível em: <https://goo.gl/bcPVMz>. Acesso em 10 de fevereiro de 2017.

GARATTONI, B. Índia proíbe novo serviço do Facebook; veja por que. *Super Interessante*, 22 de fevereiro de 2016. Disponível em: <https://goo.gl/gJwDKY>. Acesso em 10 de fevereiro de 2017.

GOMES, Helton Simões. Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE. *G1*, São Paulo, 06 de abril de 2016. Disponível em: <https://goo.gl/SZZp-cJ>. Acesso em 16 de fevereiro de 2017.

Mark Zuckerberg anuncia drones para Free Basics. *Soluciones Telcel*, 26 de fevereiro de 2016. Disponível em: <https://goo.gl/QOJ08j>. Acesso em 10 de fevereiro de 2017.

ONU. *Declaração Universal dos Direitos Humanos.* Disponível em: <https://goo.gl/ooOzZR>. Acesso em: 19/02/2017.

Parlamento Europeu aprova neutralidade da rede e extingue roaming entre países do bloco. *O Globo*, Amsterdã, 03 de abril de 2014. Disponível em: <https://goo.gl/KZOSQD>. Acesso em 10 de fevereiro de 2017.

Programa de internet gratuito é proibido no Egito. *O Globo*, Cairo, 30 de dezembro de 2015. Disponível em: <https://goo.gl/xSBTrB>. Acesso em 10 de fevereiro de 2017.

SANTOS, Vinicius W.O. Como a Índia baniu o zero rating. *Observatório da Internet no Brasil,* 11 de fevereiro de 2016. Disponível em: <https://goo.gl/Go1wBE>. Acesso em 13 de fevereiro de 2017.

UNIÃO EUROPEIA. Diretiva 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 informação, em especial do comércio eletrônico, no mercado interno (Directiva sobre o comércio eletrônico). *Jornal Oficial das Comunidades Europeias*, L 178, 17 de Julho de 2000, p. 1–16. Disponível em: <https://goo.gl/4NWod4>. Acesso em: 11/02/2017.

_____. Gabinete do Organismo de Reguladores Europeus das Comunicações Eletrónicas. Disponível em: <https://goo.gl/KHwM0p>. Acesso em 10 de fevereiro de 2017.

_____. Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. Disponível em: <https://goo.gl/u9oh0a>. Acesso em 12/02/2017.

_____. *Regulamentos, diretivas e outros atos legislativos.* Disponível em: <https://goo.gl/WEfbXI>. Acesso em 10 de fevereiro de 2017.

_____. Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) nº 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União. *Jornal Oficial da União Europeia L 310/1*, de 26 de novembro de 2015. Disponível em: <https://goo.gl/xloHrF>. Acesso em 10 de fevereiro de 2017.