CONTRIBUIÇÃO PARA A SEGUNDA ETAPA DO DEBATE PÚBLICO SOBRE A REGULAMENTAÇÃO DO MARCO CIVIL DA INTERNET

CENTRO DE TECNOLOGIA E SOCIEDADE (CTS/FGV)

MARÇO 2016

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

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

O presente documento apresenta os comentários e sugestões do Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (CTS/FGV) a respeito da minuta de decreto apresentada pelo Ministério da Justiça para consulta pública sobre a regulamentação do Marco Civil da Internet, Lei 12.965, de 23 de abril de 2014.

O CTS/FGV já participou da primeira fase de consulta e parabeniza o Ministério da Justiça pela abordagem equilibrada, bem como pela abertura às contribuições de todos os participantes nesse exercício democrático.

Acompanhando a classificação feita na minuta de decreto, o documento está dividido em três partes: (i) neutralidade de rede; (ii) proteção aos registros, aos dados pessoais e às comunicações privadas; e (iii) fiscalização e transparência. Optamos por comentar a minuta a partir da sua própria redação, a fim de apresentar considerações mais concretas nessa segunda etapa de debate público.

I) Neutralidade de rede

No que diz respeito à neutralidade da rede, cabe sublinhar que o Marco Civil da Internet considera o princípio da não discriminação, bem como a sua efetivação, como um dos fundamentos da disciplina e do uso da Internet no Brasil (art. 2°) e define de forma exaustiva as situações que justificam a discriminação e degradação do tráfego (art. 9º, §1º): (i) devido a **requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações,** e; (ii) para a **priorização de serviços de emergência**. O papel do decreto em exame é, portanto, especificar tais exceções a fim de garantir uma aplicação que preserve o raciocínio e os objetivos fundamentais da neutralidade da rede.

Nas seções seguintes exploraremos as exceções ao princípio da neutralidade, desenvolvendo os elementos já fornecidos na contribuição à primeira fase da consulta e seguindo o percurso lógico definido pela minuta do decreto.

1. Serviços especializados (art. 2°)

A minuta de decreto considera, corretamente, os serviços especializados como uma exceção ao princípio da neutralidade, como foi destacado pelo CTS/FGV na primeira fase da consulta. Nesse sentido, cabe destacar que, apesar de os serviços especializados serem semelhantes à Internet pública do ponto de vista da experiência do usuário, eles são tecnicamente distintos. Como aponta o artigo 2º da minuta, os serviços especializados podem usar os protocolos TCP/IP, sobre os quais a Internet é baseada, mas, diferentemente da Internet aberta, operam dentro de um conjunto restrito de redes, ou em apenas uma rede, gerenciada(s) por uma operadora. Assim, o princípio da neutralidade não se aplica aos serviços especializados porque esses serviços não fazem parte da Internet, embora possam compartilhar infraestrutura com os serviços de Internet. Portanto, os serviços especializados não são caraterizáveis como "sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito" (art 5°, I, do Marco Civil) porque eles são otimizados para um único serviço ou tipo de serviço, a fim de garantir um nível de qualidade ou de segurança não alcançável na Internet. Além disso, os serviços especializados não são interconectados com a Internet pública mas, ao contrário, são apenas disponíveis dentro da rede específica do provedor que os oferece e que os gerencia, controlando o acesso e garantindo as características específicas do serviço. Nesse sentido, a Organização para Cooperação e Desenvolvimento Econômico levanta que serviços e conteúdos podem ser entregues aos usuários através de redes ultrarrápidas por meio de serviços especializados, mas

esses serviços são separados dos outros tipos de tráfego de Internet (OCDE, 2014). Isto significa que os serviços especializados deveriam ser separados física ou logicamente da Internet e, como estipulam as orientações norueguesas para a neutralidade da rede - considerada a base de um dos sistemas co-regulatórios mais eficientes do mundo - "se a conexão física é compartilhada com outros serviços, deve salientar-se claramente como a capacidade é compartilhada entre o tráfego de Internet e outros serviços" (Sørensen, 2015).

Todavia, é essencial destacar que o decreto não deve criar um incentivo perverso para os operadores se afastarem da Internet aberta em razão da não regulamentação dos serviços especializados. Nesse sentido, o *Open Internet Advisory Committee* destacou claramente que a não aplicação das obrigações de não discriminação aos serviços especializados não deve tornar-se uma justificativa para que as operadoras escapem da carga regulamentar, ou reduzam investimentos na Internet aberta para concentrá-los em serviços especializados (OIAC, 2014), particularmente quando a provisão de tais serviços se mostrar uma opção mais lucrativa do que a oferta de acesso à Internet pública (Hermalin & Katz, 2007).

Além disso, cabe destacar que deve haver atenção por parte do regulador para que a oferta de serviços especializados não sirva como instrumento para contornar as obrigações de não discriminação decorrentes da neutralidade de rede. É possível imaginar tal situação, por exemplo, caso um provedor de Internet fixa imponha franquias de dados aos seus usuários, isentando os próprios serviços especializados (que não seriam considerados como Internet) de tal franquia. Nesse caso, a concorrência entre os serviços especializados e os serviços e aplicativos análogos disponíveis na Internet pode ser prejudicada, favorecendo injustamente os serviços especializados e penalizando os serviços e aplicativos disponíveis na Internet. Essa situação deveria ser evitada a fim de preservar a concorrência e manter a liberdade de escolha e a liberdade de iniciativa comercial para todos. Essa perspectiva é corroborada pelo artigo 4°, segundo o qual "*as ofertas comerciais e modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa* ". Assim, é essencial que os provedores de conexão tenham a possibilidade de oferecer serviços especializados além do acesso à Internet, desde que tais ofertas não sejam em detrimento dos serviços de conexão à Internet.

Nesse sentido, cabe reiterar que a combinação de franquias de *download* na rede fixa com a oferta de serviços especializados patrocinados pode tornar-se uma forma de contornar as obrigações de não discriminação, orientando a experiência de Internet do usuário em direção dos serviços especializados em razão da gratuidade do serviço. Além disso, é preciso especial atenção para que os serviços especializados sejam oferecidos somente quando a capacidade da rede for suficiente para disponibilizá-los de modo paralelo e complementar aos serviços de acesso à

Internet e se não implicarem prejuízos em termos de disponibilidade ou qualidade dos serviços de conexão à Internet existentes.

A fim de evitar abusos, parece importante que os serviços especializados sejam definidos claramente. Nesse sentido, o inciso II do artigo 2º deveria ser reformulado para incluir critérios específicos, nos seguintes termos:

Redação atual	Redação sugerida
II – aos serviços especializados, ainda que utilizem protocolos TCP/IP ou equivalentes, desde que não se confundam, em termos de funcionalidade, com o caráter público e irrestrito da Internet.	II – aos serviços especializados, ainda que utilizem protocolos TCP/IP ou equivalentes, desde que não se confundam, em termos de funcionalidade, com o caráter público e irrestrito da Internet. **Parágrafo único. São considerados serviços especializados, os serviços que:** **a) não permitem acesso à Internet e não constituem um substituto da Internet e, portanto, não podem ser comercializados como um substituto para a Internet;** **b) oferecem alguma função aprimorada, seja uma qualidade assegurada de serviço, velocidade ou segurança que não está facilmente disponível na Internet;** **c) são operados e controlados por um provedor de conexão específico e somente podem ser acessados pelos usuários desse provedor;** **d) não determinam prejuízos em termos de disponibilidade ou qualidade dos serviços de acesso à Internet;** **e) não são fornecidos discriminando aplicações funcionalmente equivalentes disponíveis na Internet e sua adoção por**

	usuários da Internet deve ser voluntária.

2. Finalidade do tratamento isonômico (art. 3°)

O artigo 3º desempenha um papel particularmente relevante, fornecendo elementos essenciais para a definição da finalidade da neutralidade da rede. Nesse sentido, cabe destacar que, não obstante a preservação do caráter público e irrestrito do acesso à Internet seja um objetivo fundamental do princípio de neutralidade, seria limitante afirmar que esse seja o único objetivo. Nesse sentido, destacamos que a neutralidade da rede impõe um tratamento isonômico e não discriminatório do tráfego de Internet para proteger todos os fundamentos da disciplina do uso da Internet no Brasil (Belli 2015) e para manter a natureza generativa da Internet, ou seja, a capacidade da Internet de evoluir graças às contribuições não filtradas de seus usuários (Belli 2015; Belli & De Filippi 2015). Assim, o artigo 3º poderia ser consideravelmente aprimorado adicionando uma referência a esses elementos, pelos seguintes termos:

Redação atual	Redação sugerida
Art. 3º A exigência de tratamento isonômico de que trata o art. 9º da Lei 12.965, de 23 de abril de 2014, deve garantir a preservação do caráter público e irrestrito do acesso à Internet.	Art. 3° - A exigência de tratamento isonômico de que trata o art. 9º da Lei 12.965, de 23 de abril de 2014, **deve garantir a preservação dos fundamentos da disciplina do uso da Internet no Brasil, do caráter público e irrestrito do acesso à Internet, cuja evolução funda-se nas contribuições não filtradas de seus usuários.**

3. Ofertas comerciais e modelos de cobrança (art. 4°)

O primeiro parágrafo do artigo 4° confirma o imperativo de que a discriminação ou degradação de tráfego decorram exclusivamente “de requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações ou da priorização de serviços de emergência”, em conformidade com o artigo 9° do Marco Civil da Internet e, nomeadamente, respeitando “todos os requisitos dispostos no art. 9º, §2º”. Esse primeiro parágrafo é positivo e coerente com o artigo 3° e, particularmente, com a formulação proposta na seção precedente.

Dessa forma, cabe relembrar que o fundamento da neutralidade da rede é a ideia de que os provedores de acesso à Internet tratem de maneira não discriminatória cada serviço e conteúdo na Internet, no sentido de manter a Internet como uma plataforma de inovação e de emponderamento dos usuários. Assim, da mesma forma que 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, parece uma consequência lógica que os provedores de acesso não isentem de qualquer pagamento aplicativos específicos ou não os subsidiem, pois ambos os casos introduziriam arranjos econômicos diferenciados. Nesse sentido, a regra estabelecida pelo artigo 9° prescreve explicitamente a obrigação de tratamento isonômico de quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação e sem limitar tal tratamento ao gerenciamento do tráfego da Internet em sua camada infraestrutural ou isentando as ofertas comerciais de tal tratamento não discriminatório.

Como o CTS/FGV ressaltou na contribuição enviada na primeira fase dessa consulta, o patrocínio de aplicativos, conhecido também como a prática do *zero rating,* consiste em uma discriminação de preços para serviços diferentes, permitindo que um provedor de aplicações (como uma rede social) ou uma operadora patrocinem o acesso do usuário a *sites* ou aplicativos específicos. Esse tipo de plano já está sendo oferecido no mercado brasileiro e, portanto, o exame de seu *status* e de sua permissibilidade de acordo com o Marco Civil se faz necessário. A fim de conferir ao parágrafo único mais coerência com o artigo 3°, nos parece necessário reformular o parágrafo único do artigo 4° nos seguintes termos:

Redação atual	**Redação sugerida**
Parágrafo único. As ofertas comerciais e modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio de desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória.	Parágrafo único. As ofertas comerciais e modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, **a fim de garantir o pleno desenvolvimento social e humano, permitindo a cada usuário participar na evolução da Internet, sendo vedada qualquer tipo de discriminação de natureza técnica ou econômica, nos termos do artigo 9° da Lei 12.965, de 23 de abril de 2014 e deste Decreto.**

Tal reformulação permite esclarecer que o fundamento não discriminatório do princípio da neutralidade se aplica de maneira transversal, tanto ao gerenciamento do tráfego da Internet – ou seja, as atividades de "transmissão, comutação e roteamento" – quanto às ofertas comerciais, no sentido de preservar os fundamentos da disciplina do uso da Internet no Brasil. Além disso, a reformulação proposta ofereceria ao Judiciário mais elementos para deliberar sobre a compatibilidade dos planos atualmente oferecidos no mercado com o princípio da neutralidade da rede, ainda que a regra do artigo 9° do Marco Civil da Internet já seja clara sobre este assunto. Tal

postura estaria alinhada com as decisões de países como o Canadá, Holanda, Eslovênia, Noruega e Índia, que já proibiram a prática de *zero rating* em função da sua incompatibilidade com o princípio da neutralidade da rede.

Como o CTS/FGV apontou na primeira fase da consulta, a decisão do regulador holandês de proibir o acesso patrocinado é particularmente interessante em relação as consequências no mercado. Em razão dessa decisão, 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 (Digital Fuel Monitor, 2015). Nesse sentido, cabe ressaltar que os aplicativos e conteúdos variados são a verdadeira razão de ser da Internet (Clark e Blumenthal, 2011) e que o exemplo holandês ilustra o evidente interesse das operadoras de incrementar as franquias dos usuários afim de permitir um maior consumo de dados quando os planos de *zero rating* não forem possíveis.

Portanto, nos parece claro que o legislador brasileiro, ao aprovar o artigo 9° do Marco Civil, adotou o entendimento de que, na ausência de práticas discriminatórias, os usuários de Internet poderiam continuar a se beneficiar de uma liberdade de escolha que seja orientada para a preferência dos serviços mais eficientes, de qualidade mais elevada e mais compatíveis com suas necessidades. Nesse sentido, a proibição do acesso patrocinado parece coerente com o raciocínio da Lei, na medida em que as práticas de zero rating orientam a escolha do usuário no sentido de aplicativos percebidos como gratuitos (porque patrocinados), em oposição a escolhas determinadas pela eficiência e qualidade do serviço. Ao invés de optar por uma vantagem econômica imediata – devido ao pagamento do consumo de dados pelo provedor de aplicativos ou pela operadora ao invés do usuário – o entendimento do legislador brasileiro foi o de que, em uma perspectiva de longo prazo, o patrocínio de aplicativos traz o risco de transformar a natureza da Internet de uma rede de propósito geral cujas modalidades de utilização são definidas autonomamente por cada usuário em uma rede cujos propósitos são estabelecidos de maneira centralizada pelas operadoras. Tal evolução limitaria a experiência de Internet dos usuários, desincentivando-os a se aventurar além dos serviços que lhes são fornecidos gratuitamente.

Este é o raciocínio que motivou, também, a recente decisão de proibir a diferenciação tarifária, sobre a qual se baseia o *zero rating*, da Autoridade reguladora das telecomunicações da Índia (TRAI). Segundo a TRAI, as tarifas diferenciadas prejudicam os pequenos e médios prestadores de conteúdo e aplicativos que não podem patrocinar os próprios serviços. Isto pode, portanto, criar barreiras de entrada para os atores de tamanho menor e limitar o desenvolvimento dos atores locais, logo asfixiando a inovação, ao invés de promovê-la (TRAI, 2016). Finalmente, a análise da decisão da TRAI parece interessante sob um perfil de proteção dos direitos humanos – que é um

dos fundamentos da disciplina e do uso da Internet no Brasil – uma vez que, pela primeira vez, a agência reguladora afirmou explicitamente que o patrocínio de aplicativos:

> "*can prove to be risky in the medium to long term as the knowledge and outlook of those users would be shaped only by the information made available through those select offerings. Further, to the extent that affordability of access is noted to be a cause for exclusion, it is not clear as to how the same users will be in a position to migrate to the open internet if they do not have the resources to do so in the first place*"[1] (TRAI 2016).

4. Gerenciamento razoável de redes (art. 5º)

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 poderão 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 informado 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.

O artigo 5° da minuta visa a fornecer orientação sobre quais situações podem justificar uma gestão razoável de redes a fim de garantir a prestação adequada de serviços e aplicações. O artigo 5° parece bem estruturado e reverbera algumas das sugestões do CTS/FGV na primeira fase da contribuição. Todavia, alguns elementos poderiam ser aprimorados afim de evitar que o disposto seja interpretado de maneira equivocada. Em seguida vamos analisar os diferentes parágrafos do artigo 5°, sugerindo algumas alterações.

Redação atual	Redação sugerida
Art. 5º Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações são aqueles decorrentes de:	Art. 5º Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações são aqueles **necessários e proporcionais decorrentes de:**

[1] Ou seja, a pratica de zero rating pode tornar-se arriscada no médio e longo prazo, porque a liberdade de conhecimento e de opinião dos usuários com acesso patrocinado seriam formadas apenas pelas informações disponibilizadas pelos aplicativos selecionados pelos patrocinadores".

Apesar de já serem indicados no Marco Civil, os requisitos de necessidade e proporcionalidade deveriam ser reiterados a fim de tornar o artigo mais explícito. Nesse sentido, o critério da necessidade sugere que o inteiro espectro de medidas técnicas de gerenciamento tenha sido considerado e a ferramenta usada para uma operadora seja justificada em razão da ineficiência das outras ferramentas disponíveis. Isso incluiria a consideração sobre a possibilidade de adoção de soluções pelo próprio usuário ao invés de centralizadas no nível da operadora. (Belli & van Bergen, 2013).

O critério da proporcionalidade implica a avaliação dos benefícios e das possíveis desvantagens consequentes da adoção de uma determinada medida técnica e a possibilidade de se adotar uma solução diferente, possivelmente menos discriminatória e mais eficaz, afim de alcançar a mesma finalidade. Portanto a avaliação de proporcionalidade implica um estudo de impacto das medidas utilizadas para avaliar se a solução proposta poderia ser mais onerosa do que necessário para alcançar determinado objetivo (BEREC, 2012).

Redação atual	Redação sugerida
I – tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço;	I – tratamento de questões de segurança e de **integridade das redes**, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço;

Nos parece necessário sublinhar a diferença entre segurança e integridade da rede enquanto proteção contra ameaças externas ou internas. Como destaca o *Body of European Regulators for Electronic Communications* (BEREC), a segurança da rede consiste em medidas para prevenir e controlar o acesso não autorizado, uso indevido, modificação ou negação de serviço, enquanto a integridade da rede consiste em medidas para manter ou restabelecer o nível de desempenho durante falhas de rede e mitigação ou prevenção de falhas na rede (BEREC 2012).

Em qualquer caso, os critérios da transparência, necessidade e proporcionalidade devem balizar as decisões sobre o gerenciamento de rede para fins de segurança e integridade, a fim de considerar e evitar potenciais danos colaterais. Por fim, cabe ressaltar que o termo “segurança da rede” deve ser interpretado no sentido técnico estrito e não deve ser confundido, em nenhuma hipótese, com a filtragem do conteúdo para fins de *enforcement*.

Redação atual	Redação sugerida
II – tratamento de situações de congestionamento de redes, tais como redistribuição de carga, rotas	II – tratamento de **situações temporárias e excepcionais de congestionamento de redes, tais**

alternativas em casos de interrupções da rota principal, gerenciamento em situações de emergência;	**como redistribuição de carga, rotas alternativas em casos de interrupções da rota principal, gerenciamento em situações de emergência, bem como situações de prevenção de congestionamentos, tais como uso de redes de entrega de conteúdo (Content Delivery Networks);**

É importante destacar que a primeira medida para evitar congestionamentos deve ser o investimento em infraestrutura, a fim de dispor de uma capacidade necessária para satisfazer a demanda dos usuários, entregando a capacidade e respeitando os níveis de qualidade contratados pelo usuário. O uso de medidas discriminatórias que favoreçam classes de aplicativos sensíveis deve ser considerado como admissível na medida em que seja necessário para minimizar os efeitos negativos de um congestionamento temporário e imprevisível, nos termos do inciso IV, § 1° do presente artigo e em conformidade com padrões técnicos internacionais (e.g. Bastian *et al.* 2010).

O caráter temporário e imprevisível parece necessário porque, como apontado anteriormente, o congestionamento permanente e previsível deve ser evitado investindo nas redes, favorecendo o uso de *Content Delivery Networks* (CDNs) ou adotando outras medidas que não impliquem em exceções à neutralidade. Os CDNs são sistemas de rede que realizam a intermediação entre provedores de aplicações e um provedor de acesso à Internet com o propósito de agilizar a transmissão de dados (Pallis & Vakali, 2006). Nos parece necessário reiterar a importância de acordos razoáveis e justos de interconexão entre CDNs e os demais agentes do mercado. Como o CTS/FGV ressaltou na primeira fase da consulta, 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 frequentemente não são divulgados, o que torna o monitoramento impossível, mas tal prática poderia mudar em virtude de requisitos regulatórios. Nesse sentido, o acesso aos termos e condições dos acordos de interconexão é essencial para que os reguladores possam avaliar as práticas das CDNs e emitir recomendações, se necessário, e até mesmo sancionar comportamentos anticoncorrenciais. Esse ponto é ulteriormente esclarecido nos comentários sobre o artigo 8º desse decreto.

Redação atual	Redação sugerida
III – tratamento de questões de qualidade de redes, para assegurar o cumprimento dos padrões mínimos de qualidade estabelecidos na regulamentação	III – tratamento de **questões relativas ao fornecimento da qualidade de serviço contratada, em conformidade com os padrões**

editada pela ANATEL; e IV – tratamento de questões imprescindíveis para a adequada fruição das aplicações, tendo em vista a garantia da qualidade de experiência do usuário. § 1º Nos casos elencados nos incisos III e IV do caput, o responsável pela transmissão, comutação ou roteamento poderá adotar medidas técnicas que permitam diferenciação de classes de aplicações, previstas em padrões internacionais, observada a isonomia entre as aplicações em cada classe e o disposto no inc. IV, do § 2º do art. 9 da Lei 12.965, de 2014. § 2º A ANATEL atuará na fiscalização e apuração de infrações quanto aos requisitos técnicos elencados neste artigo, consideradas as diretrizes estabelecidas pelo CGI. § 3º A discriminação ou degradação de tráfego decorrente dos requisitos técnicos indispensáveis de que trata este artigo deve respeitar o disposto no § 2º do art. 9º da Lei nº 12.965, de 2014.	**mínimos de qualidade estabelecidos na regulamentação editada pela ANATEL; e** IV – tratamento de questões imprescindíveis para a adequada fruição das aplicações, tendo em vista a garantia da qualidade de experiência do usuário. § 1º Nos casos elencados nos incisos III e IV do caput, o responsável pela transmissão, comutação ou roteamento poderá adotar de maneira temporária as medidas técnicas que permitam diferenciação de classes de aplicações, **a fim de garantir a fruição das aplicações mais sensíveis à latência, identificadas pelo CGI.br de acordo com os padrões internacionais**, observando a isonomia entre as aplicações em cada classe e o disposto no inc. IV, do § 2º do art. 9 da Lei 12.965, de 2014. § 2º A ANATEL atuará na fiscalização e apuração de infrações quanto aos requisitos técnicos elencados neste artigo, consideradas as diretrizes estabelecidas pelo CGI.br **e promovendo análises independentes das técnicas de gestão do tráfego Internet e das suas consequências.** § 3º A discriminação ou degradação de tráfego decorrente dos requisitos técnicos indispensáveis de que trata este artigo deve respeitar o disposto no § 2º do art. 9º da Lei nº 12.965, de 2014.

A estrutura e o conteúdo dos incisos III e IV do artigo 5° demandam modificações menores a fim de serem aprimorados. O inciso III poderia ser levemente reformulado para esclarecer que os níveis de qualidade de serviço concretamente fornecidos pelas operadoras devem estar em sintonia com os níveis estipulados nos acordos contratuais e, claramente, em conformidade com os padrões estabelecidos pela ANATEL.

Além do fornecimento de níveis de qualidade de serviço apropriados, o inciso IV considera a necessidade de garantir a qualidade de experiência do usuário. Como destaca o BEREC, a qualidade de experiência leva em conta a expectativa do usuário e o contexto, e é definida como a aceitabilidade de um aplicativo ou de um serviço, na percepção do usuário final (BEREC 2012). A qualidade de experiência de aplicativos mais sensíveis à latência, tais como os aplicativos de voz sobre IP, pode ser reduzida negativamente por causa de congestionamento e, portanto, é positivo que o decreto permita a utilização de tratamento diferenciado a fim de não comprometer a qualidade de tais classes de aplicativos sensíveis. Todavia, a possibilidade de tratamento diferenciado não pode se transformar em justificativa para não se aplicar as obrigações de isonomia e não discriminação. Nesse sentido, é essencial que o tratamento diferenciado seja aplicável somente temporariamente, consistindo em uma exceção no âmbito de redes com capacidade adequada, ao invés da regra no âmbito de redes carentes. Enfim, parece essencial que a identificação das classes de aplicativos mais sensíveis à latência seja feita pelo CGI.br no âmbito da sua competência relativa à definição de diretrizes técnicas.

5. Transparência (art. 6°)

O artigo 6° consagra um dos pilares fundamentais de todos os instrumentos de proteção da neutralidade da rede, ou seja, a transparência das políticas e medidas de gerenciamento de tráfego na Internet. A atual formulação deveria ser expandida a fim de fornecer elementos mais detalhados para que as operadoras possam dar cumprimento as suas obrigações de transparência mais fácil e precisamente, fornecendo informações inteligíveis para o usuário e concretamente úteis para a ANATEL no âmbito da sua tarefa de fiscalização. Nomeadamente, com relação o às informações necessárias para fiscalizar o respeito à neutralidade da rede, cabe destacar o exemplo chileno, um dos mais avançado no âmbito da transparência (SUBTEL, 2010) e no qual o Ministério da Justiça poderia se inspirar a fim de aprimorar o presente decreto. Nesse sentido, o artigo 6º poderia ser reformulado nos termos seguintes:

Redação atual	Redação sugerida
Art. 6º O responsável pela transmissão, comutação ou roteamento deverá adotar medidas de transparência ativa para explicitar ao usuário os motivos do gerenciamento que implique a discriminação ou degradação de que trata o art. 4º, tais como	Art. 6º O responsável pela transmissão, comutação ou roteamento deverá adotar medidas de transparência ativa para **comunicar os níveis de velocidade, qualidade de serviço fornecidos e explicitar as razões, a natureza e as consequências potenciais das medidas de gerenciamento**

I – indicação nos contratos de prestação de serviço firmado com usuários finais ou provedores de aplicação, apontando o impacto do gerenciamento sobre a qualidade da experiência do usuário; II – divulgação de informações referentes às práticas de gerenciamento adotadas em seus sítios eletrônicos, por meio de linguagem de fácil compreensão;	**adotadas, indicando pelo menos:** **I – a velocidade de upload e download de cada plano oferecido, os níveis mínimos de qualidade de serviço, bem como a existência de limites de download;** **II – os indicadores técnicos de qualidade de serviço, nos termos estabelecidos pela ANATEL;** **III – a lista exaustiva das medidas de gerenciamento, especificando as motivações pelas quais tais medidas podem ser utilizadas, apontando o impacto que podem ter sobre a qualidade da experiência do usuário e especificando as classes de aplicações e os protocolos que podem ser afetados por tais medidas de gerenciamento.** **Parágrafo único - As informações mencionadas no seguinte artigo devem ser comunicadas de maneira clara e compreensível, sendo incluídas nos contratos de serviço, publicadas e mantidas atualizadas, em local visível e de fácil acesso nos sítios eletrônicos de cada operadora.**

6. Content Delivery Networks (art. 8°)

Como foi destacado anteriormente, os CDNs são sistemas que atuam como intermediários entre os provedores de aplicações e um provedor de acesso à Internet com o propósito de agilizar a transmissão de dados. Os CDNs operam por meio da hospedagem local de cópias de dados selecionados (espelhamento ou "*mirroring*"). Assim, quando um usuário final solicita tais dados, a CDN intercepta a solicitação e os envia a partir do ponto de hospedagem local, ao invés da fonte remota original. Para que os CDNs não sejam explorados para contornar as garantias

estabelecidas pelo princípio da neutralidade de rede, particularmente no que diz respeito à proibição da priorização paga, é necessário que algumas obrigações de transparência sejam estabelecidas. Isso é essencial para permitir o monitoramento dos acordos de interconexão entre os provedores de acesso à Internet e os CDNs. Particularmente, informações sobre os termos técnicos e as condições de preço que governam a transmissão de dados e a interconexão devem ser disponibilizadas, uma vez que tais atividades 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. Nesse sentido o artigo 8º poderia ser reformulado nos termos seguintes:

Redação atual	Redação sugerida
Art. 8º Acordos entre provedores de conexão e provedores de aplicação devem preservar o caráter público e irrestrito do acesso à Internet. § 1º São vedados os acordos de que trata o caput que importem na priorização discriminatória de pacotes de dados. § 2º Acordos entre provedores de conexão e provedores de aplicação estão sujeitos à avaliação do órgão competente, nos termos do Capítulo IV, deste Decreto.	Art. 8º Acordos entre provedores de conexão e provedores de aplicação devem preservar o caráter público e irrestrito do acesso à Internet, **no pleno respeito dos fundamentos da disciplina do uso da Internet no Brasil.** § 1º São vedados os acordos de que trata o caput que importem na priorização discriminatória de pacotes de dados. § 2º Acordos entre provedores de conexão e provedores de aplicação estão sujeitos à avaliação do órgão competente, nos termos do Capítulo IV, deste Decreto.

II) Proteção de registros, dados e comunicações

Inicialmente, é importante destacar que o Brasil ainda não conta com uma legislação específica relativa à proteção da privacidade e dos dados pessoais, deficiência que necessita ser sanada com urgência. Quando vier a existir, essa lei terá o papel de orientar a interpretação das provisões

contidas no Marco Civil e no decreto de regulamentação.[2] Entretanto, no atual contexto de ausência dessa norma, aumenta a necessidade de uma melhor definição do significado e do alcance de alguns dos termos presentes no Marco Civil da Internet.

O decreto atualmente em discussão assume o desafio de reforçar as garantias de privacidade e proteção de dados contidas no Marco Civil, viabilizando a sua aplicabilidade, sem que isso invada a esfera de regulamentação de uma futura lei geral, cujas matérias vêm sendo amplamente discutidas, tanto em torno da minuta do anteprojeto de lei apresentado pelo Ministério da Justiça, como em outros projetos de lei que já tramitam no Congresso Nacional.

Na busca por esse ponto de equilíbrio, espera-se que o decreto delimite rigorosamente algumas previsões do Marco Civil que podem criar vulnerabilidades à vida privada. Como exemplos, pode-se apontar a possibilidade de que autoridades administrativas acessem dados cadastrais sem a necessidade de decisão judicial e a previsão de guarda obrigatória de registros de conexão.

Buscando contribuir com o debate e reforçando algumas das sugestões já feitas na primeira etapa de consulta pública, o CTS/FGV passa a comentar a redação do Capítulo III da minuta de decreto e fazer algumas proposições para a consideração do Ministério da Justiça.

1. Disposições gerais (art. 1º)

Antes de entrar no capítulo específico relativo à proteção aos registros, dados pessoais e às comunicações privadas, é importante apontar que a redação do art. 1º da minuta deixou de contemplar o acesso a dados por autoridades governamentais, assunto que, todavia, se encontra presente na minuta.

Dessa forma, sugere-se que a redação seja editada da seguinte forma:

Redação atual	Redação sugerida
Art. 1º Este Decreto trata das exceções à neutralidade de rede e indica procedimentos para a guarda de dados por provedores de	Art. 1º Este Decreto trata das exceções à neutralidade de rede e indica procedimentos para a guarda de dados por provedores de conexão e de

[2] Sobre a relação entre as normas que contêm regras relevantes para a proteção de dados pessoais, que deverá regulamentada por uma lei geral, a teoria do diálogo de fontes parece ser a melhor abordagem, uma vez que poderia assegurar ao titular de dados a regulamentação mais favorável. Desenvolvemos esse ponto em detalhes na Contribuição do CTS/FGV para a consulta sobre o Anteprojeto de Lei de Proteção de Dados Pessoais do Ministério da Justiça. Ver: http://direitorio.fgv.br/sites/direitorio.fgv.br/files/u100/contribuicao_cts-fgv_ao_debate_publico_do_marco_civil.pdf

conexão e de aplicações.	aplicações **e para se obter o acesso aos dados.**

2. Requisição de dados cadastrais (art. 9º)

O artigo 9º da minuta de decreto trata da previsão de acesso a dados cadastrais sem ordem judicial, constante no art. 10, §3º do Marco Civil.

Inicialmente, cabe ressaltar que a requisição de dados cadastrais sem ordem judicial, é uma hipótese excepcional e que a regra geral, presente no Marco Civil, é a de que a ordem judicial se faz necessária para se obter o acesso a dados. A minuta de decreto reforça a necessidade de que a autoridade administrativa requerente indique a fundamentação legal de sua competência, bem como a motivação que a leva a fazer tal requisição. Essa medida de transparência é positiva e permitirá maior controle em relação aos pedidos de acesso a dados que o Estado realiza.

Há, no entanto, aspectos em relação a esse ponto do Marco Civil que ainda carecem de maior definição, como indicamos na primeira fase das contribuições. São eles:

(i) a necessidade de deixar clara a impossibilidade de realização de pedidos em massa (de todos ou de muitos usuários ou contas ao mesmo tempo);

O texto do decreto deverá esclarecer que a motivação apresentada deve se referir a cada usuário atingido, a fim de afastar a interpretação de que seria possível estabelecer uma motivação genérica a atingir um grupo determinado ou indeterminado de pessoas.

(ii) a necessidade de esclarecimento de que a obrigatoriedade de fornecimento de dados cadastrais não impõe ou legitima por si só a coleta desses dados;

A fundamentação da coleta de dados não se confunde com a da obrigatoriedade de fornecimento a autoridades.

(iii) a necessidade do estabelecimento de critérios segundo os quais serão justificados os pedidos de acesso a dados cadastrais pelas autoridades.

É importante que o decreto esclareça os critérios que orientarão a justificativa do acesso a dados cadastrais nas hipóteses do art. 10 , § 3º do Marco Civil. Esse ponto será comentado em detalhes ao final do documento, ao tratar dos temas não enfrentados pela minuta. Isso porque os critérios orientadores sugeridos servirão não apenas para as situações aqui comentadas, relativas ao acesso a dados cadastrais sem ordem judicial, mas também para o acesso a registros mediante ordem judicial e à justificativa do pedido de guarda cautelar de dados por período superior ao estabelecido na lei.

(vi) a necessidade de **delimitar quais são as autoridades administrativas** que podem acessar dados cadastrais sem ordem judicial;

Apesar de diversas contribuições da sociedade civil e da academia terem realizados sugestões nesse sentido, a atual minuta de decreto não delimita quem são as autoridades competentes referidas no § 3º do artigo 10. Por esse motivo, o CTS/FGV reforça a sugestão feita na primeira etapa de contribuições, no sentido de que se 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.*

Pelo exposto, propõe-se a seguinte redação para o artigo 9º:

Redação atual	Redação proposta
Art. 9º As autoridades administrativas a que se refere o art. 10, § 3º, da Lei nº 12.965, de 2014, indicarão o fundamento legal de sua competência para o acesso e motivação para o pedido de acesso a dados cadastrais. **Parágrafo único.** São considerados dados cadastrais a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.	**Art. 9º** As autoridades administrativas a que se refere o art. 10, § 3º, da Lei nº 12.965, de 2014, indicarão o fundamento legal de sua competência para o acesso e **a motivação individualizada, relativa a cada usuário atingido para o pedido de acesso a dados cadastrais.** **§ 1º São considerados dados cadastrais a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.** **§ 2º O disposto no art. 10 § 3º, da Lei nº 12.965, de 2014, não cria qualquer obrigação de coleta e guarda dos dados elencados no § 1º.**

3. Acesso aos dados referidos no art. 10 do Marco Civil (art. 13)

O artigo 13 da minuta de decreto estabelece que os dados a que se refere o artigo 10 do Marco Civil (registros de conexão e de acesso a aplicações de internet, dados pessoais e conteúdo de comunicações privadas), deverão ser mantidos em formato que facilite o acesso decorrente de decisão judicial ou de determinação legal.

Dito isso, cabe esclarecer que o formato em que devem ser mantidos os dados não determina o formato em que esses dados podem ser fornecidos. Isso quer dizer que se a minuta de decreto tem o objetivo de facilitar o cumprimento do fornecimento de dados decorrente de decisão judicial ou previsão legal, bastaria prever que os dados devem ser fornecidos em formato de fácil acesso ou legível, quando demandado. Esse tipo de retificação é essencial para esclarecer que a previsão do artigo 13 da minuta não deverá enfraquecer a segurança dos dados. Isso porque tal redação poderá ser perigosa, afastando a adoção de ferramentas de criptografia, por exemplo. A esse respeito, recentemente cerca de 180 organizações, empresas e indivíduos de todo o mundo assinaram uma carta aberta para pedir aos líderes mundiais que não flexibilizem os padrões de criptografia por meio da legislação e outras políticas.[3]

Dessa forma, sugere-se as seguintes alterações no texto da minuta:

Redação atual	Redação proposta
Art. 13. Os dados de que trata o art. 10 da Lei 12.965, de 2014 deverão ser *mantidos* em formato que facilite o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 11 deste Decreto.	**Art. 13.** Os dados de que trata o art. 10 da Lei 12.965, de 2014 deverão ser **fornecidos** em formato que facilite o acesso decorrente de decisão judicial ou determinação legal, **segundo as recomendações do CGI** e respeitadas as diretrizes elencadas no art. 11 deste Decreto.

4. Relatórios de transparência (art. 10)

Considera-se positivo que a minuta de decreto tenha incorporado, em seu artigo 10, uma das sugestões feita pelo CTS/FGV, no sentido de viabilizar a prestação de contas e revisão relativa a requisição de dados cadastrais, estabelecendo a obrigatoriedade de que os órgãos públicos federais publiquem anualmente relatórios estatísticos de requisição de dados cadastrais.

[3] A carta, bem como todos os signatários, pode ser encontrada em <https://www.securetheinternet.org/#signers>

Destacamos na primeira fase de contribuição a importância de processos de revisão sistemáticos baseados em avaliações e estudos periódicos que provem a eficácia do acesso a dados cadastrais e o impacto dessa medida nos direitos humanos. A existência desse tipo de relatório dá condições para que a sociedade acompanhe e monitore de que forma seus dados podem estar sendo acessados pelos órgãos governamentais.

É preciso notar, no entanto, que **essa exigência não pode se limitar aos dados cadastrais, mas deve ser estendida aos registros de conexão e de acesso a aplicações.** Ocorre que o referido artigo encontra-se na seção I da minuta de Decreto, que versa sobre a "Requisição de Dados Cadastrais", dando a entender que a obrigação contida no artigo 10 aplica-se apenas às solicitações desse tipo de dado.

Diante disso, é preciso aprimorar a redação do artigo 10 da minuta, realocando-o para a parte geral do Capítulo III, para que ela de fato alcance a sua finalidade, apontando a necessidade de que os relatórios produzidos pelas autoridades contemplem **também os pedidos de acesso aos registros de conexão e aplicação.**

Além disso, consideramos importante incluir, além dos requisitos já presentes no decreto, os seguintes, como já sugerido pelo CTS/FGV na primeira fase de contribuição:

> *IV - O número de usuários afetados por tais solicitações;*
>
> *V - Informações sobre o solicitante dos dados (autoridades legais, investigadores privados, empresas, indivíduos, etc.);*
>
> *VI - Detalhes sobre os pedidos recebidos de autoridades legais, como, por exemplo, a fundamentação legal para a solicitação;*
>
> *VII - Informações sobre o tipo de dados solicitados (conteúdos de comunicação, registros de acesso, etc), e;*
>
> *VIII - A taxa de atendimento das solicitações divididas por categoria.*

Redação atual	Redação proposta
Art. 10. A autoridade máxima de cada órgão público federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais, contendo:	**Art. 10**. A autoridade máxima de cada órgão público federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição **a registros de conexão e de**

I – número de pedidos realizados; **II –** listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; e **III –** número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações.	**acesso a aplicações, bem como a dados cadastrais**, contendo: **I –** número de pedidos realizados; **II –** listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; e **III –** número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações. **IV - O número de usuários afetados por tais solicitações;** **V - Informações sobre o solicitante dos dados (autoridades legais, investigadores privados, empresas, indivíduos, etc.);** **VI - Detalhes sobre os pedidos recebidos de autoridades legais, como, por exemplo, a fundamentação legal para a solicitação;** **VII - Informações sobre o tipo de dados solicitados (conteúdos de comunicação, registros de acesso, etc), e;** **VIII - A taxa de atendimento das solicitações divididas por categoria.**

5. Padrões de Segurança (art. 11)

Como referido no art. 10, §4º, do Marco Civil, o regulamento estabelece em seu artigo 11 os padrões relativos às medidas e procedimentos de segurança e de sigilo. É importante, no entanto, que a redação legal deixe claro que a lista aqui enunciada é meramente exemplificativa, e não exaustiva, podendo ser ampliada para conferir maior segurança aos dados dos usuários, e que o Comitê Gestor da Internet, a que faz referência o parágrafo único, poderá recomendar padrões adicionais de segurança.

O estabelecimento do controle de acesso aos dados (art. 11, I) é um ponto muito positivo presente na redação da minuta. O Comitê Gestor da Internet, com a atribuição de "promover estudos e

recomendar procedimentos, normas e padrões técnicos e operacionais", prevista no parágrafo único desse artigo poderá, ainda, aprimorar essa regulamentação, estabelecendo parâmetros mais concretos de acordo com as especificidades e porte dos provedores de conexão e de aplicação.

O artigo 11 estabelece, ainda, que o CGI a editará recomendações de procedimentos, normas e padrões técnicos e operacionais no estabelecimento de diretrizes de padrões segurança. De fato, o órgão parece ser o mais adequado a desenvolver tal tarefa por ter a expertise necessária, bem como representatividade, tendo em vista a sua estrutura multissetorial. A fim de esclarecer que a atribuição do CGI deve ser relativa a todo o conteúdo do artigo, é importante que a expressão "no *caput*", referida no parágrafo único, seja substituída por "neste artigo".

É ainda louvável que a redação tenha endereçado a necessidade de que esses padrões atendam a igualdade comercial, a concorrência e a inovação, ao estabelecer que esses "devem ser adequados aos portes dos provedores". A previsão atende a expectativa de que o estabelecimento de padrões não sirva para aumentar a desigualdade entre grandes empresas e iniciativas ainda incipientes. Por fim, no inciso IV, a redação precisa ser aprimorada, a fim de destacar que além da integridade dos dados, devem ser garantidas a confidencialidade dos mesmos. No artigo II, algumas modificações sugeridas abaixo melhoram a terminologia empregada.

Dessa forma, são propostas as seguintes alterações ao artigo 11:

Redação atual	Redação proposta
Art. 11. Os provedores de conexão e de acesso a aplicações devem, na guarda, armazenamento e tratamento de dados, observar as seguintes diretrizes sobre padrões de segurança:	**Art. 11.** Os provedores de conexão e de acesso a aplicações devem, na guarda, armazenamento e tratamento de dados, observar as seguintes diretrizes sobre padrões de segurança:
I – estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;	**I –** estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
II – previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo	**II –** previsão de mecanismos de autenticação para o acesso aos registros, usando, por exemplo, sistemas de **autenticação de duplo fator** para assegurar a individualização do

tratamento dos registros; **III –** criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou responsável pelo acesso e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, §3º da Lei 12.965, de 2014; **IV –** uso de soluções de gestão dos registros por meio de tecnologias de criptografia ou medidas de proteção equivalentes para garantir a integridade dos dados; e **V –** separação lógica de outros sistemas de tratamento de dados para fins comerciais. **Parágrafo único.** Cabe ao CGI promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto no *caput*, de acordo com as especificidades e porte dos provedores de conexão e de aplicação.	responsável pelo tratamento dos registros; **III –** criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou responsável pelo acesso e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, §3º da Lei 12.965, de 2014; **IV –** uso de soluções de gestão dos registros por meio de tecnologias de criptografia **e outras medidas de proteção equivalentes para garantir a integridade, confidencialidade, disponibilidade e autenticidade dos dados; e** **V –** separação lógica de outros sistemas de tratamento de dados para fins comerciais. **Parágrafo único.** Cabe ao CGI promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto **neste artigo**, de acordo com as especificidades e porte dos provedores de conexão e de aplicação.

6. Conceitos de dados pessoais e tratamento de dados (art. 12)

Os conceitos de dado pessoal e tratamento de dados pessoais se mostram necessários para viabilizar a aplicabilidade do Marco Civil, visto que o Brasil ainda não conta com uma lei de proteção de dados pessoais que os defina. No entanto, sabe-se que é necessário que o Brasil avance com legislação específica sobre o tema, ocasião em que se poderá definir mais apropriadamente esses conceitos.

Nesse sentido, a fim de evitar a formação de um labirinto jurídico, é importante que a redação do decreto esclareça que os registros de conexão e acesso a aplicações bem como o conteúdo de comunicações privadas também constituem dados pessoais. Considera-se essa incorporação positiva e ela poderá atuar como uma referência ao longo da discussão do futuro projeto de lei decorrente da consulta do Ministério da Justiça.

Redação atual	Redação sugerida
Art. 12. Para os fins do disposto neste Decreto, considera-se: **I –** dado pessoal como dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos, compreendendo inclusive registros de conexão e acesso a aplicações e o conteúdo de comunicações privadas; e **II –** tratamento de dados pessoais é o conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, divulgação, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, **bloqueio ou fornecimento a terceiros de dados pessoais**, **por** comunicação, interconexão, transferência, difusão ou extração;	**Art. 12.** Para os fins do disposto ***na Lei 12.965 de 23 de abril de 2014*****,** considera-se: **I –** dado pessoal como dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos, compreendendo inclusive registros de conexão e acesso a aplicações e o conteúdo de comunicações privadas; e **II –** tratamento de dados pessoais é o conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, divulgação, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, **bloqueio ou fornecimento a terceiros de dados pessoais**, **por** comunicação, interconexão, transferência, difusão ou extração;

7. Matérias relativas à privacidade e proteção de dados pessoais ausentes na minuta do Decreto

Alguns pontos do Marco Civil pendentes de regulamentação ainda não foram abordados pela minuta. Por isso, se faz necessário que a versão definitiva do texto passe a contemplá-los.

A. Guarda obrigatória de registros de conexão e acesso a aplicações

Inicialmente, cabe ressaltar o entendimento do CTS/FGV no sentido de que a guarda obrigatória de registros prevista no Marco Civil da Internet é bastante problemática. Como referido na primeira fase de contribuições, o Comissário de Direitos do Humanos do Conselho da Europa (CDH - *Council of Europe's Commissioner for Human Rights*) declarou 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". Dito isso, espera-se que o decreto delimite rigorosamente o escopo dessa guarda, abordando os seguintes pontos:

(i) obrigatoriedade de exclusão dos dados submetidos à guarda obrigatória ao fim do período legal

Uma medida a ser observada na revisão da minuta proposta é o esclarecimento a respeito da necessidade de exclusão dos dados submetidos a guarda obrigatória nos termos do Marco Civil. O decreto deve estabelecer a obrigatoriedade de exclusão dos registros de conexão e acesso a aplicações assim que terminar o prazo de guarda obrigatória (de 1 ano e de 6 meses, respectivamente)[4]. Além disso, é importante que faça referência ao art. 12, ao art. 13, §6º e ao art. 16, §4º do Marco Civil, que preveem as penas no caso de descumprimento dos deveres de sigilo em relação a tais dados.

(ii) delimitação das situações de guarda cautelar de registros por período superior (§ 2º, do art. 13 e do art 15 do Marco Civil);

A esse respeito, é necessário que o decreto defina:

- quais autoridades administrativas têm competência para pedir guarda cautelar.
- estabelecer o **tempo limite para a guarda cautelar** de registros acima do prazo legal, após o qual os dados devem ser excluídos. Pelo texto da lei compreende-se que esse prazo não pode ser estendido por período superior a 60 dias, dentro do qual a autoridade deve obter uma ordem judicial que autorize o acesso a dados.

(iii) a obrigatoriedade de notificar o usuário a respeito de solicitações de acesso a seus dados;

Sempre que possível, o usuário deverá ser notificado a respeito das solicitações de acesso aos seus dados, a fim de que possa desafiá-las se entender pelo descabimento desse acesso, a não ser que esta medida inviabilize a finalidade do acesso, quando a notificação deverá ocorrer *a posteriori*.

Cabe trazer o exemplo da "Lei G10" alemã[5], que mesmo abordando situações de inteligência, prevê a notificação do cidadão que tem seu direito a privacidade restringido. Como o Marco Civil trata da mera observância legal, parece razoável que a regra seja a da notificação do usuário

[4] Como defendido por diversas organizações na primeira etapa de contribuições e referido no relatório elaborado pelo InternetLab# condensando todas elas: "O decreto deve criar regra estabelecendo que, passados os prazos previstos em lei, os registros de conexão e de acesso a aplicações devem ser apagados dos registros dos provedores de conexão e dos provedores de aplicações de Internet. Pode haver exceções justificadas para o caso dos registros de acesso a aplicações no caso da exclusão dos mesmos prejudique a prestação do serviço. A ideia é tornar a guarda obrigatória menos lesiva à privacidade do usuário, proibindo a guarda indiscriminada de registros dos usuários".

[5] O § 13 da referida lei estabelece que após três meses do final das medidas restritivas à confidencialidade das comunicações privadas, o titular dos dados deve ser comunicado a seu respeito.

sempre que seus dados forem solicitados. Essa medida pode funcionar, ainda, como um importante contrapeso a eventuais excessos das autoridades.

A legislação brasileira corrobora essa necessidade ao prever no art. 43 do Código de Defesa do Consumidor que o consumidor deve ser comunicado por escrito no caso de "abertura de cadastro ficha, registro e dados pessoais e de consumo quando não solicitada por ele" (art. 43).

B. . Critérios a serem atendidos nas situações de requisição de guarda obrigatória e de acesso a dados com ou sem ordem judicial

Como apontado na contribuição do CTS/FGV na primeira etapa do debate público,

> (...) 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.

Para que isso aconteça, o Decreto deve limitar as hipóteses de requisição de período superior para guarda obrigatória (art. 13, §2º e art. 15, §2º do Marco Civil) e de acesso aos dados retidos, oferecendo garantias mínimas para os cidadãos. Seja nas situações ordinárias, em que exige-se ordem judicial para acesso aos dados, ou na situação específica em que autoridades podem acessar dados cadastrais (art. 10, §3º do Marco Civil), reforça-se aqui a sugestão apontada na primeira contribuição no sentido de que o Decreto estabeleça os seguintes fatores para orientar a legitimidade do pedido de acesso ou de guarda cautelar por tempo superior[6]:

a) Existe uma alta probabilidade de que um crime grave (ou uma ameaça específica a uma atividade legitima) foi ou será cometido, e;
b) 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;
c) Outras técnicas menos invasivas foram esgotadas ou seriam inúteis, de forma que as técnicas utilizadas sejam a opção menos invasiva, e;
d) As informações acessadas serão limitadas ao que é relevante e essencial ao crime grave ou ameaça específica ao fim legítimo alegado; e

[6] Esses são os critérios reconhecidos por 400 organizações internacionais e mais de 300 mil indivíduos, propostos no documento de Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações. <https://pt.necessaryandproportionate.org/text>.

e) Quaisquer informações coletadas a mais não serão mantidas, mas prontamente destruídas ou devolvidas; e
f) As informações serão acessadas somente pela autoridade especificada e usadas apenas para a finalidade e duração para as quais foi concedida a autorização; e
g) As atividades de vigilância solicitadas e técnicas propostas não comprometem a essência do direito à privacidade ou as liberdades fundamentais.

Além dos critérios a serem adotados, O artigo 14 da minuta estabelece que as informações sobre padrões de segurança devem ser acessíveis a qualquer interessado. No entanto, o termo "preferencialmente" acaba flexibilizando a obrigação, o que permitiria que essas informações fossem fornecidas unicamente por outros meios, como através de requerimento formal na sede do provedor de conexão ou acesso a aplicações, o que se tornaria um entrave ao acesso facilitado a essas informações. Dessa forma, sugere-se a seguinte modificação na redação da minuta:

Redação atual	Redação sugerida
Art. 14. As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet.	**Art. 14.** As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, **por meio de seus sítios na internet.**

Referências

Akamai (8 December, 2015) Q3 2015 State of the Internet – Security Report. https://www.stateoftheinternet.com/resources-cloud-security-2015-q3-web-security-report.html

Bastian C. *et al.* Comcast's Protocol-Agnostic Congestion Management System. Request for Comments: 6057 https://tools.ietf.org/html/rfc6057

Belli Luca (16 de julho 2015) Regulamentação da Neutralidade da Rede. Apresentação ao V Fórum da Internet.

Belli Luca & Matthijs van Bergen. (December 2013). Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet. Council of Europe, CDMSI(2013)misc 19E.

Belli Luca & Primavera De Filippi (Eds.). (November 2015). Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. Springer.

BEREC. (2012a). Guidelines for QoS in the scope of net neutrality, see: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/1101-berec-guidelines-for-quality- -of-service-_0.pdf

Clark, David D. and Blumenthal, Marjory S. (2011) "The End-to-End Argument and Application Design: The Role of Trust," Federal Communications Law Journal: Vol. 63: Iss. 2, Article 3. http://www.repository.law.indiana.edu/fclj/vol63/iss2/3

Digital Fuel Monitor. (6 February 2015). In the Netherlands KPN just doubled the mobile internet volume caps to encourage consumers a carefree usage of TV. http://dfmonitor.eu/downloads/Banning_zerorating_leads_to_higher_volume_caps_06022015.pdf

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

Federal Communications Commission's Open Internet Advisory Committee. (2013). *2013 Annual Report*. pp. 66 - 71. http://transition.fcc.gov/cgb/oiac/oiac---2013---annualreport.pdf

OECD (2014), "The Development of Fixed Broadband Networks", OECD Digital Economy Papers, No. 239, OECD Publishing. http://dx.doi.org/10.1787/5jz2m5mlb1q2-en

Pallis, G. and Vakali, A. (2006) Insight and Perspectives for Content Delivery Networks, Communications of the ACM 49.1

SUBTEL (15 dezembro 2010) Reglamento que regula las carateristicas y condiciones de la neutralidad de la red en el servicio de acesso a internet. Decreto n°368. http://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/10d_0368.pdf

TRAI (8 February 2016). Prohibition of Discriminatory Tariffs for Data Services Regulations. (2 of 2016). http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf