Centro de Tecnologia e Sociedade da Escola de Direito da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (CTS-FGV)

Contribuição para o Debate Público sobre a regulamentação do Marco Civil da Internet

Rio de Janeiro, 30 de abril de 2015

O documento abaixo sintetiza as contribuições do Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (CTS-FGV) à consulta pública sobre a regulamentação do Marco Civil da Internet, Lei 12.965, de 23 de abril de 2014. Seguindo a classificação feita pelo Ministério da Justiça, o documento está dividido em quatro partes: (i) neutralidade de rede; (ii) privacidade; (iii) guarda de registros; e (iv) outros temas e considerações.

1. Neutralidade de Rede

O Marco Civil salienta o valor fundamental do tratamento não-discriminatório exigido pelo princípio da neutralidade da rede: quaisquer pacotes de dados devem ser tratados de maneira isonômica, independentemente de seu conteúdo, origem e destino, serviço, terminal ou aplicação. Tal princípio é essencial para garantir o pleno gozo dos direitos humanos dos usuários, promover a inovação e a participação democrática, garantir condições de concorrência equitativas e proteger a inovação na Internet. Em outras palavras, preserva a capacidade que Internet tem de evoluir espontaneamente a partir das contribuições e inovações não filtradas de seus usuários.

Nessa seção serão abordadas algumas facetas fundamentais do debate sobre neutralidade de rede. A categoria dos serviços especializados será analisada, com a apresentação de alguns critérios úteis para identificar e caracterizar de maneira apropriada esses serviços. A compatibilidade do principio da neutralidade de rede com a priorização paga, com as práticas de zero rating, bem como a introdução de taxas adicionais serão consideradas tendo em vista seu impacto e consequências sobre o desenvolvimento da Internet no médio e longo prazo. As Content Delivery Networks (CDNs), ou redes de entrega de conteúdo, serão analisadas, destacando-se os riscos e as vantagens que elas acarretam. Subsequentemente, serão fornecidos alguns critérios úteis à identificação de técnicas de gerenciamento de redes razoáveis. O alcance e o escopo da aplicação do artigo 9° do Marco Civil serão discutidos no intuito de esclarecer a quem se destina a regra que determina a neutralidade de rede e identificar as medidas mais eficazes de fiscalização e garantia desse princípio.

1.1. Serviços Especializados

Não existe uma definição uniformemente aceita de serviços especializados. O Marco Civil não tratou da natureza dos serviços especializados, nem sobre a sua admissibilidade à luz da Lei, e o processo de consulta que levou à elaboração do Marco Civil também não abordou o tema. No

entanto, como explicaremos a seguir, serviços especializados podem se assemelhar à Internet pública em termos de experiência do usuário. Por isso, é de extrema importância que sejam corretamente definidos e delimitados, para que não possam ser usados para contornar as salvaguardas e garantias estabelecidas pelo Marco Civil. Um tratamento cauteloso dos serviços especializados pode permitir tanto a experimentação de mercado desejada quanto uma proteção efetiva da Internet e da neutralidade de rede, exigida pelo Marco Civil.

A definição de serviços especializados tem se mostrado problemática. Os seguintes elementos não foram uniformemente aceitos, mas estão comumente associados com tal conceito (FCC Open Internet Order, 2010: ¶112; EU Parliament Proposal for Single Market, 2014: 242): (a) não são comercializados por provedores de acesso à internet como um substituto para a Internet; (b) são providos pelo provedor de acesso à internet por uma taxa, de forma especialmente solicitada; (c) oferecem alguma função aprimorada, seja uma qualidade assegurada de serviço, velocidade ou segurança; (d) o nível ou tipo de serviço que providenciam não estão facilmente disponíveis na Internet pública; e (e) embora sejam oferecidos ao público, só podem ser disponibilizados para um conjunto restrito de clientes e, portanto, dependem de um controle de acesso rígido.

Uma consequência da combinação de todas as características relacionadas acima é que serviços especializados sejam oferecidos em infraestruturas diferentes daquelas usadas para o tráfego da Internet, sob o ponto de vista lógico. Vale dizer, os serviços especializados e o tráfego na Internet utilizam o mesmo equipamento, mas o operador da rede dedica recursos específicos a cada meio físico (os serviços especializados e o tráfego na Internet são transportados por fios, roteadores, etc. diferentes). Exemplos de serviços especializados incluem IPTV, telemedicina e conexões corporativas protegidas.

Inicialmente, tomando como pressuposto as características acima identificadas, serviços especializados parecem estar excluídos do alcance do art. 9° do Marco Civil da Internet. As obrigações de neutralidade de rede se aplicam à Internet como definida no art. 5°, inciso I, que trata somente do fluxo de tráfego, ou seja, "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes". Ao contrário, como explicado anteriormente, serviços especializados são usualmente distintos do tráfego da Internet, disponíveis apenas sob demanda específica, e apenas dentro da rede específica do provedor que o oferece. Entretanto, devemos frisar que este é o caso se, e somente se, os serviços especializados forem, de fato, distintos do tráfego da Internet.

Algumas críticas são feitas aos serviços especializados, no sentido de que poderiam vir a competir com a Internet. Poderia haver um deslocamento dos incentivos de investimentos dos provedores de acesso, da Internet pública para os serviços especializados. De fato, embora os serviços especializados possam aumentar a produtividade e o bem-estar ao providenciar para consumidores e desenvolvedores de aplicações os meios para oferecer novos serviços e aplicações indisponíveis anteriormente (Choi & Kim), eles também podem esvaziar os serviços, aplicações e conteúdo da Internet, enfraquecendo sua posição no ecossistema de banda larga (Hermalin & Katz, 2007), especialmente se os serviços especializados se mostrarem uma opção mais lucrativa do que a Internet pública.

O fato de que o Marco Civil apostou no desenvolvimento da Internet pública é uma indicação de que os serviços especializados, se permitidos, devem se desenvolver paralelamente a ela, e não em seu detrimento, mesmo que sob a perspectiva econômica o valor gerado pelos serviços especializados possa, em tese, superar aquele gerado pelos serviços da Internet.

Devemos ter em mente que as discussões sobre quais serviços de banda larga devem ser permitidos (e sob quais condições) não devem ser tomadas em um vácuo: o Marco Civil foi votado para preservar a Internet e garantir sua continuidade nos moldes do seu desenvolvimento atual. Portanto, na medida em que novas propostas de mercado estejam em posição de prejudicar a Internet, tais propostas devem ser tratadas com cautela.

A partir do que foi acima exposto, é recomendável que os serviços especializados sejam permitidos somente sob condições estritas de que: (a) não sejam comercializados pelos provedores de acesso à internet como um substituto à Internet pública; (b) que dependam de uma infraestrutura lógica ou fisicamente distinta daquela da qual depende a Internet pública; (c) que sejam fornecidos pelos provedores de acesso à internet por uma taxa, sob demanda específica e, portanto, formalizado por um acordo específico; (d) que os serviços especializados ofereçam alguma forma de funcionalidade aprimorada, seja em termos de qualidade de serviço, velocidade ou segurança; (e) que o nível ou tipo de serviço que seja fornecido não seja prontamente disponível na Internet pública e (f) que eles não causem um deslocamento desarrazoado de investimentos na Internet pública.

Apenas sob estas condições é que os serviços especializados possuem o potencial para beneficiar o ecossistema de banda larga, sem, ao mesmo tempo, prejudicar o seu desenvolvimento.

1.2. Priorização Paga

A priorização paga é o arranjo pelo qual dois agentes da Internet (normalmente um provedor de acesso à internet e um provedor de aplicações) acordam em trocar tráfego com maior velocidade ou uma qualidade de serviço garantida, por uma taxa adicional. O tráfego com priorização paga é parte da Internet e estaria, em princípio, disponível para o mesmo conjunto de clientes que o provedor de acesso à internet normalmente atende. Os arranjos de priorização paga geralmente são iniciados pelo provedor de acesso à internet ou pelo provedor de aplicativos embora, teoricamente, se o provedor de acesso à internet o permitir, os arranjos também poderiam ser solicitados pelos usuários finais (por ex. um cliente pede ao provedor de acesso à internet que dê prioridade a determinado tipo de tráfego).

A definição de priorização paga, de acordo com as características acima apresentadas, está em conflito com a linguagem do art. 9°, que expressamente exige o tratamento igual de todo o tráfego, independentemente da fonte, destino, conteúdo ou serviço. Portanto, se um acordo de priorização paga ocorrer em uma parte da rede que esteja no âmbito de aplicação do art. 9° (ver parágrafo seguinte), é forçoso concluir que o tratamento discriminatório decorrente deste acordo ensejará a violação das regras de neutralidade de rede consagradas no art. 9°. Acordos de priorização paga contradizem a redação e o espírito do Marco Civil, uma vez que o art. 9° inclui uma exigência ampla de que o tráfego da Internet seja tratado igualmente independentemente de origem, destinação, conteúdo ou equipamento.

A redação do art. 9° não deixa claro o escopo de sua aplicação, especialmente se incide apenas sobre as práticas internas de gestão das redes dos provedores de acesso à internet ou também sobre suas relações com outros atores, incluindo provedores de aplicação (mas também outros intermediários, como as CDNs, backbones e IXPs) e de equipamentos locais aos consumidores (modem DSL ou à cabo, equipamento para conexão via satélite etc). Isso é importante pois, se o art. 9° não incide sobre certa parte da cadeia de conexão, então não se exige desta parte que trate o tráfego e as relações comerciais de forma neutra.

Um exemplo de como está sendo tratado o tema é a discussão nos Estados Unidos. Naquele país, a Open Internet Order de 2010, que dispõe sobre regras de neutralidade da rede, explicitamente incide "only to the provision of broadband Internet access service and not to edge provider activities, such as the provision of content or applications over the Internet" (FCC Open Internet Order, 2010: ¶ 50). Em outras palavras, a Open Internet Order de 2010 não proíbe a priorização paga, muito embora a FCC tenha anunciado recentemente que vai proibir tal prática. Alguns países europeus parecem entender que os encargos de neutralidade de rede também aplicam-se à relação entre provedores de acesso à internet e provedores de aplicações (a despeito da Diretiva de Serviço Universal, que, no âmbito da União Europeia, não especifica a extensão de sua incidência – ver EU Universal Service Directive, 2002, art. 20). Na Noruega, por exemplo, a autoridade nacional reguladora deu a entender, por meio de sua Avaliação Regulatória das CDNs (NKOM Report on CDNs, 2012) que as regras de neutralidade de rede não se aplicam à parte upstream da conexão. Na Holanda, as regras relevantes aplicam-se a "providers of public electronic communications network over which Internet services are provided and providers of Internet access services", o que parece implicar que as regras aplicam-se à toda cadeia de conexão e não apenas à "última milha" entre o provedor de acesso à internet e os usuários finais (Telecommunications Act, 1998: art. 7°. 4a).

Enquanto a redação ampla do art. 9° gera alguma incerteza, sua interpretação deve ser expansiva ao invés de restritiva. Quaisquer arranjos que essencialmente contrariem ou burlem as garantias de neutralidade de rede devem ser vedados, a não ser que escapem claramente do escopo do art. 9° (p.ex. como os serviços especializados) ou se enquadrem nas restritas exceções do art. 9°, como são os serviços de emergência e a utilização de requisitos técnicos indispensáveis à prestação adequada do serviço, e demais exemplos referidos abaixo.

A priorização paga não escapa do art. 9° e tampouco se enquadra em alguma de suas exceções. Assim, na ausência de esclarecimentos, os provedores de acesso à internet, como atores que encaminham e transmitem dados, devem tratá-los igualmente ao longo do caminho de transmissão em seu controle. Isto inclui tanto a gestão da rede interna quanto a relação com provedores de aplicações.

Adicionalmente, no tocante às exceções, acordos de priorização paga certamente não são serviços de emergência e também não podem ser considerados como requisitos técnicos indispensáveis à prestação adequada do serviço. A exceção da utilização de requisitos técnicos indispensáveis à prestação adequada do serviço têm como propósito garantir que os provedores de acesso à internet possam tomar as medidas necessárias para evitar o congestionamento de suas redes e

usá-las eficientemente, mas não para dar prioridade para certo tipo de tráfego sobre outros com base em um arranjo comercial.

1.3. Zero Rating e taxas adicionais

1.3.1 Análise Geral

Em grande medida, a neutralidade da rede é associada à ideia de que os provedores de acesso à Internet devem tratar igualmente os provedores de aplicações de Internet. Ou seja, os provedores de acesso à Internet não deveriam poder cobrar valores adicionais dos provedores de aplicações, além dos já cobrados à título de venda de banda. Ou ainda que os provedores de acesso à Internet não poderiam fazer acordos que isentassem os provedores de aplicações de qualquer pagamento, pois ambos os casos introduziriam arranjos econômicos diferenciados.

Alguns provedores de acesso à Internet afirmam que a quantidade do tráfego que alguns provedores de aplicações transferem às suas redes é tão grande que o custo associado ao seu transporte não seria refletido adequadamente no preço pago por acordos já existentes de conectividade e que, portanto, uma taxa adicional deveria ser cobrada do provedor de aplicações para remunerar este custo. Por exemplo, duas empresas, a Netflix e o Google (principalmente por meio do YouTube), são responsáveis por mais da metade do tráfego da Internet nos Estados Unidos em horários de pico (Sandvine, 2014). Em função dessa enorme quantidade de tráfego utilizada, se discute se tais empresas não deveriam pagar valores adicionais para cobrir os custos da grande quantidade de dados que transmitem.

Ao mesmo tempo, provedores de acesso à Internet passaram a subsidiar certos serviços, aplicações ou conteúdo, disponibilizando-os livremente ou não contabilizando o tráfego que estes geram na franquia de dados contratada pelo consumidor/usuário final (entende-se por “custo”, aqui, tanto o custo monetário ou como o custo suportado pelo consumidor relativo ao consumo de dados da franquia contratada). Em ambas situações, a questão levantada é se deve ser permitido aos provedores de acesso à Internet possuir diferentes arranjos econômicos com diferentes provedores de aplicações. Os provedores de acesso podem desonerar provedores de serviço ou aplicação ou permitir que estes subsidiem o acesso do consumidor/usuário final, o que tem sido denominado de zero rating?

Países como o Canadá, Chile, Holanda, Eslovénia e Noruega, já proibiram a prática de zero rating em função da sua incompatibilidade com o principio de neutralidade da rede. A Autoridade Norueguesa de Regulação de Comunicações considerou que no caso do zero rating é exatamente o tipo de situação que a neutralidade de rede visa evitar. Isto porque, depois de ter alcançado o seu limite de dados o tráfego que está “zero rated” ainda tem permissão para continuar, ao passo que todos os outros tráfegos serão limitados ou bloqueados (http://eng.nkom.no/topical-issues/news/net-neutrality-and-charging-models). A decisão do regulador holandês de proibir o acesso patrocinado é particularmente interessante em relação as consequências no mercado. Em razão da decisão do regulador holandês, a principal operadora nacional, KPN, decidiu dobrar – gratuitamente – o volume do limite de tráfego de seus planos para celular, para promover uma maior utilização da internet móvel (http://dfmonitor.eu/downloads/Banning_zerorating_leads_to_higher_volume_caps_06022015.pd

f), demonstrando que a proibição do zero rating pode incentivar os operadores a expandir limites de dados e reduzir o preço da conexão de Internet móvel.

Assim como no caso do Brasil, empresas já praticavam o zero rating no Chile (mais informações em: http://www.subtel.gob.cl/noticias/138-neutralidad-red/5311-ley-de-neutralidad-y-redes-sociales-gratis) no momento em que tal prática foi considerada em desacordo com as regras de neutralidade, mas ficaram sujeitas a aplicação de multas pela Subsecretaria de Telecomunicações (Subtel). Já no Canadá, a prática foi considerada uma preferência ou vantagem injusta entre serviços similares, conforme a Comissão de Radio-televisão e Telecomunicacoes do Canadá (http://news.gc.ca/web/article-en.do?nid=926529).

Devido à importância do tema para o desenvolvimento do ecossistema de Internet, o CTS chama a atenção para esses arranjos, nos termos abaixo.

A leitura do art. 9° indica que o zero rating e os acordos de taxas adicionais são proibidos. O art. 9° enuncia claramente que pacotes de dados devem ser tratados igualmente, independentemente do seu conteúdo, origem, destino, serviço, terminal ou aplicação. Como resultado, arranjos discriminatórios de preço contrariam o art. 9°.

É importante ressaltar, também, que planos de serviço construídos por meio de acordos de zero rating já estão sendo oferecidos no mercado e, portanto, o exame de seu status e de sua permissibilidade de acordo com o Marco Civil é necessário. Por exemplo, algumas operadoras de telefonia móvel têm oferecido acesso grátis à redes sociais para seus usuários (não é claro se as operadoras internalizam os custos dos serviços ou se estes são cobertos pelos provedores de aplicações). Neste caso, o mercado se antecipou à regulamentação da questão, e está, portanto, incompatível com o posicionamento legislativo estabelecido por meio do Marco Civil.

Uma análise econômica pode ser útil para a compreensão do zero rating e suas implicações. Na Internet, o sistema predominante de distribuição de preços é uma taxa fixa para os consumidores e uma taxa variável (a partir do volume de dados) para provedores de serviços, aplicações e conteúdo. Isto significa que o preço (mensal) que os consumidores pagam para seus provedores de acesso à Internet normalmente não depende da quantidade de tráfego que consomem (com exceção do acesso à Internet pela telefonia móvel, que costuma estar associados a franquias de dados), enquanto os provedores de serviço, aplicação e conteúdo pagam por sua conectividade à Internet dependendo da quantidade de dados que veiculam na rede. Os provedores de acesso à Internet estão no meio da relação entre usuários finais e os provedores de serviços, aplicações e conteúdo e, assim, desempenham o papel da plataforma que conecta ambos os lados. A construção e a operação dessa plataforma (a rede de um provedor de banda larga) possui um custo alto e os provedores de banda larga podem reavê-lo de ambos os lados nos termos dos acordos descritos acima. E efetivamente esses acordos têm sido celebrados.

Ausente uma regra que imponha ou proíba uma distribuição específica do custo entre esses dois lados da plataforma (usuários finais/consumidores por um lado e provedores de serviço, conteúdo e aplicações por outro), o dono da plataforma pode distribuir o preço como achar apropriado (Rochet & Tirole, 2006). Se completamente livre, o dono da plataforma irá fazê-lo tomando em

consideração a disposição e a capacidade de cada lado de pagar (elasticidade do preço) (Economides & Tag, 2009).

Assim, tanto o zero rating quanto a imposição de uma taxa adicional modifica essencialmente a distribuição estabelecida do preço: (a) o zero rating permitiria aos consumidores ter acesso a serviços, aplicações ou conteúdo de graça ao alocar o custo dos consumidores para o provedor de aplicação ou para o dono da plataforma. Por exemplo, quando o Facebook é oferecido de graça para os usuários de uma operadora de telefonia móvel, ou o Facebook ou a operadora de telefonia móvel incorre no custo da transmissão dos dados do Facebook; (b) a imposição de uma taxa adicional para os provedores de aplicação que gerarem uma quantidade desproporcional de dados busca reaver grande parte do custo tido com estes provedores, ao invés destes custos serem arcados pelos consumidores (através de taxas mensais mais altas) ou pelo provedor de banda larga (reduzindo sua lucratividade).

Visto sob a perspectiva econômica, a distribuição do preço resulta simplesmente na transferência do excedente de um lado para o outro ou para a plataforma (Church & Gandal, 2004). Entretanto, ao alocar o excedente, a distribuição do preço é ao mesmo tempo um mecanismo para subsidiar qualquer um dos lados da plataforma ou a própria plataforma. Por exemplo, quando o Facebook é oferecido de graça, o lado do consumidor é subsidiado. Quando uma taxa adicional é imposta ao Netflix, é a plataforma (provedor de acesso à Internet) que está sendo subsidiada, ou quando os consumidores veem uma redução em suas taxas mensais, são eles que estão sendo subsidiados.

Embora a economia forneça uma boa visão quanto aos efeitos de tais arranjos e permita amplo espaço para argumentos em sentidos opostos, quando se leva em consideração as prioridades e o espírito do Marco Civil, a conclusão deve ser no sentido de proibi-los, reforçando o afirmado no art. 9°. Aprofundaremos essa discussão abaixo.

1.3.2 Sobre taxas adicionais

Seria possível contra argumentar que uma taxa adicional cuidadosamente definida poderia alcançar uma transferência de excedente de um lado para outro de forma a aumentar o bem-estar (Hemphill, 2008). Por exemplo, não seria melhor para os consumidores se seu provedor de acesso à Internet pudesse cobrar dos gigantes da Internet uma quantia adicional relativamente pequena, a qual seria revertida em investimentos na capacidade da rede? Embora isto seja, certamente, uma possibilidade teórica, funda-se em pressupostos questionáveis e difíceis de sustentar.

Em primeiro lugar, enquanto a teoria sugere que faz parte do interesse dos provedores de acesso à Internet o fomento à um ecossistema saudável ao redor de sua plataforma (em outras palavras, seu negócio prospera quando ambos os lados que conecta também prosperam), quando o provedor de acesso à Internet tem poder de mercado, ele possui a habilidade de maximizar seu próprio bem-estar em detrimento do bem-estar de todo o ecossistema (Choi & Kim, 2010). É possível que um provedor de acesso à Internet tenha mais a ganhar ao impor uma taxa adicional, mesmo se isto implicar acesso reduzido para o lado dos serviços, aplicações e conteúdo e, concomitantemente, em uma queda na disposição dos consumidores a pagar. Na ausência de pressão competitiva para disciplinar os provedores de acesso à Internet, este tipo de pensamento poderia ser esperado.

Em segundo lugar, considerando que alguns provedores de acesso à Internet são verticalmente integrados ou possuem acordos verticais com provedores de serviços, aplicações e conteúdos, a imposição de uma taxa poderia ser utilizada para estabelecer uma desvantagem competitiva a serviços não afiliados e não como um meio para alocação ótima do preço.

Em terceiro lugar, presume-se que os provedores de acesso à Internet irão reinvestir a receita extra em atividades que beneficiam a coletividade, como a expansão da capacidade da rede ou a redução do preço de acesso para os consumidores. Mas, como empresas de capital aberto, provedores de acesso à Internet também devem priorizar os interesses dos seus acionistas, os quais não são necessariamente alinhados com o interesse público. Dessa forma, não seria correto fazer qualquer presunção quanto à alocação das receitas extras auferidas em função da cobrança de taxas extras.

Em qualquer caso, é importante reforçar que as práticas discutidas foram proibidas por decisão do Congresso Nacional ao aprovar o artigo 9° do Marco Civil da Internet, que impede os provedores de acesso à Internet de cobrar taxas diferenciadas que de qualquer forma discriminem pacotes de dados (incluindo quando esta discriminação diz respeito a um serviço ou a um tipo de serviço).

1.3.3 Outras questões envolvidas no debate de Zero Rating

A atual estrutura da Internet pública e aquela promovida pelo Marco Civil proíbem os provedores de aplicação/conteúdo de subsidiar o acesso dos usuários a seu próprio serviço. Apesar dos argumentos contrários, esta decisão possui sólidos fundamentos. O Marco Civil foi desenhado e aprovado no Congresso Nacional considerando que uma política que promova mais competição e estabeleça condições igualitárias para disputa de mercado pelos provedores de aplicações deve atrair mais consumidores ou incrementar a sua disposição em pagar pelo acesso à internet, o que por sua vez deve resultar em uma maior receita para os provedores de acesso à Internet. Se correta, a política adotada criará um círculo virtuoso, no qual mais empresas serão incentivadas a desenvolver conteúdos e serviços e disponibilizá-los no mercado, mesmo que tais empresas não tenham qualquer poder de mercado no momento de sua entrada.

O poder de mercado de algumas das empresas de Internet e sua presença quase onipresente no país são nítidos. Tal afirmação pode ser ilustrada pelo fato de que quatro entre as cinco das mais influentes empresas no Brasil são grandes empresas de tecnologia americanas (Thought Leaders 2012, Agência Ideal). Vejamos, portanto, uma das principais questões - de natureza concorrencial - envolvida na prática de zero rating, e como ela pode ser prejudicial, principalmente no médio e longo prazos, para o desenvolvimento da Internet.

É possível argumentar que o zero rating poderia ser benéfico na medida em que confere aos usuários o acesso grátis (subsidiado) a certos serviços, aplicações ou conteúdo, o que os beneficia não apenas em termos econômicos, mas também contribuiria com a inclusão digital (daqueles que não podem pagar), a adoção de banda larga e com a participação cidadã (Hemphill, 2008). O zero rating também poderia ser visto como um desenvolvimento positivo para os provedores de serviços, aplicações e conteúdos assim como para os provedores de acesso à Internet, pois poderia estimular o aumento de consumo e pode ser utilizado como uma ferramenta promocional.

Contudo, o consolidado poder de mercado de certas empresas de Internet indica que estas possuiriam um elevado poder de barganha frente aos provedores de acesso em comparação com potenciais concorrentes, notadamente novos entrantes. Portanto, apenas as empresas capazes de oferecer vantagens claras ao provedor de acesso à Internet, sejam elas vantagens financeiras ou não, conseguiriam fechar acordos de zero rating. Empresas menores não conseguiriam fazer o mesmo tipo de negociação, e consequentemente não conseguiriam fazer frente ao poder de seus concorrentes.

Conforme abordamos acima, ao usar serviços beneficiados pelo zero rating o usuário não atinge o limite de dados desde que esteja navegando dentro do aplicativo privilegiado. Assim, seu incentivo é não migrar para outras possíveis plataformas. Além disso, o efeito de rede criado pela utilização de uma plataforma pose ser ainda mais reforçado no momento em que o usuário se fecha para demais opções. Portanto, se um usuário utiliza determinada rede social sem jamais atingir seus limites de dados contratados, seus incentivos para usar outra rede social são quase nulos. Por isso, o zero rating pode facilitar o "lock-in" do usuário em certos serviços, na medida em que seus concorrentes jamais conseguirão entrar no mercado de forma competitiva ao menos que possam oferecer os mesmos incentivos aos potenciais usuários de seus serviços.

Ademais, o zero rating abre a porta para que os provedores de acesso à Internet favoreçam seus próprios serviços afiliados ou aqueles com os quais sejam integradas verticalmente, o que pode restringir a pluralidade e a inovação de base. Isto significa que exatamente pelas ofertas de zero rating serem uma escolha economicamente atraente para os usuários, elas representam o risco de levar usuários e criadores ao que é mais barato ou mais facilmente acessível e não necessariamente a aquilo que é mais diverso, de melhor qualidade ou inovador.

Finalmente, o zero rating pode fazer com que se criem agrupamentos (clusters) de serviços e aplicações dentro do ecossistema da Internet. Por exemplo, uma operadora de telefonia móvel poderia oferecer acesso grátis apenas às redes sociais ou apenas a certos aplicativos de mensagens e acesso pago ao resto da Internet. Isto vai contra o espírito da Internet indivisa, aberta e participativa que o Marco Civil busca promover. Novamente, embora seja possível identificar argumentos na literatura econômica sobre os benefícios da diferenciação de produtos e serviços no mercado (Spence, 1976; Dickson & Ginter, 1987), a proposta aprovada em Lei foi a de priorizar a promoção do desenvolvimento da Internet como um todo e não em fragmentos. Acordos de preferência potenciais com gigantes da Internet podem significar custos reduzidos para consumidores ou desenvolvedores de aplicações e serviços no curto prazo, mas também podem desincentivar a sua participação no resto do ecossistema da Internet e esta é uma consideração já feita e superada pelo Congresso Nacional ao aprovar o Marco Civil, que ponderou e sustentou que tais acordos não devem ser permitidos.

1.4. CDNs

As CDNs -- acrônimo para Content Delivery Networks (Redes de Entrega de Conteúdo) -- surgiram na década passada como o principal meio para que provedores de aplicações distribuam seus dados de forma mais eficiente ou mais econômica.

CDNs são sistemas de rede que intermedeiam o provedor de aplicações e um provedor de acesso à Internet com o propósito de agilizar a transmissão de dados (Pallis & Vakali, 2006). Elas o fazem por meio da hospedagem local de cópias (espelhamento ou "mirroring") de dados selecionados; quando um usuário final solicita estes dados, a CDN intercepta a solicitação e envia os dados a partir do ponto de hospedagem local, ao invés da fonte remota original. CDNs podem ser empresas independentes ou podem ser empresas do mesmo grupo que o que controla um provedor de acesso à Internet ou um provedor de aplicações. Exemplos de CDNs independentes são a Akamai e a Limelight. Exemplos de provedores de aplicações com funcionalidade de CDN integrada são o Facebook, o Netflix e o Youtube. Exemplos de provedores de acesso à Internet com funcionalidade de CDN integrada (nos EUA) são a Verizon e a AT&T.

A partir da redação do Marco Civil, é incerta qual a situação regulatória das CDNs no mercado brasileiro. Esta é uma questão delicada, e pode ser prematura sua regulação por regras rígidas que não permitam o pleno desenvolvimento de novas tecnologias e alternativas para o desenvolvimento da infraestrutura de Internet no Brasil.

Posto isso, algumas medidas devem ser estabelecidas para assegurar que as CDNs não sirvam para contornar as garantias estabelecidas pela neutralidade de rede. Uma medida adequada para o presente momento parece ser o monitoramento dos acordos de interconexão entre os provedores de acesso à Internet e as CDNs.

CDNs podem tanto promover como ameaçar a neutralidade da rede. Elas a promovem da seguinte maneira:

> i) Como o papel das CDNs é facilitar o tráfego dentro da rede e agilizar a transmissão de dados, elas podem ajudar agentes (players) menores a se tornarem mais eficientes no fornecimento de seus serviços e conteúdo. Na falta de CDNs, o único meio para garantir uma transmissão de dados mais rápida ou mais eficiente na rede é a interconexão direta aos principais provedores de acesso à Internet ou ao backbone da Internet. Ao permitir que players menores não precisem de acordos de interconexão custosos, as CDNs podem ajudar equilibrar a disputa no mercado;
>
> ii) Uma exceção comum à neutralidade da rede é a que decorre de requisitos técnicos indispensáveis para gestão do tráfego para evitar o congestionamento da rede (uma exceção ao art. 9°). Como exceções podem dar margem a abusos, quão mais estreita for sua aplicação, melhor. Ao limitar o congestionamento na rede, as CDNs reduzem os incentivos para que os provedores de acesso à Internet realizem uma gestão agressiva do tráfego em suas redes, limitando assim a necessidade de aplicação da exceção existente no artigo 9°.

Elas ameaçam ou seriam contra o espírito das regras que asseguram a neutralidade da rede do seguinte modo:

> i) As CDNs são mais um intermediário ao longo da cadeia de transmissão que pode afetar como o tráfego na rede flui. Deste modo, elas possuem a capacidade de discriminar pacotes de dados. Enquanto CDNs independentes podem carecer de incentivos para discriminar, os incentivos podem ser mais fortes quando a funcionalidade de CDN é integrada em um

provedor de acesso à Internet. Nos EUA, por exemplo, a Verizon, proprietária da EdgeCast, poderia ter um incentivo a discriminar outras CDNs, ou outros serviços, aplicações ou conteúdo que não utilizem a sua própria CDN;

ii) O argumento anterior pode ser invertido de modo que a entidade que discrimina não é o provedor de acesso à Internet, mas o provedor de aplicações utilizando-se de CDNs ou um provedor de aplicações com funcionalidade de CDN integrada. Por exemplo, a Netflix, que administra sua própria CDN, recusava-se até recentemente a fornecer conteúdo HD para consumidores cujo provedor de acesso à Intenet não utilizasse sua CDN;

iii) As CDNs podem ser vistas como tecnologias inerentemente não neutras, pois elas ajudam a transmitir os dados de modo mais rápido e mais eficiente para serviços, aplicações e conteúdos que as utilizem. Isto não significa que são prejudiciais ao ecossistema da Internet, mas apenas que, dada a capacidade de certos provedores de aplicações adotarem novas tecnologias, existem meios para tornar o tráfego de determinados conteúdos mais eficiente;

iv) Argumenta-se que por conta das CDNs reduzirem o congestionamento de dados na rede, elas podem desincentivar investimentos no aumento de capacidade da rede, o que é um dos objetivos secundários da neutralidade da rede. Isso não é necessariamente ruim: tudo que as CDNs fazem é contribuir para o uso mais eficiente da capacidade da rede.

1.4.1 Como situar as CDNs no Marco Civil

Como já mencionamos, é incerto se as CDNs se enquadram nas regras de neutralidade de rede, pois não é claro, a partir do artigo 9° ou das definições do Marco Civil, quem são os atores na rede sobre os quais estas regras incidem. Deve-se observar que a decisão sobre se as regras aplicam-se às CDNs não pode ser tomada independentemente da aplicação destas regras aos demais atores ou a relacionamentos similares. A questão é complexa, pois uma expansão da regulação às CDNs pode atingir, acidentalmente, atores que foram tradicionalmente não regulados (p. ex. Google, Microsoft, Facebook), já que alguns destes atores oferecem funcionalidades de CDN próprias. Por outro lado, se as regras não atingirem as CDNs, há um risco potencial de que a funcionalidade CDN passe a ser utilizada por provedores de acesso à Internet (sujeitos, definitivamente, às regras) para burlar as obrigações de neutralidade de rede.

Por exemplo, ao invés de manipular o tráfego dentro da rede de um provedor de acesso à Internet (o que claramente violaria a neutralidade da rede), um provedor poderia alcançar resultado similar solicitando aos provedores de aplicações que conectem à sua CDN para que aumentem a velocidade do tráfego de seus dados, ou, ao contrário, o provedor de conexão à Internet poderia reduzir a velocidade dos dados ou reduzir a velocidade do tráfego na interconexão com uma CDN que transmita os dados de um provedor de aplicações cujo tráfego o provedor de aplicações queira a degradar.

Até alguns anos atrás, as CDNs não eram de grande interesse na cadeia de valor do mercado de banda larga, mas o rápido aumento no tráfego tornou seu uso necessário e difundido. Dada sua importância crescente, seria insensato ignorar o fenômeno, mas seria igualmente insensato

determinar que as CDNs se enquadrem no art. 9° do Marco Civil, proibindo-as de contratar livremente com outros agentes do mercado, sem evidências de comportamento anticoncorrenciais.

No estágio em que a indústria se encontra, a melhor solução parece ser insistir em acordos razoáveis e justos de interconexão entre CDNs e os demais agentes do mercado, ao invés de proibir acordos que poderiam ser benéficos para a rede como um todo.

Os termos e condições dos acordos de interconexão definem, em larga medida, a estrutura da indústria e são uma ferramenta poderosa para monitorar o mercado. Acordos de interconexão são frequentemente não divulgados, o que torna o monitoramento impossível, mas isto pode mudar em virtude de requisitos regulatórios.

Acesso aos termos e condições dos acordos de interconexão permitira que reguladores avaliassem as práticas das CDNs, emitissem recomendações, se necessário, e até mesmo suprimissem comportamentos anticoncorrenciais, se estes surgirem e persistirem. Particularmente, informações sobre os termos técnicos e as condições de preço que governam a transmissão de dados e a interconexão devem ser disponibilizadas, quando estas têm o potencial de afetar significativamente a quantidade de tráfego na internet de banda larga brasileira ou a estrutura concorrencial do mercado de banda larga brasileiro.

1.5 Gerenciamento razoável de redes

A regra da neutralidade de rede possui uma exceção no art. 9° do Marco Civil, segundo a qual a discriminação e a redução de tráfego poderá decorrer de "requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações". Uma série de requisitos especificam os limites de gerenciamento de redes permitido pela Lei: (a) o gerenciamento não deve causar dano aos usuários, de acordo com o art. 927 da Lei 10.406/2002; (b) ao gerenciar sua rede, o responsável deve agir com proporcionalidade, transparência e isonomia; (c) deve ser avisada previamente, de maneira transparente, clara e descritiva aos usuários, e; (d) o responsável pela rede deve oferecer os serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

Estes requisitos gerais devem ser melhor detalhados para fornecer orientação clara aos operadores sobre o que eles deve ser considerado como uma gestão razoável de redes. Esta é a única forma para permitir que as regras possam ter um valor normativo efetivo e, ao mesmo tempo, evitar potenciais *chilling effects* decorrentes de restrições excessivas.

Primeiramente, é preciso observar que a gestão de rede é uma função utilizada diariamente pelos operadores no processo ordinário de aceitar, processar e transmitir pacotes de dados. Neste processo, operadores de rede precisam tratar, em determinadas situações, pacotes de dados de modos que violariam a regra de neutralidade de rede do art. 9°. Tal tipo de gestão de rede discriminatória pode ser aceitável sob certas circunstâncias, mas, porque se desvia dos princípios da neutralidade de rede, deve ser permitida de forma excepcional, como descrito abaixo.

Dessa forma, ela deve ser entendida e interpretada restritivamente. Isso significa que a não ser que uma prática enquadre-se claramente no âmbito do gerenciamento de redes, não deve ser considerada como permitida pela Lei.

Em segundo lugar, o gerenciamento de redes, como o nome sugere, é um termo técnico e assim deve ser utilizado e compreendido. Isso significa que a exceção deve ser utilizada para justificar práticas tecnicamente necessárias e não arranjos comerciais. Em outras palavras, a justificativa principal para o emprego do gerenciamento de redes deve ser uma escolha técnica sobre como a rede pode melhor processar o tráfego eficientemente e não uma escolha de negócios sobre como oferecer novos serviços ou garantir novas fontes de receitas. De acordo com o Instituto de Engenheiros Elétricos e Eletrônicos (IEEE, Network Traffic Management and the Evolving Internet, 2010) as áreas chaves da gestão aceitável de tráfego incluem:

- Oferecer qualidade de serviço suficiente em momentos de congestionamento temporários e excepcionais: o gerenciamento discriminatório de rede pode ser necessário para garantir qualidade de serviço suficiente e para garantir a fruição de serviços de emergência em momentos de congestionamento temporários e excepcionais. Nesses casos, práticas de gerenciamento de rede que impliquem discriminação de tráfego devem ser permitidas como uma exceção à neutralidade de rede. Deve-se assegurar, entretanto, que tal decisão seja proporcional, transparente e isonômica, implicando que, a não ser que seja absolutamente imperativo, por razões técnicas razoáveis, nenhum tipo de serviço de uma determinada origem ou para um destino específico devem ser tratados de maneira diferente de serviços do mesmo tipo de outras origens ou para outros destinos.

- Tráfego prejudicial para a rede: o gerenciamento de rede deve ser permitido quando tem por finalidade filtrar o tráfego que é prejudicial à operação da rede (e.g. spam, malware). A segurança e a integridade da rede devem ser objetivos legítimos da gestão de redes. Novamente, transparência, proporcionalidade e isonomia, bem como a consideração de danos colaterais, devem constar de qualquer decisão ou norma técnica que balize o gerenciamento para fins de segurança. Ressalte-se que “segurança da rede” deve ser interpretado no sentido estrito e não deve ser confundido, em nenhuma hipótese, para filtragem de conteúdo para fins de *enforcement.*

- Prevenção de congestionamento de tráfego: redes de pacotes como a Internet podem sofrer de congestionamento quando existe uma demanda de envio e recebimento de mais dados do que a rede pode lidar naquele momento. Gerir o tráfego de modo a evitar o congestionamento é uma operação complexa e operadores da rede devem ter liberdade neste sentido, particularmente se considerarmos que diferentes tecnologias e topologias de rede necessitam diferentes tipos de gestão de congestionamento. Por isto, a permissibilidade das práticas de gerenciamento de rede devem ser avaliadas considerando a arquitetura e a tecnologia utilizadas na rede sob exame. Isto significa, também, levar em consideração as diferenças entre redes *wireless* e fixas. Em particular, enquanto redes *wireless* não são isentas das regras de neutralidade de rede, elas podem necessitar de um gerenciamento de rede mais intenso e detalhado por várias razões, incluindo a limitação de banda, imprevisibilidade da difusão de rádio, o consumo flutuante de cada célula, entre

outros. De qualquer maneira, mesmo nas redes *wireless* a necessidade de gerenciamento de rede deve ser especialmente substantiva e justificada.

Esta não é uma lista exaustiva. Enquanto houver fundamentação técnica sólida e enquanto o tratamento diferenciado necessário ao gerenciamento de rede for aplicado de forma isonômica e não discriminatória (art. 9°, § 2°, II), os engenheiros de redes devem ser respeitados. Pelo mesmo motivo, é preferível que definições bastante específicas de gerenciamento de redes sejam evitadas no Decreto, pois elas poderiam restringir severamente as escolhas técnicas. Definições rígidas estabelecidas na regulamentação da Lei correm sério risco de gerar problemas em nível tecnológico e de tornarem-se rapidamente obsoletas, tendo em vista o acelerado desenvolvimento de novas práticas e tecnologias.

De qualquer forma, considerando a linha tênue que pode separar práticas de gerenciamento de rede que objetivam assegurar a qualidade do serviço e infrações à regra da neutralidade de rede, é importante assegurar transparência e um amplo escrutínio das diversas autoridades para evitar abusos que provoquem danos à ordem econômica e aos direitos dos usuários.

1.6 Escopo de Aplicação

Dada a abrangência do art. 9 do Marco Civil, não foram especificados com clareza quais atores e relações estão sujeitos aos seus comandos. Definir seu alcance é fundamental, porque determina a quem se destina a regra que determina a neutralidade da rede.

Para começar com a parte incontroversa, a lei se aplica à como o tráfego é tratado dentro das redes de um provedor de conexão à internet, notadamente entre o usuário final e o provedor. Isso decorre diretamente do comando do art. 9°, que se aplica ao "responsável pela transmissão, comutação ou roteamento" do tráfico de dados, atividade claramente relacionada aos provedores de acesso à Internet. Historicamente, as regras de neutralidade de rede tiveram como objetivo a proteção contra os provedores de acesso à Internet, assumindo que estes possuem uma condição de monopólio ou quase monopólio, e que a partir de sua interação com os usuários finais poderiam afetar diretamente a maneira como o público em geral é capaz de enviar e receber dados. Mas na cadeia de valor da Internet há mais atores envolvidos na transmissão, comutação e roteamento de tráfego. Os líderes desse segmento são os provedores de b*ackbone* e os provedores de transito/*peering*, que também parecem estar sujeitos ao art. 9°. É questionável que haja realmente necessidade de intervenção nessas áreas da cadeia de valor, porém é provável que a abrangência do Art. 9 deixe uma pequena margem para desconsiderar provedores de conexão que atuem de maneira semelhante aos ISPs, com a diferença de que operam no atacado e não no varejo.

As Redes de Entrega de Conteúdo (CDNs, em inglês) são diferentes dos atores mencionados acima, porque sua função principal está mais orientada para o armazenamento e espelhamento de conteúdos de conteúdos do que para estabelecer conexão entre provedor de conteúdo e o usuário. Mesmo que os fornecedores de conteúdo necessariamente atuem na transmissão e encaminhamento de dados ("*routing*"), essas funções são só um acessório para a função principal que eles desempenham na cadeira de valor, quais sejam, o armazenamento e a entrega de conteúdo de maneira mais veloz e eficiente.

Além da questão de quais atores estão sujeitos às regras de neutralidade de rede, há também a questão sobre quais relações estão abrangidas. Trata-se de como atores - tais quais provedores de acesso à Internet, provedores de *backbone*, CDNs - se relacionam entre si, e não como eles tratam o tráfego de dados dentro de seus limites. Por relações se entende a conexão técnica, também conhecida por interconexão, e os arranjos de negócio/econômicos entre os atores. A linguagem do art. 9° (devido ao processo de bases isonômicas) parece estar delimitada o suficiente para cobrir relações econômicas e técnicas. Colocada de outra maneira, a neutralidade de rede não trata apenas sobre discriminação técnica, mas sobre discriminação econômica, porque os dois tipos podem ser criar um tipo de vantagem injusta ou desvantagem que a lei procura prevenir em nome da competição saudável e da inovação inclusiva.

É seguro afirmar que o art. 9 se aplica à relação entre provedores de conexão e usuários finais. Como mencionado, essa é a parte da cadeia de transmissão de dados que representa os maiores desafios para a competição e garante ao provedor de conexão poder para determinar como usuários receberão e enviarão dados. Também é razoável dizer que o art. 9° cobre a relação entre provedores de conexão e provedores de conteúdo. A neutralidade de rede não objetiva proteger somente os usuários finais, mas também proteger os provedores de aplicações e de conteúdo de discriminação por parte dos provedores de conexão. Além disso, por uma questão de lógica, se aos provedores de conexão fosse permitido tratar provedores de aplicações/conteúdo de uma maneira discriminatória, seria possível obter um efeito igual ou equivalente ao que seria obtido por meio do gerenciamento de tráfego (bloqueio, filtro ou degradação) em suas redes, o que poderia frustrar o propósito das regras de neutralidade. e a objetividade da neutralidade de rede. Em outras palavras, se o propósito das regras de neutralidade de rede é assegurar que os provedores de conexão servirão como um meio transparente para conectar aplicações e usuários, essas regras devem aplicar-se aos dois lados da relação (aplicações e usuários).

O comentário anterior sobre quais atores estão sujeitos à neutralidade de rede logicamente indica que a relação entre um ator que não está abarcado pelo art. 9° e um que está não deve ser regulamentada. Por exemplo, a relação entre um provedor de conexão e uma CDN não está no âmbito do referido artigo. Isso é necessário para permitir o surgimento de novos atores no mercado que podem melhorar o "ecossistema" da Internet, e que não representam nenhum tipo de ameaça que a regra de neutralidade de rede procurou evitar.

1.7 Fiscalização e garantia da observância da regra de neutralidade de rede

Um dos principais pontos não definidos pela Lei 12.985 de 2011 diz respeito a quem deve ser o órgão responsável por realizar a fiscalização e garantir a observância da regra de neutralidade de rede contida no artigo 9°. No intuito de contribuir com as discussões e considerando os debates sobre possíveis limites de competência das diversas autoridades da administração pública que estão relacionados com o tema, serão apresentadas abaixo sugestões sobre um possível desenho institucional para a fiscalização da neutralidade de rede. Conforme o exposto abaixo, é possível que tal competência seja atribuída a uma instituição, ou que seja compartilhada por diversas autoridades, respeitando os limites de cada uma delas.

Em primeiro lugar, é preciso notar que há interpretações discordantes sobre a amplitude da competência da ANATEL, órgão regulador das telecomunicações, para atuar em relação à neutralidade de rede. O art. 61. da Lei Geral de Telecomunicações (LGT) estabelece que Serviço de Valor Adicionado (SVA) é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde. Já o provimento de conexão à Internet, por sua vez, não é considerado um serviço de telecomunicações, mas um tipo de SVA, de acordo com o disposto na Norma 04/95. Por outro lado, o artigo 61, § 2° da LGT estabelece que a ANATEL deve garantir que SVAs tenham acesso às redes de telecomunicações. De acordo com esta interpretação, portanto, o serviço de telecomunicações não se confunde com o SVA e tampouco com a relação entre SVA e usuário final. Assim, a ANATEL não poderia interferir nas relações na última milha e haveria limitações em sua competência.

A regulamentação do Marco Civil precisará enfrentar esta questão dos limites da competência da ANATEL. Caso se reconheça a ausência de sua competência para atuar na última milha, não será possível que se determine o contrário por meio de Decreto, pois usar instrumento para tanto seria extrapolar os limites de seu poder regulamentar. Desse modo, a melhor solução no âmbito do Decreto que regulamentará o Marco Civil da Internet parece ser a de construir uma forma de atuação conjunta de vários órgãos na fiscalização e monitoramento do cumprimento das regras de neutralidade de rede. Nesse sentido, propõe-se para discussão e debate um modelo de monitoramento e observância composto por mais de uma instituição, explicado melhor abaixo.

Um modelo de monitoramento e fiscalização pluri-institucional

Vejamos quais seriam as possibilidades referentes ao compartilhamento de competências em relação à fiscalização das regras de neutralidade. Conforme o artigo 61, § 2° da LGT, a Anatel tem o poder e dever de garantir que Serviços de Valor Adicionado tenham acesso às redes de telecomunicações. Não obstante, a relação entre o provedor de conexão e o consumidor final pode e deve ser supervisionada por outras instituições. Dentre as instituições que atualmente possuem competências afins e capacidade para atuar em questões relativas à neutralidade de rede, destacam-se: (i) o CADE, (ii) SENACON; e o (iii) CGI. Vejamos abaixo como tais instituições se relacionam com a neutralidade de rede.

i) CADE e neutralidade de rede

O tema da neutralidade já foi submetido ao Conselho Administrativo de Defesa Econômica (CADE), autarquia que tem como missão zelar pela livre concorrência no mercado. Não obstante à existência de casos relacionados à neutralidade, estes chegaram ao CADE à medida em que demandas foram submetidas ao órgão. Conforme o exposto acima, a própria LGT prevê no art. 19, inc. XIX, a complementariedade da atuação do CADE e da Anatel.

Além disso, é importante notar que as questões relativas à concorrência estão fundamentalmente ligadas à noção de neutralidade de rede. Um dos objetivos centrais da regra do artigo 9° do Marco Civil da Internet é, justamente, assegurar ampla competição no mercado de aplicações e conteúdo. Dessa forma, entende-se como pertinente a atuação e participação do CADE como uma das entidades num modelo pluri-institucional de fiscalização e monitoramento da neutralidade de rede.

ii) SENACON e neutralidade de rede

A Secretaria Nacional do Consumidor (SENACON) é responsável pela coordenação da política do Sistema Nacional de Defesa do Consumidor, e por garantir a proteção e exercício dos direitos dos consumidores. A Secretaria conta, inclusive, com uma Coordenação de Consumo e Sociedade da Informação. Ademais, a SENACON está voltada para a análise de questões que tenham repercussão nacional e interesse geral, tal como a questão da garantia da neutralidade, que afeta consumidores de todo o país.

É importante destacar que a proteção do consumidor está intimamente ligada com a questão da neutralidade de rede. Com efeito, a neutralidade de rede busca, entre outras coisas, assegurar a experiência de navegação do usuário, evitando a influência dos provedores de conexão sobre a capacidade do consumidor de usufruir das diversas aplicações e conteúdos. As regras contidas no capítulo de neutralidade de rede ainda tocam pontos importantes para a privacidade e liberdade de expressão dos usuários/consumidores, impedindo o provedor de conexão de bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados transmitidos em suas redes.

iii) CGI e neutralidade de rede

A inclusão do Comitê Gestor da Internet (CGI) como parte de um sistema de apuração de irregularidades ou violações à neutralidade, se justifica em função das competências estabelecidas no Decreto n. 4.829/03, que o criou. Dentre as atribuições definidas no referido Decreto, podemos destacar, por exemplo, os incisos VII e VIII do art. 1º, que estabelecem que o comitê deve adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, e deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País. Além disso, o Comitê é composto por membros da indústria, da sociedade civil e do Governo Federal. Esta gestão multissetorial, participativa e democrática é uma referência de governança institucional, sendo frequentemente apontada como um exemplo a ser seguido no âmbito internacional.

Além do exposto, o CGI possui capacidade técnica para acompanhamento de infraestruturas e redes por meio das instituições por ele coordenadas. O Núcleo de Informação e Coordenação do Ponto BR (NIC.br), por exemplo, realiza testes de qualidade da banda larga no Brasil em parceria com outras entidades,. O NIC.br continua desenvolvendo soluções para a melhoria da qualidade da Banda Larga no Brasil. Como exemplo, aponta-se o desenvolvimento de um software (SIMET - http://simet.nic.br) usado para avaliar a qualidade do serviço Banda Larga Fixa no país.

Dentre as instituições mencionadas há inclusive algumas com poder de fiscalização e sanção - CADE e SENACON - que já contam com recursos humanos e mecanismos de controle legalmente estabelecidos e poderão acrescentar às suas atividades um trabalho de monitoramento e observância da neutralidade. Com a cooperação das referidas instituições, é possível abranger não apenas os aspectos da neutralidade de rede cobertos claramente pela competência da ANATEL, mas também a relação entre provedores de conexão e usuários finais.

Diante do exposto acima, seja qual for a posição adotada pelo Decreto em relação aos limites da competência da ANATEL para atuar no monitoramento e fiscalização da neutralidade de rede, é necessário imaginar um modelo que contemple a atuação de mais de uma entidade. Assim, mesmo que se decida por um modelo predominantemente centrado na ANATEL, a participação de órgãos

de proteção e defesa do consumidor, do CGI e do CADE permitiria maior escrutínio sobre o processo de fiscalização da neutralidade de rede.

Em um modelo descentralizado, cada uma das entidades atuaria dentro da sua esfera de competência, sendo possível também pensar na criação de um mecanismo de coordenação entre elas. A colaboração das instituições em um modelo como este incrementará a legitimidade na fiscalização da neutralidade de rede, ampliará sua capilaridade, bem como promoverá a capacitação e o aproveitamento de recursos técnicos e humanos já disponíveis.

2. Privacidade

2.1 Definições relativas à privacidade: dados pessoais, tratamento de dados, controlador de dados e processador de dados

Embora o Marco Civil se refira a "dados pessoais" em 10 ocasiões diferentes e a "tratamento de dados" em dois artigos (art. 7°, incisos VIII e IX e art. 11 *caput* e parágrafo 3°), esses termos não são explicitamente definidos. Espera-se que essas definições sejam abordadas em uma futura lei de proteção de dados pessoais. Entretanto, enquanto o Brasil ainda carece de uma lei específica, a ausência de um entendimento compartilhado sobre esses termos pode ser um empecilho à plena aplicação do Marco Civil.

Algumas definições presentes na legislação europeia, particularmente na Convenção do Conselho da Europa para a Proteção de Indivíduos relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108) podem servir de inspiração para a interpretação desses conceitos no âmbito brasileiro. A Convenção 108 é um dos principais instrumentos internacionais em vigor sobre o tema e encontra-se aberta à adesão de Estados não-europeus (o Brasil não é um dos seus signatários). As definições presentes no Anteprojeto de Lei para Proteção de Dados Pessoais, atualmente em debate público se alinham em grande medida com esse texto legal. É preciso destacar, ainda, que a compatibilização entre os quadros legais europeu e brasileiro poderia ser benéfica em termos econômicos, criando segurança jurídica e maior possibilidade de negócios.

A definição de "dados pessoais" encontra-se no artigo 2° da Convenção 108, segundo o qual "os dados pessoais, são qualquer informação relativa a uma pessoa singular identificada ou identificável", ou seja, ao titular dos dados (data subject). O atual marco europeu de proteção de dados clarifica que uma "pessoa singular identificada ou identificável" é qualquer pessoa que "pode ser identificada, direta ou indiretamente, particularmente por referência a um número de identificação ou por um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social" (ver EU Data Protection Directive 95/46/EC, disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML)

No que diz respeito à expressão "tratamento de dados", pode-se defini-la, com inspiração na Convenção 108, como "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais, com ou sem meios automatizados, tais como a coleta,

registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de disponibilização, o alinhamento ou combinação, eliminação ou destruição". O tratamento de dados refere-se a atividades manuais e automatizadas, que abrangem, portanto, todos os tipos de processamento online e offline. Deve ser guiado por princípios essenciais de proteção de dados a fim de evitar eventuais abusos.

De modo a esclarecer as responsabilidades das entidades de tratamento – o que é extremamente útil para a aplicação efetiva dos artigos que tratam da guarda e proteção de registros no Marco Civil –, parece aconselhável adotar, como a Convenção 108 e o Anteprojeto de Lei para Proteção de Dados Pessoais uma definição de "controlador de dados" ("responsável", no texto do APL para Proteção de Dados Pessoais), ou seja qualquer um que sozinho ou em conjunto com outras pessoas tem o poder de decidir os fins e os meios de tratamento de dados pessoais; e de "processador de dados" ("operador", no APL) ou seja, qualquer pessoa física ou jurídica responsável pelo tratamento em nome de um controlador de dados. O processador, portanto, caracteriza-se por ser uma entidade separada e por receber instruções do controlador. A responsabilidade de cumprir a legislação de proteção de dados encontra-se com o controlador (ver OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), art. 14). A responsabilidade do controlador implica uma obrigação geral de colocar em prática medidas técnicas e de organização adequadas, bem como documentar a sua implementação. É importante ressaltar que um processador se torna controlador quando ele decide utilizar dados pessoais para fins que diferem do estabelecido pelo controlador original.

Particularmente, o controlador tem a responsabilidade pelo tratamento de dados, devendo: (i) assegurar que os dados pessoais permaneçam confidenciais; (ii) definir e documentar a lógica de tratamento de dados; (iii) fiscalizar a transferência de dados a terceiros, quando essa operação é permitida; (iv) ser acionado em caso de necessidade de acesso a dados pessoais, tanto por parte do titular dos dados e das autoridades, quando possível; (iv) notificar violações de dados ao titular dos dados afetados, bem como às autoridades competentes.

2.2 Necessidade de clarificar o significado de "dados cadastrais", de dados que permitem a "qualificação pessoal" e também quais são as autoridades administrativas às quais o art. 10, § 3º faz referência

O art. 10, § 3º do Marco Civil especifica que a norma contida no *caput* — o dever de preservação da intimidade, vida privada honra e imagem na guarda e disponibilização de registros de conexão e acesso a aplicações de internet, dados pessoais e conteúdo de comunicações privadas —, "não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição".

Uma interpretação recorrente acerca do Marco Civil é a de que os dados a que o artigo 10, § 3º faz referência poderiam ser obtidos sem a necessidade de prévia ordem judicial, tendo em vista a existência de leis que explicitamente admitem tal possibilidade. Como se trata, aqui, de casos excepcionais, é de fundamental importância delimitar exatamente em que situações isso poderia ocorrer, e entender o conteúdo exato de determinados termos inseridos no art. 10.

Primeiramente, é necessário maior clareza no que diz respeito aos tipos de dados que devem ser considerados como "dados cadastrais". A depender da natureza do serviço ou da plataforma, o usuário pode ser instado a prestar uma ampla gama de dados pessoais a título de cadastro. É possível que até mesmo dados considerados sensíveis sejam obtidos, como aqueles que revelam origem racial, as opiniões políticas, filiação sindical, crenças religiosas ou outras informações sobre a saúde ou vida sexual. Os dados sensíveis merecem medidas reforçadas de proteção e o acesso a eles sempre deve estar sujeito à obtenção prévia de uma ordem judicial. Dessa forma, seria importante delimitar a expressão "dados cadastrais".

Em segundo lugar, de modo a esclarecer o conteúdo do dispositivo, é importante que o decreto presidencial explicite que por “autoridades administrativas”, no âmbito do art. 10, § 3º do Marco Civil, entende-se: (1) a autoridade policial e (2) o Ministério Público. Conforme o art. 17-B da Lei 9.613/98 (Lavagem de Bens, Direitos ou Valores) e o art. 15. da Lei 12.850/13 (Crime Organizado), a autoridade policial e o Ministério Público podem solicitar, sem ordem judicial, dados cadastrais que informem "qualificação pessoal, filiação e endereço” de investigados em procedimentos que apurem crimes de lavagem de bens, direitos ou valores, bem como praticados por organizações criminais.

Ainda para melhor esclarecer o dispositivo, cabe ao decreto explicitar o que se entende por “qualificação”. Usualmente, “dados de qualificação pessoal” são aqueles necessários à individualização de uma pessoa, de modo que tenhamos certeza de que nos referimos a um indivíduo específico e não a outro. Ou seja, informações que indiquem que fazemos referência a João e não a José. O novo Código de Processo Civil indica, no art. 319, II, como informações necessárias para a qualificação das partes em uma petição inicial, os "os nomes, os prenomes, o estado civil, a existência de união estável, a profissão, o número de inscrição no Cadastro de Pessoas Físicas ou no Cadastro Nacional da Pessoa Jurídica, o endereço eletrônico, o domicílio e a residência do autor e do réu”. Não especifica outros dados usualmente encontrados tanto em petições iniciais quanto contratos, como RG, por exemplo. Assim, uma maneira de tornar mais claro o art. 10, § 3º no decreto poderia ser a seguinte:

> "Art. XXX. Para efeito do disposto no art. 10, § 3º, da Lei 12.965/14, entende-se por autoridades administrativas a autoridade policial e o Ministério Público, conforme estabelecido pelo art. 17-B da Lei 9.613/98 e pelo art. 15 da Lei 12.850/13, no contexto de investigações criminais envolvendo lavagem de bens, direitos ou valores, e organizações criminosas.
> § 1.º Os dados solicitados sem ordem judicial podem apenas ser os de qualificação pessoal, filiação e endereço do investigado.
> § 2.º Considera-se dados de qualificação pessoal aqueles especificados no art. 319, II do Código de Processo Civil.

Em nenhuma hipótese, dados além dos especificados devem ser fornecidos sem ordem judicial. É importante que isso seja reforçado no texto do Decreto.

3. Guarda de Registros

A presente seção tem como objetivo delimitar a aplicação dos artigos 10, 13 e 15 do Marco Civil que tratam da guarda de registros de conexão e acesso a aplicações de Internet.

Cabe ressaltar que organismos internacionais ao se depararem com a questão, concluíram que a "retenção em massa, de dados de comunicações, sem que haja uma suspeita, é fundamentalmente contrária ao Estado de Direito, incompatível com os princípios fundamentais de proteção de dados e ineficaz" (Council of Europe's Commissioner for Human Rights, "The Rule of Law on the Internet and in the Wider Digital World", http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf). Isso porque a retenção e guarda de dados como registros de conexão e acesso a aplicações de Internet interfere no direito à privacidade e, portanto, deve estar submetida ao escrutínio das leis internacionais de direitos humanos.

Nesse sentido, a coleção e retenção massiva de dados dos usuários de Internet – como a guarda de registros de conexão e acesso a aplicações –, pode ter um impacto significativo sobre seus direitos fundamentais. Considerando essa particularidade, apresentamos algumas opções de como a regulamentação poderia tratar o tema de modo a estabelecer garantias necessárias para evitar abusos de poder e observar os limites que estão plasmados na Constituição Federal, assim como os tratados de direitos humanos ratificados pelo Estado brasileiro.

A ordem constitucional brasileira afirma a presunção de inocência no artigo 5°, inciso LVII, assim como o sigilo das comunicações e dados dos cidadãos, como direitos fundamentais. Tal sigilo somente pode ser quebrado mediante ordem judicial e, especificamente, para fins de persecução criminal. Em outros termos, até que se prove o contrário, todos são inocentes e a quebra do sigilo das comunicações e dados deve se dar somente mediante ordem judicial. Pode-se compreender, portanto, que se tal provisão restringe, por exemplo, a realização de interceptações telefônicas sem nenhuma suspeita, o mesmo raciocínio poderia ser aplicado à retenção massiva de registros de conexão e acesso a aplicações de Internet. Por isso, parece discutível o fundamento constitucional dos dispositivos sobre a retenção de dados no que diz respeito à opção de determinar que os dados pessoais de todos os usuários podem ser retidos sem autorização judicial.

É importante destacar que mecanismos internacionais de direitos humanos também têm apresentado preocupações com relação à introdução de medidas de retenção massiva de dados. Um dos pontos considerados é, justamente, se provisões legais que obrigam a retenção de dados de todos os usuários de Internet para fins de investigação contrariam o princípio da presunção de inocência - parte fundamental Pacto Internacional sobre Direitos Civis e Políticos (art. 14), adotado pelo Brasil em 1992.

Além disso, argumenta-se que medidas nas quais os Estados requerem a guarda de dados por parte de companhias telefônicas e operadores de Internet não aparentam ser proporcionais ou necessárias do ponto de vista dos direitos humanos, conforme reconheceu um recente relatório do Escritório do Alto Comissário das Nações Unidas para os Direitos Humanos (EACDH), Navi Pillay (http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf). De fato, a retenção de dados sem nenhuma forma de direcionamento e seleção ou qualquer

exigência às autoridades para que mostrem uma suspeita razoável parece ser inevitavelmente desproporcional.

Diante disso, é de extrema importância que a regulamentação do Marco Civil da Internet delimite rigorosamente as situações especificadas em lei nas quais os dados dos cidadãos possam ser acessados pelas autoridades, bem como crie medidas de transparência que permitam o escrutínio público sobre como o Estado e suas autoridades têm atuado nas suas funções de persecução criminal. Ao avançar nesse sentido, o Decreto pode desempenhar papel fundamental em assegurar a privacidade dos cidadãos em um contexto de crescente vigilância e vulnerabilidade da vida privada.

3.1 Limitações às hipóteses de acesso aos dados retidos

Como pontuamos anteriormente, a guarda de registros de conexão e acesso a aplicações de Internet pode se tornar um ato intrusivo capaz de interferir nos direitos humanos e ameaçar os fundamentos de uma sociedade democrática. Nesse sentido, o acesso a esses dados deve, necessariamente, envolver uma consideração sobre a sensibilidade da informação e a gravidade da infração cometida aos direitos humanos ou outros interesses concorrentes.

Isso requer que o Estado limite as hipóteses de acesso aos dados retidos, estabelecendo garantias mínimas para os cidadãos. No contexto europeu, por exemplo, um dos fundamentos para a declaração da inconstitucionalidade da diretiva sobre retenção de dados referiu-se ao termo vago *"serious crimes",* que alargava as hipóteses em que as autoridades competentes poderiam requerer o acesso aos dados retidos pelos provedores de Internet.

O Marco Civil já estabelece que a decisão judicial é o requisito para o acesso aos registros de conexão e acesso a aplicações. A autorização judicial prévia é essencial porque os demais ramos do governo não podem conferir o grau de independência e objetividade necessário para evitar abusos de poder. No entanto, considerando que esses dados podem ter um caráter altamente intrusivo na privacidade dos indivíduos na atualidade, o decreto deveria limitar as hipóteses e os meios por meio dos quais os registros poderão ser fornecidos às autoridades competentes, estabelecendo garantias para a privacidade dos usuários.

Uma abordagem possível e reconhecida por 400 organizações internacionais e mais de 300 mil indivíduos é a proposta de Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações (Ver https://pt.necessaryandproportionate.org/text). Segundo o documento, os seguintes fatores devem ser levados em consideração no momento de se avaliar o acesso aos registros guardados:

1. Existe uma alta probabilidade de que um crime grave (ou uma ameaça específica a uma atividade legitima) foi ou será cometido, e;
2. Existe alta probabilidade de que evidências ou materiais relevantes para tal crime grave (ou ameaça específica a uma atividade legitima) seriam obtidos acessando as informações protegidas procuradas, e;
3. Outras técnicas menos invasivas foram esgotadas ou seriam inúteis, de forma que as técnicas utilizadas sejam a opção menos invasiva, e;

4. As informações acessadas serão limitadas ao que é relevante e essencial ao crime grave ou ameaça específica ao fim legítimo alegado; e
5. Quaisquer informações coletadas a mais não serão mantidas, mas prontamente destruídas ou devolvidas; e
6. As informações serão acessadas somente pela autoridade especificada e usadas apenas para a finalidade e duração para as quais foi concedida a autorização; e
7. As atividades de vigilância solicitadas e técnicas propostas não comprometem a essência do direito à privacidade ou as liberdades fundamentais.

Em resumo, o acesso às informações de registros de conexão e acesso a aplicações só deveria ser conduzido mediante ordem judicial quando for a única forma de atingir um fim legítimo ou quando for a forma de menor impacto nos direitos humanos (o ônus de estabelecer esta justificativa recai sempre sobre o Estado).

3.2 Sobre a necessidade de uma autoridade garantidora independente

A proteção de dados é em grande parte dependente da criação de autoridades cuja governança, recursos e conhecimentos técnicos sejam suficientes para que suas competências sejam exercidas. Nesse sentido, é importante notar que autoridades de proteção de dados foram adotadas por todos os membros da Convenção 108, pela maioria dos países membros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), bem como em dois países da América do Sul (Argentina e Uruguai) e vários países africanos.

De acordo com o artigo 12.bis da versão modernizada da Convenção 108 do Conselho da Europa (ver http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm), no respeito ao tratamento dos dados pessoais (Convenção 108), as autoridades garantidoras são obrigadas a agir com total independência e imparcialidade, a ter todos os recursos necessários e poderes para, no mínimo: (i) monitorar e promover a proteção de dados; (ii) aconselhar o governo, os controladores de dados e o público em geral sobre a forma mais eficaz de proteger os dados pessoais; (iii) definir medidas de segurança contra riscos, tais como o acesso acidental ou não autorizado, destruição, perda, utilização, modificação ou divulgação de dados pessoais; (iv) investigar e intervir, sobretudo no que diz respeito à adoção das medidas acima mencionadas pelos fornecedores e de uma definição de um ambiente estritamente confidencial, controlado e seguro para a retenção de registros de conexão na Internet; (v) emitir decisões – que podem ser objeto de recurso aos tribunais – no que diz respeito a violações das disposições do quadro de proteção de dados, sobretudo, a imposição de sanções administrativas; (vi) iniciar um processo judicial, ou para chamar a atenção das autoridades judiciárias competentes às violações da lei geral de proteção de dados; (vii) promover estudos e propor normas tendentes à concretização da proteção de dados e princípios de privacidade no contexto das novas TIC e objetos interconectados.

Uma vez que o Marco Civil estabelece princípios e obrigações que tocam os direitos à privacidade e dados pessoais - principalmente no que diz respeito à guarda compulsória de registros de conexão e acesso à aplicações -, a criação de uma autoridade garantidora nos moldes mencionados acima e com recursos e capacidade técnica necessários pode ser justificável, para a definição de padrões de segurança e sigilo a serem observados na coleta e armazenamento desses registros, após a realização de estudos e consulta aos diversos setores afetados.

Uma autoridade garantidora independente também seria responsável por realizar revisões sistemáticas aos padrões e normas vigentes de modo a garantir que estejam atualizados e sejam eficazes a seus propósitos. Em particular, deverá produzir estatísticas sobre a conservação de dados gerados ou tratados, no contexto da oferta de acesso à Internet e acesso a aplicativos de Internet. As estatísticas não devem conter dados pessoais e devem incluir: (i) os casos em que as informações foram prestadas à autoridade competente; (ii) o tempo entre a data em que os dados foram conservados e a data em que as autoridades competentes solicitaram a transmissão dos dados e (iii) os casos em que os pedidos de dados não puderam ser satisfeitos.

3.3 Criação de um consórcio multissetorial independente

A definição de padrões de segurança de dados deveria ser feita em conjunto com um consórcio de entidades privadas ou a um organismo multissetorial que englobe empresas privadas, sociedade civil, especialistas técnicos e representantes do governo. Essas soluções poderiam ser mais eficientes do que a definição de padrões estáticos através de normativa estatal. Com efeito, como discutiremos adiante, é necessária uma revisão permanente das especificações técnicas que definem as medidas de segurança para a proteção de dados, a fim de mantê-las atualizadas de acordo com a evolução tecnológica.

Tal consórcio deveria contar com competências e recursos suficientes para desenvolver estudos e consultas que embasarão a criação de padrões para segurança e sigilo dos registros de conexão e acesso a aplicações armazenados no marco da lei. A redação dos padrões seria feita com base nos estudos e recomendações do consórcio e deveria incluir a previsão de mecanismos de revisão sistemática periodicamente.

A participação de agentes do setor privado permitiria equilibrar as exigências de armazenamento e segurança com as necessidades do mercado de modo a não criar um ônus que comprometa a inovação tecnológica. Tal instância seria composta, ainda, por autoridades públicas, comunidade técnica, e entidades da sociedade civil não-empresarial, que buscarão garantir as normas estejam em plena conformidade com as exigências de interesse público e o respeito aos direitos humanos. Cabe ressaltar, porém, que tal consórcio não substitui a criação de uma autoridade garantidora independente, pois não cumpre com os requisitos e competências explicitados no item II acima e nas melhores práticas internacionais.

3.4 Estabelecimento de parâmetros de segurança

A leitura dos artigos 10, 13 e 15 leva a concluir que o regulamento determinará os parâmetros de segurança que devem ser observados pelos provedores ao armazenar registros de conexão e acesso a aplicações de Internet. Essa opção, porém, parece ser a menos eficaz, uma vez que, em razão da velocidade das mudanças tecnológicas, essas medidas podem se tornar obsoletas e falhar em proteger os direitos fundamentais dos usuários de Internet de forma efetiva.

Identificamos a seguir alguns parâmetros de segurança que podem servir como base para tal regulamento, mas novamente destacamos a necessidade de se prever mecanismos para a revisão

periódica desses padrões. Reforçamos que, em todos os casos, os dados conservados só deverão ser fornecidos às autoridades competentes em casos específicos e de acordo com o estabelecido no Marco Civil (artigo 13, § 5°, 15, § 3° e 22) e regulamento.

Enquanto armazenados, os dados devem ser protegidos contra a destruição ilegal, acidental ou deliberada, a perda ou alteração acidental, a divulgação e o tratamento ou o acesso não autorizado ou ilegal. Além disso, medidas adequadas são necessárias a fim de garantir que os registros possam ser acessados apenas por pessoas especialmente autorizadas e que todos os dados sejam destruídos no final do período de retenção estabelecido pela lei.

Medidas de segurança de dados, incluindo criptografia e autenticação por meio de técnicas criptográficas, devem ser definidas de acordo com os riscos e danos potenciais que podem ocorrer nas seguintes etapas:

- A criação e manutenção de bases de dados destinadas a armazenar os registros de conexão e de acesso a aplicações;
- O processo de transferência dos registros de conexão e de acesso a aplicações às autoridades;
- O armazenamento dos registros de conexão e de acesso a aplicações pelas autoridades.

A experiência da União Europeia (UE) com relação às disposições sobre retenção de dados pode ser interessante para a definição de medidas de segurança apropriadas. Particularmente, o Grupo de Trabalho Artigo 29, que reúne todas as autoridades de proteção dos dados pessoais da UE), recomenda:

- Um controle estrito sobre o acesso aos registros mediante a definição de responsabilidades sobre as pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo apenas para determinados usuários;
- O estabelecimento de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla (tais como senha e biometria) para assegurar a presença física do responsável pelo tratamento dos registros;
- Criação de um inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações com, ao menos, a identidade do usuário, o momento e duração do acesso e o arquivo acessado;
- Uso de soluções de gestão dos registros por meio de tecnologias de criptografia - ou medidas de proteção equivalentes - para garantir a integridade dos dados;
- A separação lógica de outros sistemas de tratamento de dados para fins comerciais.

Por último, o Grupo de Trabalho Artigo 29 destaca que a aplicação das medidas de segurança deveria ser incorporada em um programa de certificação de segurança a ser executado em intervalos regulares - de preferência por uma entidade externa - a fim de avaliar a robustez das medidas implantadas em relação os riscos de vulnerabilidades. Por fim, parece importante ressaltar que apenas as autoridades públicas podem ser responsáveis pela fiscalização da aplicação das normas sobre a segurança dos dados armazenados. Logo, a existência de uma autoridade capaz de realizar auditorias ou solicitar auditorias relativas à aplicação das normas de segurança parece ser

essencial para o desenvolvimento de um quadro apropriado de segurança dos registros de conexão e de acesso a aplicações.

3.5 Limites para a guarda de registros de conexão e acesso a aplicações de Internet

O Marco Civil não define um período máximo de retenção de registros de conexão e acesso às aplicações de Internet. Tal lacuna fragiliza o direito à privacidade e proteção de dados pessoais e um regulamento sobre o tema deve estabelecer que esses dados sejam deletados após o período de retenção estipulado na lei, exceto nas situações previstas nos artigos 13, § 2º, e 15, § 2º.

Quanto à possibilidade de pedido de guarda cautelar por prazo maior do que o previsto, o Marco Civil não deixou claro de que maneira seria delimitado o escopo de tal pedido. Como a comunicação dos dados às autoridades está vinculada ao pedido de autorização judicial de acesso - a ser feito em até 60 dias da data do requerimento de guarda cautelar, conforme os artigos 13, § 3º, e 15, § 2º - , natural que os dois primeiros requisitos incluídos no rol do artigo 22 do Marco Civil orientem também o pedido de guarda cautelar. Em outras palavras, ao requerer o armazenamento cautelar de registros de conexão ou de acesso a aplicação de Internet para além dos prazos de, respectivamente, 1 ano e 6 meses, as autoridades devem especificar "fundados indícios da ocorrência do ilícito" (art. 22, I) e oferecer "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória" (art. 22, III). Caso contrário, corre-se o risco de que pedidos que sejam substancialmente mais abrangentes do que o autorizado pelo Marco Civil sejam direcionados aos provedores.

Além disso, para evitar abusos, o regulamento deveria determinar que após o material obtido ser utilizado para os propósitos para os quais foram solicitados, deve ser destruído ou devolvido aos afetados. Recomenda-se também determinar sanções para as situações em que houver compartilhamento de dados sobre registros de conexão e acesso a aplicações de forma ilegal.

3.6 Revisão e Prestação de Contas

O regulamento deve estabelecer mecanismos para a revisão e atualização das medidas relativas à guarda de registros de conexão e acesso a aplicações na Internet. Elas devem estar sujeitas a processos de revisão sistemáticos baseados em avaliações e estudos periódicos que provem sua eficácia e seu impacto nos direitos humanos. Tais processos de revisão devem, sempre que possível, incluir instâncias de ampla participação multissetorial.

Além disso, a sociedade deve ter condições de acompanhar e monitorar como as medidas de retenção de registros estão sendo cumpridas e utilizadas por parte das autoridades governamentais. Nesse sentido, sugerimos que o regulamento estipule informações básicas a serem oferecidas pelos provedores de acesso ou aplicações como parte de suas obrigações em cumprir com o previsto no artigo 11º, parágrafo 3º, que afirma que "os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações". Entre outras informações, pode-se sugerir a publicação de dados como:

(i) O número total de solicitações de dados pessoais recebido;
(ii) O número de usuários afetados por tais solicitações;
(iii) Informações sobre o solicitante dos dados (autoridades legais, investigadores privados, empresas, indivíduos, etc.);
(iv) Detalhes sobre os pedidos recebidos de autoridades legais, como, por exemplo, a fundamentação legal para a solicitação;
(v) Informações sobre o tipo de dados solicitados (conteúdos de comunicação, registros de acesso, etc);
(vi) A taxa de atendimento das solicitações divididas por categoria;

Os relatórios de transparência deveriam ser publicados periodicamente, no mínimo uma vez por ano, e disponibilizados para download nas páginas institucionais dos provedores ou das autoridades públicas em formato aberto, interoperável e processável por máquinas. Como consideramos no item II, acima, tanto as medidas de segurança (item IV), quanto as obrigações de prestação de contas por parte do setor privado, deveriam ser supervisionadas por uma autoridade garantidora independente.

3.7 Transparência e Escrutínio Público

Sugerimos também, com base nas obrigações de publicidade e transparência presentes na Constituição Federal e na Lei de Acesso à Informação Pública (Lei 12.527/2011), que o decreto explicite que o Estado deve fornecer informações suficientes para que os indivíduos possam compreender plenamente o escopo, natureza e aplicação das medidas de guarda de registros de conexão e acesso a aplicações de Internet. Além disso, que também deixe claro que não haverá interferência nas iniciativas dos agentes privados de publicar dados sobre o cumprimento às exigências estatais.

Nesse sentido, sugerimos que regulamento obrigue as autoridades a publicar periodicamente relatórios e dados estatísticos (disponibilizados de forma aberta e processável por máquina) de transparência sobre o uso dos mecanismos previstos no Marco Civil da Internet. Tais relatórios deveriam conter, pelo menos, informações agregadas sobre o número de pedidos aprovados e rejeitados, um detalhamento por provedor e autoridade investigatória, tipo, propósito e número de indivíduos afetados por cada pedido. Além disso, sugere-se que tais relatórios informem o tipo de infração investigada que ensejou a solicitação dos dados e permita averiguar se os dados já solicitados serviram efetivamente para a apuração de ilícitos (ensejando a oferta de denúncia pelo Ministério Público, por exemplo)[109].

Cabe ressaltar a centralidade das obrigações de transparência envolvidas no caso particular da guarda de registros de conexão e acesso a aplicações de Internet em uma democracia. Assim, além dos critérios mencionados anteriormente para a limitação do acesso (item I), os funcionários que tenham atribuído o poder de realizar algum tipo de vigilância a partir do acesso aos dados armazenados, devem estar sujeitos a uma supervisão eficaz, inclusive do público em geral, de modo a restringir eventuais abusos e o uso arbitrário desse poder.

4. Outros Temas e Considerações

4.1 Efetividade dos requisitos de publicidade e clareza das politicas de uso

A relação entre usuários e plataformas ou provedores de conexão costuma ser regulada por uma espécie de contrato de adesão conhecido no ambiente online como “Termos de Uso” ou “Termos de Serviço”, que pode ser complementado por outros documentos como a “Política de Privacidade” e os “Padrões da Comunidade”, entre outros. Para o efetivo cumprimento do art. 7º, inciso XI, é preciso que esses contratos sejam facilmente acessados e que expressem com clareza o tratamento de dados e de conteúdo que possa implicar em restrição de direitos dos usuários.

Além das implicações decorrentes da relação de consumo característica dessa interação, esses contratos podem impactar em direitos fundamentais como a privacidade e a liberdade de expressão. O art. 7º, inciso XI, do Marco Civil garante que as políticas de uso dos provedores de conexão à internet e de aplicações devem ser publicadas e explicitadas com clareza. Dessa forma, entende-se que, uma vez consciente da política de uso a que está sujeito, o usuário poderá eleger os serviços que melhor atendem aos seus interesses e respeitam seus direitos, bem como se comportar de forma consciente e condizente com suas escolhas em relação à exposição pessoal e manifestação do seu pensamento online.

No entanto, esses documentos costumam ser longos e redigidos em linguagem jurídica e pouco acessível para o usuário comum. Segundo um estudo da Universidade Carnegie Mellon, nos Estados Unidos, um usuário precisaria reservar 8 horas diárias e 76 dias para ler somente as Políticas de Privacidade de uma média de 1.462 páginas visitadas em um ano. No caso de alguns serviços, pode ser difícil até mesmo de encontrar as políticas relevantes ou de identificar quais são aquelas com as quais o usuário se compromete ao acessar uma plataforma.

Além disso, esses contratos fazem uso frequente de expressões genéricas e ambíguas, que impedem que o usuário conheça a real abrangência dos termos aos quais está se submetendo, bem como seus impactos sobre os direitos individuais e coletivos na utilização da internet.

Não raras vezes, esses documentos preveem, ainda, a possibilidade de sua alteração unilateral pela plataforma sem garantir a preservação das condições iniciais aceitas pelo usuário ou, em casos ainda mais extremos, sem oferecer qualquer tempo hábil para notificação e aceite (consentimento) do usuário, estabelecendo que a mera utilização após a mudança implicaria na aceitação irrestrita de todas as condições alteradas. Em muitos casos, o contrato inicialmente acordado sequer é disponibilizado para consulta ou *download*, impedindo qualquer forma de controle das condições estabelecidas entre as partes.

De modo geral, os termos de uso e documentos correlatos manifestam a intenção de proteger as empresas contra eventuais disputas judiciais – inclusive eximindo-as de responsabilidade em certas situações – e colocam em segundo plano o oferecimento de informações claras e relevantes aos usuários sobre seus direitos, como seus dados pessoais são tratados e como seus conteúdos podem ser afetados pelas políticas da plataforma.

A título de exemplo, é bastante comum encontrar cláusulas afirmando que todos os riscos provenientes do uso da plataforma são assumidos inteiramente pelo usuário e que as plataformas podem suspender seus serviços a qualquer tempo e por qualquer razão, com ou sem a notificação de seus usuários e sem oferecer qualquer garantia de *backup* de seus dados e conteúdos pessoais. Há casos em que é estabelecido, ainda, um valor máximo a ser indenizado ao usuário na eventual hipótese de a plataforma ser condenada em ação judicial, que costuma consistir em cerca de cem dólares.

Embora no Brasil o efeito de cláusulas abusivas seja amenizado pela proteção conferida pelo Código Brasileiro de Defesa do Consumidor (Lei 8078/1990) -- que declara as declara nulas de pleno direito --, as barreiras para o exercício de direitos podem persistir, já que em casos de abusos a vítima deve recorrer à Justiça para ter seus direitos reconhecidos.

Além disso, o ambiente online tem particularidades que podem ser devidamente exploradas no sentido de se garantir que obrigações concretas de transparência sejam observadas.

A necessária regulamentação dos requisitos de publicidade e clareza estabelecidos no Marco Civil não precisa e nem deve estar congelada em uma norma de difícil alteração, mas deve ser flexível no sentido de acompanhar as inovações tecnológicas, adequando a interpretação do alcance desses requisitos às especificidades das diferentes ferramentas e serviços online, que experimentam constantes inovações. A previsão de uma autoridade garantidora viabilizaria o estabelecimento de parâmetros claros que permitam a implementação dos princípios garantidos no Marco Civil, bem como mecanismos de controle de seu cumprimento.

Algumas das questões a serem tratadas seriam: (i) a garantia de que as plataformas online disponibilizem de forma gratuita e independente da criação de uma conta os Termos de Uso, Políticas de Privacidade e demais documentos legais que regem sua relação com os usuários; (ii) o uso de uma linguagem acessível nos contratos; (iii) o estabelecimento de compromissos claros com a garantia dos direitos do cidadão utilizando-se de exemplos, glossários, ícones, hiperlinks e outros elementos explicativos que ajudem a tornar o contrato mais acessível para o usuário comum, e; (iv) a garantia de que o usuário tenha acesso às versões anteriores do contrato, especialmente àquelas referentes ao momento em que se cadastrou na plataforma, e que possa visualizar as alterações posteriores com facilidade e transparência, gozando de tempo hábil para efetuar escolhas conscientes em relação às mudanças.

Ressaltamos, por fim, que todos os países da União Europeia contam com autoridades garantidoras de proteção a dados pessoais. Alguns deles possuem uma autoridade de supervisão geral, com a função de garantir o monitoramento e o respeito à legislação de proteção de dados dentro de seus territórios. Outros possuem uma autoridade de competência geral, e outras agências para setores específicos, como saúde, correios e telecomunicações.

Em alguns casos, foram criadas autoridades em âmbito nacional que supervisionam autoridades regionais ou estaduais. Certos modelos contemplam também um "ombudsman", que de maneira complementar atua na proteção de dados pessoais. Uma fundamental característica partilhada por tais autoridades é sua independência funcional. De acordo com a Diretiva de Proteção de Dados e o Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento

Automatizado de Dados de Caráter Pessoal, a autonomia das autoridades deve ser completa, e seus poderes de decisão devem ser independentes, livres de quaisquer influências diretas ou indiretas.

Ainda que não seja possível assim proceder por meio de um decreto presidencial, é importantíssimo ter em mente que os objetivos do Marco Civil da Internet de garantir a privacidade e proteção de dados pessoais apenas serão plenamente atingidos com a instituição de uma autoridade garantidora, que estabeleceria e daria efetividade a padrões relativos à publicidade, clareza e acessibilidade dos termos de uso, promovendo assim maior equilíbrio nas relações entre usuários e plataformas.

Referências

Neutralidade da Rede

Arcep, Decision No. 2012-0366
Economides, N. & Tag, J., Net Neutrality on the Internet: A Two-Sided Market Analysis, Information Economics and Policy 24.2 (2012): 91-104.
European Union Parliament, Proposal for a Regulation of the European Single Market for Electronic Communications, COM (2013) 627 final (Mar. 26, 2014)
Choi, J., and Kim, B., Net Neutrality and Investment Incentives, The RAND Journal of Economics 41.3 (2010): 446-471
Church, J. & Gndal, N., Platform Competition in Telecommunications, The Handbook of Telecommunications Vol 2 (Cave, M. et al. eds, 2004): 119-155
Dickson, Peter R., and James L. Ginter. Market Segmentation, Product Differentiation, and Marketing Strategy, The Journal of Marketing (1987): 1-10.
Directive 2002/22/EC of the European Parliament and of the Council on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, OJ L 108, 24.04.2002, p. 51
FCC, In the Matter of Preserving the Open Internet. GN Docket No. 09-191, Report and Order (Dec. 23, 2010)
Hart, Oliver, et al., Vertical Integration and Market Foreclosure, Brookings papers on economic activity. Microeconomics (1990): 205-286.
Hemphill, SC., Network Neutrality and the False Promise of Zero-Price Regulation, Yale J. on Reg. 25 (2008): 135
Hermalin, E., and Katz, M., The Economics of Product-Line Restrictions with an Application to the Network Neutrality Debate, Information Economics and Policy 19.2 (2007): 215-248
NKOM, Norwegian report on Content Delivery Networks (CDN) (May 24, 2012)
OPTA, Telecommunications Act, BWBR0009950
Pallis, G., and Vakali, A., Insight and Perspectives for Content Delivery Networks, Communications of the ACM 49.1 (2006): 101-106.
Perry, M., Vertical Integration: Determinants and Effects, Handbook of industrial organization 1 (1989): 183-255.
Rochet, JC. & Tirole, J. (2006), Two-Sided Market: A Progress Report, The RAND Journal of Economics, 37.3 (2006): 645-667
Spence, Michael, Product Differentiation and Welfare, The American Economic Review (1976): 407-414.

Wu, T., and Lee, R., Subsiding Creativity Through Network Design: Zero-Pricing and Net Neutrality, Journal of Economic Perspectives, 23.3 (2009): 61-76.

Privacidade

Article 29 Working Party, Opinion 15/2011 on the definition of consent
Article 29 Working Party, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive Adopted on 13 July 201
European Parliament legislative resolution on the proposal for a General Data Protection Regulation
Convention 108, Modernised version
OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows
OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
NETmundial Multistakeholder Statement
Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm
Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações https://pt.necessaryandproportionate.org/text