5

Neutralidade de rede: mudanças na infraestrutura da internet e como isso influencia na sua vida

LEONARDO PARENTONI

Doutor em Direito (USP). Professor Adjunto (UFMG e IBMEC/MG). *Research Fellow* na Universidade do Texas em Austin (Estados Unidos da América). Procurador Federal (AGU).

Artigo recebido em 27/10/2016 e aprovado em 18/06/2017.

SUMÁRIO: *1 Introdução • 2 Breve histórico da internet • 3 Do que a internet é feita? Design da rede e suas camadas • 4 Como a internet está mudando • 5 O que isto influencia na sua vida • 6 A principal resposta regulatória: neutralidade de rede • 7 O design da internet e os limites da neutralidade de rede • 8 Conclusão • 9 Referências.*

RESUMO: Este texto aborda a neutralidade de rede. Inicia contextualizando como a internet surgiu, seus propósitos, os princípios utilizados no seu *design* e como era sua arquitetura originária. Na sequência, descreve algumas das principais mudanças pelas quais vem passando, nos últimos anos, com destaque para o monitoramento e controle dos pacotes de dados, viabilizando o tratamento discriminatório entre eles. Explica-se como essas mudanças afetam bilhões de pessoas, mundialmente. Por fim, aborda-se a neutralidade de rede como principal resposta regulatória a essas mudanças, a fim de preservar o potencial inovador e o compartilhamento de conteúdo típicos da internet. Frisa-se que essa neutralidade decorre dos próprios princípios utilizados no *design* original da internet, devendo ser interpretada em sintonia com eles, a fim de compatibilizar, de um lado, a livre concorrência, as estratégias empresariais e suas vantagens competitivas; e, de outro, a privacidade, a liberdade de expressão, a inovação e a autonomia dos usuários.

PALAVRAS-CHAVE: Internet • *Design* de Redes • Neutralidade de Rede • Inovação.

Network Neutrality: Changes in the internet infrastructure and how it affects your life

ABSTRACT: This article analyses net neutrality. It starts by contextualizing internet's birth, its purposes, the main principles used on its design and how was its original architecture. Next, it describes some recent changes on the internet's structure, highlighting the monitoring and control of data packets, in order to enable a discriminatory treatment between them. This part explains how this subject affects the life of billions, worldwide. Finally, the paper focuses on net neutrality as the main legal response to the previously described problems, explaining how it derivates from the original design principles of internet, in order to support a conclusion that reconciles, at one side, free competition and investment strategies, and, at the other side, privacy, freedom of speech, innovation and internet users decision-making autonomy.

KEYWORDS: Internet • Network Design • Network Neutrality Innovation.

Neutralidad de la red: cambios en la infraestructura de internet y cómo esto afecta tu vida

CONTENIDO: En este artículo se analiza la neutralidad de la red. Se inicia contextualizando el nacimiento de internet, sus propósitos, los principios básicos utilizados en su diseño y cómo fue su arquitectura original. Entonces, se describen algunos cambios recientes en la estructura de la internet, destacando el monitoreo y control de los paquetes de datos, con el fin de discriminarlos. Entonces se explica cómo este tema afecta a la vida de miles de millones en todo el mundo. Por último, el artículo se centra en neutralidad de la red, ya que es la principal respuesta jurídica a los problemas anteriormente descritos, explicando cómo se derivan de los principios de diseño originales de internet, con el fin de apoyar la conclusión de que reconcilia, por un lado, la libre competencia y las estrategias de inversión y, en el otro lado, la privacidad, la libertad de expresión, la innovación y la autonomía en la toma de decisiones de los usuarios de internet.

PALABRAS CLAVE: Internet • Arquitectura de Internet • Neutralidad de la Red • Innovación.

1 Introdução

Este texto não encerra unicamente considerações de ordem jurídica. Tampouco considerações próprias da Tecnologia da Informação. Até porque o autor não tem formação específica nesta última área. Ao contrário, busca *mesclar ambas*, por entender que a sua análise conjunta é indispensável para compreender o real funcionamento da internet e, consequentemente, propor soluções jurídicas que sejam plausíveis e viáveis, não apenas do ponto de vista teórico, mas principalmente prático. Afinal, a melhor teoria é aquela que funciona na prática.

Com base nessa premissa, pretende-se abordar o surgimento da internet e suas características originais, responsáveis por tê-la tornado o sucesso que é hoje. Após, demonstra-se como a internet vem mudando e os reflexos dessa mudança na vida das pessoas, dos empresários e no próprio funcionamento dos mercados.

Em seguida, aborda-se aquela que, na visão do autor, é a principal resposta regulatória aos novos problemas: a neutralidade de rede. Conceitua-se esse termo na literatura jurídica estrangeira e o tratamento dado pelo Marco Civil da Internet no Brasil. Ao final, o autor expõe o seu entendimento acerca de como deve ser aplicada a neutralidade de rede.

2 Breve histórico da internet

Os antecedentes da internet encontram-se na década de 1950. Muito antes, portanto, de sua expansão mundial. Como qualquer outra tecnologia, ela foi fruto de um contexto socioeconômico, o qual influenciou, diretamente, a forma e os objetivos para os quais foi desenvolvida. Compreender isto é indispensável para analisar criticamente a internet dos dias de hoje (CASTELLS, 2001, p. 23).

Com efeito, o mundo vivia a *guerra fria*, num embate entre Estados Unidos da América e União Soviética. Nesse período, a comunicação mais rápida se processava por telefone. A rede telefônica, porém, era muito vulnerável a ataques militares e o Departamento de Defesa dos EUA desejava criar uma alternativa mais segura. Ainda na década de 1950, Paul Baran, programador de sistemas da Rand Corporation, sugeriu um modelo de rede computacional semelhante à internet. O Departamento de Defesa, então, consultou a AT&T, companhia que monopolizava a comunicação telefônica do país, para verificar se ela teria interesse em desenvolver esse modelo. A AT&T imediatamente rechaçou a ideia, dizendo que ela era inviável.

> A AT&T considerou as ideias de Baran fora de mão. A maior e mais rica corporação do mundo não estava disposta a permitir que alguns jovens *whippersnapper* ensinassem-na como construir um sistema de telefonia. Eles disseram que a rede de Baran não poderia ser construída e a ideia morreu. (TANENBAUM, 2011, p. 55, tradução nossa).

Em outubro de 1957, a União soviética deu um passo mundialmente noticiado rumo ao progresso tecnológico, lançando o satélite *Sputnik*. Em reação a isto, o então Presidente norte-americano, Dwight Eisenhower, criou, em setembro de 1959, dentro do Departamento de Defesa, uma agência para projetos de pesquisa avançada (*Advanced Research Projects Agency* – ARPANET), dedicada, especificamente, ao aprimoramento das redes de comunicação. O objetivo era suplantar a União Soviética.

Entre outros fins, a ARPANET deveria desenvolver uma rede de comunicação mais segura, que se mantivesse disponível mesmo quando um de seus componentes fosse danificado. Por exemplo, em caso de destruição de uma base militar, as informações nela armazenadas permaneceriam acessíveis (TANENBAUM, 2011, p. 45-46).

Ocorre que a ARPANET tinha, naquela época, infraestrutura modesta, sem cientista ou laboratórios e com orçamento pequeno e, por isso, recorreu ao meio acadêmico – por meio da emissão de subsídios e contratos com Universidades e empresas cujas ideias pareciam promissoras ao desenvolvimento de seus objetivos (TANENBAUM, 2011, p. 56). Os professores e alunos, então, resgataram as ideias de Paul Baran, demonstrando a viabilidade de se criar uma rede de computadores baseada no padrão que havia sido sugerido por ele (HAFNER; LYON, 1996).

Na década de 70 já existiam várias redes locais (*Local Area Networks* – LAN) nos Estados Unidos da América, mas que não estavam interconectadas. Por exemplo, nas universidades. Ou, ainda, as redes privadas do tipo BBS (*Bulletim Board Systems*)[1]. O desafio era desenvolver um *padrão universal* de comunicação, capaz de interconectar todas elas, dando origem a uma *rede de redes*. Para isso, a ARPANET passou a fomentar pesquisas na área, as quais resultaram, em 1978, na criação dos protocolos TCP/IP, ainda hoje o padrão da internet (CASTELLS, 2001, p. 25). Com base neles, as várias redes locais se integraram e possibilitaram um intercâmbio de dados e experiências acadêmicas nunca antes visto. Poucos anos depois, no final da década de 1980, o número de instituições, dispositivos e pessoas conectados já era tão grande que a

1 Uma BBS muito famosa na década de 80 era a BITNET, sigla que representa a curiosa expressão *because it's there network*, em alusão ao fato de que esse tipo de rede já existia.

http://dx.doi.org/10.20499/2236-3645.RJP2018v19e119-1365

ARPANET foi substituída por uma rede mais robusta, denominada NSFNET (*National Science Foundation Newtwork*), alcançando todo o país. A internet se descolava das origens militares.

A esta altura, não seria mais viável manter a internet sob a responsabilidade exclusiva do Governo norte-americano. Foi, então, criada uma sociedade privada controlada pelo Estado (*Advanced Networks and Services - ANS*) para gerenciar a progressiva transferência da rede à exploração comercial (*privatização* da internet). Isto *se consolidou na década de 1990*, quando inúmeras empresas privadas já atuavam como provedoras de acesso e a ARPANET foi definitivamente encerrada (TANENBAUM; WETHERALL, 2011, p. 60). Foi também nessa época que a rede se expandiu em âmbito mundial. Ou seja, a efetiva internacionalização da internet e sua exploração comercial se deram cerca de 40 anos após as primeiras pesquisas a respeito do tema.

Este breve histórico pretendeu demonstrar que *a internet não surgiu por iniciativa do mercado*. Pelo contrário, a AT&T demonstrou completo desinteresse por ela, na década de 1950. Em verdade, a rede mundial de computadores foi fruto de uma parceria entre o Governo norte-americano e instituições de ensino superior. Sua gênese é tanto militar quanto acadêmica (PARENTONI, 2007, p. 27-29). Na feliz síntese de Manuel Castells: *"a internet nasceu na insólita encruzilhada entre a grande ciência, a investigação militar e a cultura libertária"* (2001, p. 31).

Como se analisará adiante, tal característica histórica foi de vital importância para o sucesso da rede mundial de computadores.

3 Do que a internet é feita? Design da rede e suas camadas.

Para se construir algo, é preciso não apenas definir como a construção será, mas também concretizar essa ideia por meio de um projeto. A arquitetura/projetação é a etapa preliminar à implementação da obra. No que toca às redes informatizadas, essa etapa denomina-se arquitetura de redes (*network architecture* ou *network design*) (VAN SCHEWICK, 2010, p. 20-21)[2]. É ela que define como será toda a infraestrutura de uma rede informatizada, condicionando o seu funcionamento, o custo e as possibilidades de modificação futura (OLIVEIRA; PARENTONI, 2007).

Existem diversas possibilidades para a arquitetura de rede, a depender do direcionamento seguido pelos seus idealizadores. Este direcionamento, por

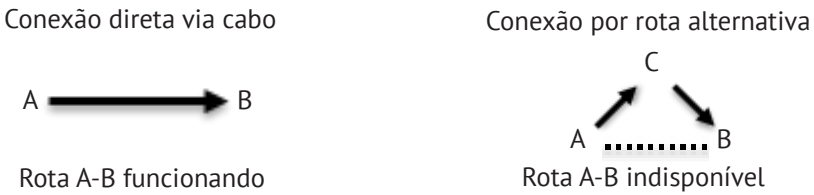
2 Vide também: LESSIG, 2006, p. 24; TANENBAUM; WETHERALL, 2011, p. 31 e WHITT, 2013, p. 704.

sua vez, é dado pelos princípios da arquitetura de redes (*design principles*) (VAN SCHEWICK, 2010, p. 23). No desenvolvimento da internet, foram aplicados *4 princípios fundamentais*: 1) comutação de pacotes (*packet switching*); 2) modularidade (*modularity*); 3) camadas de rede (*network layers*); e 4) execução de aplicações na camada superior (*end-to-end*).

Compreender o *design* original da internet é indispensável para perceber como ela vem mudando nos últimos anos e quais são as consequências disto.

Com efeito, a característica básica da internet é dividir os dados em parcelas menores, denominadas pacotes (*packets*), transmitindo-os separadamente. Cada pacote recebe informações a respeito de quem é o seu remetente e qual o destino (*addressing*). Até aqui, algo semelhante ao correio tradicional, em papel. A grande diferença é que os vários pacotes podem trafegar simultaneamente, por rotas diversas, inclusive mudando de trajeto durante o percurso, para privilegiar o que for mais rápido e eficaz (*switching*). Chegando ao destino, os pacotes são reagrupados para formar o dado original e então são entregues. Este princípio viabiliza a transmissão de dados mesmo se um ou alguns dos componentes da rede estiverem desconectados, congestionados ou por qualquer motivo inacessíveis (ROBERTS, 1978, p. 1307). Foi esta a solução sugerida por Paul Baran, na década de 1950, e posteriormente acolhida pelo Governo norte-americano, via ARPANET. A figura seguinte compara a comunicação tradicional de dados, via conexão direta por cabo, com a comutação de pacotes:

Figura 1: Rotas alternativas de comunicação via internet.

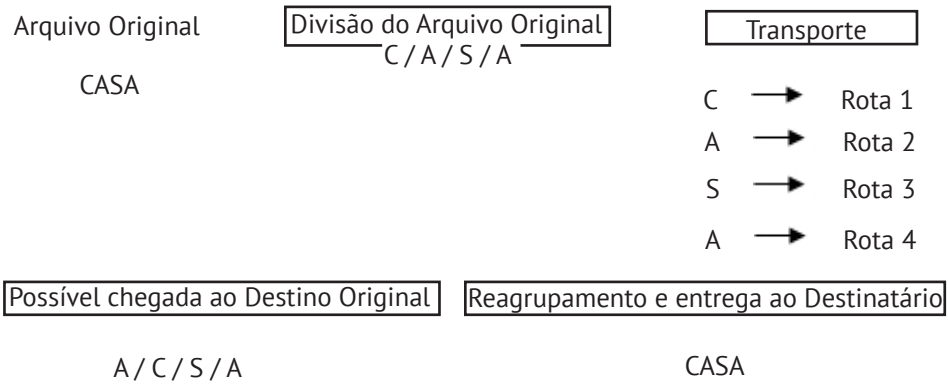


Fonte: elaborada pelo autor.

Perceba-se que a diferença é a possibilidade de que os dados cheguem de *A* até *B*, mesmo se a ligação direta entre eles estiver comprometida, pois existe a rota alternativa passando por C. Na internet, para cada rota existem centenas ou mesmo

milhares de alternativas. A figura a seguir ilustra como os dados são divididos durante a transmissão e posteriormente recompostos no destino:

Figura 2: Comunicação de dados via comutação de pacotes.



Fonte: elaborada pelo autor.

O segundo princípio aplicado no *design* original da internet foi a *modularidade*. Com base nele, a rede deve ser formada por diversos componentes, independentes uns dos outros, chamados de módulos (VAN SCHEWICK, 2010, p. 38). A intenção é reduzir ao máximo a dependência da rede, como um todo, em relação a cada componente. Para lograr isso, todo módulo possui dois tipos de informação, a visível e a *invisível* (TANENBAUM; WETHERALL, 2011, p. 29). *Informação visível* é aquela que qualquer componente da rede precisa conhecer para se conectar com determinado módulo. Ela deve permanecer inalterada e disponível a qualquer interessado, durante toda a vida da rede, para não prejudicar a comunicação entre os módulos. Por exemplo, o formato da porta VGA, utilizado para a conexão de monitores a PCs, é um dado visível. Conhecendo essa informação, qualquer fabricante é capaz de produzir um monitor compatível com essa porta. Outro exemplo é a porta USB. De posse de sua informação visível (formato da porta e o que é necessário para se conectar a ela), qualquer fabricante pode desenvolver um produto compatível, como *mouses*, impressoras, câmeras fotográficas, celulares, *tablets*, etc. O fato de cada produto ter uma configuração interna diferente não prejudica a conexão.

Diversamente, a informação necessária para o funcionamento interno de cada módulo é chamada de *informação invisível*. Ela normalmente é conhecida apenas

pelo fabricante do módulo, consubstanciando sua vantagem competitiva em relação aos concorrentes. Por exemplo, a resolução e a forma de funcionamento do monitor. Contanto que a informação visível permaneça a mesma, módulos com diferentes configurações internas serão compatíveis. Ou seja, o mesmo PC poderia se conectar a vários modelos de monitores. *A grande vantagem da modularidade é possibilitar aprimoramentos internos em cada componente da rede sem que para isto seja preciso alterar sua infraestrutura como um todo*[3].

Por sua vez, a comunicação entre os diversos módulos se faz por meio de suas especificações internas (*protocolos*) e da conexão com as camadas que lhe são imediatamente superiores e inferiores (*serviços*).

> Serviços e protocolos são conceitos distintos. [...] Um serviço é um conjunto de primitivas (operações), que uma camada fornece para a camada acima dela. O serviço define as operações que a camada está preparada para executar em nome de seus usuários, mas não diz nada sobre como essas operações são implementadas.
>
> Um serviço refere-se a uma interface entre duas camadas, com a camada inferior sendo a prestadora de serviços e a camada superior sendo a utilizadora do serviço.Um protocolo, em contraste, é um conjunto de regras que rege a estrutura e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares dentro de uma camada. (TANENBAUM; WETHERALL, 2011, p. 40, tradução nossa).

Assim, as camadas de rede são organizadas verticalmente (*stack of layers*), com relativa autonomia entre si (TANENBAUM; WETHERALL, 2011, p. 29).

Yochai Benkler considera que qualquer sistema de comunicação deveria apresentar, ao menos, 3 camadas (BENKLER, 2000, p. 561-579). No tocante especificamente à internet, há divergência sobre quantas e quais seriam elas, existindo mais de uma classificação[4]. Neste texto, *optou-se pela descrição* que compreende *6 camadas*: 1) física (*physical*); 2) de conexão (*data link*); 3) de rede (*network*); 4) de transporte de dados (*transport*); 5) de aplicações (*application*); e 6) de conteúdo (*content*).

---

3 Afasta-se a lógica do *all or nothing* (tudo ou nada), viabilizando alterações pontuais, além de reduzir o custo de adaptação da rede a cada alteração.

4 Dependendo da classificação, certas camadas são agrupadas ou desmembradas. Há, por exemplo, quem considere que a camada física não faz parte da rede propriamente dita, pois ela não corresponderia a um de seus módulos, limitando-se a transmitir os dados em forma bruta (*raw data*).

A camada inicial, de baixo para cima, é a física. Ela compreende os equipamentos que transmitem os dados em sua forma bruta (*raw data*), tais como cabos de rede, satélites e torres de telefonia celular. A seguir, vem a camada de conexão, responsável por realizar a conexão entre os equipamentos que transmitem os dados brutos e a rede propriamente dita (YOO, 2013, p. 1745-1747). A terceira camada é a que atribui identificação aos dados, por meio do protocolo de internet *(internet protocol* ou IP). Com efeito, qualquer dispositivo conectado à internet deve possuir um número de identificação. É por meio desse número que o protocolo IP individualiza o dispositivo, assegurando o envio e recebimento corretos dos dados que lhe são direcionados. De maneira simplificada, o endereço IP funciona, para a internet, como o endereço domiciliar da pessoa funciona para os Correios. Cada dispositivo possui um único IP, mas o mesmo sujeito pode ter vários dispositivos conectados à rede, simultaneamente, cada qual com um IP diferente. Por exemplo, celular, PC, *tablet*, etc. O que importa é individualizar os dispositivos, não o seu titular (TANENBAUM. WETHERALL, 2011, p. 43).

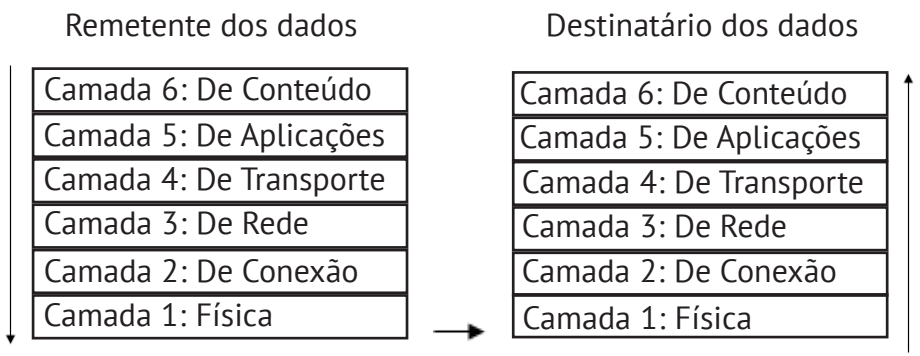
Após a identificação dos dados com os IPs de origem e destino (*end host*s), vem a quarta camada, denominada TCP (*transfer control protocol*), responsável por fragmentar os dados originais em pacotes menores, se necessário, e efetivamente transmiti-los corretamente à outra camada (TANENBAUM; WETHERALL, 2011, p. 44).

O IP e o TCP funcionam em conjunto, consubstanciando o coração da internet: um individualiza os dados, inserindo os endereços de origem e destino; o outro os fraciona, transmite e reagrupa no destino (SOLUM, 2004, p. 839). Por isto se costuma falar em protocolo TCP/IP (no singular), quando, na realidade, são duas coisas diferentes e complementares (*protocol suite*). A opção por fundi-los em único protocolo, que seria denominado *Internetwork Transmission Control Protocol* – ITCP, foi cogitada nos primórdios da internet, porém logo descartada (VAN SCHEWICK, 2010, p. 96-98).

A quinta camada de rede é a de aplicações (YOO, 2013, p. 1742). Nela são executados (em linguagem de programação) todos os *softwares* e funcionalidades típicos da internet, como os navegadores utilizados para acessar *sites*, as redes sociais e o *download* de arquivos. O resultado final dessas aplicações é, então, transmitido ao usuário, pela sexta e última camada. Para a generalidade dos usuários, é como se a internet fosse composta apenas dessa última camada, já que ela representa tudo o que eles efetivamente enxergam na tela de seus dispositivos. As camadas inferiores normalmente são conhecidas e exploradas apenas pelos programadores de sistemas e provedores de serviços.

Essa arquitetura modular, organizada em camadas, define a maneira como se processa a comunicação de dados via internet. Com efeito, não existe transferência direta de uma camada da rede, no dispositivo de origem, para a camada equivalente, no dispositivo de destino. Na verdade, os dados primeiro fluem *de cima para baixo*, do dispositivo utilizado pelo usuário para gerar os dados, passando pelo TCP/IP, que irá individualizá-los, roteá-los e fracioná-los em pacotes, até que atinjam a camada física. Daí por diante, serão transmitidos em sua forma bruta até alcançarem o local em que se situa o dispositivo de destino. Feito isso, passam a fluir *de baixo para cima*, indo da camada física para a de conexão, passando pelo TCP/IP, que se encarregará de conferir se a destinação está correta e, em caso afirmativo, reagrupar os pacotes, reconstituindo os dados originais para, em seguida, transmiti-los à aplicação que irá processá-los (em linguagem de programação), até que o resultado final seja exibido no dispositivo de destino (SOLUM; CHUNG, 2004, p. 816-817). A figura a seguir facilita a visualização desse percurso:

Figura 3. Camadas de rede na internet.



Fonte: elaborada pelo autor.

O traço característico dessa arquitetura de rede é que as camadas centrais, como o TCP/IP, não são capazes de identificar o conteúdo dos dados que estão transmitindo. Para elas, é indiferente se os dados representam um texto jurídico, reportagem jornalística ou qualquer outra manifestação do pensamento. Também é indiferente o tipo de aplicação a que se referem. Por exemplo, se dizem respeito a uma página da internet, à transmissão de um filme ou a uma postagem em rede social. O mesmo e universal padrão é seguido para o transporte de *quaisquer* dados, direcionados a *qualquer* tipo de aplicação (VAN SCHEWICK, 2010, p. 72). Quem fica responsável por identificar o conteúdo dos dados e para qual finalidade devem ser aplicados são apenas as aplicações, situadas na penúltima camada superior. Isto representa o quarto e último princípio de *design* utilizado na construção da internet: execução de aplicações na camada superior (*end-to-end*).

Essa simplicidade no funcionamento das camadas centrais da internet, aliada à ausência de filtros, possibilita que qualquer nova aplicação possa ser disseminada imediatamente, em âmbito mundial, sem que para isto seja necessária qualquer adaptação na infraestrutura básica da rede (VAN SCHEWICK, 2010, p. 140). Por esse motivo, a internet se tornou um grande condutor, aberto à transmissão, compartilhamento e construção coletiva dos mais diversos tipos de conteúdo, estimulando, assim, a inovação e o diálogo (RANCHORDÁS, 2015, p. 14-15). *O sucesso da internet, portanto, está intimamente relacionado ao design original da rede*.

> A inovação é um conceito amplo que pode ser definido de forma diferente, dependendo do contexto e do campo em questão. [...] A inovação é definida como 'a capacidade de assumir novas ideias e traduzi-las em resultados comerciais [ou socialmente eficaz] por meio de novos processos, produtos ou serviços [...]'. A inovação é mais do que uma ideia ou uma novidade; deve ser a primeira concretização bem sucedida de uma ideia no mercado ou na sociedade. (RANCHORDÁS, 2015, tradução nossa).

Por outro lado, como a especificação interna de cada módulo permanece visível apenas ao seu fabricante (consequentemente, oculta para todos os outros serviços que se conectam a esse módulo), a integração entre eles não é a melhor possível. Há, destarte, *perda de performance* no modelo da arquitetura modular, se comparado com o da plena integração entre os componentes da rede.

Essas vantagens e desvantagens da arquitetura original da internet serão abordadas com mais detalhes, posteriormente. Por ora, basta frisar que não há uma opção perfeita, capaz de proporcionar apenas qualidades. O *design* de redes envolve, necessariamente, *trade off* entre perdas e ganhos.

4 Como a internet está mudando.

Nos tópicos anteriores, demonstrou-se que a internet é uma *construção humana*, pautada por determinados *princípios* e *objetivos*. "Não há escolha que não inclua algum tipo de construção. Codificação nunca é encontrada; só é sempre feita, e só é sempre feita por nós" (LESSIG, 2006, p. 6, tradução nossa). Como toda construção humana, ela pode sofrer alterações, afinal, existem outras configurações possíveis, cada qual guiada por diferentes propósitos sociais, políticos e econômicos (LEMOS, 2015, p. 79). Ocorre que, dependendo do tipo de mudança e da intensidade com a qual for implementada, isso pode dar origem a uma nova internet, complemente diferente daquela que o mundo se habituou a conhecer. Neste tópico pretende-se pontuar, brevemente, algumas dessas mudanças. No tópico seguinte, será feita uma análise crítica a respeito delas, sob a ótica jurídica.

É sabido que as linhas telefônicas foram construídas pensando, prioritariamente, na transmissão de sons. Assim como os cabos de TV destinavam-se, apenas, ao serviço de TV por assinatura. Nenhuma dessas tecnologias foi planejada para o fluxo de dados típico da internet, até porque ela surgiu posteriormente. Em consequência, a velocidade de transmissão para aplicações da internet era, originalmente, muito reduzida. Alterações posteriores nesses instrumentos, porém, viabilizaram a transmissão de dados a velocidades antes inimagináveis, o que rendeu às novas tecnologias o nome de *banda larga* (*broadband*) (TANENBAUM; WETHERALL, 2011, p. 95-111). Assim, os cabos de cobre foram paulatinamente substituídos por fibra ótica, enquanto as linhas de telefone tradicionais evoluíram para o ADSL (*asymmetric digital subscriber line*)[5]. O mesmo ocorreu em relação ao acesso à internet via redes de transmissão de energia elétrica, satélites, ondas de rádio, micro-ondas ou WiFi (*wireless fidelity*).

Cada uma dessas tecnologias, à sua maneira e para diferentes contextos, permitiu o aperfeiçoamento das comunicações via internet. Em comum está o fato de que *todas puderam ser implementadas apenas nas camadas física e de conexão, sem que para isso fosse preciso alterar o funcionamento da rede como um todo*. Dessa maneira, dispositivos conectados à internet por diferentes formas permaneceram

5 No Brasil, por exemplo, *Oi* e *GVT* fornecem acesso via ADSL, enquanto *NET* e *SKY* utilizam o sistema de cabos de fibra ótica. Em regiões menos urbanizadas, onde as redes telefônicas e o cabeamento ainda são precários, costuma-se utilizar tecnologias alternativas de acesso, via rádio ou satélite.

plenamente interoperáveis. Isso somente foi possível graças ao *design* original em camadas e à modularidade.

Ao longo da evolução da internet, outras diversas modificações foram sendo realizadas somente na *camada de aplicações*, também *preservando o núcleo da rede*. Foram criados, por exemplo, protocolos para a transferência direta de arquivos entre os dispositivos (*file transfer protocol* – FTP) e a comunicação via *e-mail* (*simple mail transfer protocol* – SMTP).

Uma das mudanças de maior impacto na forma como se utiliza a internet foi o desenvolvimento do DNS (*domain name system*) (TANENBAUM; WETHERALL, 2011, p. 611-612). Com efeito, já foi dito que todo dispositivo conectado à rede possui um endereço IP. Para acessar o dispositivo era preciso, então, digitar este endereço, composto por sequências numéricas, como *200.251.4.1*. Ocorre que tais sequências são difíceis de serem memorizadas e podem sofrer alterações ao longo do tempo. Isso fazia com que a navegação na internet fosse extremamente complexa. Era difícil para as pessoas decorarem uma sequência como essa para cada site habitualmente acessado, além de conferir se os números não haviam mudado.

Para solucionar esse problema, surgiu uma aplicação capaz de associar cada endereço IP a um nome específico, de modo que a digitação do nome substituía a digitação do endereço numérico. Essa aplicação chama-se DNS. Ela é a responsável pela maneira fluida e intuitiva como se navega atualmente na rede, bastando digitar *www.google.com* ou *www.facebook.com* para acessar o respectivo site, quaisquer que sejam os seus números de IP. O DNS não fazia parte da arquitetura original da rede, tendo sido introduzido posteriormente, pouco antes de sua exploração comercial.

Outra importante mudança recente, que também tem passado despercebida da generalidade dos usuários da internet, é a transição do IPv4 para o IPv6. Com efeito, IPv refere-se à *versão* do protocolo IP. Quando a internet foi criada, adotou-se a versão de número 4 (*IPv4*)[6]. Nela, os endereços eram formados por quatro sequências numéricas, cada uma variando de 0 a 255. Por exemplo, *200.251.0.1*. Tal versão possibilitava um total de aproximadamente 4,29 bilhões de dispositivos conectados simultaneamente. Pode parecer muito, mas não é, pois a tendência é que cada vez mais pessoas físicas e jurídicas tenham acesso à internet e que cada uma delas possa consumir, sozinha, dezenas ou até mesmo centenas de endereços IP.

6 Descrição técnica completa em: UNITED STATES OF AMERICA, 1981. As três versões anteriores foram utilizadas nos primórdios da rede, quando ela ainda era restrita aos EUA.

Logo se conclui que a quantidade total de endereços iniciais estava fadada a acabar algum dia, inviabilizando a inclusão de novos usuários e/ou dispositivos[7].

Para superar tal problema, desenvolveu-se outra versão do protocolo IP, denominada *IPv6*[8]. Por meio dela é possível oferecer, simultaneamente, alguns trilhões de vezes o número máximo de endereços suportados pelo IPv4. Um montante assustador, que dificilmente se esgotará, por mais que aumente o número de dispositivos conectados à rede.

O IPv6 baseia-se num sistema hexadecimal, combinando letras e números. Ele está sendo implantado paulatinamente, coexistindo com o IPv4. Por exemplo, o endereço eletrônico *www.facebook.com* correspondia, em março de 2016, ao IPv4 *200.175.89.139* e ao IPv6 *2a03:2880:2130:cf24:face:b00c:0:25de66.220.158.68*[9].

Até aqui foram pontuadas algumas mudanças em camadas periféricas da internet (camadas física, de conexão e de aplicações). Nenhuma delas, porém, atingiu o coração da rede, a ponto de alterar os princípios do *design* original, como o funcionamento dos protocolos TCP/IP. Ocorre que também esse tipo de mudança – muito mais grave e polêmica – já está acontecendo. Ela consiste na introdução de tecnologias para o monitoramento do próprio *conteúdo* dos pacotes (*deep packet inspection* – DPI) (GEIST, 2015, p. 646).

O DPI consiste num *software* capaz de examinar tanto as informações de roteamento dos pacotes (*headers*), que indicam sua origem e destino, quanto o próprio conteúdo de cada pacote de dados. Isso ocorre quando os dados passam por determinado ponto da rede, onde o *software* está programado para agir[10]. Deste ponto em diante, é possível *discriminar pacotes*, definindo se eles devem prosseguir ou ser descartados, bem como impor velocidades diferenciadas para a transmissão de cada um deles. O acesso aos *headers* é necessário e lícito, pois é indispensável ao fluxo de dados na internet. O que não se admite é a discriminação entre pacotes, feita a partir dessas informações.

Isto era absolutamente *impensável* nas origens da internet, pois, como visto, a rede mundial de computadores foi concebida com base no princípio da modularidade. Ademais, *os protocolos TCP/IP funcionavam de maneira neutra*, transmitindo quaisquer

7 Fenômeno apelidado, jocosamente, de *IPcalypse*.

8 Descrição técnica completa em: UNITED STATES OF AMERICA, 1998.

9 O uso de IPs dinâmicos não foi levado em consideração, para simplificar o exemplo.

10 Tais programas normalmente são operados pelos provedores de acesso à internet.

pacotes de dados, independentemente de sua origem, destino ou de qual espécie de dado se tratava. Somente na camada superior da rede é que os dados seriam identificados, por cada aplicação específica, a fim de gerar o resultado final (um filme, música, texto, etc).

Ocorre que isso mudou. Atualmente, boa parte da infraestrutura física da internet pertence à iniciativa privada (VERGUEIRO, 2015, p. 634-635). Assim, não é surpresa que interesses patrimoniais privados estejam por trás das principais mudanças recentes no funcionamento da rede. Uma das mais polêmicas é justamente a introdução do DPI. A partir desta tecnologia, os provedores de serviços na internet adquiriram poder antes inimaginável. Eles são capazes de manipular a forma como os usuários percebem a rede, conferindo maior velocidade a alguns pacotes de dados em detrimento de outros. Ou até mesmo interrompendo a transmissão de determinados pacotes. Retomando o exemplo dos Correios, é como se os provedores pudessem ler todas as correspondências postadas, escolhendo se e quando irão entregar cada uma delas. O destinatário tenderia a pensar que alguns serviços são mais eficientes do que os outros, porque as correspondências relativas a eles (por exemplo, os boletos para pagamento), sempre chegam primeiro, enquanto outros costumam atrasar. Imagine, agora, a gama de interesses comerciais, políticos e ideológicos que poderiam pautar esse tipo de discriminação.

Práticas desta natureza, por parte dos Correios, soariam absurdas e inaceitáveis. Porém, na internet elas já vêm ocorrendo com grande frequência e muitos usuários sequer sabem disto (GEIST, 2015, p. 650). Essa mudança estrutural na internet, então, *desnaturou a sua principal característica*, que era justamente a *neutralidade* dos protocolos TCP/IP em relação ao conteúdo transmitido.

O tópico seguinte irá demonstrar como essa mudança estrutural nas camadas centrais da rede ocasiona gravíssimas consequências, tanto micro quanto macroeconômicas, em âmbito mundial.

5 O que isto influencia na sua vida

O tema deste texto não interessa apenas às grandes corporações, ainda que interesse também a elas. Tampouco se restringe a programadores de sistemas ou a internautas engajados (os conhecidos *ativistas*). Ele afeta a vida de *todas* as pessoas que usam, já usaram ou algum dia pretendem utilizar a internet. Apenas no Brasil, cerca de 86 milhões de pessoas utilizam frequentemente a internet (CAPUTO, 2016). Em suma, bilhões de pessoas espalhadas pelo mundo. Este assunto afeta, indiretamente,

até mesmo quem ainda não tem acesso à rede mundial de computadores. Trata-se de um problema com repercussões micro e macroeconômicas, tanto no plano interno do Brasil quanto no plano internacional, capaz de interferir na própria organização e funcionamento dos mercados.

Com efeito, a arquitetura de uma rede influencia diretamente no custo para alterá-la no futuro. No caso da internet, seu *design* original propiciava *baixo custo de inovação*, porque novos produtos ou serviços, em regra, demandariam alteração apenas na camada superior, de aplicações, permanecendo intactas todas as demais (VAN SCHEWICK, 2010, p. 116; 151). É claro que esta regra não é absoluta, uma vez que certos tipos de inovação na camada de aplicações demandam alteração também nas camadas inferiores da rede, para assegurar a boa qualidade dos serviços. Por exemplo, a transmissão de vídeos em tempo real (*streaming*) tornou necessários certos aprimoramentos nas camadas física e de conexão, a fim de que o aumento no fluxo de dados não sobrecarregasse a rede. Até mesmo nas camadas TCP/IP são necessárias, eventualmente, mudanças nos protocolos para adequá-los a novas aplicações. O IPv6, já citado, é um bom exemplo. O que importa deixar claro é que, em todos esses casos, o *design* original da rede – e os princípios que guiaram a sua criação – foram *preservados*.

Diversamente, nas redes que apresentam *design* integrado, o custo de qualquer alteração tende a ser maior, pois não basta a mudança em apenas um ou alguns módulos, é necessária a adaptação da infraestrutura por inteiro (VAN SCHEWICK, 2010, p. 121). E quanto maior o custo, mais difícil se torna para os pequenos empreendedores lançarem novos produtos ou serviços. Consequentemente, as redes integradas apresentam duas desvantagens: 1) encarecem a inovação; e 2) tendem a concentrá-la em um número menor de sujeitos, justamente aqueles que disponham dos recursos suficientes para suportar os custos de alterações profundas na infraestrutura da rede.

Dessa forma, a arquitetura de uma rede de computadores certamente influencia *quem* é capaz de inovar. Mas não apenas isso. Ela repercute, ainda, sobre outros aspectos. Sendo os custos da inovação proibitivos para os pequenos empreendedores, ela tende a se concentrar apenas nas grandes companhias, como Google, Facebook, Apple e Microsoft. Então, são os interesses destas companhias que irão pautar *o que* deve ser criado e *quando*.

> Em um modelo extremo, o fortalecimento do núcleo central da arquitetura pode levar a modelos de comunicação similares ao que ocorre na televisão tradicional – ainda que os usuários tenham a escolha de mudar o canal, o fluxo de comunicação será fundamentalmente unidirecional, e as decisões sobre disponibilidade de conteúdo e uso de aplicações será restrita aos interesses daqueles que gerenciam o *core* da rede. (RAMOS, 2015, p. 149).

Numa arquitetura de rede plenamente integrada, criações que hoje trazem imenso conforto e satisfação aos usuários, como *WhatsApp* e *Skype*, provavelmente não existiriam. Essas aplicações têm em comum o fato de terem surgido como alternativa à comunicação tradicional, por telefone, razão pela qual enfrentaram forte resistência por parte das operadoras de telefonia. É de se supor, então, que essas operadoras não teriam desenvolvido algo que, à época, conflitava com o seu modelo de negócios.

Assim, a criação desses aplicativos somente foi possível graças ao *design* original da internet. Neste modelo, *o poder criativo é deslocado* do centro (grandes companhias) para as pontas (usuários finais). Contanto que qualquer usuário possa se valer da infraestrutura de rede previamente construída, sem necessidade de adaptações, torna-se consideravelmente mais simples e barato desenvolver novos produtos ou serviços e, ato contínuo, disponibilizá-los ao mercado, eventualmente, até em âmbito mundial. Mark Zuckerberg, fundador do *Facebook*, por exemplo, custeou os primeiros servidores que abrigaram a famosa rede social por apenas USD 85,00 ao mês (VAN SCHEWICK, 2010, p. 206).

Mesmo quando necessário financiamento externo, a arquitetura modular mostra-se mais favorável. Ela permite a captação de recursos de forma alternativa ao mercado financeiro e a menor custo, como no caso do *crowdfunding*.

> [...] pode-se afirmar que o crowdfunding consiste numa forma alternativa de financiamento que conecta diretamente, por meio da internet e das redes sociais, aqueles que podem ofertar, emprestar ou investir recursos com aqueles que necessitam de financiamento para projetos ou negócios específicos. (MARTINS; DA SILVA, 2014, p. 26).

Isso confere *maior liberdade e maleabilidade aos desenvolvedores*, na medida em que não precisam se sujeitar a ingerências externas em suas ideias e planos de negócio, o que fatalmente ocorreria se dependessem do financiamento proveniente de fundos de investimento ou de grandes companhias.

Ocorre que o *design* original da internet, capaz de propiciar a inovação descrita anteriormente, mesmo contra a vontade das grandes companhias do setor, está

sofrendo várias mudanças, e as mudanças são ainda muito mais profundas do que as experimentadas em épocas passadas. Dependendo do tipo e da maneira como elas se consolidarem, podem ficar comprometidas: a inovação, a liberdade de expressão, a privacidade e o próprio funcionamento dos mercados.

Com efeito, se a internet não houvesse sido projetada com base na comutação de pacotes, na modularidade, na divisão em camadas e na execução de aplicações na camada superior, certamente ela não teria se tornado o que é hoje. Funcionalidades e aplicativos com os quais o mundo se acostumou simplesmente não existiriam. E o pior de tudo, as pessoas não perceberiam isso nem sentiriam falta, porque sequer teriam experimentado essas funcionalidades.

Um exemplo ilustra bem o ponto. Hoje, a tecnologia *peer-to-peer* ou P2P está consolidada e permite o fácil compartilhamento de arquivos, para as mais diversas finalidades (KRISHNAN; SMITH; TELANG, 2003, p. 1)[11]. Porém, quando foi desenvolvida, ela sofreu duros ataques e somente persistiu graças ao *design* original da internet.

A primeira plataforma *online* que permitiu aos usuários compartilhar músicas gratuitamente, em escala mundial, foi o Napster[12]. Este aplicativo era fortemente baseado na tecnologia P2P. Diante do seu sucesso e rápido crescimento, o Napster foi processado pela indústria fonográfica norte-americana, uma vez que as músicas estavam sendo transferidas sem o pagamento de *copyrights*[13]. Este processo judicial redundou na extinção da empresa. Apesar disto, a tecnologia P2P, em si mesma, não foi atingida. O caso preservou a configuração original da internet, na medida em que suas consequências se restringiram à camada superior da rede, alcançando especificamente a aplicação Napster.

Justamente por isso, a tecnologia P2P continuou disponível e, através dela, foram posteriormente desenvolvidos vários outros produtos e serviços de enorme sucesso, sem os vícios de ilegalidade do Napster, como o *Skype*. Outros serviços de base tecnológica ainda trazem desafios jurídicos, como o *Uber* e o *Airbnb*. O fato é que não teria sido possível o surgimento de qualquer um deles se, em decorrência do caso Napster, a infraestrutura da internet, em suas camadas inferiores, tivesse sido atingida a fim de inviabilizar o P2P.

---

11 Algumas delas, evidentemente, ilícitas. O que não significa que a tecnologia P2P seja, em si mesma, nociva. Afinal, toda tecnologia tende a ser neutra. O uso que fazemos dela é que a torna boa ou ruim.

12 Para maiores detalhes sobre o Napster, consulte-se: WU, 2003.

13 Sobre este caso, vide: UNITED STATES OF AMERICA, 2000; PARENTONI, 2007, p. 178-184.

No entanto, alterações deste tipo estão ocorrendo atualmente, com bastante intensidade e rapidez. A crença de que as características originais da internet permaneceriam sempre as mesmas já foi superada[14]. É inegável que, nos últimos anos, ela vem sofrendo alterações com o nítido propósito de possibilitar *maior monitoramento e controle*[15]. Uma das mais agressivas mudanças é a interferência nos protocolos TCP/IP, substituindo a característica original da neutralidade pelo monitoramento dos pacotes de dados, não apenas quanto à origem e ao destino, mas também em relação ao próprio conteúdo de cada pacote. *Um dos efeitos colaterais disto é a possibilidade de discriminar o fluxo de dados, segundo determinados interesses*.

No caso da China, por exemplo, esses interesses são de natureza política e buscam institucionalizar a censura. Com efeito, o governo chinês interfere nas camadas da rede a fim de bloquear o acesso a quaisquer *sites* que, supostamente, disponibilizem *conteúdo impróprio*, assim entendido qualquer conteúdo de natureza política contrário aos interesses do próprio governo (LEMOS, 2015, p. 79). Isto é possível porque os grandes provedores de conexão às redes internacionais (*backbones*), na China, são todos submetidos à estrita fiscalização e controle governamental.

> No topo da cadeia alimentar está um pequeno punhado de empresas, como a AT&T e a Sprint, que operam grandes redes internacionais de *backbone* com milhares de roteadores conectados por links de banda larga de fibra óptica. Esses ISPs não pagam para o trânsito. Eles são geralmente chamados Nível 1 ISPs e se diz que formam a espinha dorsal da Internet, uma vez que todas as pessoas devem se conectar a eles para serem capazes de alcançar toda a internet. (TANENBAUM; WETHERALL, 2011, p. 64, tradução nossa).

Esses provedores, então, asseguram que endereços IP provenientes da China fiquem impedidos de acessar determinados *sites* estrangeiros, sobretudo jornais e portais de notícias[16]. Numa analogia jocosa com as famosas Muralhas da China, esta prática ficou mundialmente conhecida como *The Great Firewall of China* (SOLUM; CHUNG, 2004, p. 896-910).

Não só os Estados têm interferido no funcionamento da internet, o mercado também tem feito isso. Grandes *players* internacionais, como Google, Microsoft, Facebook, Apple e congêneres continuamente monitoram o uso da rede. A intenção

14 Emblemático a esse respeito: BARLOW, 1996.

15 Vide, por exemplo: LESSIG, 1991, p. 501-549; LESSIG, 2006; ZITTRAIN, 2008; RODOTÀ, 2008.

16 Para saber se determinado site está ou não bloqueado na China, basta fazer um teste digitando o seu endereço em: http://www.greatfirewallofchina.org/

é identificar hábitos de consumo e, a partir disto, traçar um perfil dos internautas capaz de viabilizar a venda de produtos e serviços direcionados a eles (BAKER, 2009). Neste contexto, os dados adquirem considerável valor econômico (DE FRANCESCHI; LEHMANN, 2015, p. 51), sendo os principais responsáveis por custear serviços aparentemente gratuitos, como as contas de *e-mail* ou as redes sociais. Em todos estes casos, o pagamento é feito indiretamente. Ao invés de pagar em dinheiro, da maneira tradicional, permite-se que o prestador do serviço tenha acesso à privacidade do usuário e lucre a partir dela (LEONARDI, 2015, p. 528). É o interesse econômico guiando a discriminação no fluxo de dados. Por essa e outras razões é que se diz, atualmente, estar em curso a *Era dos Grandes Dados* (vide, por inteiro: MAYER-SCHÖNBERGER; CUKIER, 2013).

Outra forma de discriminação baseada no interesse econômico é o *traffic shaping*. Ela consiste em aumentar a velocidade e a qualidade dos serviços próprios e, ao mesmo tempo, reduzir a dos concorrentes, para prejudicar estes últimos. Isto causa no usuário final a falsa impressão de que um dos serviços é melhor do que o outro. Imagine, por exemplo, um provedor de conexão à internet (responsável, portanto, pela velocidade e pela qualidade da conexão) que também é – diretamente ou via empresa do mesmo grupo econômico – prestador do serviço de *streaming* de vídeo. Graças às mudanças pelas quais a internet passou nos últimos anos, este provedor pode reduzir a velocidade de acesso de seus usuários ao serviço concorrente, prejudicando a sua qualidade, a fim de induzi-los a utilizar o serviço prestado pelo próprio provedor de acesso. No Brasil, a NET (provedora de conexão) poderia aumentar a velocidade do serviço *Now* (seu *streaming* de vídeo) e, ao mesmo tempo, reduzir a do *Netflix* (principal concorrente do *Now*). Nesse contexto, os assinantes da NET teriam a falsa impressão de que o *Now* é muito melhor do que o *Netflix*. Em outros países, práticas deste tipo resultaram em acirradas disputas judiciais.

Nos EUA, por exemplo, o maior provedor de acesso do país (*Comcast*) artificialmente reduziu a velocidade do principal serviço concorrente (*Netflix*), a fim de induzir seus clientes a optarem pelo serviço do próprio provedor (NBC). O caso gerou uma demanda judicial que terminou com acordo por meio do qual a *Netflix* passou a pagar valores extras à *Comcast*, para que esta não reduzisse a velocidade de acesso de seus usuários ao serviço prestado pela *Netflix*. Na sequência, os demais concorrentes se viram forçados a buscar acordos semelhantes com a *Comcast* (ESTADOS UNIDOS DA AMÉRICA, 2010).

Outra espécie de *traffic shaping* ocorre quando o provedor de acesso à internet deliberadamente reduz a velocidade de certas aplicações, não para prestigiar serviço próprio, mas simplesmente porque deseja *inviabilizar* o uso dessas aplicações. Isto é muito comum em relação ao P2P. A diferença em relação ao caso Napster é que agora não estão sendo combatidas, simplesmente, algumas aplicações baseadas nessa tecnologia, ao argumento de que estimulariam fraudes. O próprio funcionamento da internet vem sendo alterado para prejudicar o P2P como um todo, quaisquer que sejam as aplicações que o utilizem ou as suas finalidades.

Para justificar isso, o argumento dos provedores de acesso é o de que o P2P normalmente é utilizado para transmitir grandes pacotes de dados, o que poderia sobrecarregar a rede, diminuindo a velocidade disponível para as demais aplicações. Numa metáfora, é como se a internet fosse uma grande avenida. Quanto mais carros trafegando simultaneamente, mais lento tende a ser o fluxo geral do trânsito. Os carros, nesta alegoria, seriam os pacotes de dados e o P2P representaria lentos caminhões que travam o fluxo dos demais veículos. Nos próximos tópicos, será demonstrado que esse argumento é falacioso, pois existem alternativas diferentes da restrição ao P2P, como, por exemplo, a implantação da largura de banda simétrica, em substituição do atual modelo de banda assimétrica (VAN SCHEWICK, 2010, p. 69-70).

Por ora, basta frisar que o *traffic shaping* claramente subverte as características originais da internet. Ele tende a acentuar a formação de monopólios e a concentração de poder econômico, sufocando a inovação e o compartilhamento de conteúdo, sobretudo aquele proveniente de pequenos desenvolvedores. Também significa censura velada, uma vez que o usuário se vê impedido de utilizar certas aplicações com a qualidade e a velocidade que delas se espera, em virtude de escolha unilateral do provedor de acesso. Isto repercute diretamente sobre *quem* será capaz de inovar, *o que* poderá ser criado, *quando* haverá inovação e com base em *quais valores/objetivos*. Afeta, portanto, a vida de bilhões de pessoas e o funcionamento da internet em âmbito mundial. Como o Direito vem reagindo a tudo isso? Este é o assunto do próximo tópico.

6 A principal resposta regulatória: neutralidade de rede

Diante das inúmeras repercussões que acarreta, a mudança na infraestrutura da internet vem atraindo a atenção das mais diversas áreas da ciência, inclusive do Direito. A principal resposta jurídica a esse problema é conhecida como princípio da neutralidade de rede (*net neutrality*) (WU, 2003, p. 165).

> Embora a definição da neutralidade da rede está aberta a algum debate, em sua essência é o compromisso de assegurar que os fornecedores de serviços de Internet (ISPs) tratem todos os conteúdos e aplicações igualmente, sem privilégios, sem degradação de serviço ou priorização baseado em fonte, em propriedade do conteúdo ou em destino. [...] A adoção de uma abordagem neutra, em outras palavras, exige a adesão estrita a regra de um cardinal: que os ISPs transportem dados, sem discriminação, preferência ou consideração por conteúdo. (GEIST, 2015, p. 641, tradução nossa).

> [Neutralidade da rede existe] para proibir operadores de banda larga, na ausência de uma exibição de dano, de restringir o que os usuários fazem com a sua conexão de internet, dando ao operador a liberdade geral para gerenciar o consumo da largura de banda e outros assuntos de interesse local. O princípio consegue isso por meio da adoção do princípio básico de que operadoras de banda larga devem ter plena liberdade de 'policiar eles próprios' (rede local) enquanto que as restrições com base em indícios inter-rede devem ser vistas com desconfiança. (WU, 2003, p. 165, tradução nossa).

De acordo com Wu, os provedores de serviços na internet – sobretudo os provedores de acesso (ISPs) – não podem, dentro de certos limites, discriminar os pacotes de dados que trafegam por sua infraestrutura, em virtude da origem, do destino ou do conteúdo desses dados. Busca-se, com isso, preservar a plena informação e a autonomia decisória dos usuários da internet, a fim de que não sejam ilicitamente manipulados para optar por determinado produto ou serviço.

A neutralidade de rede é um assunto polêmico, em âmbito mundial. Nos EUA, emblemático a respeito das divergências sobre o tema foi o debate público entre Tim Wu, (favorável à neutralidade de rede) e Christopher Yoo (contrário a ela) (WU, 2007, p. 575-592). No Brasil, o embrião deste princípio já constava da Lei Geral das Telecomunicações, no art. 3º, III e IV, bem como no art. 7º, V e VI. Após longos e acalorados debates, o tema foi positivado também no Marco Civil da Internet, em abril de 2014. Esta lei incluiu a neutralidade de rede como princípio sobre o uso da internet no Brasil, tendo-lhe dedicado, ainda, seção específica:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
[...]
IV - preservação e garantia da neutralidade de rede;
Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
[...]
V - manutenção da qualidade contratada da conexão à internet;
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

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; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo. (BRASIL, 2014).

A neutralidade de rede, inclusive, foi um dos pontos mais polêmicos do Marco Civil da Internet, tendo sido discutida durante toda a tramitação legislativa[17]. Estima-se que se não fosse pelo escândalo de interceptação das comunicações eletrônicas de diversos Estados, por parte do Governo dos Estados Unidos da América (conhecido como *caso Edward Snowden*), talvez até hoje o Marco Civil não houvesse sido aprovado no Congresso Nacional. Principalmente porque a prioridade, nos anos seguintes, passou a ser a grave crise econômica e política que se instalou no país.

Em geral, a literatura jurídica brasileira tem se mostrado favorável ao Marco Civil da Internet, ainda que existam, evidentemente, críticas à maneira como a neutralidade de rede foi tratada. Exemplos de críticos são Casseb: "Perdoem-me os ardorosos defensores do novel Estatuto, mas com os olhos postos na Constituição da República não se constata grande novidade na disciplina legislativa recém nascida" (2015, p. 255; 257); e Tomasevicius Filho:

> Em tese, essa pretensão de neutralidade pode ser benéfica aos usuários de Internet no Brasil, mas talvez tenha pouco efeito prático porque, se a rede é de escala mundial, com tráfego de dados de um ponto a outro do mundo, de nada adianta tal neutralidade se outros países não exigem a neutralidade de suas redes em seus territórios. Não parece ser possível que os dados trafeguem no Brasil com neutralidade se esses mesmos dados não trafegarem nas mesmas condições nas redes dos demais países. (2015, p. 59-60).

Entende-se que essa lei – apesar de relevante e oportuna – não é um fim em si mesma. Ela representa, tão somente, mais um passo rumo à regulação jurídica do tema. Para que a neutralidade de rede de fato atinja os objetivos a que se propõe, na visão deste autor, é preciso: 1) contextualizá-la segundo o *design* original da internet e sua infraestrutura; e 2) compreender os seus limites.

Vale destacar, ainda, que no apagar das luzes de seu governo, *menos de 24h antes de ser afastada* em razão do processo de impeachment, a então Presidente Dilma Rousseff editou o Decreto nº 8.771, de 11 de maio de 2016, regulamentando o Marco Civil da Internet, no que toca a dois temas polêmicos: 1) neutralidade de rede; e 2) tratamento de dados pessoais (BRASIL, 2016).

Apesar da eventual censura quanto ao momento – político e jurídico – no qual esse Decreto foi editado, as normas dele constantes, em geral, estão em sintonia com as ideias defendidas neste texto e podem ser consideradas um avanço na matéria.

17 Para um histórico detalhado do tema, recomenda-se: LEMOS, 2015.

7 O design da internet e os limites da neutralidade de rede

Tanto no Brasil quanto no mundo[18], o debate sobre a neutralidade de rede é altamente polarizado.

> O tema da neutralidade da rede é muitas vezes carregado de vieses e discursos ideológicos que pouco tem a ver com a pesquisa científica. Empresas, ativistas políticos, lobistas e parlamentares, ainda que desempenhando papéis válidos dentro do debate político, muitas vezes carregam seus discursos com argumentos rasos e com pouca evidência empírica, em nada contribuindo para o debate mais profundo sobre os efeitos da regulação da neutralidade da rede para a sociedade. (RAMOS, 2015, p. 152).

De um lado, aqueles *contrários* a ela argumentam, basicamente, que a neutralidade absoluta contraria a própria noção de mercado, pois elimina vantagens competitivas, desestimulando o investimento em pesquisa e inovação. Afinal, o que motiva a inovação é justamente o monopólio temporário conferido pelo sistema de propriedade intelectual, para que o criador se reembolse dos custos em que incorreu e ainda obtenha lucro. Caso ele não receba tratamento diferenciado a seus produtos, serviços ou processos, em detrimento dos concorrentes, não haverá estímulo para inovar. Os que assim pensam também defendem que o tratamento diferenciado a certos pacotes de dados é ínsito ao próprio gerenciamento das redes informatizadas, de modo que uma rede plenamente neutra teria baixa qualidade dos serviços e acarretaria a insatisfação dos usuários. Certos controles são indispensáveis, como, por exemplo, a filtragem dos pacotes para combater o *spam* (PARENTONI, 2012, p. 48) ou para evitar que alguns poucos usuários (*heavy users*) consumam toda a conexão, prejudicando os demais. Esses e outros argumentos são típicos dos provedores de acesso à internet e das grandes companhias do setor de telecomunicações. Em última análise, tais agentes pretendem assegurar-se plena liberdade para gerenciar a conexão dos usuários, como bem entenderem.

No extremo oposto encontram-se os *defensores* da neutralidade de rede, geralmente alguns governos, organizações não governamentais, internautas mais engajados e certos acadêmicos. Sustentam que a neutralidade de rede se coaduna com o *design* original da internet, tendo sido a grande responsável pelo fato de a rede mundial de computadores ter se tornado o sucesso que é. Acrescentam que preservar este *design* é vital para manter o caráter colaborativo e o potencial

18 Para argumentos tanto a favor quanto contra a neutralidade de rede, confira: LENARD; MAY, 2006.

inovador da internet. Assim, qualquer filtragem dos pacotes de dados seria, *a priori*, nociva. Mesmo aquelas baseadas em razões de segurança ou no gerenciamento da rede deveriam ser justificadas e adotadas apenas em caráter excepcional. Além disso, a filtragem de pacotes poderia ocasionar censura ou restringir ilegalmente as escolhas do usuário, como no caso do *traffic shaping*. Portanto, apontam no sentido de dilatar, ao máximo, o alcance da neutralidade de rede.

O presente texto não se vincula a qualquer destes extremos. Na realidade, considera-se que ambos trazem argumentos relevantes, os quais precisam ser ponderados, a fim de compreender os limites da neutralidade de rede. Busca-se, com isto, uma *via intermediária*, que reconheça a necessidade de preservar as vantagens competitivas do empresário (qualquer que seja o seu porte econômico) e, ao mesmo tempo, possibilitar que desenvolvedores independentes e pessoas comuns utilizem a internet como ferramenta para a inovação e o compartilhamento de conteúdo. Nesse sentido, *o que se propõe é uma regulação jurídica que primeiro compreenda o funcionamento da internet para então fixar limites à neutralidade de rede, consentâneos com as mudanças estruturais experimentadas nos últimos anos*.

Ora, se o *design* original da internet se baseou em determinados princípios, já abordados neste texto, assim também deve ocorrer quanto a sua regulação jurídica. Dois princípios jurídicos merecem destaque: 1) comunicação de ponta a ponta (*end-to-end*); e 2) preservação das camadas de rede (*layers principle*).

Do ponto de vista da arquitetura de redes de computadores, o princípio *end-to-end* é antigo e dispõe que as camadas inferiores da rede devem ser projetadas para funcionar da maneira mais simples possível, ficando a complexidade reservada à camada superior, de aplicações (SALTZER; REED; CLARK; 1984, p. 277-288). Desse modo, aplicações as mais diversas e com diferentes graus de complexidade poderiam coexistir, todas se beneficiando da mesma infraestrutura padrão para a transferência dos dados, o que demanda menos alterações na rede, tornando-a estável. No caso da internet, isso significa que os protocolos TCP/IP deveriam sofrer o mínimo possível de intervenções. A inovação deveria ocorrer, preferencialmente, na camada superior, com o desenvolvimento de novas aplicações.

Transposto para o Direito, décadas depois, este princípio dispõe que *a regulação jurídica da internet deve focar na camada de aplicações, preservando, tanto quanto possível, o design original das demais camadas de rede* (LESSIG, 2006, p. 44). O caso Napster, já citado, é um bom exemplo. Nele foi possível combater uma conduta ilícita sem, com isto, alterar a estrutura da internet ou comprometer a tecnologia

P2P. Tanto que aplicações surgidas posteriormente se valeram do P2P para prestar novos serviços. Por outro lado, o modelo chinês utilizou os protocolos TCP/IP para censura política, o que seria proibido segundo este princípio.

Há autores que destrincham o princípio em duas vertentes. Pela vertente ampla (*broad version*) (VAN SCHEWICK, 2010, p. 96), o *end-to-end* determina que *as camadas de rede inferiores devem prestar serviços cada vez mais padronizados e simplificados*. Por exemplo, a camada física (cabos de conexão) cuida exclusivamente de transportar os dados em sua forma bruta. A maneira de se conectar a ela é padrão. Inversamente, a camada superior, de aplicações, desempenha as mais diversas atividades. Nela são realizadas desde tarefas simples até as mais complexas, envolvendo o processamento dos dados para gerar resultados como textos, imagens, vídeos, etc. Em consequência, *alterações em alguma camada da rede somente devem ser feitas caso possam ser integralmente implementadas nessa camada, sem necessidade de alteração das demais*. E, ainda, quando essas alterações forem *imprescindíveis para todos os serviços que se utilizam dessa camada*. Por exemplo, não se justifica alterar os protocolos TCP/IP para melhorar a qualidade de uma aplicação específica, porque isso não é imprescindível para o funcionamento das demais. Essa atitude acarretaria quebra do padrão das camadas inferiores, acrescentando-lhes uma complexidade desnecessária. Ademais, esse tipo de mudança pode comprometer a simplicidade e a estabilidade da rede. Por outro lado, a substituição dos cabos de cobre por fibra ótica é uma alteração passível de ser implementada exclusivamente na camada física, capaz de beneficiar a todos os serviços que dela se utilizem, sem que haja aumento de complexidade nessa camada. Esta substituição, portanto, estaria de acordo com o princípio em exame.

A versão restrita desse princípio (*narrow version*) (VAN SCHEWICK, 2010, p. 90) dispõe que *todas as alterações que não possam ser implementadas exclusivamente numa camada da rede*, ou que não beneficiem indistintamente todos os serviços que se utilizam dessa camada, *devem ser implementadas na camada de aplicações, funcionando de ponta a ponta*, exclusivamente entre remetente e destinatário (*end-to-end*). Assim, caso seja desenvolvida aplicação que requer funcionalidade até então inexistente (como um novo tipo de identificação biométrica, por exemplo), é preciso que toda a tecnologia necessária para o seu funcionamento seja embutida na própria aplicação. Dessa forma, basta que os usuários tenham essa aplicação instalada em seus dispositivos para que possam se comunicar, sem necessidade de qualquer alteração na infraestrutura da internet.

Outro princípio jurídico relevante é a preservação das camadas de rede (*layers principle*) (SOLUM; CHUNG, 2004, p. 817-818). Segundo ele, *somente em casos excepcionais a regulação direcionada a uma camada pode interferir no funcionamento das demais*. Voltando ao caso da China, a solução adotada pelo governo é contrária a esse princípio porque, para combater um problema na camada de aplicações (acesso a conteúdo político), atingiu camadas centrais da rede (protocolos TCP/IP). Exemplo extremo seria um país que, pretendendo exercer máximo controle sobre a internet, mantivesse um único provedor de acesso, rigidamente fiscalizado pelo Estado. Nesse caso, o controle que deveria recair sobre a camada de aplicações incide sobre a de conexão.

A regulação que extrapola camadas de rede traz dois problemas aparentemente antagônicos: abrangência excessiva (*over inclusiveness*) e abrangência insuficiente (*under inclusiveness*). Novamente reportando ao caso da China, fica proibido o acesso a quaisquer *sites* que contenham conteúdo político extraoficial. Não obstante, muitos desses *sites* também disponibilizam outras informações, sobre assuntos variados, que não precisariam ser bloqueadas (abrangência excessiva). Por outro lado, *sites* que não se dedicam expressamente à discussão política, mas que a façam de maneira disfarçada, estariam imunes ao bloqueio (abrangência insuficiente). Por tudo isso, *a melhor regulação jurídica é aquela direcionada exclusivamente à camada onde se situa o problema – normalmente a de aplicações –, sem produzir efeitos nas demais*.

Tanto o *end-to-end* quanto o *layers principle* servem de *fundamento* à neutralidade de rede. É fato que os protocolos TCP/IP passaram por profundas mudanças nos últimos anos. Sua neutralidade originária foi substituída pela investigação pormenorizada dos pacotes. Assim, torna-se necessário fixar *limites jurídicos*, para evitar as consequências negativas desse monitoramento. Tais limites são dados, justamente, pela neutralidade de rede. Cumpre, então, melhor sistematizá-la.

A neutralidade de rede – como, aliás, qualquer outro princípio – *não* é um valor absoluto[19]. Ela deve ceder diante de certas *razões jurídicas* ou das próprias *características fáticas* da rede.

Com efeito, algumas características fáticas da internet demandam tratamento diferenciado a certos pacotes de dados, a fim de que o resultado final do seu processamento seja satisfatório (WU; YOO, 2007, p. 577). Por exemplo, a própria

19 Lembre-se que, no Brasil, sequer a vida é um valor absoluto, pois o art. 5º, XLVII, '*a*' da Constituição admite a pena de morte em caso de guerra declarada.

natureza do *e-mail*, se comparada à transmissão de vídeos em tempo real, justifica o tratamento diferenciado, pois o atraso de alguns segundos para a entrega de um *e-mail* não compromete o funcionamento dessa aplicação. Na realidade, sequer será percebido pelo destinatário. Diversamente, atrasos constantes na exibição de um vídeo (*travamento*), mesmo que por poucos segundos, prejudicam o funcionamento dessa aplicação. Dos pontos de vista fático e técnico-operacional, portanto, justifica-se o tratamento diferenciado a esses pacotes de dados, reservando-se maior velocidade de transmissão ao *streaming* de vídeo, se comparado ao *e-mail*. O Marco Civil da Internet no Brasil *admite*, expressamente, esse tipo de discriminação no art. 9º, § 1º, I (gerenciamento de redes), desde que amparada em razões técnicas, em prol da maior qualidade dos serviços (BRASIL, 2014). O Decreto nº 8.771/2016, editado para regulamentar o Marco Civil da Internet, esclarece como podem e devem ocorrer essas limitações. Principia dizendo que elas alcançam apenas os *provedores de conexão e de aplicações de internet*.

> Art. 1º Este Decreto trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações contidas na Lei nº 12.965, de 23 de abril de 2014.
>
> 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.
>
> Art. 6º Para a adequada prestação de serviços e aplicações na internet, é permitido o gerenciamento de redes com o objetivo de preservar sua estabilidade, segurança e funcionalidade, utilizando-se apenas de medidas técnicas compatíveis com os padrões internacionais, desenvolvidos para o bom funcionamento da internet, e observados os parâmetros regulatórios expedidos pela Anatel e consideradas as diretrizes estabelecidas pelo CGIbr. (BRASIL, 2016).

Não atingem, por exemplo, *serviços de telecomunicações que não se destinem ao provimento de conexão de internet* ou aqueles *destinados a grupos específicos de*

usuários com controle estrito de admissão, como é o caso das redes privadas (*intranets*), conforme art. 2º, parágrafo único, do mencionado Decreto.

Outra causa fática lícita para a discriminação no fluxo de dados diz respeito aos *serviços de emergência* mencionados no art. 9º, § 1º, II da Lei nº 12.965/2014. É inclusive recomendável priorizar os pacotes de dados que lhes digam respeito, tais como as informações policiais ou de saúde pública, conferindo-lhes maior velocidade de transmissão. Quais são especificamente esses serviços é matéria que deverá constar de normativa a ser expedida pela Agência Nacional de Telecomunicações – ANATEL, conforme art. 8º, I do Decreto nº 8.771/2016.

Em situações ainda mais excepcionais, como a guerra formalmente declarada, seria lícito até mesmo interferir nas camadas física e de conexão, a fim de dificultar ou suprimir o acesso à internet do Estado beligerante. Se, como visto, nesse contexto até a pena de morte é admissível, mais ainda as restrições sobre a internet (VERGUEIRO, 2015, p. 633-634).

De qualquer forma, mesmo nos casos em que razões técnico-operacionais justificam o tratamento diferenciado de dados, *é dever do administrador da rede informar aos usuários quais são os critérios utilizados e como serão tratadas as diversas espécies de dados* (BRASIL, 2014, art. 9º, § 2º, III) (BRASIL, 2016, art. 5º e 7º). Até para que os usuários, eventualmente, possam questionar eventuais posturas desprovidas de embasamento técnico ou desproporcionais.

Essas e outras exceções levam à conclusão de que, apesar de internacionalmente consagrada, a nomenclatura *neutralidade de rede* talvez não seja a mais adequada. Afinal, a internet dos dias de hoje não é neutra. Existem distinções absolutamente necessárias e legalmente admitidas. O que esse princípio busca, na realidade, é prevenir e coibir discriminações *abusivas*. Com efeito, o que a neutralidade de rede proíbe é o tratamento discriminatório a pacotes de dados *da mesma natureza*, com base no seu conteúdo, origem ou destino (FORGIONI; MIURA, 2015, p. 113-114). Por exemplo, a distinção entre dois filmes, simplesmente porque um deles é proveniente do *Netflix* e outro do *Net Now*. Distinção que pode ser feita de inúmeras formas, não apenas alterando a velocidade de acesso a alguma dessas aplicações, mas também, por exemplo, fixando que o acesso a uma delas é *grátis* (no sentido de que não será deduzido da franquia de dados do usuário), enquanto o acesso à(s) outra(s) será normalmente cobrado.

Dessa forma, é *plenamente admissível* que os provedores de acesso ofereçam *variados pacotes de serviços*, com características diferentes em cada um deles. Por

exemplo, serviços com menor velocidade e menor franquia de dados, mais baratos, e serviços com velocidade superior e maior franquia de dados (ou até sem franquia), a custo mais elevado. Isto é inerente à economia de mercado. A estratificação de um determinado serviço em planos diferentes, com características próprias e custo distinto, é algo comum nas mais diversas áreas, até mesmo na saúde, em que cada administradora de planos de saúde oferta diferentes planos. Aliás, é bom que seja assim, pois cada pessoa ou grupo possui necessidades e capacidades de pagamento específicas, não sendo razoável nem eficiente impor único modelo a todos.

O que não se admite é que o administrador da rede, fora das exceções legalmente admissíveis, manipule a conexão de seus usuários, influenciando, ainda que indiretamente, na maneira como eles utilizarão seu pacote de dados. A escolha sobre como utilizar o acesso à internet é individual, cabendo aos próprios usuários. Os provedores de acesso não podem manipular a conexão, com o objetivo de direcionar os usuários para determinados aplicativos. Esta regra, que já poderia ser perfeitamente extraída da interpretação sistemática do Marco Civil da Internet, agora consta, de maneira expressa, nos artigos 3º, 9º e 10 do Decreto nº 8.771/2016. Desde que a velocidade de conexão e os demais aspectos técnicos permaneçam os mesmos, é o próprio usuário que irá decidir entre utilizar o *Netflix* ou o *Net Now*, o *WhatsApp* ou qualquer outro aplicativo semelhante.

Além disso, *a neutralidade de rede incide sobre as camadas inferiores*, principalmente os protocolos TCP/IP, preservando a sua compatibilidade com quaisquer aplicações que já existem ou venham a existir. *Na camada de aplicações, por sua vez, a regra é a livre concorrência*. Cada desenvolvedor pode e deve criar tecnologias inovadoras, cada vez mais complexas e específicas, explorando-as onerosamente e com exclusividade, nos limites da legislação. Ou seja, a inovação se processa na camada de aplicações, de ponta a ponta (*end-to-end*), enquanto a neutralidade de rede incide sobre as camadas inferiores, para que elas não sejam manipuladas segundo objetivos antijurídicos.

Entende-se que, dessa forma, é possível assegurar, de um lado, a livre concorrência, as estratégias empresariais e suas vantagens competitivas; e, de outro, a privacidade, a liberdade de expressão, a inovação e a autonomia decisória dos usuários.

Neste ponto, há que se questionar o art. 2º, *caput*, do Decreto nº 8.771/2016, na parte em que estende a neutralidade também aos provedores de *aplicações de internet*, ou seja, à camada superior. Esse dispositivo padece de dois vícios. O primeiro é a *ilegalidade*, uma vez que inova em relação ao Marco Civil da Internet,

ampliando restrição que não está expressamente prevista em lei. Afinal, o art. 9º do Marco Civil é claro ao dispor que a neutralidade de rede se aplica ao *responsável pela transmissão, comutação ou roteamento* dos dados. Em outras palavras, se aplica aos administradores da conexão, que operam as camadas inferiores da rede, como o TCP/IP. Não há na lei previsão para que a neutralidade alcance também a camada de aplicações. São várias as razões para isso, conforme demonstrado ao longo do texto. O fato de o referido art. 9º situar-se em Capítulo intitulado *Da Provisão de Conexão e de Aplicações de Internet* não altera esse aspecto. Com efeito, *entende-se que a neutralidade de rede é direcionada especificamente aos provedores de conexão*, enquanto as demais disposições do capítulo, como a *Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas*, dirigem-se *também* aos provedores de aplicações. Visto desta forma, então, o mencionado art. 2º, *caput* exorbita dos limites fixados pela lei que pretende regulamentar.

Esse dispositivo padece ainda de um segundo vício. Com efeito*, estender a neutralidade de rede também aos provedores de aplicações, que atuam exclusivamente na camada superior da internet, conflita com os princípios constitucionais da livre iniciativa e da livre concorrência*. Como dito ao longo do texto, nessa camada a regra é que cada empresário pode beneficiar-se de vantagens competitivas, fruto das inovações a que der causa, dentro dos limites da legalidade. É justamente o privilégio *temporário* de exploração das criações intelectuais, com exclusividade (como nas patentes e no *software*), que justifica e fomenta a inovação, estimulando investimentos na área de pesquisa e desenvolvimento. Suprimir isto pode ocasionar efeitos colaterais graves.

Pelo exposto, e em sintonia com as ideias desenvolvidas ao longo de todo o texto, reitera-se que *a neutralidade de rede incide sobre as camadas inferiores*, principalmente os protocolos TCP/IP, preservando a sua compatibilidade com quaisquer aplicações que já existem ou que venham a existir. *Na camada de aplicações, por sua vez, a regra é a livre concorrência*. Cada desenvolvedor pode explorar com exclusividade, nos limites da legislação, as criações intelectuais que desenvolver. Sendo assim, *neutralidade de rede é a proibição de que os administradores da rede manipulem a conexão dos usuários, a fim de discriminar pacotes de dados da mesma natureza, com base no seu conteúdo, origem ou destino, fora das exceções legalmente admitidas*.

8 Conclusão

A internet não é obra da natureza, mas fruto de uma construção humana. Ela surgiu em decorrência de um singular momento histórico, que reuniu o interesse militar do Governo dos EUA, preocupado com a segurança nacional, e a participação da elite acadêmica daquele país, centrada no ideal de liberdade e compartilhamento de ideias. Com essas características ela se consolidou e evoluiu, tornando-se uma das mais importantes invenções da história recente da humanidade.

Todavia, a internet vem mudando consideravelmente nos últimos anos. Algumas de suas principais características foram substituídas para possibilitar maior monitoramento e controle. Os protocolos TCI/IP, que antes funcionavam de forma neutra, agora inspecionam os pacotes de dados, discriminando-os conforme a origem, o destino ou o conteúdo transmitido. Essas mudanças abriram a porta para inúmeras formas de censura e manipulação dos usuários, o que sequer era cogitado nos primórdios da internet.

Tais mudanças atraíram a atenção das mais diversas áreas da ciência, inclusive do Direito. Este texto procurou contextualizar, definir e sistematizar aquela que, na visão do autor, é a principal resposta jurídica aos novos desafios: a neutralidade de rede. A partir de sua correta aplicação talvez seja possível resgatar o equilíbrio de forças presente nas origens da internet.

9 Referências.

BAKER, Stephen. **Numerati**. Tradução: Ivo Korytowski. São Paulo: Saraiva, 2009.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Davos, 1996. Disponível em: <https://projects.eff.org/~barlow/Declaration-Final.html>. Acesso em: 28 dez. 2015.

BENKLER, Yochai. From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. **Federal Communications Law Journal**, v. 52, n. 3, 2000, p. 561-579.

BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. **Diário Oficial da União. Brasília**, 1988. Disponível em: <http://www.planalto.gov.br;ccivil_03/Constituicao.htm>. Acesso em: 22 nov. 2017.

_____. Decreto nº 8.771, de 11 de maio de 2016. **Diário Oficial da União**. Brasília, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 18 out. 2016.

_____. Lei nº 9.472, de 16 de julho de 1997. **Diário Oficial da União**. Brasília, 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9472.htm>. Acesso em: 18 out. 2016.

_____. Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial da União**. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 out. 2016.

CAPUTO, Victor. Mais da metade dos brasileiros são usuários da internet. Caderno Tecnologia. **Revista Exame**, São Paulo, 26 jun. 2014. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/mais-da-metade-dos-brasileiros-sao-usuarios-da-internet>. Acesso em: 7 abr. 2016.

CASSEB, Paulo Adib. Fundamentos Constitucionais do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015.

CASTELLS, Manuel. **La Galaxia Internet**. Tradução: Raúl Quintana. Barcelona: Plaza & Janés Editores, 2001.

COMPARATO, Fábio Konder. Capitalismo e Poder Econômico. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, número especial: em memória do Professor Washington Peluso Albino de Souza, p. 167-195, 2013.

DE FRANCESCHI, Alberto; LEHMANN, Michael. Data as Tradeable Commodity and New Measures for their Protection. **The Italian Law Journal**, Napoli, v. 1, n. 1, p. 51-72, mar. 2015.

ESTADOS UNIDOS DA AMÉRICA. Comcast Corp. *versus* F.C.C. **United States Court of Appeals for the District of Columbia**. 600 F.3d 642, j. 06.04.2010.

FORGIONI, Paula Andrea; MIURA, Yuriko Rocha. O Princípio da Neutralidade de Rede e o Marco Civil da Internet no Brasil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

GEIST, Michael. The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

HAFNER, Katie; LYON, Matthew. **Where Wizards Stay Up Late**: The origins of the internet. New York: Simon & Schuster, 1996.

KRISHNAN, Ramayya; SMITH, Michael D.; TELANG, Rahul. The Economics of Peer-To-Peer Networks. **Journal of Information Technology Theory and Application**, v. 5, n. 3, p. 1-24, 2003.

LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

LENARD, Thomas M; MAY, Randolph J. (Coord.). **Net Neutrality or Net Neutering**: Should Broadband Internet Services Be Regulated? New York: Springer, 2006.

LEONARDI, Marcel. Marco Civil da Internet e Proteção de Dados Pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

_____. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

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

_____. The Law of the Horse*:* What cyberlaw might teach. **Harvard Law Review**, n. 113, p. 501-549, Dec. 1999.

MACIEL, Rafael Fernandes. A Requisição Judicial de Registro de Conexão e Aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

MARTINS, Norberto Montani; DA SILVA, Pedro Miguel Bento Pereira. Funcionalidade dos sistemas financeiros e o financiamento a pequenas e médias empresas: o caso do *crowdfunding*. **Revista Economia Ensaios**, v. 29, n. especial (Associação Keynesiana Brasileira), p. 25-56, dez. 2014.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**. New York: HMH, 2013.

OLIVEIRA, Raquel Diniz; PARENTONI, Leonardo. Uma Advertência sobre Interoperabilidade e o Artigo 154, Parágrafo Único, do CPC. **Revista Magister de Direito Civil e Processual Civil**, Ano IV, n. 19, p. 51-73, jul./ago. 2007.

PARENTONI, Leonardo. **Documento Eletrônico**: Aplicação e Interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007.

_____. SPAM: presente, passado e futuro. **Revista de Direito das Comunicações**, ano 3, n. 5, p. 13-48, jan./jun. 2012.

RAMOS, Pedro Henrique Soares. O Marco Civil e a Importância da Neutralidade de Rede: Evidências Empíricas no Brasil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

RANCHORDÁS, Sofia. Does Sharing Mean Caring? Innovation in the Sharing Economy. **Minnesota Journal of Law, Science & Technology**, v. 16, n. 1, p. 1-63, winter 2015.

ROBERTS, Lawrence Gilman. The evolution of packet switching. **Proceedings of the IEEE**. New York: IEEE Foundation. v. 11, p. 1307-1313, Nov. 1978.

RODOTÀ, Stefano. **A Vida Na Sociedade da Vigilância**. Tradução: Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SALTZER, Jerome Howard; REED, D. P.; CLARK, David Dana. End-to-End Arguments in System Design. **ACM Transactions in Computer Systems**, v. 2, n. 4, p. 277-288. New York: ACM New York, 1984.

SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **Notre Dame Law Review**, v. 79, n. 3, p. 815-948, Jan. 2004.

TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th ed. Boston: Pearson, 2011.

TOMASEVICIUS FILHO, Eduardo. O Marco Civil da Internet e as Liberdades de Mercado. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho da União Europeia. **Carta dos Direitos Fundamentais da União Europeia**. Estrasburgo, 12 dez. 2007. Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:12012P>. Acesso em: 4 abr. 2016.

UNITED STATES OF AMERICA. The Internet Engineering Task Force – IETF. **Internet protocol**. DARPA internet program protocol specification. Arlington, setembro de 1981. Disponível em: <https://tools.ietf.org/html/rfc791>. Acesso em: 21 mar. 2016.

_____. The Internet Engineering Task Force – IETF. **Internet Protocol**, Version 6 (IPv6) Specification. 1998. Disponível em: <https://tools.ietf.org/html/rfc2460>. Acesso em: 21 mar. 2016.

_____. United States Court of Appeals for the Ninth Circuit. **Case nº 00-16401. 239 F.3d 1004**. A&M Records, Inc. v. Napster, Inc. Decided in October 2, 2000.

VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: MIT Press, 2010.

VERGUEIRO, Luiz Fabricio Thaumaturgo. Marco Civil da Internet e Guerra Cibernética: Análise Comparativa à Luz do Manual de Talin Sobre os Princípios do Direito Internacional Aplicáveis à Guerra Cibernética. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

WHITT, Richard S. A deference to protocol: Fashioning a three-dimensional public policy framework for the internet age. **Cardozo Arts & Entertainment Law Journal**, v. 31, n. 3, p. 689-768, Jul. 2013.

WU, Tim. Network Neutrality, Broadband Discrimination. **Journal of Telecommunications and High Technology Law**, v. 2, n. 1, p. 141-176, Fall 2003.

WU, Tim; YOO, Christopher S. Keeping the Internet Neutral? Tim Wu and Christopher Yoo Debate. **Federal Communications Law Journal**, v. 59, n. 3, p. 575-592, June. 2007.

YOO, Christopher S. Protocol Layering and Internet Policy. **The University of Pennsylvania Law Review**, v. 161, n. 6, p. 1707-1771, 2013.

ZITTRAIN, Jonathan. **The Future of the Internet**: And how to stop it. London: Yale University Press, 2008.