O QUE ESTÁ EM JOGO NA REGULAMENTAÇÃO DO **MARCO CIVIL DA INTERNET?**

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA PARA A REGULAMENTAÇÃO DA LEI 12.965/2014

Autores

Francisco Carvalho de Brito Cruz
Jonas Coelho Marchezan
Maike Wile dos Santos

Contribuíram

Dennys Marcelo Antonialli
Jacqueline de Souza Abreu
Mariana Giorgetti Valente
Pedro Henrique S. Ramos

INTERNET LAB pesquisa em direito e tecnologia

Também disponível em **www.internetlab.org.br**

O QUE ESTÁ EM JOGO NA REGULAMENTAÇÃO DO

MARCO CIVIL DA INTERNET?

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA PARA A REGULAMENTAÇÃO DA LEI 12.965/2014

***

EQUIPE INSTITUCIONAL **Diretor Presidente** Dennys Antonialli **Diretor Vice-Presidente** Francisco Brito Cruz **Coordenadora de Pesquisa** Mariana Giorgetti Valente / EQUIPE DO PROJETO **Líder de projeto** Francisco Brito Cruz **Estagiário de pesquisa** Jonas Coelho Marchezan **Estagiário de pesquisa** Maike Wile dos Santos

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2015.

INTERNETLAB / Rua Augusta, 2690, Galeria Ouro Fino, Loja 326 / www.internetlab.org.br

O QUE ESTÁ EM JOGO NA REGULAMENTAÇÃO DO

MARCO CIVIL DA INTERNET?

RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA PARA A REGULAMENTAÇÃO DA LEI 12.965/2014

/sumário

EQUIPE ENVOLVIDA NESTE PROJETO

AUTORES

FRANCISCO CARVALHO DE BRITO CRUZ / Mestre em Filosofia e Teoria Geral do Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo (FDUSP) e, durante o curso, bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica. Foi pesquisador visitante (2013) no *Center for Study of Law and Society* da Universidade da Califórnia – Berkeley, por meio de programa de intercâmbio da Rede de Pesquisa Empírica em Direito (REED). Foi ganhador do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). É advogado com atuação nas áreas de direito digital, propriedade intelectual, imprensa e direito do consumidor. Foi fundador e coordenador do Núcleo de Direito, Internet e Sociedade (NDIS FDUSP) entre 2012 e 2014. Atualmente é diretor do InternetLab.

JONAS COELHO MARCHEZAN / Graduando em Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Voluntário na Equipe Societária do Departamento Jurídico da ONG "*Un Techo para Mi Pais* – Teto Brasil".

MAIKE WILE DOS SANTOS / Graduando em Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Fez parte da Escola de Formação na Sociedade Brasileira de Direito Público – SBDP (2014). Foi monitor-bolsista do Programa de Estímulo ao Ensino de Graduação – PEEG da disciplina Instituições de Direito para Economistas, na FEA (2013), e pesquisador-bolsista do Programa Ensinar com Pesquisa no Núcleo de Direito, Internet e Sociedade – NDIS (2014), ambos vinculados à USP. Atualmente é membro do Centro de Análise e Pesquisa em Educação Jurídica – CAPEJur, vinculado ao Departamento de Filosofia e Teoria Geral do Direito da FDUSP, e estagiário de pesquisa no InternetLab.

CONTRIBUÍRAM

DENNYS MARCELO ANTONIALLI / Doutorando em direito constitucional pela Universidade de São Paulo, com graduação em direito pela mesma universidade (2008), mestrado em direito pela Universidade de Stanford (JSM, 2011) e mestrado profissional em "*Law and Business*", conjuntamente oferecido pela *Bucerius Law School* e pela WHU *Otto Beisheim School of Management* (MLB, 2010). Atuou junto à equipe de políticas públicas em tecnologia e direitos civis na *American Civil Liberties Union of Northern California* (ACLU/NC) e como consultor jurídico do "*Timor Leste Legal Education Project*", da *Stanford Law School/Asia Foundation*. Foi ganhador do 1º lugar do *Steven M. Block Civil Liberties Award* da *Stanford Law School* (2011) e do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). Foi pesquisador do *Alexander von Humboldt Institute for Internet and Society (*Berlim) e participou do *Summer Doctoral Program* do *Oxford Internet Institute*. Advogado, atualmente é coordenador do Núcleo de Direito, Internet e Sociedade da FDUSP (NDIS) e diretor do InternetLab.

JACQUELINE DE SOUZA ABREU / Mestranda em Direito na *Ludwig-Maximilians-Universität* em Munique (LMU). Graduada em Direito pela Faculdade de Direito da Universidade de São Paulo (2014). Durante a graduação, foi bolsista de iniciação científica da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Programa de Estímulo ao Ensino de Graduação (PEEG) nas áreas de Filosofia e Teoria Geral do Direito e membro do Núcleo de Direito, Internet e Sociedade da USP. Realizou intercâmbio acadêmico de graduação também na LMU, período em que foi bolsista do Serviço Alemão de Intercâmbio Acadêmico (DAAD). Foi também pesquisadora-júnior na FGV DIREITO SP.

MARIANA GIORGETTI VALENTE / Doutoranda e mestre em Sociologia Jurídica pela USP. Pesquisadora do projeto Acervos Digitais, no Centro de Tecnologia e Sociedade da FGV, onde também co-coordenou o projeto *Open Business Models*, sobre direitos autorais e música na era digital (2012-2014). Pela FGV, foi também uma das coordenadoras legais do projeto Creative Commons Brasil. É membro do Núcleo Direito e Democracia do Centro Brasileiro de Análise e Planejamento (Cebrap), no qual foi coautora de pesquisas do programa Pensando o Direito (SAL/MJ). Graduou-se em Direito pela Universidade de São Paulo em 2009 e possui especialização em propriedade intelectual pela Organização Mundial de Propriedade Intelectual (*Summer School*, 2011). Foi coordenadora jurídica do Museu de Arte Moderna de São Paulo e coordena o grupo Direitos Autorais do GT Arquivos de Museus e Pesquisa (Capes). É coordenadora do Núcleo de Direito, Internet e Sociedade da FDUSP (NDIS). No InternetLab, é Coordenadora de Pesquisa e líder do projeto Gênero e Tecnologia.

PEDRO HENRIQUE S. RAMOS / Mestre em Direito e Desenvolvimento pela Escola de Direito da Fundação Getúlio Vargas. Foi pesquisador visitante do *Center of Internet and Society* da *Stanford Law School*, na área de *Architecture & Public Policy*, onde desenvolveu pesquisas sobre a neutralidade da rede no Brasil e o impacto de iniciativas de zero-rating em países em desenvolvimento. Graduado pela Universidade de São Paulo e com pós-graduação pelo Instituto Internacional de Ciências Sociais e pela *University of Southern California*, foi também apresentador, em 2014, de um painel sobre zero-rating na TPRC, principal conferência de telecomunicações dos EUA. É advogado com atuação nas áreas de direito digital, transações de tecnologia e propriedade intelectual, e pesquisador associado do InternetLab.

1. INTRODUÇÃO

1.1. A ideia de um debate público para a regulamentação do Marco Civil da Internet

A consulta pública sobre a regulamentação da lei federal n. 12.965/14 (que ficou conhecida internacionalmente como o **Marco Civil da Internet**) foi criada dentro do projeto *Pensando o Direito*, desenvolvido pela Secretaria de Assuntos Legislativos do Ministério da Justiça. Esse projeto, criado em 2007, tem como escopo promover a maior participação da sociedade na elaboração de leis e regulamentos no Brasil e, assim, criar normas mais efetivas e conectadas com a realidade atual e as demandas dos cidadãos.

A participação na plataforma de debate público, iniciada no dia 28 de janeiro de 2015, dividiu-se em quatro eixos temáticos que, por sua vez, referiam-se a pontos de grande relevância na discussão da lei: "**neutralidade de rede**", "**privacidade na rede**" (restrições a coleta de dados pessoais dos cidadãos e cidadãs e maneiras de fiscalizar tais restrições), "**registros de acesso**" (definições sobre como rastros dos usuários de Internet podem ser guardados e entregues a autoridades de investigação ou a terceiros) e "**outros temas e considerações**" (como a postura do Estado no desenvolvimento de políticas de Internet ou inovação tecnológica). O usuário pôde, dentro de cada um desses eixos, criar tópicos contendo sugestões e propostas de debate de forma livre.

Com o fim do debate online no dia 30 de abril, o Ministério da Justiça abriu um novo prazo, dessa vez para a **sistematização dos resultados** obtidos na consulta. Os participantes foram convidados a propor soluções de sistematização das contribuições e até mesmo enviar minutas do decreto que serão usadas como subsídios para a construção do texto oficial.

1.2. A postura do InternetLab: informação e pluralidade acadêmica

Sabendo do papel que a academia deve exercer no debate de políticas públicas, o InternetLab desenvolveu, no período de consulta, o projeto **InternetLab Reporta: Consultas Públicas**.

Enquanto a consulta esteve aberta, reportamos, todas as sextas-feiras, um boletim semanal com as principais contribuições ou discussões que ocorrerem na plataforma. Buscamos destrinchar temas complexos que surgiram durante esses processos, inclusive por meio de entrevistas com pesquisadores especialistas. **O objetivo foi dar visibilidade a esse momento importantíssimo para a definição do futuro da Internet brasileira**, fomentando a participação e possibilitando a entrada de outros interessados na discussão por meio da divulgação de informação concisa, organizada e de qualidade sobre as pautas e principais debates na plataforma.

Este documento representa o resultado final de nossa análise e acompanhamento da plataforma, sistematizando as contribuições e produzindo um panorama com os principais argumentos.

2. DADOS GERAIS SOBRE O DEBATE PÚBLICO: NÚMEROS E PERFIL DA PARTICIPAÇÃO

A plataforma teve um total de **1843** usuários cadastrados e **1200** comentários, divididos em **339** pautas criadas pelos usuários. O eixo mais abordado foi o "*Outros Temas e Considerações*" com 124 pautas, seguido por *Neutralidade de rede*, com 98 pautas; *Guarda de Registros*, com 70 pautas; e *Privacidade na Rede*, com 68 pautas.

Boa parte dos participantes preferiram contribuir nos dias imediatamente anteriores ao prazo final para participar. Houve, inclusive, um grande número de contribuições (o número total de contribuições dobrou) nos últimos dias de março devido ao fato que, inicialmente, o fim do debate online estava previsto para o dia 31 de março. Com a prorrogação do prazo final para o dia 30 de abril, vimos novamente um pico de contribuições de última hora: o número de comentários saltou de 780 para 1131. Veja no **anexo** gráficos produzidos pelo InternetLab com alguns números.

3. METODOLOGIA: COMO ORGANIZAR CENTENAS DE OPINIÕES E ARGUMENTOS?

Analisamos todas as contribuições à consulta pública sobre a regulação do Marco Civil da Internet, e que foram enviadas ao Ministério da Justiça por meio da plataforma "Pensando o Direito" durante todo o período de consulta, ocorrido entre os dias 28 da janeiro de 2015 e 30 de abril do mesmo ano.

A plataforma de consulta organizou as contribuições em quatro eixos temáticos: **(i)** neutralidade da rede, **(ii)** privacidade, **(iii)** guarda de registros e **(iv)** outros temas e considerações. A construção de pautas foi livre, o que significa dizer que os cidadãos tinham liberdade de escolher entre os eixos e propor quaisquer debates e sugestões que lhe parecessem convenientes.

3.1. Como foi feita a análise?

Da totalidade das contribuições, foram selecionadas para análise **apenas aquelas que diziam respeito a algum assunto abordado pela lei federal n. 12.965/14** (Marco Civil da Internet), **e que não apresentavam o intuito de requisitar a mudança de qualquer parte da lei**. Ou seja, **foram excluídas da nossa abordagem as contribuições que não diziam respeito estritamente a nenhum assunto endereçado pela lei ou que buscavam reformar da lei por meio do decreto**.

A partir desse recorte, buscamos identificar, em cada uma das contribuições, as teses e argumentos defendidos, assim como relacioná-los com os agentes que atuaram na plataforma. Desse trabalho de triagem inicial, foi possível elaborar duas categorias organizadoras das contribuições:

- **Questões Controversas**: essa categoria diz respeito àquelas contribuições que fizeram parte de debates e chocaram-se com posições conflitantes. É importante ressaltar que, na maioria das vezes, a contraposição não se deu dentro da mesma pauta de discussão, mas sim em pautas diversas.
- **Propostas Avulsas**: essa categoria diz respeito àquelas contribuições que não encontraram contraposição na plataforma. Cabe a observação de que nem todas as propostas esparsas analisadas integram este relatório, e que algumas foram resumidas para melhor compor o resultado.

3.2. Comentários da equipe do InternetLab

Este relatório também conta com comentários feitos pela equipe do InternetLab para aprofundamento contextual de discussões travadas na plataforma.

3.3. O que esperar do presente relatório?

O relatório busca realizar **uma descrição do processo de consulta**, **mapeando os pontos em debate**, os **principais argumentos levantados** e os **agentes engajados**, para que, a partir deste

trabalho analítico, **sejam apresentadas as propostas que podem ser compreendidas como mais relevantes**. Destarte, espera-se oferecer subsídios à construção do decreto de regulamentação do Marco Civil da Internet e informações sobre o resultado da consulta pública a interessados em geral.

3.4. Licença de uso de conteúdo

A integralidade do conteúdo publicado na plataforma do Ministério da Justiça está sujeito à licença *Creative Commons* – Atribuição 4.0 Internacional (CC BY 4.0), como determinado nos Termos de Uso da plataforma. Este relatório em si está licenciado sob uma licença *Creative Commons* CC BY 3.0 BR. Essa licença permite que outros remixem, adaptem e criem obras derivadas sobre a obra original, inclusive para fins comerciais, contanto que atribuam crédito ao autor corretamente.

4. MAPA DE ARGUMENTOS DA REGULAMENTAÇÃO DO MARCO CIVIL

4.1. Neutralidade da rede

4.1.1. De que forma o decreto de regulamentação do Marco Civil deve tratar planos de Internet móvel com ofertas de acesso grátis a aplicativos (conhecidas como *zero-rating*)?

A expressão *zero-rating* refere-se a uma estratégia comercial em que operadoras oferecem gratuidade no tráfego de dados para determinada aplicação ou serviço específico. Um exemplo: após o cliente esgotar sua franquia de dados, a operadora permite que ele continue usando uma aplicação ou serviço específicos, sem custos.

Esse tipo de estratégia comercial é bastante popular há vários anos em países em desenvolvimento, e desde 2014 tem sido popularizado também na Europa e nos EUA. No Brasil, estratégias de *zero-rating* são utilizadas por operadoras desde pelo menos 2009, tendo se popularizado nos últimos anos graças a promoções comerciais que passaram a oferecer gratuidade no tráfego de aplicativos populares como *Facebook*, *Twitter*, *Waze* e *WhatsApp*.

Nosso levantamento identificou que esse foi o tema mais debatido na plataforma. Embora as contribuições tenham apresentado peculiaridades, é possível reduzi-las a três posições paradigmáticas:

Respostas controversas coletadas na plataforma de debate:
(A) A avaliação sobre a legalidade ou não de estratégias *zero-rating* deve ser feita de forma incidental e *ex post*. Essa prática não deve ser proibida pelo decreto de regulamentação do Marco Civil.
(B) *Zero-rating* representa uma exceção à regra da neutralidade de rede, portanto, não deve ser vedado pelo decreto de regulamentação do Marco Civil.
(C) *Zero-rating* representa uma violação da neutralidade de rede e deve ser proibido por meio do decreto.

Resumo das respostas e seus defensores:

(A) *A avaliação sobre a legalidade ou não de estratégias zero-rating deve ser feita de forma incidental e ex post. Essa prática não deve ser proibida pelo decreto de regulamentação do Marco Civil.*

Essa tese baseia-se no argumento de que a obrigação de não discriminação de dados prevista no artigo 9º do Marco Civil da Internet abrange tão somente as atividades relacionadas com o tráfego de pacotes de dados (camada lógica da rede) e, logo, não alcançam discriminações entre pacotes de dados que possam ocorrer em nível comercial (camada de conteúdo da rede), desde que respeitadas as demais regras previstas na legislação (e.g. direitos do consumidor, vedação a práticas anticoncorrenciais).

Além disso, os defensores dessa tese argumentam que não se pode dar como certo que planos de *zero rating* terão efeito negativo na concorrência. Ao contrário, pode-se até argumentar que a diferenciação dos planos para melhor beneficiar o consumidor é positiva para a concorrência **(Tim Brasil).** Do ponto de vista consumerista, os argumentos dessa tese defendem que planos de *zero rating* proporcionam ampliação do acesso à internet, principalmente entre as classes sociais menos favorecidas – a prática permitiria às populações mais carentes o acesso a serviços relacionados a educação, saúde, comunicação e informação. Por fim, ressaltam que, no caso de planos de Internet móvel, é determinante para a proteção dos consumidores e dos princípios do Marco Civil da Internet a garantia da transparência em relação às informações dos planos e a capacidade de determinar se os planos estão sendo cumpridos. **(CISCO Brasil)**

Quem defendeu isso? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, Tim Brasil, Cisco Brasil, Brasscom.*

***(B)** Zero-rating representa uma exceção à regra da neutralidade de rede, portanto, não deve ser vedado pelo decreto de regulamentação do Marco Civil.*

Argumenta-se que, como reconhecido pela *Federal Communications Commission* (FCC) dos Estados Unidos, ainda que o *zero-rating* viole a neutralidade de rede, ele deve ser tratado como uma exceção justificável em razão de seus efeitos econômicos benéficos aos usuários de internet. Ademais, o Marco Civil da Internet tem como um dos seus princípios a livre concorrência – é de se esperar, portanto, que a lei beneficie o mercado e o consumidor.

Quem defendeu isso? *Claro S/A.*

***(C)** Zero-rating representa uma violação da neutralidade de rede e deve ser proibido por meio do decreto.*

Defensores dessa tese interpretam o artigo 9º do Marco Civil de forma diversa: para eles, o Marco Civil prescreve a provedores de acesso o dever de tratar pacotes de dados de forma isonômica em qualquer modalidade, seja no nível lógico, no de infraestrutura ou no de ofertas comerciais. Logo, práticas de *zero-rating* violariam a obrigação imposta pelo Marco Civil.

Na esfera socioeconômica, argumenta-se que a existência de planos de *zero-rating* causa prejuízo à concorrência na medida em que cria uma barreira de entrada no mercado de provedores de aplicações. Ressaltam-se também os malefícios para os usuários dos planos de *zero-rating*: ao limitar o número de plataformas pelas quais os usuários poderão se comunicar e trocar informações, planos de *zero-rating* acabam por facilitar a vigilância e a censura, e contribuem para replicar no ambiente online o que ocorre no offline, criando uma divisão entre o pleno acesso à Internet para quem pode pagar e o acesso limitado a algumas aplicações para as populações mais carentes.

Quem defendeu isso? *COGPC/SEAE/MF, AccessNow, artur, Sergio Deliconi, ABSTARTUPS, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação*

Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, ABRINT e CTS-FGV.

4.1.2. Quem deverá fiscalizar a regra da neutralidade da rede?

Outro tema bastante discutido na plataforma diz respeito à aplicação e fiscalização das regras sobre neutralidade da rede. Uma das funções típicas de um decreto regulamentador é acomodar o aparelho administrativo do Poder Executivo para garantir que determinada lei seja cumprida, estabelecendo procedimentos para sua aplicação e também regras para a apuração de infrações. Três posições foram identificadas:

Respostas controversas coletadas na plataforma de debate:
(A) A Anatel deverá ser responsável pela fiscalização da neutralidade de rede
(B) A Anatel deverá ser responsável pela fiscalização com necessária oitiva do CGI.br
(C) Modelo de monitoramento e fiscalização pluri-institucional: ANATEL, CADE, SENACOM, CGI

Resumo das respostas e seus defensores:

(A) *A Anatel deverá ser responsável pela fiscalização da neutralidade de rede*

Esse argumento defende que a Internet é serviço de valor adicionado, segundo a Lei Geral de Telecomunicações (LGT). Assim, segundo o artigo 61 da LGT, a ANATEL possui autoridade legal para fiscalizar a interação entre serviços de valor adicionado e serviços de telecomunicação. Portanto, a ANATEL deve ser responsável pela supervisão da neutralidade.

Quem defendeu isso? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, CLARO S/A, ABDTIC, Netflix Brasil, Cisco Brasil.*

(B) *Anatel deverá ser responsável pela fiscalização com necessária oitiva do CGI.br*

O argumento admite que a competência da Anatel para fiscalização da neutralidade de rede já tem base legal no Brasil (artigo 19 da LGT), e que a agência reguladora possui mecanismos institucionais já estabelecidos capazes de facilitar a fiscalização e execução da lei. Todavia, o pesquisador **Pedro Ramos** propôs que, como forma de reduzir a seleção adversa, o risco moral na apuração das violações da neutralidade da rede e conferir maior legitimidade institucional, o decreto poderia incluir a necessidade

de oitiva do CGI.br nos procedimentos de apuração de descumprimento de obrigações ou de averiguação de denúncias relativas à violação das disposições do artigo 9º do Marco Civil.
Quem defendeu isso? *Pedro Ramos (pesquisador do InternetLab).*

(C) *Modelo de monitoramento e fiscalização pluri-institucional: ANATEL, CADE, SENACOM, CGI.*

Diversas entidades da sociedade civil defenderam um modelo pluri-institucional para apuração de violações à neutralidade da rede. Para esses defensores, essa tarefa só poderá ser realizada se for resultado do trabalho articulado de mais de um órgão ou entidade. Esses corpos técnicos seriam formados pelas seguintes entidades: Anatel, o Conselho Administrativo de Defesa Econômica (CADE), Secretaria Nacional do Consumidor (Senacom) e o Comitê Gestor da Internet no Brasil/ Núcleo de Informação e Coordenação do Ponto BR (CGI.br/NIC.br).
Quem defendeu isso? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, CTS-FGV, Cristiana Gonzalez.*

4.1.3. Como o decreto deverá abordar as exceções à regra de neutralidade da rede prevista no Marco Civil?

Esse tema refere-se diretamente aos requisitos técnicos indispensáveis à prestação de serviços de provisão de acesso à Internet, e que muitas vezes podem envolver práticas que irão, direta ou indiretamente, gerar algum tipo de discriminação entre diferentes pacotes de dados. Algumas das propostas enviadas à plataforma buscaram endereçar como essas exceções à neutralidade da rede devem ser tratadas.

Respostas controversas coletadas na plataforma de debate:
(A) O decreto deve prever todas as hipóteses em que práticas de gerenciamento de redes serão permitidas em um rol taxativo.
(B) O decreto deve prever princípios que ajudem a diferenciar as boas práticas de gerenciamento das práticas abusivas.
(C) Não deve haver um rol taxativo de hipóteses em que o gerenciamento será permitido no decreto. Porém, a liberdade das prestadoras para utilizar técnicas de gerenciamento deve ser reduzida.

(D) O Decreto deve estabelecer expressamente o caráter agnóstico da rede.

Resumo das respostas e seus defensores:

(A) *O decreto deve prever todas as hipóteses em que práticas de gerenciamento de redes serão permitidas em um rol taxativo.*

Argumenta-se que somente por meio da construção de um rol taxativo de hipóteses de permissão de gerenciamento de rede é que será preservado o caráter essencialmente técnico dessas hipóteses, tal como previsto no Marco Civil da Internet. O estabelecimento de um rol taxativo também contribuiria para o controle de eventuais abusos e arbitrariedades por parte dos prestadores de serviço.

Quem defende isso? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, ANER, IASP, ABRANET e ANJ.*

(B) *O decreto deve prever princípios que ajudem a diferenciar as boas práticas de gerenciamento das práticas abusivas.*

Segundo os defensores dessa tese, um rol exaustivo de hipóteses em que o gerenciamento de rede será permitido correria o risco de se tornar obsoleto rapidamente, impedindo que novas formas de gerenciamento sejam implementadas para melhor uso das redes e satisfação do usuário. Além disso, tal engessamento das hipóteses em decreto acabaria por desestimular a inovação.

Tendo isso em mente, seria preciso que o decreto, com uma abordagem principiológica ou pelo uso de exemplos, se concentrasse em tentar definir a distinção entre o gerenciamento de rede razoável e aquilo que representa uma quebra da neutralidade de rede. Dessa forma, as próprias prestadoras de serviço poderiam determinar quais são as melhores práticas a serem utilizadas na gestão técnica das redes em cada situação.

Em contrapartida, o decreto deveria estabelecer mecanismos de proteção rígidos e claros que assegurem uma Internet e uma autoridade regulatória competente para fiscalizar o cumprimento das proteções existentes (argumento levantado pela Cisco Brasil). Os casos de abuso de gerenciamento de rede deveriam ser punidos.

Quem defende isso? *TIM Brasil, Telcomp, FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, ILCO (Instituto Liberal do Centro Oeste), Cisco Brasil, Sky Brasil.*

(C) *Não deve haver um rol taxativo de hipóteses em que o gerenciamento será permitido no decreto. Porém, a liberdade das prestadoras para utilizar técnicas de gerenciamento deve ser reduzida.*

Alguns limites do gerenciamento de tráfego já são especificados pelo próprio Marco Civil da Internet: "(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*".

O papel da regulação deve ser proporcionar um melhor detalhamento desses limites impostos em lei de forma a orientar, de forma clara, o que deve ser considerada uma gestão razoável das redes. Deve-se evitar, ao mesmo tempo, restrições efetivas que podem ocasionar o desencorajamento do uso de técnicas de gestão de rede que, afinal, fazem parte do dia-a-dia das prestadoras de serviço.

Ademais, o gerenciamento de redes deveria ser usado em função de preocupações estritamente técnicas, não sendo permitido usá-lo por razões comerciais.

Quem defende isso? *ABDTIC e CTS-FGV (embora o CTS sugira uma restrição maior).*

(D) *O Decreto deve estabelecer expressamente o caráter agnóstico da rede.*

O pesquisador Ademir Antonio Pereira Júnior propôs que a rede deve ser agnóstica de forma a impedir qualquer forma dediscriminação entre aplicações e classes de aplicações, impedindo que o detentor da rede possa influenciar quais aplicações passarão por suas redes. Para o pesquisador, provedores de acesso devem adotar técnicas de gerenciamento de tráfego agnósticas, isto é, não baseadas na diferenciação entre aplicações ou classes de aplicações, sugerindo que o decreto "*proíba qualquer forma de discriminação de aplicações ou classes de aplicações, especificando que são expressamente vedadas (i) a contratação de tratamento prioritário a determinada aplicação ou classe de aplicações ou de degradação de tráfego alheio (mediante contraprestação onerosa ou não), e (ii) o favorecimento de aplicações de empresas do mesmo grupo econômico do detentor da rede*". Para o pesquisador, medidas não agnósticas podem ser admitidas, desde que pontuais e desenhadas para lidar unicamente com problemas de segurança e congestão, observados os limites já estabelecidos pelo Marco Civil.

Quem defende isso? Ademir Antonio Pereira Junior.

4.1.4. O decreto deve autorizar o monitoramento do cabeçalho dos pacotes de dados que trafegam na rede?

Comentário INTERNETLAB – Autor: Pedro Ramos (pesquisador associado)

Os protocolos técnicos que baseavam as primeiras redes de comutação por pacotes estabeleciam poucas garantias técnicas de que os pacotes de dados que trafegam por meio de sua infraestrutura atingiriam o destino no tempo e com a qualidade desejada, já que congestões de rede podiam gerar efeitos de latência e perda de pacotes, por exemplo. Esse padrão ficou conhecido como *best efforts delivery*: a entrega de pacotes de dados segue a regra de "melhores esforços", e, em casos de congestão na rede, os pacotes são colocados em espera obedecendo ao critério de *first come, first served* (isto é, os pacotes que forem enviados primeiro à rede serão entregues primeiro).

Todavia, o *best efforts* nunca foi um paradigma absoluto para a internet: o próprio protocolo TCP/IP, em sua estrutura básica, prevê que os pacotes de dados transmitidos por meio da rede são individualmente empacotados e identificados por meio de um cabeçalho de informações (*IP header*), contendo os dados necessários para que provedores de acesso possam identificar de onde veio o pacote, para onde este deve ser entregue e como tratá-lo em suas redes.

Entre as informações contidas nesse cabeçalho, é importante destacar o campo *traffic class*, que cumpre duas funções básicas: (i) sinalizar a existência de uma congestão na rede, a partir de uma função conhecida *como Explicit Congestion Notification* (ECN), permitindo a operadores de rede identificar rapidamente a existência de uma congestão e reorganizar os pacotes de dados de forma a reduzir a latência e *jitter*; e (ii) permitir a utilização da função *Differentiate Services* (DiffServ), que permite classificar o tipo de dado contido em determinado pacote, endereçando maior ou menor prioridade de tráfego para pacotes que estejam carregando dados mais sensíveis à latência. Ambas as funções foram discutidas e incorporadas aos padrões técnicos utilizados pela internet após anos de discussão e consolidação desses padrões perante o *Internet Engineering Task Force*, principal fórum internacional de debate e uniformização dos protocolos técnicos que integram a rede.

Esse modelo estrutural do protocolo TCP/IP, com diversos hardware e software de gerenciamento de tráfego atualmente utilizados por provedores de acesso, busca endereçar, de forma dinâmica, uma das questões cruciais para a qualidade de experiência dos usuários: nem todos os pacotes de dados são iguais, e determinados pacotes são mais sensíveis à latência que outros (vídeo é mais sensível que e-mail, por exemplo). Por outro lado, o limite entre práticas legítimas de priorização de tráfego e práticas discriminatórias de diferenciação de conteúdos nem sempre é fácil de traçar, e muitas dessas práticas não são informadas aos usuários e podem ser, na verdade, escapatórias para que provedores de acesso dificultem a utilização de um tipo de conteúdo que consome recursos importantes de sua rede e pode trazer poucos benefícios do ponto de vista financeiro.

Respostas controversas coletadas na plataforma de debate:

(A) A proibição do monitoramento de pacotes contida no *§* 3º do artigo 9º não deve se aplicar aos metadados contidos no cabeçalho dos pacotes de dados.

(B) Segundo o artigo 9º, *§* 3º, o provedor de conexão está impedido de monitorar o cabeçalho dos pacotes de dados que trafegam na rede.

Resumo das respostas e seus defensores:

(A) *A proibição do monitoramento de pacotes contida no § 3º do artigo 9º não deve se aplicar aos metadados contidos no cabeçalho dos pacotes de dados.*

Para os defensores dessa tese (todos os representantes das prestadoras de serviços de provimento de Internet), o monitoramento desses metadados é fundamental, pois é o que possibilita a gestão de rede.

Quem defende isso? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL e ABINEE.*

(B) *Segundo o artigo 9º, § 3º, o provedor de conexão está impedido de monitorar o cabeçalho dos pacotes de dados que trafegam na rede.*

Com tal proibição expressa evita-se que os provedores de conexão privilegiem o fluxo de pacotes de dados provenientes de provedores de acesso a aplicação com os quais detêm algum tipo de parceria econômica.

Quem defende isso? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega e PROTESTE – Associação de Consumidores.*

4.1.5. *Content Delivery Networks* (CDNs) violam a neutralidade da rede?

CDNs são redes que buscam alocar um conteúdo mais próximo, geograficamente, de potenciais usuários finais. Elas atuam, portanto, como um intermediário da relação entre os provedores de acesso a aplicações e os usuários finais. A maior proximidade entre conteúdo e usuários economiza recursos e melhora a experiência do usuário (já que o conteúdo viaja menos pela Internet para chegar a ele).

Poucos agentes, em suas contribuições, endereçaram o tema das CDNs. As contribuições seguiram duas linhas argumentativas: uma que privilegiava mais as consequências econômicas do uso de CDNs, e outra focada no seu papel no fluxo de informações na rede.

Respostas controversas coletadas na plataforma de debate:
(A) CDNs não são uma forma de quebra da neutralidade de rede.
(B) CDNs, a depender das circunstâncias, podem ser uma forma de violação da regra da neutralidade de rede. O uso das CDNs deve ser regulado de forma a garantir a criação de acordos justos para o uso dessas redes.

Resumo das respostas e seus defensores:

(A) *CDNs não são uma forma de quebra da neutralidade de rede.*

Argumenta-se que CDNs são somente uma forma de alocar de forma inteligente o conteúdo da rede, aproximando geograficamente o conteúdo do usuário. Trata-se, portanto, de um arranjo na camada de conteúdo da rede em que não há qualquer estrutura física ou lógica que permita diferenciação de tráfego. Além disso, trata-se de uma necessidade inerente à prestação de serviço de internet que sempre foi utilizada pelas prestadoras de telecomunicações.

Ressalta-se ainda que o uso de CDNs traz benefícios para todos os envolvidos no fluxo de informações pela rede. O usuário e o provedor de aplicações beneficiam-se da entrega mais rápida do conteúdo, enquanto o provedor de conexão é favorecido pelo menor congestionamento da rede. Por fim, os defensores dessa posição afirmam que os custos de serviços de CDNs não são significativos a ponto de serem considerados uma barreira para a entrada de novos provedores de acesso a aplicações no mercado.

Quem defende isso? *Pedro Ramos, Roberto Taufick e Claro S/A*.

(B) *CDNs, a depender das circunstâncias, podem ser uma forma de violação da regra da neutralidade de rede. O uso das CDNs deve ser regulado de forma a garantir a criação de acordos justos para o uso dessas redes.*

O defensor dessa posição afirma que não está claro se o Marco Civil da Internet, em seu artigo 9º, proíbe o uso de CDNs. É verdade que as CDNs aliviam o congestionamento das redes e, portanto, a necessidade de gestão do tráfego (que pode levar a potenciais abusos) e podem beneficiar pequenos provedores de acesso a aplicação, garantindo acesso mais rápido ao seu conteúdo.

Porém, as CDNs discriminariam o tratamento de pacotes de dados, o que poderia ser problemático principalmente quando a CDN é de propriedade de algum provedor de conteúdo ou aplicação.

Quem defende isso? *CTS-FGV.*

4.1.6. Redes empresariais violam a neutralidade da rede?

Redes empresariais, como *intranets* e *extranets*, funcionam em estruturas separadas da chamada "Internet Pública" que acessamos e usamos diariamente. Esse tipo de rede é contratada sob medida para atender a necessidades especiais de cada cliente, em geral empresas que possuem uma demanda muito grande demanda de dados ou, ainda, querem estabelecer níveis de segurança maiores para o compartilhamento de arquivos entre seus colaboradores. A dúvida quanto à compatibilidade das redes empresariais com a neutralidade de rede surge porque, muitas vezes, na busca por atender a essas necessidades especiais, é necessária a realização de discriminação do tráfego de pacotes de dados.

Respostas controversas coletadas na plataforma de debate:
(A) Redes empresarias não violam a neutralidade de rede e, portanto, devem ser isentadas da obrigação de tratamento isonômico de pacotes.
(B) É necessária uma definição precisa sobre exatamente do que se trata "rede de IP privado" dentro da regulamentação do Marco Civil da Internet, sob pena de violação da regra da neutralidade da rede.

Resumo das respostas e seus defensores:

(A) *Redes empresariais não violam a neutralidade de rede e, portanto, devem ser isentadas da obrigação de tratamento isonômico de pacotes.*

Segundo os defensores dessa tese, redes empresariais são distintas e apartadas da Internet pública, funcionam por meio de IPs privados, e buscam satisfazer necessidades específicas.

A isenção da obrigação de tratamento isonômico para redes empresariais respeitaria o equilíbrio entre a necessidade de uma Internet aberta e neutra e da proteção dos diferentes requisitos dos modelos de negócios das empresas que utilizam Internet atualmente.

Muitas vezes o gerenciamento da rede e, portanto, a discriminação dos pacotes de dados é a única ferramenta do provedor de conexão para satisfazer as demandas de seus clientes empresariais.

Ressalta-se ainda que as empresas têm maior capacidade e poder de barganha para negociar planos de Internet com os provedores de acesso. Sendo assim, as empresas seriam capazes de requisitar às provedoras serviços diferenciados e mais bem adaptados às suas necessidades.

Quem defende isso? *Telecommunications Industry Association.*

(B) *É necessária uma definição precisa sobre exatamente do que se trata "rede de IP privado" dentro da regulamentação do Marco Civil da Internet, sob pena de violação da regra da neutralidade da rede.*

Redes empresariais não estariam dentro do escopo da neutralidade de rede pelo fato de serem redes de IP privado e, portanto, não estarem dentro da chamada "Internet Pública".

Porém, seria necessária uma definição precisa sobre o que é uma rede de IP privado. Dessa forma, seriam evitadas tentativas de burla da regra da neutralidade baseadas no argumento de que determinadas ações ocorreram em uma "rede privada" e não da Internet pública.

Um exemplo trazido pelo participante **Barão de Itararé** mostra a importância da definição precisa de rede de IP privado:

> *"Por exemplo, uma empresa do setor privado, que utiliza VoIP para comunicação interna, tem total direito de estabelecer prioridade para o protocolo SIP na sua rede interna. Entretanto, é temerário se esta mesma empresa possa contratar serviço diferenciado de um provedor de acesso que priorize o SIP em detrimento de outros protocolos, como modelo de negócio.*
>
> *Ou seja, o provedor de acesso, a empresa de telecom, não pode oferecer um serviço diferenciado, a título de contrato privado, com diferenciação de tráfego, para que a empresa hipotética possa trafegar VOIP de maneira prioritária".*

Quem defende isso? *Laura Tresca e Barão de Itararé*.

4.1.7. A regulamentação deve permitir bloqueio de pacote de dados para a proteção de direitos autorais?

Deverá haver no decreto uma exceção expressa à neutralidade de rede para o bloqueio de pacotes de dados provenientes de servidores que hospedam conteúdo ilegal (e.g., violação de direitos autorais)? É bem verdade que direitos autorais não são diretamente abordados pelo Marco Civil da Internet. No entanto, surgiu na plataforma uma discussão que relaciona a proteção dos direitos autorais e a neutralidade de rede.

O debate gira em torno da possibilidade de bloqueio (que implica tratamento discriminatório de pacotes de dados) por parte dos provedores de conexão de sites que hospedem conteúdos ilegais em geral e, mais especificamente, conteúdo que viole direito autoral.

Comentário INTERNETLAB – Autora: Mariana Giorgetti Valente (coordenadora de pesquisa)

Durante a negociação do Marco Civil da Internet na Câmara dos Deputados, ficou determinado que o regime de remoção de conteúdos publicados por terceiros, em uma aplicação, por razão de violação a direito autoral deveria ser relegado para um segundo momento. A razão alegada pelos atores envolvidos foi que o Marco Civil da Internet envolvia interesses de ordens muito distintas, e que manter a pauta dos direitos autorais nessa lei obstaria sua aprovação. Assim, ainda não existe, no Brasil, a especificação legal de qual procedimento deve ser seguido pelo detentor de direito de autor ou conexo que vê seu direito violado, ou qual é a responsabilidade do provedor de conteúdo por material infringente. Ficou estabelecido, no entanto, no art. 18, que o provedor de conexão não será responsável por danos decorrentes de conteúdo de qualquer natureza – aí incluído o direito autoral.

A previsão de bloqueio de pacotes de dados provenientes de servidores que hospedam conteúdo ilegal, como uma exceção a ser estabelecida no art. 9º, que trata da neutralidade de rede, envolve três problemas. O primeiro é de ordem interpretativa, e diz respeito às exceções estabelecidas no art. 9º ao princípio da neutralidade, dentre as quais não está o bloqueio de pacotes de dados de servidores específicos, para a persecução de outros fins que possam ser entendidos como desejáveis. Além disso, a isenção concedida aos provedores de conexão parece apontar para a ideia de que as políticas para persecução a conteúdos infringentes não deveriam se focar nesses atores.

O segundo problema é de ordem política: estabelecer, na regulamentação do Marco Civil, um regime para a persecução a conteúdos infringentes a direito autoral significaria antecipar-se às discussões que devem ser estabelecidas democraticamente acerca de como melhor atingir a finalidade, que levasse em conta também outros direitos dos cidadãos. Os proponentes da possibilidade de bloqueio alegam que isso seria desimportante diante do fato de que não haveria outra forma de remover certos conteúdos, pela dificuldade em se obter remoções de conteúdos hospedados em outros países. Trata-se do problema da jurisdição, que diz respeito, em verdade, a toda sorte de conteúdos (e não somente aos protegidos por direito autoral). Não são poucas nem simples as discussões hoje travadas internacionalmente acerca dessa dificuldade. O ponto é que não parece ser a regulamentação do Marco Civil o lugar adequado para resolução desse problema.

O terceiro está ligado a disputas já historicamente estabelecidas em torno da proteção a modelos de negócios baseados em exploração de direito autoral *versus* inovação tecnológica e outros interesses legítimos. O bloqueio de pacotes com o objetivo de obstar acesso a serviços por completo pode não diferenciar entre usos lícitos e ilícitos deles, o que pode significar uma abertura à censura de conteúdos legítimos. Não são poucas as vezes que vimos isso acontecer – um exemplo foi o bloqueio do *YouTube* inteiro, no Brasil, em 2007; outro foi a decisão de bloquear o *WhatsApp* também no país todo, em 2015, revertida antes de ser efetivada. A identificação de conteúdos específicos advindos de determinados sites, por outro lado, levanta preocupações graves a respeito de monitoramento.

Respostas controversas coletadas na plataforma de debate:

(A) A regulamentação deve trazer expressa a possibilidade de se bloquear pacotes provenientes de determinadas fontes (servidores) que hospedem conteúdo ilegal.

(B) Não deve haver uma exceção à neutralidade de rede para bloquear conteúdos ilegais.

Resumo das respostas e seus defensores:

(A) *A regulamentação deve trazer expressa a possibilidade de se bloquear pacotes provenientes de determinadas fontes (servidores) que hospedem conteúdo ilegal.*

Para esse argumento, a possibilidade de bloqueio por meio de ordem judicial deve ser enxergada como uma premissa da prestação adequada de serviços e aplicações a que se refere o artigo 9º, *§* 1º, inciso I, que trata das exceções da neutralidade de rede.

O bloqueio por parte do provedor de conexão, requisitado por ordem judicial é, muitas vezes, a única forma de capacitar os tribunais a dar efetividade a proteção de vários direitos. Sem ele, as decisões podem deixar de ter efeito, ou, no caso de uso de carta rogatória, só terão efeito depois de um longo período de tempo.

Quem defende isso? *MPAA, Fórum Nacional Contra a Pirataria e Ilegalidade e ABPI.*

(B) *Não deve haver uma exceção a neutralidade de rede para bloquear conteúdos ilegais.*

A existência de conteúdo ilícito em determinado site não justificaria o bloqueio de todo o seu conteúdo por parte dos provedores de conexão. Dever-se-ia preservar o direito dos usuários de utilizar o site para fins legítimos, gozando de sua presunção de inocência.

Quem defende isso? *Ivella.*

4.1.8. Como deverá ser tratada, na regulamentação, a exceção da regra da neutralidade da rede para "serviços emergenciais"?

Nota dos autores*: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:
(A) A priorização paga não pode ser interpretada como um serviço de emergência. O uso da exceção da regra da neutralidade de rede em nome de "serviços emergenciais" deve ocorrer somente em hipótese de congestão de rede, não mediante pagamento. **Autor da proposta:** *CTS-FGV.*
(B) A regulamentação deve conceituar o que significa "serviço de emergência" e, na medida do possível, já listar, *numerus clausus*, as entidades que podem fazer jus a essa condição. **Autor da proposta:** *Comissão Especial de Propriedade Intelectual (CEPI) junto à OAB/RS.*

(C) Os serviços considerados "de emergência" podem ser aferidos tendo como parâmetro a lei 7.783/1989, que trata dos serviços considerados "essenciais", e a resolução da Anatel nº 614, de 28 de maio de 2013, que regula os procedimentos de serviços de comunicação multimídia.

Autor da proposta: *Procon/SP.*

(D) Os "serviços de emergência" devem ser conceituados como: serviços públicos de emergência (polícia, bombeiros, serviços médicos prestados por ambulâncias e hospitais) e serviços ou aplicativos usados para enviar mensagens oficiais em situações de calamidade pública ou desastres naturais.

Autor da proposta: *Cristiana Gonzalez.*

4.2. Guarda de registros e privacidade

4.2.1. Como o decreto deve tratar a guarda e o acesso pelas autoridades aos registros de que tratam os artigos 13 e 15 do Marco Civil da Internet?

Comentário INTERNETLAB – Autora: Jacqueline de Souza Abreu (pesquisadora)

Obrigações de guarda preventiva de metadados gerados na utilização de meios de telecomunicação são, em geral, defendidas com base no argumento de que estas obrigações são essenciais para evitar "brechas" que impeçam (i) a responsabilização de usuário por ilícitos cometidos através do meio de telecomunicação em questão ou (ii) a utilização desses dados como auxílio na prevenção e repressão de outros delitos e solução de conflitos. No caso das obrigações de guarda de registros de conexão à Internet e de acesso a aplicações dos arts. 13 e 15 do Marco Civil da Internet, o objetivo seria garantir a eficácia da responsabilização de usuários da Internet que cometam ilícitos pela rede e a disponibilidade desses dados como meios investigatórios ou probatórios mesmo para casos penais e cíveis de fora da rede.

Tais previsões geram, contudo, controvérsias. No âmbito do discurso político, as preocupações giram em torno da expansão da vigilância do Estado sobre os cidadãos. No âmbito jurídico, dúvidas são levantadas sobre a constitucionalidade dessas medidas. Isso porque a análise de metadados como os registros de conexão do art. 13 e, principalmente, os de acesso a aplicações do art. 15 é capaz de oferecer retratos sobre personalidade, hábitos, interesses, círculo social e localização do usuário, que estão diretamente relacionados à sua privacidade e afetam o sigilo das comunicações. Soma-se a isso o fato de que a guarda de registros ocorre preventivamente, sem estar conectada a um perigo concreto ou a uma suspeita individual, o que estaria em desacordo com o princípio da presunção de inocência.

No debate jurídico, enquanto alguns defendem a incompatibilidade de obrigações de guarda preventiva de metadados com direitos fundamentais, outros tentam uma saída pelo princípio da proporcionalidade, principalmente pela delimitação das hipóteses e requisitos de acesso aos registros guardados, como também pela restrição apenas a fins de persecução penal de crimes graves, na existência de indícios concretos de autoria e participação, e estabelecimento de regras de segurança na guarda dos dados e de transparência sobre a utilização.

Quando o Tribunal de Justiça da União Europeia, em abril de 2014 invalidou a Diretiva Europeia que estipulava guarda obrigatória de dados gerados no uso de serviços de telecomunicações para fins de prevenção e repressão criminal, sob o fundamento de que a restrição a direitos fundamentais levada a cabo nos termos da Diretiva seria desproporcional, as repercussões no Brasil foram imediatas e refletem-se no debate sobre a regulamentação do Marco Civil. Vale destacar, contudo, que, ao mesmo tempo em que diversas leis nacionais de países europeus que seguiram os termos da Diretiva caíram por serem "desproporcionais" (como recentemente na Holanda), já começam a surgir projetos de lei que pretendem ser regulações "proporcionais" de obrigações de guarda de metadados (como atualmente na Alemanha). Esta ainda não é uma questão resolvida nem mesmo por lá.

Respostas controversas coletadas na plataforma de debate:
(A) O decreto deve limitar as hipóteses de acesso.
(B) O decreto deve ampliar a coleta de registros.
(C) O decreto não deve regular o assunto.

Resumo das respostas e seus defensores:

(A) *O decreto deve limitar as hipóteses de acesso*

As contribuições que argumentam em favor da limitação das hipóteses de acesso aos registros guardados de acordo com os artigos 13 e 15 do Marco Civil partem do pressuposto de que tal guarda de registros é, na verdade, inconstitucional.

Foi citado, inclusive, o exemplo da União Europeia, no qual o Conselho Europeu de Direitos Humanos (CEDH, *Council of Europe's Commissioner for Human Rights* em inglês) 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" (**CTS-FGV**).

A solução para limitar o acesso diferiu entre os participantes. O **CTS-FGV** argumentou pela adoção dos Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações[1]. Outro grupo de participantes argumentou que, à semelhança dos casos de quebra de sigilo telefônico, o acesso a registros somente poderá ser disponibilizado mediante ordem judicial proferida no âmbito de investigação criminal ou instrução processual penal, conforme estabelecido no artigo 5º, XII, da Constituição, e nos artigos 1º e 3º da Lei nº 9.296/96, estando fora, portanto, do alcance da jurisdição de ordens emanadas de juízos não criminais.

Quem defende isso? *CTS-FGV, Câmara Brasileira de Comércio Eletrônico, Associação Brasileira de Marketing Direto - ABEMID, ANER, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

[1] Ver: https://pt.necessaryandproportionate.org/text

(B) *O decreto deve ampliar a coleta de registros*

Em função do esgotamento dos números de IP públicos "versão 4" (IPv4) e do consequente compartilhamento desses números de IP entre vários usuários ao mesmo tempo, há uma impossibilidade de individualizar e localizar potenciais infratores por meio somente do número de IP e da hora e data de acesso.

Tendo isso em vista, pede-se que sejam guardados adicionalmente os dados relativos à porta lógica utilizada. Essa medida possibilitará a individualização de suspeitos enquanto não for implementada a nova versão de IP (IPv6). Além da porta lógica, a **OAB/SC** também defende a criação de obrigação de guarda do endereço *MAC* (*media access control*), numeração produzida pelo roteador de redes domésticas ou profissionais que permitiria identificar ao certo o dispositivo ligado à atividade investigada.

Além disso, com relação ao artigo 13, o **Ministério Público Federal (MPF)** defende que a guarda de registros de conexão seja realizada em relação a qualquer usuário, não havendo espaço para exceções, nem mesmo para pessoas que forneçam acesso gratuito à Internet nas dependências de seus estabelecimentos privados. Tal proposta representa uma ampliação do escopo do Marco Civil da Internet à medida que ele obriga somente que os administradores de sistemas autônomos[2] a guardar registros de conexão, e não qualquer empresa, organização ou indivíduo que ofereça algum tipo acesso à Internet. O **MPF** não cita tal classificação em sua contribuição.

Quem defende isso? *TIM Brasil, MPF e OAB/SC.*

(C) *O decreto não deve regular o assunto*

No caso do artigo 15, também partindo do pressuposto da inconstitucionalidade da retenção em massa de registros e alinhado com o entendimento europeu, uma alternativa para remediar a inconstitucionalidade da lei seria não a regular. Dessa forma, ela permaneceria sendo uma norma de eficácia contida, conforme recente entendimento do Tribunal de Justiça do Estado de São Paulo[3], não

---

[2] Segundo o *Request For Comments* (RFC) 1930 da IETF (Força Tarefa de Engenharia da Internet, ou *Internet Engineering Task Force,* em inglês), entidade técnica internacional que acompanha a Internet desde seu início e que propõe padrões para tecnologias e protocolos, "sistema autônomo" corresponde a uma "*coleção de prefixos de roteamento conectados por Protocolo Internet (IP) sob o controle de um ou mais operadores de rede que apresenta uma política comum e claramente definida de roteamento para a Internet*". No Brasil, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço operativo do Comitê Gestor da Internet, é o responsável por criar as regras sobre como provedores de conexão podem inscrever-se como "sistemas autônomos", participando assim da distribuição de blocos de números IP feita pelo NIC.br, Segundo o NIC.br, as entidades precisam possuir, por exemplo, "uma mínima infraestrutura de rede" e "ter 2 ou mais conexões independentes à Internet ou então uma conexão com uma operadora e uma conexão a um ponto de troca de tráfego", além de uma série de padrões técnicos e equipe compatível. Fontes: <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao> e <ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf >.

[3] Entendimento do acórdão do Agravo de Instrumento nº 2168213-47.2014.8.26.0000, relatoria do Desembargador Rômolo Russo (10/03/2015).

gerando, portanto, efeitos. O **ITS-Rio** também forneceu uma alternativa para regular o tema, caso fique decidido que o decreto deve abordar a questão da retenção de dados (ver abaixo no tópico "*Limites para a guarda e para o acesso de registros de conexão e acesso a aplicações de internet*").

Quem defende isso? *ITS-Rio.*

4.2.2. Quais provedores de aplicações devem ser obrigados a guardar registros de acesso a aplicações de usuários (regulamentação do artigo 15 do Marco Civil)?

O debate público revelou uma controvérsia sobre quais provedores de aplicações devem ser obrigados a guardar registros de seus usuários. O cerne do debate está em definir quais aplicações podem estar excluídas da regra de guarda.

Respostas controversas coletadas na plataforma de debate:
(A) A guarda só deve ser obrigatória para aplicações que hospedem conteúdo produzido por usuários.
(B) A guarda só deve ser obrigatória para aqueles provedores de acesso a aplicação que obtêm lucro mediante tratamento de dados pessoais.

Resumo das respostas e seus defensores:

(A) *A guarda só deve ser obrigatória para aplicações que hospedem conteúdo produzido por usuários*

Sugere-se que o decreto indique que a guarda só é obrigatória para aplicações que hospedem conteúdo produzido por usuários. Essa sugestão leva em conta aquilo que se busca com a obrigação de armazenamento de registros: a identificação de responsáveis pela violação de direitos de terceiros.

Quando não há hospedagem de conteúdo produzido por usuários, não há tampouco a possibilidade de violação de direitos por parte dos usuários, o que torna desnecessária a guarda de registros. Nesse sentido, o **ITS-Rio** expôs que:

> *"Importante salientar que, mesmo com relação aos serviços financeiros essa obrigação não se mostraria adequada sob o argumento de investigação de crimes de lavagem de dinheiro e de outros crimes financeiros, pois já há Lei que versa sobre o assunto e que obriga essas empresas a enviar informações relacionadas a movimentações financeiras 'suspeitas' para o COAF, o que tornaria desnecessária e redundante a guarda de registros de acesso".*

Quem defende isso? *ITS-Rio, ABRANET, CNseg.*

(B) *A guarda só deve ser obrigatória para aqueles provedores de acesso a aplicação que obtêm lucro mediante tratamento de dados pessoais.*

O perfil da obrigação de guarda pode ser delimitado por meio de requisitos, tais como como teto de faturamento, finalidade das atividades e, por último, a necessidade ou não de realização de *login* (momento em que efetivamente se configura a existência de um usuário cadastrado que realiza ações).

Quem defende isso? *Cristiana Gonzalez, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega e PROTESTE – Associação de Consumidores.*

4.2.3. Quais regras adicionais o decreto deve criar a respeito da guarda de registros de acesso a aplicações e de conexão de usuários?

Nota dos autores*: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:
(A) Decreto deveria estabelecer uma exceção expressa quanto à guarda de registros relativos a atividades relacionadas à chamada "Internet da Coisas". Essa exceção se daria por três motivos: (i) o volume deste tipo de registro é enorme, o que geraria custos elevados e desproporcionais, (ii) existem implicações para a privacidade dos cidadãos; e (iii) a maior parte desses dados seria exorbitante para atividades de exequibilidade ("*enforcement*") legal. **Autor da proposta:** *ITS-Rio.*
(B) A regulamentação deve esclarecer os termos finais e iniciais da contagem de prazo para guarda de registros, por um imperativo de segurança jurídica. **Autores da proposta:** *IASP, ABPI, José Antônio Milagre, ANER, ABRANET e Fundação Procon – SP.*
(C) O decreto deve trazer os critérios segundo os quais serão justificados os pedidos de acesso a informações pelas autoridades (motivação, período ao qual se referem os registros, fundados indícios de ocorrência de ilícito, entre outros). **Autores da proposta:** *FIESP, GEPI – FGV, ABRANET, Câmara Brasileira de Comércio Eletrônico.*

(D) O regulamento deve tratar da padronização do fornecimento e do acesso aos registros e demais dados (artigo 10, caput). Segundo a participante *Laura Tresca,* tal padronização deve levar em consideração a definição do artigo 5º sobre os elementos que compõem registros de conexão e de acesso a aplicações de internet.

Autores da proposta: *FIESP, José Antônio Milagre, ANER, ABRANET e Laura Tresca.*

(E) 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.

Autores da proposta: *ITS-Rio, Veridiana Alimonti, Joana Varon, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

4.2.4. Como o decreto deve tratar a possibilidade de requisição de guarda cautelar de dados por "prazo superior"?

Há previsão no Marco Civil da Internet da possibilidade de requisição, por parte de autoridade policial ou administrativa, de guarda de registros de usuários por um prazo superior ao já previsto no caso dos provedores de acesso à aplicação (6 meses) e dos provedores de conexão (1 ano).

Essa possibilidade é, no entanto, pouco detalhada no texto legal e, por esse motivo, suscitou vários debates na plataforma.

Quais são os requisitos que legitimam a requisição de guarda de dados por prazo superior?

Propostas avulsas para a regulação deste tema:

(A) Autoridades competentes devem especificar "fundados indícios da ocorrência do ilícito" (artigo 22, I, do Marco Civil) e oferecer justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória (artigo 22, III)

Autores da proposta: *CTS-FGV, IASP, ABRANET, ITS-RJ, ANER.*

(B) Decreto deverá delimitar quais autoridades administrativas e policiais têm competência para pedir guarda cautelar.

Autores da proposta: *Sky Brasil, ITT, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega e PROTESTE – Associação de Consumidores.*

Quanto deveria durar o "prazo superior" de que falam os artigos 13, § 2º, e 15, § 2º?

Propostas avulsas para a regulação deste tema:

(A) Não poderá ser maior que o prazo de 60 dias para que a autoridade ingresse com o pedido de autorização judicial de acesso aos dados, sob pena de impor ônus injustificado e desconhecido.

Autores da proposta: *IASP, GEPI – FGV, Barão de Itararê, Laura Tresca, Veridiana Alimonti, Cristiana Gonzalez, ABRANET, Ana Cristina Azevedo, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

(B) Além do prazo de 60 dias para o pedido de autorização judicial, o decreto deverá determinar um prazo subsequente (sugere-se de mais 60 dias) no qual o provedor será obrigado a continuar guardando os dados. Terminado o prazo subsequente o provedor poderá cessar a guarda cautelar de dados.

Autor da proposta: *Brasscom.*

(C) Guarda cautelar deverá durar no máximo 1 ano adicional para os provedores de conexão e 6 meses adicionais para os provedores de acesso a aplicações.

Autor da proposta: *Sky Brasil.*

(D) Por ser mais benéfico ao consumidor, sugere-se que o prazo máximo para prorrogação obedeça ao lapso temporal de 3 anos, previsto no art. 206, § 3º, V, do Código Civil Brasileiro e adotado pelo STJ (Agravo Regimental no AREsp 614778 , Relator Ministro Marco Aurélio Bellizze).

Autor da proposta: *Fundação Procon – SP.*

(E) O ideal do prazo, no caso de crime, seria o período prescricional do delito investigado. E na esfera cível, o prazo de decadência do direito de ação.

Autor da proposta: *Emerson Wendt*

Quais regras adicionais o decreto deve criar a respeito do pedido cautelar de guarda de dados por prazo superior ao estipulado no Marco Civil?

Propostas avulsas para a regulação deste tema:
(A) Decreto deveria criar mecanismos de contestação do pedido cautelar por parte dos provedores. **Autores da proposta:** *Sky Brasil.*
(B) Decreto deverá delimitar um prazo máximo para a guarda cautelar de registros na hipótese de silêncio por parte do judiciário. Sugere-se 180 dias a contar da entrada do pedido de guarda cautelar da autoridade administrativa, policial ou do Ministério Público. **Autores da proposta:** *SINDITELEBRASIL e CLARO.*
(C) Decreto deverá delimitar um prazo máximo de guarda cautelar, a ser respeitado pelo juiz, quando este acatar o pedido de guarda cautelar da autoridade policial, administrativa ou do Ministério Público **Autores da proposta:** *SINDITELEBRASIL, CLARO e Procon –SP.*
(D) Usuário deve ser informado do pedido de guarda cautelar adicional dos registros de suas atividades. **Autores da proposta:** *Veridiana Alimonti, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega e Proteste - Associação de Consumidores*

4.3. Como o decreto deve abordar a questão dos dados cadastrais e a possibilidade de sua requisição pelas autoridades?

Além das propostas consideradas abaixo, muitos participantes ressaltaram a importância de melhor definir quais seriam dados cadastrais, apesar da especificação já trazida na lei: "dados cadastrais que informem qualificação pessoal, filiação e endereço".

4.3.1. Quais autoridades são competentes para requisitar dados cadastrais?

Proposta avulsa para a regulação deste tema:

(A) Decreto deverá seguir o mesmo entendimento do art. 17-B da Lei n. 9.613/1998 (Lei de Lavagem de Dinheiro) e da Lei nº 12850/13 (Lei das Organizações Criminosas).

Autores da proposta: *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações, Câmara Brasileira de Comércio Eletrônico, CTS-FGV, SindiTeleBrasil, ANER, ABRANET, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega e Proteste - Associação de Consumidores.*

4.3.2. Quais regras adicionais o decreto deve criar a respeito dos dados cadastrais?

Propostas avulsas para a regulação deste tema:

(A) Decreto deverá tornar obrigatório informar o usuário de que seus dados foram acessados por finalidades diferentes daquelas às quais ele deu seu consenso - mesmo quando se tratar de finalidade investigativa (casos de exceção devem também ser previstos e os pedidos de exceção, justificados).

Autores da proposta: *Cristiana Gonzalez, Francisco Brito Cruz, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

(B) Para atingir as garantias previstas no *caput* do artigo 10, deve estar claro na regulamentação que tais dados cadastrais só podem ser acessados com a indicação de um nome de usuário ou outra informação pertencente à conta de serviço do usuário de Internet em questão. Caso contrário, o *§* 3º pode permitir que qualquer autoridade de posse de um IP possa pedir ao provedor de conexão (o

"administrador de sistema autônomo"), responsável pela administração do número IP em questão, o cadastro do usuário que o utilizou, sem crivo judicial adequado.

Autor da proposta: *Francisco Brito Cruz*

4.4. Necessidade de uma autoridade independente para proteção de dados pessoais

***Nota dos autores**: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.* ***Apesar das duas propostas elencadas abaixo serem convergentes no sentido de criação de um órgão, optamos por dividir e realçar os nuances de cada uma**.*

Propostas avulsas para a regulação deste tema:

(A) É necessária a criação de uma autoridade garantidora independente que aplique as disposições sobre privacidade e dados pessoais presentes no Marco Civil da Internet nos seguintes moldes:

> *"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".*

Autor da proposta: *CTS-FGV.*

(B) Para a implementação do previsto nos artigos 7, 8, 10, 13, 14, 15 e 16 do Marco Civil da Internet é necessária uma autoridade de proteção de dados pessoais.

Não há de se ignorar que órgãos de proteção de defesa do consumidor e o Ministério Público terão um papel importante, mas, à luz das boas práticas, particularmente em países da Europa, conhecido por alto padrão de proteção da privacidade, outro tipo de autoridade seria necessário para a aplicação eficaz de tais disposições legais. Entre suas atribuições estariam assegurar que estes dados são guardados com segurança; que o consentimento foi feito de forma clara, livre e expressa, ou até mesmo para que se estabeleçam procedimentos para o fornecimento das "informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados", de maneira que possa haver efetividade quanto ao cumprimento da lei e garantias de que tais procedimentos não estejam sendo usados de maneira abusiva contra os usuários, com eventuais compartilhamentos de dados para fins comerciais ou possíveis violações do direito à privacidade por parte do Estado.

Nesse sentido, seria bem-vinda a discussão da regulamentação do Marco Civil de forma paralela ao debate do Anteprojeto de Lei de Dados Pessoais, que deverá analisar qual a melhor composição deste

tipo de autoridade de proteção de dados, mas cuja existência deveria ter referência, ainda que ampla, na regulamentação do Marco Civil da Internet.

Autores da proposta: *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

4.5. Estabelecimentos de Padrões de Segurança

4.5.1. Como devem ser estabelecidos os padrões de segurança dos dados?

Respostas controversas coletadas na plataforma de debate:
(A) Regulamento não é o lugar correto para definir parâmetros de segurança.
(B) Regulamento deve somente definir padrões mínimos de segurança.
(C) A regulação deve ser tecnologicamente neutra e não deve impor a divulgação dos padrões de segurança adotados.

Resumo das respostas e seus defensores:

(A) *Regulamento não é o lugar correto para definir parâmetros de segurança***.**

Para os defensores dessa posição, parâmetros definidos por decreto podem acabar por se tornar obsoletos. Caso os parâmetros sejam estabelecidos por meio do decreto, este deve prever, ao menos, formas de revisão e atualização de seus dispositivos

Conforme colocou o **CTS-FGV** em sua contribuição, "*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*"

Ademais, devem ser levadas em conta a experiência da União Europeia no assunto. Em especial, do Grupo de Trabalho do Artigo 29[4] da Comissão Europeia.

Quem defende isso? *CTS-FGV.*

[4] Ver mais em: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>.

(B) *Regulamento deve somente definir padrões mínimos de segurança.*

Para assegurar a proteção da privacidade e intimidade dos cidadãos, o regulamento do Marco Civil deve definir como padrão mínimo de segurança a encriptação obrigatória de banco de dados compostos por informações de usuários (como por registros de conexão e acesso à aplicação armazenados). Esta obrigação deve ser imposta a toda guarda de dados e informações, não somente aqueles confeccionados para o cumprimento da lei. Os provedores de conexão e de aplicações de Internet apenas deverão fornecer a chave criptográfica diante de ordem judicial que ordena acesso aos dados

Quem defende isso? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores*

(C) *A regulação deve ser tecnologicamente neutra e não deve impor a divulgação de formas a divulgação dos padrões de segurança adotados.*

O regulamento não deve detalhar excessivamente os padrões de segurança a serem adotados sob pena de, com o passar do tempo e a evolução da tecnologia, acabar por dificultar ou inviabilizar novos negócios (conflitando, assim, com a liberdade econômica dos provedores de conexão ou de aplicação de Internet).

Ao invés de um detalhamento minucioso dos padrões de segurança, o decreto deve encorajar a inovação e a escolha por parte dos agentes de padrões de segurança que, de acordo com sua experiência no ramo, melhor satisfazem as necessidades de seu serviço.

Com relação à obrigação de divulgação dos padrões de segurança (artigo 10, § 4º), sugere-se que a obrigação deve ser limitada a fins meramente informativos para o público em geral, sem colocar em risco segredos comerciais e a própria segurança. Os defensores dessa posição afirmam que este tipo de divulgação não é garantia de maior segurança para o usuário, e sim possível comprometimento da segurança da informação.

Quem defende isso? *ABRANET e Câmara Brasileira de Comércio Eletrônico*

4.6. Sanções

O artigo 12 do Marco Civil da Internet prevê um rol de sanções para os agentes que não cumpram de forma adequada com as obrigações de guarda e disponibilização de dados previstas nos artigos 10 e 11 da lei. Participantes enviaram contribuições no sentido de detalhar a forma com que essas sanções deveriam ser aplicadas.

4.6.1. Como o decreto deve tratar as sanções impostas pelo artigo 12 do Marco Civil?

***Nota dos autores**: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:
(A) Decreto deve prever a autoridades competentes para aplicar sanções. O MPF defende que essa provisão deve vir sem prejuízo da previsão de sanções por meio do Poder Judiciário, sempre que este for provocado, inclusive por ação do Ministério Público. **Autor da proposta:** *MPF.*
(B) É necessário que uma autoridade federal única seja a responsável pela aplicação das multas, a fim de verificar a aplicação uniforme dentro do Brasil. Além disso, com relação ao inciso II que prevê multa de até 10% do faturamento, é preciso esclarecer que o faturamento constitui só a renda gerada a partir da atividade que deu origem à multa no Brasil. **Autor da proposta:** *Information Technology Industry Council.*
(C) Tal como disposto no artigo 11, *§* 4º, o decreto deverá, em casos de desrespeito a obrigações e deveres na guarda de registros, fazer referência a lei de processo administrativo federal (lei n. 9.784/99). **Autores da proposta:** *GEPI–FGV, ABRANET e Câmara Brasileira de Comércio Eletrônico.*
(D) O decreto deve tomar por base o artigo 50 do anteprojeto de lei de proteção de dados pessoais para determinar sanções, a saber: *Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:* *I – multa simples ou diária;* *II – publicização da infração;* *III - dissociação dos dados pessoais;*

IV - bloqueio dos dados pessoais;

V - suspensão da operação de tratamento de dados pessoais, por prazo não superior a dois anos;

VI - cancelamento dos dados pessoias;

VII - proibição de tratamento de dados sensíveis, por prazo não superior a dez anos;e

VIII - proibição de funcionamento de banco de dados, por prazo não superior a dez anos.

§ 1º As sanções poderão ser aplicadas cumulativamente.

§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.

§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

Autor da proposta: *FIESP.*

(G) A regulamentação deve cuidar para que reste claro que, com exceção da multa estabelecida no inciso II, inexiste solidariedade ou corresponsabilidade entre pessoas jurídicas do mesmo grupo quanto às sanções previstas. Significa que, em observância aos princípios da autonomia da personalidade jurídica e de que nenhuma pena deve passar da pessoa do acusado, as sanções dispostas nos incisos I, III e IV somente podem ser aplicadas à pessoa jurídica que efetivamente tiver violado as normas previstas nos artigos 10 e 11, não se estendendo a outras pessoas jurídicas do mesmo grupo de empresas.

Autor da proposta: *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (ABDTIC).*

4.7. Transparência

***Nota dos autores**: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:

(A) O artigo 11, *§* 3º, do Marco Civil estabelece que todos os provedores de conexão e de aplicações 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. Sugere-se que, no regulamento, seja esclarecido que tais informações devam ser prestadas ao Ministério Público sempre que requisitado, com base nas suas respectivas leis orgânicas. O Ministério Público, como instituição que tem, dentre suas funções, a proteção de direitos coletivos, deve ter acesso a esses dados sempre que necessário para a proteção do cidadão.

Autor da proposta: *MPF.*

(B) Decreto deve demandar que às autoridades a publicação periódica de 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 devem incluir a totalidade de dados e informações acessadas e quantos desses foram utilizados em procedimentos administrativos ou judiciais.

Autores da proposta: *CTS-FGV, Francisco Brito Cruz, Laura Tresca, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

4.8. Dados pessoais

O Marco Civil da Internet, em especial no art. 7º, traz expressões como "dados pessoais" e "tratamento de dados" sem, no entanto, defini-las.

4.8.1. O decreto deve definir expressões que dizem respeito a dados pessoais?

***Nota dos autores**: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:
(A) Tais definições devem ser abordadas na futura lei de proteção de dados pessoais. **Autores da proposta:** *CTS-FGV, GEPI-FGV, Associação Nacional de Jornais - ANJ, Associação Brasileira de Marketing Direto - ABeMD, Associação Brasileira de Internet - ABRANET.*
(B) No decreto, devem constar (i) critérios mínimos para os contratos de prestação de serviços com base na legislação consumerista; (ii) que dados pessoais só poderão ser utilizados para finalidades que se justifiquem diante do serviço/produto oferecido; (iii) a autorização específica e separada quanto à coleta, uso, armazenamento, tratamento e finalidade da coleta de dados pessoais; e (iv) que o consentimento não deve ser único para todas as funcionalidades do produto. **Autores da proposta:** *Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

5. OUTROS TEMAS E CONSIDERAÇÕES

5.1 Questões de Jurisdição: como o decreto deve abordar o artigo 11 do Marco Civil da Internet?

***Nota dos autores**: em razão da disparidade entre as propostas sobre esse tema, as contribuições sobre o tema forma organizadas como "propostas", e não como respostas diversas. A diferença é que a escolha regulatória por uma das propostas não inviabiliza que se escolham as outras também.*

Propostas avulsas para a regulação deste tema:

(A) Contribuição do pesquisador **Nicolo Zingales** busca mostrar os sentidos de expressões do artigo 11 e responder algumas perguntas: (i) o que são considerados no Brasil "conteúdo das comunicações"? (ii) Quando uma oferta pode ser considerada uma "oferta de serviço ao público brasileiro"? (iii) Quando se pode considerar uma coleta de dados no Brasil? (iv) E o que significa "possuir estabelecimento no Brasil"?

(i) Conteúdo de comunicações deve ser entendido como conteúdos que podem, provavelmente, causar danos aos direitos dos usuários brasileiros. Dessa forma, será possível evitar a extensão do Marco Civil para situações sem nexo territorial suficiente.

(ii) Só deve ser considerada uma oferta de serviços aquela ação que, de fato, procure ter como alvo (*target*) o público brasileiro. Exemplos de elementos que podem determinar o *targeting* do público brasileiro: (a) uso de moeda ou língua brasileira, (b) listar número de telefones com o código de área brasileiro, (c) marketing ou propaganda focada nas características do público consumidor brasileiro, e (d) uso de domínio brasileiro (.br).

(iii) Coleta de dados deve se referir àquelas coletas que visam criar um perfil do usuário (*profiling*). Ou seja, não são inclusos as atividades que não possam, potencialmente, causar danos aos usuários (e.g. *cookies*)

(iv) Para que uma empresa seja considerada estabelecida no Brasil, esta deve ter, permanentemente, recursos humanos e técnicos necessários para prover determinados serviços, sendo muito importante considerar a conexão entre os serviços fornecidos e as atividades nas quais os dados estão sendo tratados.

Autor da proposta: *Nicolo Zingales.*

(B) O decreto deve cuidar para que reste claro que o objeto do artigo 11 é exclusivamente a aplicação da legislação brasileira, não sobre legitimidade ou responsabilidade de pessoa jurídica brasileira em relação a atos praticados por pessoa jurídica estrangeira do mesmo grupo, como vem sendo frequentemente alegado em juízo e acolhido por juízes (ou seja a responsabilidade segue sendo da pessoa jurídica estrangeira, não há transmissão de responsabilidade).

Autor da proposta: *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic)*

(C) Regulamento deve deixar claro que somente sites que tomem medidas objetivas para atrair consumidores brasileiros serão responsabilizados no escopo do artigo 11 do Marco Civil da Internet. São exemplos: serviços de marketing para os brasileiros, usando a linguagem em português; fornecer contratos, termos de serviço e acordos de usuário em Português; e oferta de conteúdo local.

Autor da proposta*: Information Technology Industry Council*

5.2. Requisitos objetivos de indicação de conteúdo a ser removido da Internet

5.2.1. Como deve ser feita a indicação dos conteúdos alvos de ordem judicial de retirada (regulamentação do artigo 19)?

Respostas controversas coletadas na plataforma de debate:
(A) Indicação deve ser feita por meio de URL (*uniform resource locator*)
(B) URL é só um dos meios passíveis de serem utilizados para a identificação inequívoca do conteúdo.

Resumo das respostas e seus defensores:

(A) *Indicação deve ser feita por meio de URL (*uniform resource locator*).*

***Nota dos autores**: o uso de URL como método de indicação é defendido pelos participantes não só no caso de pedido de retirada por ordem judicial (artigo 19) como também de pedido de retirada por "notificação para indisponibilização" (artigo 21), como colocado abaixo.*

A indicação da URL é suficiente para a localização inequívoca do conteúdo. Tendo, inclusive, a jurisprudência do STJ já apontado o entendimento de que este deve ser o requisito objetivo para identificação clara e específica do conteúdo.

Ademais, este tipo de identificação evita que o provedor de aplicações seja obrigado por ordem judicial a estabelecer qualquer tipo de filtro ou monitoramento de conteúdo sem que este conteúdo tenha sido especificamente analisado pelo Poder Judiciário.

Quem defende isso? *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic), ABRANET, Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI) e IASP.*

(B) *O URL é só um dos meios passíveis de serem utilizados para a identificação inequívoca do conteúdo.*

Argumenta-se que decreto deve listar os meios passíveis de serem utilizados para identificação do conteúdo a ser retirado através de ordem judicial. São exemplos desses critérios **(i)** o URL do conteúdo; **(ii)** código de publicação do conteúdo; **(iii)** o nome de usuário do infrator (ou seu código de identificação), em conjunto com a data e hora de publicação do conteúdo; dentre outros critérios.

A regulamentação deveria ainda trazer exemplos de meios de identificação que não atendam aos requisitos legais, tal como a identificação de palavras-chave.

Por fim, visando proteger a liberdade de expressão, o decreto deveria esclarecer os deveres do provedor após a exclusão do conteúdo. Não deveria o provedor ser obrigado a realizar um controle continuado temendo eventuais repostagens do conteúdo alvo da ordem judicial de remoção.
Quem defende isso? *Associação Brasileira da Propriedade Intelectual – ABPI.*

5.2.2. Como deve ser feita a indicação dos conteúdos alvos de notificação para indisponibilização de conteúdo (regulamentação do artigo 21)?

Esse dispositivo estabelece que o provedor de aplicações de internet será responsabilizado pelo conteúdo gerado por terceiros no caso de divulgação de imagens, vídeos ou outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado, sem autorização de seus participantes, a partir do recebimento de notificação pelo participante ou de seu representante legal, deixando de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Respostas controversas coletadas na plataforma de debate:
(A) Indicação deve ser feita por meio de URL (*uniform resource locator*).
(B) O decreto deve prever outros requisitos para além de URL.

Resumo das respostas e seus defensores:
(A) *Indicação deve ser feita por meio de URL* (uniform resource locator).

Segundo os defensores dessa tese, a indicação da URL seria suficiente para a localização inequívoca do conteúdo. A jurisprudência do STJ já teria apontado o entendimento de que este deve ser o requisito objetivo para identificação clara e específica do conteúdo.

Ademais, este tipo de identificação evitaria que o provedor de aplicações fosse obrigado por ordem judicial a estabelecer qualquer tipo de filtro ou monitoramento de conteúdo sem que este conteúdo tenha sido especificamente analisado pelo Poder Judiciário.
Quem defende isso? *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic), ABRANET, Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI) e IASP.*

(B) *O decreto deve prever outros requisitos para além de URL.*

Para que o conteúdo seja retirado, a notificação deveria ser feita conjuntamente à apresentação de documento pessoal ou por representante legal com procuração, além de uma declaração da vítima confirmando que é mesmo a participante do conteúdo violador. A pessoa que publicou o conteúdo

deveria ser notificada a fim de que possa tomar as medidas cabíveis caso considere que a remoção do conteúdo foi indevida e afeta seu direito à liberdade de expressão.

Quem defende isso? *Laura Tresca, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

5.2.3. Qual deve ser o prazo para a retirada do conteúdo a partir da notificação (regulamentação do artigo 21)?

Proposta avulsa para a regulação deste tema:

(A) Em que pese que a responsabilização do provedor por conteúdos ilícitos tenha como regra geral a necessidade de ordem judicial específica, o próprio Marco Civil da Internet criou algumas exceções. Esse é o caso, por exemplo, do artigo 21, aplicável às hipóteses de conteúdos envolvendo "nudez ou de atos sexuais de caráter privado". Nesses casos, "após o recebimento de notificação pelo participante ou seu representante legal", o provedor deve indisponibilizar o conteúdo, de forma diligente, no âmbito e nos limites técnicos de seu serviço, sob pena de responder subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização, do conteúdo infrator.

Os proponentes dessa proposta recomendam que seja regulamentada a forma como deve ocorrer essa indisponibilização. Acredita-se que condicionar o provedor ao cumprimento da exclusão apenas de "forma diligente" pode levar à ineficácia do artigo, em conflito com entendimento jurisprudencial consagrado.

A jurisprudência do STJ já tratava acerca do prazo de 24h para a retirada de conteúdos ilícitos em aplicações de Internet:

> *"Uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, o provedor deve retirar o material do ar no prazo de 24 (vinte e quatro) horas, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada".* (RESP 1323754/RJ, Terceira Turma, Min. Nancy Andrighi, data: 19/06/2012)

Assim, os proponentes recomendam a regulamentação dessa 'forma diligente' num prazo específico, que poderia ser o mesmo já trazido pelo STJ, ou seja, 24h.

Autores da proposta: *Comissão Especial de Propriedade Intelectual (CEPI) junto à OAB/RS.*

5.3. Como decreto deve endereçar a questão do estímulo ao uso de formatos abertos?

Proposta avulsa para a regulação deste tema:

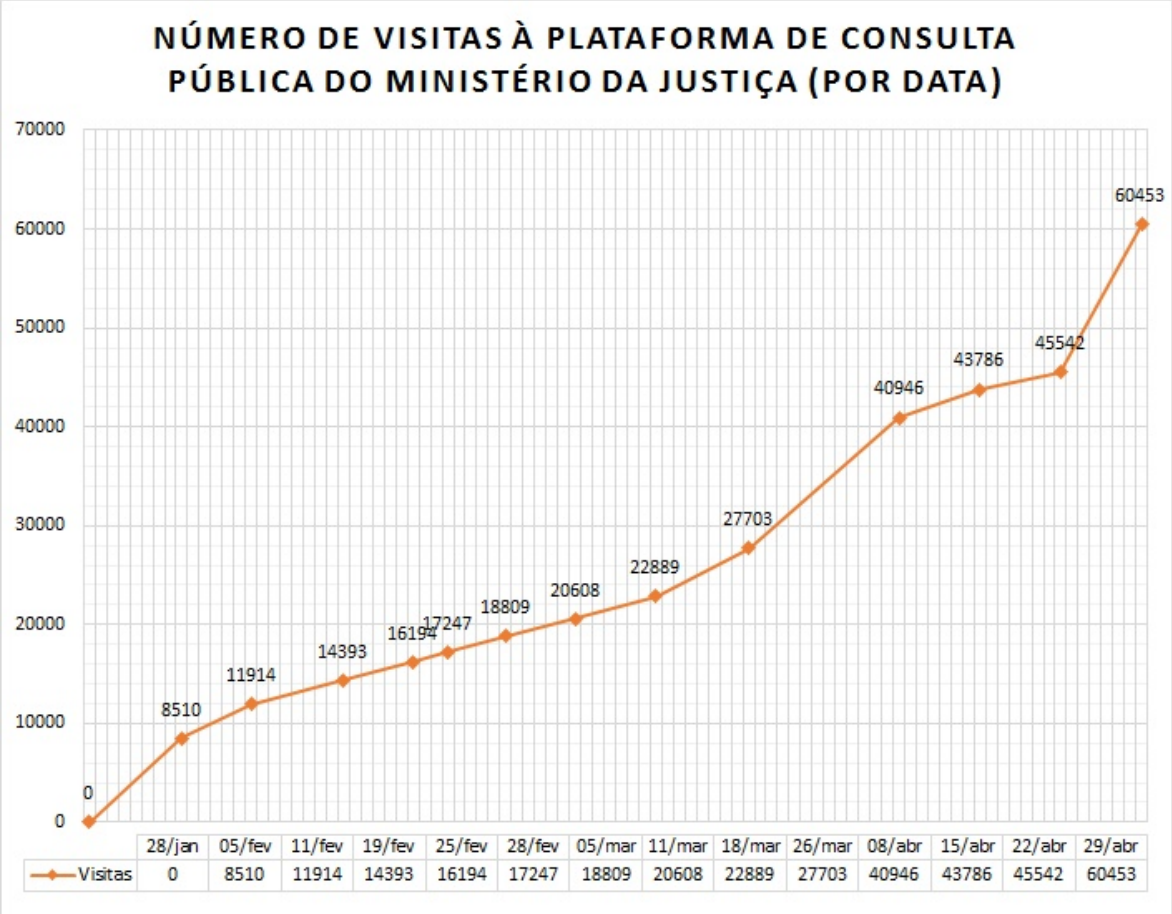
(A) "*Ressaltamos que inciso III do artigo 25 do Marco Civil da Internet prevê que 'as aplicações de internet de entes do poder público devem buscar (...) compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações'.*

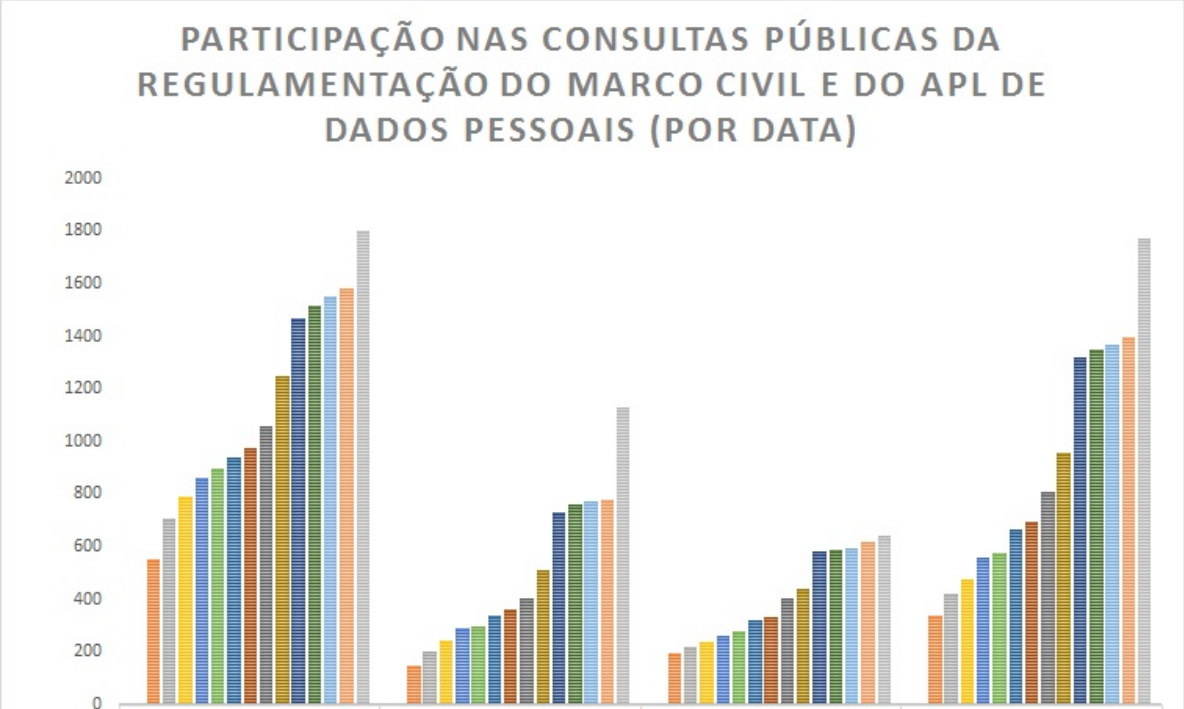
Consideramos a Regulamentação uma excelente oportunidade para nortear, de forma concreta, como o Poder Público deve tratar e disponibilizar seus dados de forma a contemplar a lógica da Web Semântica. É apenas por meio do estabelecimento de requisitos técnicos de comunicação para a operacionalização de dados, bem como pela obrigatoriedade de adoção de dados padronizados, que uma efetiva política de dados abertos pode gerar resultados concretos que aprimorem os mecanismos democráticos da sociedade.

*Não são poucos os casos em que informações são disponibilizadas, contudo, seus diferentes formatos impedem a real apropriação por parte de atores interessados e relevantes no debate da democracia digita*l".

Autor da proposta: *Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI)*

6. GRÁFICOS DO PERFIL QUANTITATIVO DA PARTICIPAÇÃO





	Número de usuários	Comentários sobre a regulamentação do Marco Civil	Comentários sobre o APL Dados Pessoais	Comentários Total
28/jan	0	0	0	0
05/fev	552	147	194	341
11/fev	707	204	219	423
19/fev	789	241	235	476
25/fev	865	292	264	556
28/fev	900	300	278	578
05/mar	941	341	322	663
11/mar	974	364	334	698
18/mar	1058	402	406	808
26/mar	1248	513	443	956
01/abr	1469	732	585	1317
08/abr	1516	759	589	1348
15/abr	1554	773	592	1365
22/abr	1581	780	616	1396
29/abr	1802	1131	641	1772