

PROJETO DE LEI DO SENADO Nº , DE 2014

Altera a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O CONGRESSO NACIONAL decreta:

Art. 1º O inciso VII do art. 7º da Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação, revogando-se a alínea “c” do inciso VIII e o inciso IX:

“**Art. 7º**

VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo nas hipóteses previstas em lei;

VIII.....

c) REVOGADO

IX – REVOGADO

.....” (NR)

Art. 2º O inciso IV do § 2º e o § 3º do art. 9º da Lei da 12.965, de 23 de abril de 2014, passam a vigorar com a seguinte redação:

“**Art. 9º**

§ 2º.

IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais e de degradar o tráfego de serviços de outros fornecedores.

.....” (NR)



SF/14851.45486-96

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

Art. 3º O § 3º do art. 11 da Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação:

“**Art. 11.**

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar ao Comitê Gestor da Internet informações que permitam a verificação do cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento e ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

.....” (NR)

Art. 4º O *caput* do art. 13 da Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação:

“**Art. 13.** Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de enviar os registros de conexão ao Comitê Gestor da Internet no Brasil (CGI.br), conforme os parâmetros técnicos por ele definidos, e de manter esses registros, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano.” (NR)

Art. 5º Acrescente-se à Lei nº 12.965, de 23 de abril de 2014, o seguinte art. 13-A:

“**Art. 13-A.** O poder público, em todas as suas esferas, para armazenamento, gerenciamento e disseminação de dados utilizará, exclusivamente, estruturas localizadas em território nacional.”



Art. 6º O *caput* do art. 15 da Lei da 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação:

“**Art. 15.** O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá, conforme os parâmetros técnicos definidos pelo Comitê Gestor da Internet no Brasil (CGI.br), enviar os registros de acesso a aplicações de internet a esse Comitê e manter os respectivos registros, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses.

.....” (NR)

Art. 7º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Apesar do imenso avanço representado pela aprovação do Marco Civil da Internet, um instrumento jurídico avançado, moderno e que responde à boa parte dos desafios trazidos com a implementação da rede mundial de computadores, julgo adequado que assim como a rede tem evoluído, este texto também incorpore alterações que não puderam ser apreciadas no debate no Senado, mas que aperfeiçoam, clarificam e reforçam os princípios exarados na Lei 12.695/14. As mudanças propostas neste projeto de lei são fruto de um grande debate com os atores desta nova realidade tais como os usuários da rede, as empresas do setor e também as ações de transparência e eficiência do poder público alcançadas com as novas tecnologias.

O presente Projeto de Lei apresenta em seu Artigo 1º alterações no artigo 7º que visam aprimorar os mecanismos de proteção à intimidade e à privacidade já presentes no texto.

O usuário da internet está sujeito a contratos e termos de uso que, por falta de clareza, podem subordiná-lo a regras desfavoráveis relativas à utilização de seus dados pessoais.



Da mesma forma, a política de adesão adotada pelas empresas tem condicionado a utilização dos serviços e aplicativos fornecidos à concordância com suas regras de uso de dados pessoais. Desse modo, os usuários acabam por aceitar qualquer política de privacidade imposta sob pena de não ter acesso ao serviço ou conteúdo de seu interesse.

Por essas razões, o fornecimento de dados pessoais a terceiros somente deve se restringir às hipóteses previstas em lei. É uma limitação razoável e suficientemente ampla, que melhora o equilíbrio entre o direito dos usuários e o dos provedores.

Os dispositivos suprimidos tratam dos mecanismos de informação ao usuário da internet sobre a coleta, o uso, o armazenamento e o tratamento de seus dados pessoais, bem como sua utilização pelos provedores de serviço.

Ainda que o texto aprovado pelo Congresso Nacional tente conferir proteção à privacidade e ao sigilo das comunicações dos internautas especificando que o uso de seus dados somente ocorrerá “mediante consentimento livre, expresso e informado”, sabe-se que os contratos de adesão e termos de utilização celebrados com os provedores de serviços são extensos e complexos. Com isso, é difícil para o usuário da internet ter disponibilidade para ler e, de fato, compreender em que medida permitem a utilização de seus dados pessoais por essas empresas.

A dificuldade se acentua pelo fato de, a cada aplicação que o usuário deseja acessar, ser necessário cancelar um novo contrato de prestação de serviços e de uso de dados pessoais. Para agravar esse cenário, os provedores modificam, periodicamente, suas políticas de privacidade, requerendo dos usuários concordância com um novo contrato. Na prática, é inviável a qualquer pessoa, mesmo aos mais experientes usuários, dominar todas as disposições e variações desses muitos contratos.

Ademais, a maioria das empresas condiciona o uso de seus serviços e aplicativos à concordância com suas políticas de uso de dados pessoais. Trata-se, portanto, de contratos de adesão, sobre os quais os usuários não têm poder de gerência ou possibilidade de negociação. De tal modo, efetivamente, são obrigados a aceitar qualquer política de privacidade apresentada pelos provedores, sob pena de não ter acesso ao serviço ou conteúdo desejados.

Por essas razões é necessário estabelecer claramente que o uso, o armazenamento e o tratamento dos dados pessoais dos usuários da



Internet somente poderão ocorrer para finalidades que (a) justifiquem sua coleta e (b) não sejam vedadas pela legislação, conforme já previsto nas alíneas ‘a’ e ‘b’ do inciso VIII do art. 7º. São limitações razoáveis e suficientemente amplas, que melhoram o equilíbrio entre o direito dos usuários e o dos provedores.

Outra preocupação que buscamos clarificar com o presente Projeto é a Neutralidade de Rede. Os dispositivos do projeto do Marco Civil da Internet que garantem a efetiva neutralidade de rede são indispensáveis para manter suas características de inovação, de livre concorrência e de liberdade de expressão, tais como definidas no Capítulo I da proposição. Nesse sentido, a precisa delimitação das formas e condições em que serão possíveis práticas de discriminação e de degradação do tráfego é essencial para evitar abusos ou interpretações equivocadas.

O atual texto do inciso IV do § 2º do art. 9º estabelece a proibição de condutas anticoncorrenciais na discriminação do tráfego. Contudo, essa é uma determinação genérica, passível de interpretações nem sempre adequadas ao interesse público.

Por essa razão, mostra-se necessário alterar o texto do dispositivo em tela pela adição de trecho que explicita a vedação da degradação do tráfego de serviços de outros fornecedores. Com esse ajuste, não será possível utilizar subterfúgios para prejudicar a livre concorrência na internet, o que beneficiará todos os usuários.

A redação atual do § 3º do art. 9º da Lei 12.695/14 determina que é vedado bloquear, monitorar, filtrar ou analisar o **conteúdo** dos pacotes de dados, “respeitado o disposto neste artigo”. Note-se que a expressão em destaque pode provocar a interpretação equivocada de que há situações em que o conteúdo dos pacotes de dados pode ser monitorado ou analisado.

Monitorar ou analisar o conteúdo dos pacotes de dados que trafegam na rede equivale a acessar o efetivo conteúdo das informações postadas, em quaisquer formatos, sejam de texto, sejam de áudio, sejam de imagem ou de vídeo. Dessa maneira, a atual redação do dispositivo abre margem para que os provedores de conexão e os demais responsáveis pelo tráfego na rede procedam a quebra do sigilo das comunicações dos usuários da internet à revelia do Poder Judiciário.

No Brasil, o acesso ao conteúdo das comunicações de qualquer pessoa depende de específica ordem judicial. Mesmo nesse caso,



não caberia ao provedor de conexão, de transmissão ou de roteamento o monitoramento ou a análise do conteúdo dos dados. Essas empresas devem restringir-se a disponibilizar o conteúdo ao conjunto de entes estatais responsável pela investigação. Somente os agentes públicos diretamente envolvidos com a investigação é que devem ter acesso ao conteúdo dos dados monitorados.

As técnicas de monitoramento do conteúdo dos pacotes, geralmente denominadas de *deep packet inspection* (DPI), são sabidamente utilizadas por governos autoritários para coletar dados individuais e para censurar o tráfego de determinados conteúdos pela internet. São usos que não se compatibilizam com os fundamentos e princípios elencados no Capítulo I do Marco Civil da Internet, nem com os direitos estabelecidos no art. 7º.

Portanto, para que não haja brechas legais para violações do sigilo das comunicações dos usuários da internet, torna-se imperativo o acatamento da alteração proposta.

O Brasil dispõe de um sistema de governança da Internet lastreado na participação de cidadãos, empresas e governo referenciado e admirado em todo o mundo. Baseada nesta constatação, objetivamos com este Projeto, também reforçar o papel deste modelo avançado e participativo.

Os artigos 3º, 4º e 6º aperfeiçoam o texto neste sentido. No artigo 3º propomos a modificação do § 3º do art. 11 do projeto de Marco Civil da Internet, para substituir a expressão “na forma da regulamentação” pela expressão “ao Comitê Gestor da Internet”.

São dois os objetivos da alteração proposta. Inicialmente, a emenda busca conferir eficácia imediata ao dispositivo, evitando que a demora na elaboração da regulamentação originalmente prevista retarde a aplicação do texto legal.

No artigo 4º buscamos fortalecer o papel do CGI.br em prol da melhoria da qualidade e da segurança da internet para todos os usuários brasileiros.

No artigo 6 objetivamos alterar o art. 15 da Lei 12.695/14 para determinar que, além de manter os registros de acesso a aplicações de internet sob sigilo pelo período de 6 meses, os provedores de aplicações



também deverão enviar esses registros ao Comitê Gestor da Internet no Brasil (CGI.br).

Adicionalmente, deve-se ressaltar que, como definido no Decreto nº 4.829, de 3 de setembro de 2003, o Comitê Gestor da Internet no Brasil (CGI.br) é a instituição responsável pela elaboração de procedimentos, normas e padrões técnicos e operacionais para a segurança das redes e serviços da internet.

Dessa forma, para aperfeiçoar sua atuação, entendemos que o CGI.br deva receber as informações pertinentes que permitam a verificação do cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

Por fim, apresentamos no artigo 5º, uma preocupação premente com a segurança de dados estratégicos do nosso país. Recentemente, foi noticiada a existência programas de monitoramento da internet realizados por governos estrangeiros. Entre os alvos desses programas, estavam autoridades e empresas brasileiras. Trata-se de evidente violação do sigilo das comunicações, com implicações para a intimidade e a privacidade das pessoas, as relações comerciais de empresas brasileiras, e mesmo as ações governamentais. Também há nítida violação da soberania nacional.

Para mitigar o monitoramento das comunicações estratégicas brasileiras, produzidas e trafegadas pelos órgãos do poder público, propõe-se que o armazenamento, gerenciamento e disseminação de seus dados deva ser realizada, exclusivamente, em território nacional.

Portanto, a fim de evitar a violação de dados de cidadãos e de empresas brasileiras constantes dos bancos de dados governamentais, e como forma de submeter qualquer eventual infração à Justiça do Brasil, é necessário que esses dados se localizem no território nacional. Dessa maneira, não poderão ser interceptados por empresas ou governos estrangeiros sem que os responsáveis sejam submetidos à lei brasileira.

Senadora VANESSA GRAZZIOTIN

PCdoB/Amazonas



LEI Nº 12.965, DE 23 ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.



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

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

II - agir com proporcionalidade, transparência e isonomia;

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

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

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

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

