Comitê Gestor da Internet no Brasil

Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei

12.965/2014 – o Marco Civil da Internet

1. Introdução

O Comitê Gestor da Internet no Brasil – CGI.br, criado pela Portaria Interministerial nº 147, de 31 de maio de 1995, e posteriormente regulamentado pelo Decreto 4.829, de 3 de setembro de 2003, conforme suas atribuições bem como o que foi estabelecido pelos Artigos 9º e 24 da Lei 12.965, de 23 de abril de 2014, apresenta sua contribuição ao processo de regulamentação do Marco Civil da Internet (MCI), que se dará pela edição de Decreto Presidencial, nos termos do artigo 84, inciso IV, da Constituição Federal.

As contribuições aqui apresentadas tratarão de três tópicos: 1) hipóteses de discriminação de pacotes de dados na Internet e degradação de tráfego a serem admitidas nos termos do § 1º, do Art. 9º, do MCI, com fundamento em requisitos técnicos; 2) aspectos relacionados à proteção de registros, dados pessoais e comunicações privadas; e 3) guarda de registros de conexão e de acesso a aplicações de Internet. Em particular, esclarecemos que as contribuições deste documento não tratam de questões relacionadas a modelo de negócios.

Destacamos que as propostas apresentadas com esta contribuição, além de terem como base a legislação brasileira em vigor, orientaram-se pelas boas práticas assentadas internacionalmente no ecossistema de governança da Internet.

2. A Internet

A Internet é uma “rede de redes” de alcance global. Com base em uma estrutura aberta, é composta por uma coleção de “redes” definida por Sistemas Autônomos que se relacionam de forma estruturada por meio da arquitetura de protocolos TCP/IP. Os protocolos dessa arquitetura são definidos num foro mundial e aberto denominado IETF (Internet Engineering Task Force), em um processo de discussão e consenso.

Sistema Autônomo (AS), cf. RFC 1930, é uma rede ou um grupo de redes IP sob uma única administração, a qual determina como trafegar e distribuir os pacotes de dados em seu interior. A integração dos diversos sistemas autônomos que conformam a Internet é implementada por meio de um protocolo adotado por todos que dela participam, o BGP (Border Gateway Protocol) (cf. RFC 4271).

Na Internet, vige o regime da livre iniciativa e inovação: não é necessária autorização prévia para se criar um novo serviço ou aplicação, desde que seguidas as recomendações técnicas do IETF.

As redes de telecomunicações existentes em cada país servem como alternativas de suporte para o funcionamento da “rede de redes” que é a Internet. Apesar de estarem intimamente relacionadas, Internet e telecomunicações são atividades distintas.

É importante frisar que há serviços específicos, como “links” dedicados, circuitos virtuais e VPNs que, mesmo utilizando internamente o protocolo TCP/IP e a estrutura da Internet, não se confundem com a Internet. Tais serviços são específicos e seu propósito é distinto do serviço de conexão à Internet.

3. A Neutralidade de Rede

Conceito geral: O princípio da neutralidade de rede previsto na Lei 12.965/2014 consiste na garantia de tratamento isonômico dos pacotes de dados pelas redes dos sistemas autônomos sem degradação nem discriminação por conteúdo, origem e destino, serviço, terminal ou aplicação (cf. MCI, Art. 9º).

Na transmissão, comutação ou roteamento estão sujeitos ao cumprimento da obrigação de dar tratamento isonômico aos pacotes de dados na Internet no Brasil: O administrador de Sistema Autônomo, a quem são designados um ou mais blocos de endereços IP pelo NIR (“National Internet Registry”) brasileiro, que é o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), em conformidade com as resoluções do Comitê Gestor da Internet no Brasil (CGI.br), e que utiliza tais endereços para prover serviços ou acesso a terceiros; As entidades que se destinam a prover acesso à Internet a usuários e às quais forem delegados sub-blocos específicos de endereços IP por parte de um Administrador de Sistema Autônomo.

3.1 Hipóteses de discriminação de pacotes de dados na Internet e de degradação de tráfego que serão admitidas

A discriminação dos pacotes de dados na Internet e a degradação de tráfego somente poderão ocorrer como medida excepcional devida a fatores ocasionais e com base em justificativas razoáveis, para atender: 1) aos requisitos técnicos indispensáveis à adequada prestação dos serviços e aplicações; e 2) à priorização de serviços de emergência.

O gerenciamento rotineiro de tráfego poderá ser realizado desde que em conformidade com os padrões técnicos universalmente aceitos.

Por discriminação, entende-se qualquer ação que implique bloqueio, redirecionamento, filtragem e/ou diferenciação de pacotes de dados na Internet. Por degradação, entende-se o resultado da ação que interfere no tráfego propositalmente, prejudicando de qualquer forma a transmissão de pacotes de dados na Internet.

3.2 Requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações

Na Internet, entende-se por “requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações” aqueles que devem ser observados pelo responsável pela transmissão, comutação ou roteamento, no âmbito de sua respectiva rede e até os limites de suas bordas, que visem à preservação da estabilidade, da segurança e da integridade de suas redes, e de serviços fundamentais como endereçamento, resolução de nomes e interligação com redes de outros AS's.

Os requisitos técnicos indispensáveis aqui tratados referem-se apenas aos casos em que ações de discriminação de pacotes de dados na Internet e/ou de degradação de tráfego são absolutamente indispensáveis para garantir que seja preservado o encaminhamento possível de pacotes de dados na Internet. Tais ações serão consideradas requisitos técnicos indispensáveis:

Se sua ausência inviabilizar a conectividade à Internet contratada; e/ou

Quando, em situações contingenciais (ex.: tempestade solar que interfira na comunicação via satélite; rompimento de cabo submarino), sua ausência ocasionar desequilíbrio entre os clientes do provedor, mas de forma a minimizar o prejuízo a outras partes interessadas; e/ou
Quando houver escassez momentânea de recursos de telecomunicações, tais como capacidade disponível das redes.
Nas hipóteses acima, o prazo para regularização do serviço deve ser informado de maneira clara e transparente a todas as partes interessadas, levando-se em conta a complexidade envolvida em cada caso ou a eventual sobrevenda de banda.

Em ações gerais, como as acima descritas, os provedores de serviços e as aplicações devem ser tratados de forma isonômica, com base em padrões universalmente aceitos, sendo vedada a prática de medidas anticoncorrenciais por parte dos responsáveis pela transmissão, comutação ou roteamento.

3.2.1 Situações notórias de segurança em que serão admitidas a discriminação dos pacotes de dados na Internet e a degradação de tráfego

São exemplos de situações notórias de segurança de rede em que serão permitidas práticas de discriminação de pacotes de dados na Internet e a degradação de tráfego para a mitigação de prejuízos à prestação de serviços e acesso à Internet:
Filtragem de endereços IP específicos para mitigação de DoS (Negação de serviço, ou Denial of Service): admite-se filtragem de endereços IP envolvidos na origem de um ataque DoS, técnica pela qual um atacante, valendo-se tipicamente de recursos arregimentados de alguma forma na rede (DDoS – Distributed Denial of Service), visa a tirar de operação um serviço ou aplicação.
Bloqueio da porta 25 (SMTP – Simple Mail Transfer Protocol): admite-se e estimula-se o bloqueio da porta 25 para o combate a spam (correio eletrônico não solicitado, geralmente enviado para um grande número de usuários). Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail).
A exclusivo pedido do usuário final discriminações tais como controle parental poderão ser implementadas pelo provedor de acesso na relação provedor-usuário.

3.3 Priorização de Serviços de Emergência

De acordo com o Artigo 9º da Lei 12.965/2014 (inciso II, § 1º), será admitida a discriminação de pacotes de dados na Internet e/ou a degradação de tráfego quando houver necessidade de priorização de serviços de emergência, como forma de possibilitar atendimento imediato a situação emergencial ou condição de urgência, em que eventual demora ou atraso na resposta possa frustrar sua finalidade.

4. Privacidade, proteção aos registros e guarda de logs

4.1 Introdução

A regulamentação da Lei 12.965/2014 também disporá regras no que diz respeito à proteção aos registros, aos dados pessoais e às comunicações privadas e à guarda de registros de conexão e de acesso a aplicações de Internet(também comumente referidos como logs). Conforme garantido no Marco Civil da Internet, “a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas” (Art. 10, caput).

Um log é um registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados. É um termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo, de conexão (informações sobre número IP, incluída a data e hora de seu uso, atribuído a um computador ou

dispositivo que utiliza a Internet) e de acesso a aplicações (informações de acesso de um computador ou dispositivo a uma aplicação de Internet).

Conforme previsto no Marco Civil da Internet:

Registro de conexão é o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. Aplicações de Internet são o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet. Os registros de acesso a aplicações de Internet, por sua vez, são o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

4.2 Escopo de incidência para a regulamentação:

O que é específico na Internet é o número associado a cada dispositivo que a utiliza, conhecido como endereço IP. Nos termos do art. 5o, inciso III, do MCI, endereços IPs identificam terminais (dispositivos), não pessoas;
Ao endereço que identifica um dispositivo deve-se adicionar a data e hora, devidamente especificadas em UTC e sincronizadas via NTP (Network Time Protocol);
O provedor deverá informar de modo claro e transparente os parâmetros de segurança e infraestrutura empregados na guarda e controle dos registros dos clientes;
A requisição de acesso aos registros deve ser necessariamente direcionada ao poder Judiciário (artigo 10, par. 1o.), a quem compete expedir a ordem que autoriza a disponibilização dos dados;
O decreto não pode ampliar o conjunto de informações que compõem os registros de conexão e de acesso a aplicações de Internet;
Ordem judicial pode ampliar a guarda prospectiva de informações adicionais desde que viável tecnicamente. O prazo de extensão da guarda será definido pelo próprio juiz;
Na provisão de serviço de conexão à Internet, apenas os administradores de sistemas autônomos ISP têm obrigação de guardar registros de conexão. Demais empresas, organizações e indivíduos que ofereçam algum tipo de conexão à Internet e não são administradores de AS's não estão obrigados a essa guarda.

4.3 Para a necessária preservação da intimidade e privacidade do usuário:

1) O acesso aos dados cadastrais independentemente de ordem judicial por autoridades somente deverá ocorrer nas hipóteses determinadas em Lei. Por exemplo, Lei n.º 12.850/2013 (Lei das Organizações Criminosas) ou na Lei n.º 9.613/1998 (Lei da Lavagem de Dinheiro, tal como reformada pela Lei n.º 12.683/2012);

2) O usuário final deve ter informação clara sobre o início e o término esperado da guarda dos registros de conexão e de acesso a aplicações de Internet, bem como do procedimento para que se formalizem solicitações para o fornecimento dessas informações.

3) Ordem judicial que determine a guarda de logs por prazo superior ao expresso no Marco Civil da Internet deve observar, em cada caso, o tempo remanescente do prazo prescricional pertinente, conforme o previsto no ordenamento jurídico nacional.