FERRAMENTAS AUXILIARES PARA MEDIÇÃO DA NEUTRALIDADE DA REDE PELOS USUÁRIOS

NATHALIA SAUTCHUK PATRÍCIO

INTRODUÇÃO

Uma rede neutra é aquela em que não há o favorecimento de uma aplicação em detrimento de outra (WU, 2013). A neutralidade da rede pode ser melhor definida como um princípio de projeto de redes. A ideia é a de que uma rede de informação pública útil aspira tratar todos os conteúdos, *sites* e plataformas de forma igual (WU, [s.d.]). Isso significa, por exemplo, que um pacote transportando conteúdos de uma ligação por voz não pode ser transmitido mais lentamente que um pacote de mesmo tamanho contendo informações de um *e-mail*. Nos estudos de redes de computadores, a neutralidade tem por ancestral o princípio fim a fim. Segundo Kurose e Ross (2013) esse princípio afirma que, visto ser dado certo que certas funcionalidades – detecção de erro, por exemplo – devem ser executadas fim a fim, funções colocadas nos camadas mais baixas da Internet podem ser redundantes ou adicionar pouco valor em comparação ao custo de implementá-las em uma camada mais alta. Ou seja, em uma rede de uso geral, como a Internet, funções específicas das aplicações devem estar nos dispositivos terminais da rede ao invés de nos nós intermediários, como roteadores e repetidores (WU, [s.d.]).

Dentre os temas debatidos no campo da governança da Internet, o conceito de neutralidade da rede tem causado polêmica no Brasil e em outros países e por isso tem cada vez mais atraído a atenção da opinião pública internacional. De um lado, provedores de conteúdo e comunidade técnica defendem o modelo de neutralidade, de outro lado, empresas de telecomunicações vislumbram formas de maximizar seus lucros por meio da cobrança de vias rápidas – *fast lanes*, em inglês – para o tráfego de dados, ou por meio de outros artifícios que beneficiam ou prejudicam certo tipo, origem ou destino de tráfego de dados em detrimento dos demais.

Apesar desse cenário de disputa, a Lei nº 12.965, conhecida como Marco Civil da Internet, está em vigor desde 2014 e garante no Brasil a neutralidade da rede na Internet (BRASIL. Lei 12.965, 2014, Art. 3º, IV). Estão previstos alguns casos em que a discriminação e a degradação de tráfego podem ser executadas pelo provedor de conexão a Internet, porém estes são tratados como uma exceção.

De acordo com Ramneek *et al*. (2015), uma lei aceitável para a neutralidade da rede deve ser uma combinação objetiva de aspectos políticos e técnicos, enquanto leva em consideração o mínimo de requisitos de qualidade de experiência do usuário final. Dentro desse contexto, duas questões são relevantes para este artigo:

I. como fiscalizar ou verificar tecnicamente se a neutralidade da rede tem sido cumprida pelos provedores;

II. a ocorrência de discriminação de tráfego apenas nos casos previstos pelo Marco Civil da Internet.

Se no Brasil não há estudos publicados relativos a esse tema, em outros países a questão da medição da neutralidade da rede é tratada de maneira parcial e fragmentada por meio de um conjunto de iniciativas não coordenadas entre si.

Esse texto está estruturado em quatro seções. Na primeira seção é apresentada um pouco da discussão sobre a neutralidade da rede, inclusive no contexto do Marco Civil da Internet. A segunda seção é dedicada às métricas de rede enquanto a terceira seção apresenta algumas ferramentas que se propõem a medir a neutralidade da rede. Por fim, na seção quatro são apresentadas algumas considerações sobre os desafios para fiscalizar tecnicamente a neutralidade da rede de acordo com o Marco Civil da Internet.

NEUTRALIDADE DA REDE NO CONTEXTO DO MARCO CIVIL DA INTERNET

A neutralidade da rede é um tema que tem sido debatido desde o início dos anos 2000 e continua envolto em muita polêmica. Existem diversas definições para ela, sendo uma dentre elas:

> A neutralidade é um princípio que está no cerne do funcionamento da Internet e estabelece tratamento isonômico ao tráfego de pacotes de dados na Internet, não fazendo distinção de acordo com conteúdo, origem e destino, serviço, terminal ou aplicação, sendo que a Internet apenas transportará os pacotes de dados, deixando para o usuário final as decisões em relação ao tipo de uso que fará e aos dados que acessará. (SANTOS, 2016)

De acordo com Santos (2016), para muitos autores que estudam o assunto, uma Internet neutra garante um ambiente propício às inovações tecnológicas, protege a liberdade de expressão, fomenta oportunidades de desenvolvimento socioeconômico além de facilitar a difusão e compartilhamento de bens culturais.

Porém, a manutenção de uma Internet neutra não é algo simples, uma vez que nesse ecossistema há diversos atores com diferentes interesses em relação ao funcionamento rede.

Ramos (2015) coloca que, no caso dos provedores de conexão a Internet, ao serem impedidos de discriminar conteúdos e aplicações, eles perdem um instrumento de controle de suas redes, o que pode levar a redução de lucros e diminuição do potencial de eficiência de suas redes. Essas perdas podem levar à redução de incentivos para inovação na infraestrutura de telecomunicações e à redução na geração de empregos do setor.

Já para os grandes provedores de aplicações a neutralidade da rede tem um papel dúbio. Com a garantia da neutralidade, eles não precisam negociar condições especiais para o tráfego de seus conteúdos com os provedores de conexão, e assim poderiam investir mais recursos em inovação e geração de empregos. Por outro, a proibição de acordos para priorização de tráfego reduz os instrumentos disponíveis para que eles mantenham sua hegemonia, tendo em vista que pequenos provedores terão condições de oferta semelhantes (RAMOS, 2015).

Segundo Ramos (2015) os pequenos provedores de aplicações são beneficiados pela neutralidade da rede, uma vez que, com o tráfego de seus conteúdos sendo tratados da mesma forma que o dos grandes, há uma redução nas barreiras de entrada no mercado. Eles não vão precisar negociar com provedores de conexão para terem uma oferta de qualidade de seus aplicativos, e a maior diversidade de iniciativas levará a um aumento na inovação como um todo.

Os usuários também se beneficiam com a neutralidade da rede, pois terão acesso a conteúdos mais diversificados, impedindo efeitos de filtro de conteúdo que são hoje aplicados pelos grandes provedores de aplicações. Há um ganho na capacidade de autonomia, já que usuários terão maiores incentivos para também se tornarem provedores de aplicação, bem como ganhos expressivos no campo da liberdade de expressão, uma vez que a neutralidade da rede impediria que provedores de conexão criem bloqueios de conteúdo. Por outro lado, há uma potencial consequência negativa que

é o aumento de custos de acesso para *heavy users*[1] de aplicações específicas (RAMOS, 2015).

Segundo Ramos (2015) um provedor de conexão a Internet pode discriminar um conteúdo ou uma aplicação específica na Internet, violando a neutralidade da rede através da:

- restrição completa de acesso a determinadas aplicações;
- redução da velocidade de acesso a determinadas aplicações ou classe de aplicações;
- aumento da velocidade de acesso a determinadas aplicações específicas;
- cobrança de tarifas adicionais para acesso a determinadas aplicações ou classe de aplicações; e
- redução de tarifas para acesso a determinadas aplicações.

No contexto do Marco Civil da Internet, o artigo 9º diz que "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". Apenas há a previsão de discriminação ou degradação do tráfego em casos de requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e priorização de serviços de emergência (BRASIL. Lei 12.965, 2014, Art. 9º, § 1º).

A questão da neutralidade da rede foi regulamentada pelo artigo 5º do Decreto 8.771 (BRASIL, 2016), no qual foram explicitados os requisitos técnicos indispensáveis à prestação adequada dos serviços, sendo aqueles decorrentes de:

I. tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa – *spam* – e controle de ataques de negação de serviço;

II. tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência.

1 Algumas empresas de conexão à Internet usam o termo *heavy users* com a intenção de distinguir usuários com "uso aceitável" de banda e outros que fazem um alto uso e, de certa forma, indevido. Esse termo tem sido usado como justificativa para diversas restrições, como a implementação de franquia de dados e *traffic shaping*.

MÉTRICAS DE REDE

Existem diversas métricas que são usadas para mensurar o desempenho de uma rede de computadores, incluindo a Internet. Essas métricas podem ser exploradas para ajudar as autoridades competentes e aos usuários finais na fiscalização da neutralidade da rede de acordo com o Marco Civil da Internet.

Uma das principais métricas é a vazão – em inglês, *throughput* –, podendo ser de dois tipos: instantânea e média. Segundo Kurose e Ross (2013) a vazão instantânea é a taxa – em *bits/s* – em que um dispositivo está recebendo um arquivo em um determinado momento. Já a vazão média consiste na quantidade de *bits* que foram transferidos em uma unidade de tempo. Por exemplo, se o arquivo consistir em F *bits* e a transferência levar T segundos para o dispositivo receber todos os F *bits*, então a vazão média da transferência do arquivo é F/T bits/s (KUROSE e ROSS, 2013). Quando se fala especificamente no protocolo TCP[2] (KUROSE; ROSS, 2013), a RFC[3] 6349 define vazão como a quantidade de dados por unidade de tempo que o TCP transporta quando está em estado de equilíbrio (IETF, 2001).

Existe uma outra métrica similar a vazão, conhecida como *goodput*. Segundo Tanenbaum e Wetherall (2011), *goodput* é a taxa em que pacotes úteis são entregues pela rede. Na RFC 2647, *goodput* é definido como o número de *bits* por unidade de tempo encaminhados para a interface correta de destino de um dispositivo conectado à rede, menos os *bits* perdidos ou retransmitidos (IETF, 1999). Comparando-se *throughput* e *goodput*, pode-se dizer que essas métricas se diferem uma vez que o *goodput* não leva em conta os dados dos protocolos, como os cabeçalhos e a retransmissão de pacotes, enquanto o *throughput* considera tudo isso em sua medição.

Outras duas métricas relevantes para redes em geral são o atraso – ou latência – e a variação de atraso – *jitter*. De acordo com Kurose e Ross (2013), o atraso fim a fim é o acúmulo de atrasos de processamento, transmissão e de formação de filas nos roteadores; atrasos de propagação nos enlaces e atrasos de processamento em sistemas finais. O atraso ou a latência de uma rede é geralmente variável e depende basicamente das condições de carga dos diversos segmentos envolvidos (CARISSIMI *et al.*,

2 TCP (Transmission Control Protocol) é o protocolo encarregado do transporte dos pacotes de dados pelas diferentes rotas da Internet.

3 Um RFC (Request For Comments) pode ser um documento de padronização da Internet, um documento informativo ou um documento de boas práticas. Ele é desenvolvido no âmbito do Internet Engineering Task Force (IETF).

2009). Um componente crucial do atraso fim a fim são os atrasos variáveis de fila que os pacotes sofrem nos roteadores. Por isso, o tempo decorrido entre o momento em que um pacote é gerado na fonte e o momento em que é recebido no destinatário pode variar de pacote para pacote, o que é denominado de variação de atraso (KUROSE; ROSS, 2013).

Outro aspecto importante em uma rede é a questão da perda de pacotes. Kurose e Ross (2013) afirmam que, do ponto de vista de um sistema final, a perda de pacote é vista como um pacote que foi transmitido para o núcleo da rede, mas sem nunca ter emergido dele no destino. As filas dos roteadores são finitas e, portanto, podem estar cheias em um determinado instante de tempo. Se um pacote chegar nessas condições, o roteador o descartará por não ter espaço em memória para armazená-lo. Quanto maior for a intensidade de tráfego, maior será a fração de pacotes perdidos pelo descarte. Sendo assim, o desempenho em um nó da rede não é medido apenas em termos de atraso, mas também da probabilidade de perda de pacotes (KUROSE; ROSS, 2013).

Por fim, outras duas métricas que podem ajudar na análise de uma rede são o tempo de viagem de ida e volta – em inglês *round-trip time* (RTT) – e a taxa de entrega média – em inglês, *packet delivery ratio*. De acordo com Kurose e Ross (2013) o RTT é o tempo que leva para um pequeno pacote viajar do cliente ao servidor e de volta ao cliente, incluindo atrasos de propagação de pacotes, de fila de pacotes em roteadores e comutadores intermediários e de processamento de pacotes. Já a taxa de entrega média é a razão entre a quantidade de pacotes de dados recebidos e a quantidade de pacotes de dados enviados (HARRISMARE, 2011; CHENG *et al*., 2012).

Quando se pensa em caracterizar o desempenho de uma rede, as métricas apresentadas são importantes. No caso da vazão e da taxa de entrega, quanto maiores forem os seus valores, melhor será o desempenho da rede. Já no caso do atraso fim a fim, quanto menor o valor dele melhor será o desempenho.

Segundo Kurose e Ross (2013) é desejável, para algumas aplicações ter um atraso baixo e uma vazão instantânea acima de algum patamar – por exemplo, superior a 24kbits/s para aplicações de telefonia via Internet, e superior a 256 kbits/s para algumas aplicações de vídeo em tempo real. Já outras aplicações, incluindo as de transferência de arquivo, o atraso não é importante, mas é recomendado ter a vazão mais alta possível (KUROSE; ROSS, 2013).

Kurose e Ross (2013) também afirmam que, para aplicações de áudio interativas em tempo real, como o VoIP, atrasos fim a fim menores do que 150ms não são percebidos pelo ouvido humano; enquanto 150 a 400ms podem ser aceitáveis, apesar de não ideais e os que excedem 400ms atra-

palham seriamente a interatividade. Normalmente, o lado receptor de uma aplicação de telefone por Internet desconsiderará quaisquer pacotes cujos atrasos ultrapassam um determinado patamar, sendo que esses pacotes são efetivamente perdidos (KUROSE; ROSS, 2013).

FERRAMENTAS DISPONÍVEIS PARA MEDIÇÃO DA NEUTRALIDADE DA REDE

De acordo com Miorandi *et al*. (2013), a análise técnica da neutralidade da rede de um provedor em relação a uma aplicação específica requer uma investigação profunda do seu comportamento de comunicação, o que é extremamente complexo. A impossibilidade de se conhecer a arquitetura completa da Internet dificulta essa análise, sendo comum a medição da comunicação entre duas pontas. Há três metodologias de medição que diferem entre si na forma em que os dados são gerados e coletados para análise futura:

- ativa: são gerados pacotes de dados específicos para serem trafegados pela rede do provedor com o objetivo de serem medidos algumas métricas técnicas – como *jitter*, vazão, etc;
- passiva: os pacotes trafegados pela rede do provedor são logados e são extraídos indicadores de desempenho relevantes para serem analisados; e
- híbrida: é a combinação das metodologias ativa e passiva.

As ferramentas existentes para detectar discriminações são tipicamente específicas para uma aplicação ou para um mecanismo específico de discriminação e dependem de testes de medição ativos (MIORANDI *et al*., 2013; RAMNEEK, 2015b).

Existem ferramentas que se propõem a fazer a medição de métricas que podem ser usadas como indicadores da violação da neutralidade da rede. Porém, muitas delas ainda são experimentais, fazendo parte de pesquisas na área de redes. Neste trabalho, foram escolhidas cinco ferramentas com abordagens distintas que podem ser aplicadas na medição da neutralidade de rede para serem analisadas em profundidade.

O Neubot é uma dessas ferramentas que mede vários indicadores de forma ativa, incluindo vazão, atraso, *jitter*, assim como o desempenho de protocolos específicos comumente usados, incluindo o Real-Time Transport Protocol – usado na maioria das aplicações de multimídia na Internet –, o protocolo *peer-to-peer* BitTorrent e o protocolo proprietário *peer-to-peer* do Skype Voice over IP (DE MARTIN; GLORIOSO, 2008). A arquitetura do

Neubot é do tipo cliente-servidor.[4] Usuários voluntários podem instalar em seus computadores uma aplicação cliente *open-source*.[5] A aplicação cliente roda em *background* e automaticamente realiza um conjunto de medidas, periodicamente enviando resultados para um servidor central.

Segundo Ramneek (2015b), o ponto forte do Neubot é o monitoramento contínuo da conexão do usuário final em oposição ao envio de pacotes de sondagem aos provedores. Porém, a variação no desempenho pode resultar de outros fatores como por exemplo o congestionamento da rede, anulando a hipótese de discriminação realizada pelo provedor.

Outra ferramenta de medição ativa é a Glasnost, que detecta diferenciação de tráfego baseado tanto nos parâmetros do cabeçalho do protocolo de transporte (número da porta[6]) (KUROSE; ROSS, 2013) quanto no *payload* do pacote – também conhecido como *Deep Packet Investigation* – (MIORANDI *et al.*, 2013). Ela é baseada na arquitetura cliente-servidor. Cada cliente se conecta a um servidor através do navegador *web*, rodando diversos testes. Cada teste mede o caminho entre cliente e servidor gerando *streams* de tráfego no nível da aplicação. A ideia principal da Glasnost é a emulação de dois streams de tráfego transportando dados, idênticos em todos os sentidos, menos na característica suspeita de provocar a discriminação ao longo do caminho. Por exemplo, no caso do teste do protocolo BitTorrent, metade dos fluxos de teste usam a porta 6881, uma porta conhecida por ser usada pelo protocolo BitTorrent, enquanto a outra metade usa uma porta aleatória não associada a nenhum protocolo específico (DISCHINGER *et al.*, 2008). Essa ferramenta possui página web em que se podia testá-la diretamente através de um navegador.[7]

---

4 A arquitetura cliente-servidor é aquela em que há dispositivos que disponibilizam conteúdos (servidores) para serem acessados por outros (clientes). Ela se contrapõe à arquitetura *peer-to-peer*, em que um dispositivo pode fazer o papel tanto de cliente quanto de servidor ao mesmo tempo. O BitTorrent utiliza a arquitetura *peer-to-peer*.

5 O guia de instalação do cliente do Neubot pode ser encontrado em: NETWORK MEASUREMENTS FROM THE EDGES. Neubot install guide. Disponível em: <http://neubot.org/neubot-install-guide>. Acesso em: 15 abr. 2017.

6 Cada número de porta é um número de 16 bits na faixa de 0 a 65535. Os números de porta entre 0 e 1023 são denominados números de porta bem conhecidos e são reservados para utilização por protocolos de aplicação bem conhecidos, como HTTP (porta 80) e FTP (porta 21). Quando se desenvolve uma nova aplicação é necessário atribuir a ela um número de porta.

7 Após 8 anos em funcionamento, a ferramenta Glasnost foi descontinuada em 2017, uma vez que foi desenvolvida como Java applet e os navegadores modernos não possuem mais suporte a essa tecnologia. Informações sobre a ferramenta podem ser

Além de mostrar os resultados das medições, a ferramenta Glasnost dava um veredicto sobre a discriminação de pacotes na rede. As mensagens exibidas na interface da ferramenta podem conter basicamente três indicações:

1. não há evidência que o provedor limita o tráfego de *upload/download*;
2. os dados medidos apresentam muito ruído para detectar se o provedor limita o tráfego de *download/upload* e era pedido para que os testes fossem rodados novamente assegurando que não havia outros processos fazendo *download/upload*;
3. o provedor parece limitar o *download/upload*, embora algumas das medições possam ser afetadas por ruído, o que limita a habilidade de detecção pela ferramenta.

A Glasnost também apresentava alguns detalhes do porquê fazia suas avaliações. Por exemplo, no caso de uma possível limitação poderia ser mostrada a seguinte mensagem: "Seu provedor parece permitir uma banda maior para *downloads* usando o protocolo HTTP[8]. Em nossos testes, *downloads* usando fluxos de controle atingiram a taxa de no máximo 226 Kbps enquanto downloads usando HTTP atingiram até 1597 Kbps". No caso em que não parecia haver limitação poderia ser exibida uma mensagem similar a essa: "Não há indicação de que seu provedor limite os *downloads* na porta 8080[9] ou na 57732. Em nossos testes, os *downloads* na porta 8080 atingiram taxas de até 1416 Kbps enquanto os *downloads* pela porta 57732 atingiram taxas de até 1597 Kbps". Além disso, era exibida uma tabela com todos os testes realizados e seus dados individuais.

A ferramenta Glasnost *é* a que fazia um diagnóstico mais interessante do que acontece em uma rede, pois mensurava diversas métricas, de diferentes protocolos. De acordo com Ramneek (2015b), o ponto forte da Glasnost se concentra na sua acurácia e simplicidade de uso. Porém, ela é focada na diferenciação no usuário final e pode não ser capaz de detectar a discriminação entre provedores de conteúdo feitas pelo provedor de conexão.

---

encontradas em: MAX PLANCK INSTITUTE. Glasnost: Test if your ISP is shaping your traffic. Disponível em: <http://broadband.mpi-sws.org/transparency/bttest.php>. Acesso em: 15 abr. 2017.

8 O HTTP (Hypertext Transfer Protocol) é o protocolo para a transferência de hipertexto, que é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre diferentes nós contendo texto (páginas web). Ele é a base para a comunicação de dados da World Wide Web.

9 A porta 8080 é usada tipicamente pelo protocolo HTTPS.

O Network Diagnostic Tool (NDT), por sua vez, é uma ferramenta que mede a vazão do protocolo TCP entre um *software* cliente instalado em um dispositivo de usuário e um servidor. O NDT é atualmente usado pela FCC – sigla para Federal Communications Commission –[10] como seu *software* oficial de medição de banda larga (DOVROLIS *et al*., 2010). O NDT possui uma página *web* em que pode ser testado diretamente através de um navegador.[11]

A ferramenta NDT tem uma interface de uso bastante fácil por se tratar de um *applet* Java[12] rodando em uma página *web*. Porém, suas métricas são bastante limitadas. As métricas medidas por essa ferramenta de forma isolada não permitem dizer se está ocorrendo uma discriminação de tráfego, pois não compara com outros protocolos ou com o que acontece em outros provedores. Além disso, existem diversas ferramentas semelhantes a ela, podendo-se citar o SIMET aqui no Brasil.[13]

A ferramenta ShaperProbe detecta se um provedor está empregando algum tipo de *traffic shapping*[14] (SANTOS, 2016), através de uma medição ativa dos caminhos de fluxo da rede (RAMNEEK, 2015b). Para isso, ela tenta identificar se o provedor está classificando certos tipos de tráfego como baixa prioridade, fornecendo diferentes níveis de serviço para eles, através de uma técnica conhecida como *token bucket* (MIORANDI *et al*., 2013). A ferramenta ShaperProbe precisa ser instalada localmente para testes[15].

---

10 A *Federal Communications Commission* é a agência norte americana que regula os serviços de telecomunicações.

11 O teste com a ferramenta NDT pode ser feito diretamente em: MEASUREMENT LAB. NDT (Network Diagnostic Tool). Disponível em:<http://www.measurementlab.net/tools/ndt/>. Acesso em: 15 abr. 2017.

12 *Applet* é um pequeno software que executa uma atividade específica, dentro de um outro programa maior (como por exemplo em uma página web).

13 O SIMET possui três versões: Web, Mobile e Box. Ele mede a vazão, o *jitter*, a latência e a perda de pacotes. Mais informações em: SIMET. Disponível em: <https://simet.nic.br/>. Acesso em: 15 abr. 2017.

14 Traffic shaping é a prática de bloquear/degradar certos "tipos" de tráfego de dados. Foi bastante usada com as redes *peer-to-peer* (P2P), em especial que usavam protocolo BitTorrent.

15 O guia de instalação da ferramenta ShaperProbe pode ser encontrado em: NETINFER. <http://netinfer.net/diffprobe/shaperprobe.html>. Acesso em: 15 abr. 2017.

Ela necessita que o *firewall*[16] da rede esteja com as portas TCP 55000 – saída –, TCP 55005 – saída –, e UDP 55005 – ambas as direções – abertas. Normalmente, os provedores fecham várias portas em conexões residenciais, principalmente para entrada de fluxo de dados por motivos de segurança. Com isso, os testes que usam portas para entrada podem não funcionar nesta ferramenta.

As quatro ferramentas acima descritas usam a plataforma do Measurement Lab, o M-Lab.[17] Ele fornece uma plataforma para desenvolver, testar e implantar novas ferramentas de medição ativa (DOVROLIS *et al.*, 2010). Os servidores do M-Lab estão distribuídos geograficamente em localizações estratégicas ao redor do mundo. Para cada ferramenta são alocados recursos dedicados na plataforma M-Lab para facilitar medições com maior acurácia.

Já como ferramenta de medição passiva há a Network Neutrality Access Observatory (NANO). Esse sistema detecta discriminação de um provedor coletando passivamente os dados de desempenho dos clientes. Os agentes NANO, implantados nos clientes participantes ao longo da Internet, coletam dados de desempenho para serviços selecionados e reportam essas informações para servidores centralizados, que analisam as medidas para estabelecer relações causais entre um provedor e degradações de desempenho (MIORANDI *et al.*, 2013).

Segundo Ramneek (2015b), ela infere a diferenciação, comparando o desempenho alcançado em um provedor específico em comparação a outros provedores, para uma aplicação específica. A inferência produzida pela NANO tem maior acurácia quanto maior o número de fatores são levados em consideração nos testes. Porém, há muitos fatores que podem afetar os resultados e que podem não ser levados em consideração, o que pode levar a um resultado errado em muitos casos. Também, os cálculos são passivos, e podem não fornecer informação em tempo real.

As ferramentas de medição ativa acima expostas se relacionam com as métricas:

16 Firewall é um sistema de segurança de rede que monitora e controla o tráfego de rede. Normalmente, ele protege uma rede interna contra acessos não autorizados vindos da Internet.

17 Informações sobre todas as ferramentas que usam os servidores do M-Lab: MEASUREMENT LAB. Disponível em: <http://www.measurementlab.net/>. Acesso em: 15 abr. 2017.

1. Vazão do protocolo TCP;
2. Vazão do protocolo UDP;
3. Vazão do protocolo BitTorrent;
4. Vazão do protocolo HTTP;
5. (Goodput do protocolo TCP;
6. Goodput do protocolo BitTorrent;
7. Goodput do protocolo HTTP;
8. RTT do protocolo TCP;
9. Latência do protocolo HTTP;
10. Latência do protocolo TCP; e
11. *Jitter* do protocolo TCP.

Na Tabela 1 é possível ver a relação de métricas com cada ferramenta. A ferramenta NANO foi excluída dessa análise por ter sido encontrado que ela trabalha com métricas como o RTT e a vazão, mas sem haver detalhes de quais protocolos são analisados (TARIQ *et al.*, 2008).

Tabela 1: Métricas medidas por cada ferramenta

	Neubot	Glasnost	NDT	ShaperProbe
Vazão do protocolo TCP	Não	Não	Sim	Não
Vazão do protocolo UDP	Não	Não	Não	Sim
Vazão do protocolo BitTorrent	Não	Sim	Não	Não
Vazão do protocolo HTTP	Não	Sim	Não	Não
Goodput do protocolo TCP	Sim	Não	Não	Não
Goodput do protocolo BitTorrent	Sim	Não	Não	Não
Goodput do protocolo HTTP	Sim	Não	Não	Não
RTT do protocolo TCP	Não	Não	Sim	Não
Latência do protocolo HTTP	Sim	Não	Não	Não
Latência do procolo TCP	Sim	Não	Não	Não
Jitter do protocolo TCP	Não	Não	SIm	Não

Fonte: Elaborado pela autora.

No mesmo espírito do que foi apresentado anteriormente, Garret *et al* (2018) apresenta uma descrição aprofundada de dez ferramentas existentes na literatura, analisando como cada solução endereça cada aspecto da detecção da diferenciação de tráfego, quais técnicas são empregadas por cada solução e quais são os tipos de diferenciação detectadas por cada solução.

Setenareski (2017) propôs a criação de um observatório, como instrumento de acompanhamento da Neutralidade da Rede no Brasil, sendo um repositório de ferramentas ou mecanismos computacionais relacionados ao monitoramento do tráfego da Internet, em especial à Neutralidade da Rede; e um fórum de discussão, no qual os usuários possam relatar os resultados encontrados, por meio do uso das ferramentas de monitoramento de tráfego da Internet, e debater estes resultados com outros usuários.

Em Schaurich *et al*. (2018) é proposta uma ferramenta chamada ISPANN, com a qual os países que possuem legislações voltadas a neutralidade da rede podem configurar as regras aplicáveis em seus países, permitindo que a ferramenta audite a rede de um ISP, identificando violações a neutralidade da rede no país em questão. O estudo de caso apresentado compara as legislações dos Estados Unidos, da Europa e do Chile em relação a quatro práticas de violações a neutralidade: bloqueio, discriminação de usuário, discriminação de aplicação/serviço e priorização paga.

Já Rocha (2018) apresenta a criação de um método que identifique a quebra da neutralidade de maneira agnóstica, independentemente do tipo de protocolo, da aplicação, do serviço, do tamanho do pacote ou de qualquer outra informação que o fluxo possuir em um ambiente controlado. O método proposto também é capaz de distinguir entre diferenciação de tráfego e a degradação que ocorre sobre os fluxos.

O Body of European Regulators for Electronic Communications (BEREC) publicou em outubro de 2017 uma especificação para uma ferramenta voltada a medição da neutralidade da rede. Segundo esse documento de especificações, as funções tidas como mandatórias para supervisão e monitoramento da qualidade dos serviços de acesso a Internet são as medidas de velocidade – *downlink* e *uplink* – e as de atraso. Além dessas, são previstas como funções adicionais as medidas de variação de atraso, as de perda de pacote – para *downlink* e *uplink* – e a disponibilidade de conectividade (BEREC, 2017).

Adicionalmente às funções de medição de qualidade dos serviços de acesso a Internet, a especificação do BEREC solicita funções que permitam a revisão dedicada a como os fluxos de dados que aplicativos específicos geram são tratados pelas redes prestadoras de serviço, sendo obrigatórias a verificação do bloqueio de portas no uso dos protocolos TCP e UDP. Ainda são previstas funções adicionais de medição específicas para certas aplicações como (BEREC, 2017):

- DNS: manipulação de requisições específicas de DNS, realizado pela rede subjacente;
- *Proxy*: detectar se há algum intermediário ao longo do caminho da rede que, de uma forma ou de outra, modifique uma requisição;
- *Web*: desempenho de navegação;
- Áudio/Vídeo: detectar se o tratamento de streaming de áudio/vídeo pode afetar o desempenho conforme percebido pelo usuário final;
- VoIP: detectar como o tráfego para ou de tais aplicativos é tratado; e
- *Peer to peer*: esse tipo de comunicação é bloqueada ou está sendo exposta a algum gerenciamento de tráfego.

No primeiro semestre de 2018, o BEREC abriu uma chamada para que instituições ou pessoas físicas se candidatem para o desenvolvimento dessa ferramenta.

DISCUSSÃO E CONSIDERAÇÕES FINAIS

Essa seção explicou diversas métricas que podem ser usadas para verificar o desempenho de uma rede, incluindo a Internet. Além disso, apresentou ferramentas que usam algumas dessas métricas com a finalidade de medir discriminações de rede e, assim, detectar se haveria violação no princípio da neutralidade da rede.

Pode-se perceber que as ferramentas existentes para detectar as discriminações são específicas para uma aplicação, um protocolo ou para um mecanismo específico de discriminação e, na maioria das vezes, dependem de testes de medição ativos. O uso desse tipo de teste nem sempre é ideal, pois gera um maior fluxo de pacotes na rede, sem que esteja de fato transportando alguma informação útil, podendo contribuir em um cenário de congestionamento da rede. Além disso, os provedores de conexão podem descobrir o padrão dos pacotes de testes de medição – por exemplo, pelo IP de destino – e começar a discriminá-los, seja descartando propositadamente, ou até mesmo favorecendo seu caminho para que tenham melhores resultados do que os pacotes úteis. Esse cenário não aconteceria com ferramentas de medição passiva, pois não há pacotes especificamente gerados para esse fim. Por outro lado, como há uma inspeção dos pacotes trafegados pelos usuários, isso pode se transformar em um problema de privacidade. Além disso, ferramentas de medição passiva são difíceis de serem implementadas na prática.

A maioria das ferramentas usam poucas métricas de rede para inferir seus resultados, o que pode torná-las imprecisas. E por fim, as ferramentas não fazem uma comparação entre os resultados de diferentes provedores de conexão, o que poderia ser útil para compreender o comportamento dos pacotes de cada aplicação na rede.

Com o uso de apenas uma dessas ferramentas existentes pouco se pode afirmar sobre a violação da neutralidade da rede de acordo com a definição do Marco Civil da Internet. Um diagnóstico mais completo poderia ser feito através da análise em conjunto das métricas monitoradas pelas várias ferramentas. Mas ainda assim há uma dificuldade em se dizer que elas são suficientes para serem adotadas na fiscalização da neutralidade da rede e que constituem evidências para uma possível ação judicial em caso de violação. Há um desafio ainda em inferir se uma discriminação ocorrida pode estar em conformidade com alguma das exceções regulamentadas através do Decreto.

Verifica-se que há uma necessidade da escolha de métricas de rede que possam ajudar na fiscalização da manutenção da neutralidade da rede, bem como o desenvolvimento de ferramentas que possam monitorá-las e gerar resultados que possam ser usados como provas para ações judiciais no âmbito do Marco Civil da Internet.

REFERÊNCIAS

BEREC. Net neutrality measurement tool specification. Disponível em: < http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296-net-neutrality-measurement-tool-specification >. 10 Out. 2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei n 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. Portal da Legislação. Brasília, 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 15 abril 2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Portal da Legislação. Brasília, 23 abril 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 15 abr. 2017.

CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. *Redes de computadores.* Porto Alegre: Bookman, 2009.

CHENG, Y.; ÇETINKAYA, E. K.; STERBENZ, J. P. G. Dynamic Source Routing (DSR) Protocol Implementation in ns-3. Proceedings of the ICST SIMUTools Workshop on ns-3 (WNS3). Março, 2012. Disponível em: <http://www.ittc.ku.edu/resilinets/papers/Cheng-Cetinkaya-Sterbenz-2012.pdf>. Acesso em: 15 abr. 2017.

DE MARTIN, J. C.; GLORIOSO, A. The Neubot Project: A Collaborative Approach To Measuring Internet Neutrality. IEEE International Symposium on Technology and Society, Fredericton (Canada), 26-28 June 2008.

DISCHINGER, M.; MISLOVE, A.; HAEBERLEN, A.; GUMMADI K. P. Detecting BitTorrent Blocking. Proceedings of the 8th ACM SIGCOMM conference on Internet measurement – IMC'08, October 20–22, 2008, Vouliagmeni, Greece.

DOVROLIS, C.; GUMMADI, K.; KUZMANOVIC, A.; MEINRATH, S. D. Measurement Lab: Overview and an Invitation to the Research Community. *ACM SIGCOMM Computer Communication Review*, v. 40, n. 3, July 2010.

GARRETT, T.; SETENARESKI, L. E.; PERES, L. M.; BONA, L. C. E.; DUARTE, E. P. Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE Communications Surveys & Tutorials,* v. PP, n. 99, mar. 2018.

HARRISMARE. Packet Delivery Ratio, Packet Lost, End to End Delay. 14 julho 2011. Disponível em: <https://harrismare.wordpress.com/2011/07/14/packet-delivery-ratio-packet-lost-end-to-end-delay/>. Acesso em: 15 abr. 2017.

IETF. RFC 2647 - Benchmarking Terminology for Firewall Performance, 1999. Disponível em: <http://tools.ietf.org/html/rfc2647#section-3.17>. Acesso em: 15 abr. 2017.

IETF. RFC 6349 - Framework for TCP Throughput Testing. 2011. Disponível em: <https://tools.ietf.org/html/rfc6349>. Acesso em: 15 abr. 2017.

KUROSE, J.; ROSS, K. W. *Redes de computadores e a internet:* uma abordagem top-down. 6. ed. [S. l.]: Pearson, 2013.

MAX PLANCK INSTITUTE. Glasnost: Test if your ISP is shaping your traffic. Disponível em: <http://broadband.mpi-sws.org/transparency/bttest.php>. Acesso em: 15 abr. 2017.

MEASUREMENT LAB. NDT (Network Diagnostic Tool). Disponível em:<http://www.measurementlab.net/tools/ndt/>. Acesso em: 15 abr. 2017.

MEASUREMENT LAB. Update: Paris Traceroute bug from Early 2018. Disponível em: <http://www.measurementlab.net/>. Acesso em: 15 abr. 2017.

MIORANDI, D.; CARRERAS, I.; GREGORI, E.; GRAHAM, I.; STEWART, J. Measuring Net Neutrality in Mobile Internet: Towards a Crowdsensing-based Citizen Observatory. IEEE International Conference on Communications 2013: IEEE ICC'13 – Workshop on Beyond Social Networks: Collective Awareness.

NETINFER. <http://netinfer.net/diffprobe/shaperprobe.html>. Acesso em: 15 abr. 2017.

NETWORK MEASUREMENTS FROM THE EDGES. Neubot install guide. Disponível em: <http://neubot.org/neubot-install-guide>. Acesso em: 15 abr. 2017.

RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. Disruptive Network Applications and their Impact on Network Neutrality. 17th International Conference on Advanced Communication Technology (ICACT), 2015.

RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. Detecting Network Neutrality Violations through Packet Loss Statistics. 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015b.

RAMOS, P. H. S. *Arquitetura da rede e regulação:* a neutralidade da rede no Brasil. 2015. 218 f. Dissertação (Mestrado em Direito) – Escola de Direito de São Paulo, Fundação Getúlio Vargas, São Paulo, 2015.

ROCHA, A. M. *Método Agnóstico de Detecção da Quebra da Neutralidade na Internet pelos ISPs*. 2018. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Santa Maria, Santa Maria. 2018.

SANTOS, V. W. O. *Neutralidade da rede e o Marco Civil da Internet no Brasil:* atores, políticas e controvérsias. 2016. Tese (Doutorado em Política Científica e Tecnológica) – Universidade Estadual de Campinas, Campinas, 2016.

SCHAURICH, V. G.; CARVALHO, M.; GRANVILLE, L Z. ISPANN: A policy-based ISP Auditor for Network Neutrality violation detection. 32nd IEEE International Conference on Advanced Information Networking and Applications (AINA 2018), 16-18 May 2018, Krakow, Poland.

SETENARESKI, L. E. *Fiscalização da Neutralidade da Rede e seu Impacto na Evolução da Internet*. 2017. Tese (Doutorado em Informática) – Universidade Federal do Paraná, Curitiba. 2017.

SIMET. Disponível em: <https://simet.nic.br/>. Acesso em: 15 abr. 2017.

TANENBAUM, A. S.; WETHERALL, D. J. *Computer Networks*. 5. ed. [S. l.]: Pearson, 2011.

TARIQ, M. B.; MOTIWALA, M.; FEAMSTER, N. Nano: Network access neutrality observatory. Georgia Institute of Technology, 2008. Disponível em: <http://conferences.sigcomm.org/hotnets/2008/papers/22new.pdf>. Acesso em: 15 abr. 2017.

WU, T. Network Neutrality FAQ. Disponível em: <http://www.timwu.org/network_neutrality.html>. Acesso em: 15 abr. 2017.

WU, T. Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law*, v. 2, p. 141, 2003.