

## **1. Wi-Fi - Riscos e limites da responsabilidade pelo compartilhamento**

---

### **Wi-Fi - Risks and limitations of liability sharing**

**TARCISIO TEIXEIRA**

*Doutor e Mestre em Direito Empresarial pela Faculdade de Direito da USP. Professor adjunto de Direito Empresarial da Universidade Estadual de Londrina-PR (UEL). Autor de várias obras. Palestrante, parecerista, advogado e consultor de empresas. [tarcisioiteixeira@tarcisioiteixeira.com.br](mailto:tarcisioiteixeira@tarcisioiteixeira.com.br)*

#### **Sumário:**

Introdução

1. Marco Civil da Internet

2. Compartilhamento de Wi-Fi

3. Riscos e atribuição de responsabilidade

Considerações finais

Bibliografia

#### **Área do Direito: Civil**

#### **Resumo:**

O presente artigo tem por fim analisar quais são os riscos e as responsabilidades das pessoas, empresas e instituições que compartilham com outros o acesso à Internet via Wi-Fi. Para tanto, foram analisadas disposições do Marco Civil da Internet (Lei 12.965/2014), conceitos jurídicos e técnicos, sobretudo acerca das operações tecnológicas que envolvem o compartilhamento para acesso à Internet sem fio, com o fim de se apontar qual é o nível de responsabilidade para os agentes envolvidos nesse tipo de situação.

#### **Abstract:**

This article aims to analyze what the risks and responsibilities of individuals, businesses and

institutions that share with others access to the Internet via Wi-Fi. To this end, provisions have analyzed the Civil Marco Internet (Law 12.965/2014), legal concepts and technicians, especially concerning the technological operations that involve sharing for free access to the Internet in order to point out what level responsibility for the agents involved in this type of situation.

**Palavra Chave:** Compartilhamento de Wi-Fi - Acesso à Internet - Riscos - Responsabilidade.

**Keywords:** Wi-Fi sharing - Internet access - Risks - Responsibility.

## Introdução

É cada vez mais comum o acesso à Internet sem o uso de fio, o que se tem chamado de Wi-Fi, tratando-se de uma abreviação de *wireless fidelity* (“fidelidade sem fio”). Wireless ou Wi-Fi é uma tecnologia de comunicação sem o uso de cabos, que pode ser feita por frequência de rádio, por exemplo. Dessa forma, o usuário pode se conectar à rede mundial de computadores sem a necessidade de usar cabeamento.

Tal sistema de acesso à Internet pode ser usado de forma restrita, por exemplo, no ambiente doméstico; ou de forma ampla, como no caso de empresas que fornecem esse serviço não só aos colaboradores como aos seus clientes. Para muitas empresas, o fornecimento de Wi-Fi tem sido considerado indispensável pelos seus clientes, no caso de hotéis, academias, escolas, companhias de transporte rodoviário etc. Esse fornecimento geralmente é dado como cortesia.

O serviço de acesso sem fio pode ser utilizado de forma aberta ou fechada. No sistema aberto, o usuário não precisa de prévio cadastro ou mesmo de chave/senha para usar o serviço Wi-Fi que está sendo oferecido. Já no sistema fechado, o usuário precisa obter a chave/senha, que pode ser fornecida livremente a qualquer um que esteja naquele ambiente (sendo muitas vezes ostentadas em painéis de aviso); ou a senha é entregue mediante prévio cadastro junto à instituição que está oferecendo o serviço (o que seria mais adequado).

## 1. Marco Civil da Internet

Para tratarmos da responsabilidade daquele que fornece acesso à Internet a terceiros por meio de *Wi-Fi* é indispensável analisarmos o que dispõe o Marco Civil da Internet (Lei 12.965/2014), que em seu art. 13<sup>1</sup> inaugura o tratamento jurídico a respeito da guarda de logs, sem prejuízo do cotejamento com outros dispositivos legais e questões técnicas relacionadas.

Log é uma expressão empregada para descrever os rastros (histórico) em um sistema eletrônico. Os logs são importantes meios de prova computacional, pois permitem a identificação de quem praticou certo ato em ambiente eletrônico, incluindo ilícitos de cunho civil e penal. O log também é conhecido como log de dados.

Por sua vez, *provedor de conexão* (ou de acesso) é aquele que oferece ao usuário o serviço de conexão à Internet. Nos termos do art. 5.º, II c/c o inc. V, do Marco Civil da Internet, conexão à Internet é a habilitação de um terminal (computador ou qualquer dispositivo que se conecte à Internet) para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP – Internet Protocol (número de identificação do computador para fins de registro de conexão).

Conceitualmente, *administrador de sistema autônomo* é “a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP

geograficamente referentes ao País [CGI.br]" (Lei 12.965/2014, art. 5.º, IV).

Esse conceito, a princípio, diz respeito ao provedor de conexão (acesso) que tem a finalidade de conectar o usuário por meio do roteamento (encaminhamento)<sup>2</sup> de IPs, cujo bloco ele administra por delegação do CGI.br, entidade na qual deve estar devidamente cadastrado. Assim, os provedores de acesso são os responsáveis pela conexão, devendo manter condições de privacidade e que permitam a identificação dos seus clientes.

Por "sistema autônomo" deve-se considerar a rede capaz de divulgar seus blocos de endereços IP para os seus usuários que visam acessar a Internet. Ou seja, o sistema autônomo deve possuir os seus próprios endereços IP registrados junto à autoridade competente para assim distribuí-los via roteamento.<sup>3</sup>

Não é uma regra universal, mas normalmente pequenos usuários (como para fins residenciais ou empresas de menor porte) utilizam-se das redes de provedores de acesso (que detém endereços de IP), que por sua vez são considerados "sistemas autônomos". Dessa forma, o computador ou a pequena rede local do usuário faz parte do sistema autônomo de um provedor.

No entanto, também não sendo uma regra absoluta, muitas instituições (normalmente de grande porte) podem ser um sistema autônomo, como, por exemplo, bancos, seguradoras, universidades, órgãos públicos etc. São casos de "grandes usuários" que podem se cadastrar no CGI.br para receber e administrar blocos de IPs específicos e assim roteá-los como melhor lhe convier (por exemplo, entre colaboradores, clientes etc.). O CGI.br usa a expressão "usuários finais" para as organizações que utilizam os endereços IP exclusivamente em suas próprias infraestruturas. Nesta situação há uma equiparação destes usuários aos provedores de acesso em sentido amplo.

Dessa forma, o art. 5.º, IV, contempla duas possibilidades de sistema autônomo: provedor de acesso (conexão) em sentido estrito e o provedor de acesso em sentido amplo, que contempla qualquer instituição que detenha bloco de IPs para administrá-lo e roteá-lo. É por isso que na definição do referido dispositivo não se emprega expressamente a expressão provedor, valendo o mesmo comentário em relação ao *caput* do art. 13.

Porém o que acontece quando o provedor de acesso fornece um endereço IP ao modem de um usuário? Neste momento, tal provedor deve fazer o registro da conexão e, para ele, qualquer acesso à Internet que advenha daquele usuário será registrado com o número de IP que foi atribuído naquela conexão, independentemente dos endereços IP atribuídos aos dispositivos na rede local daquele usuário. A partir desse momento, o provedor tem condições de monitorar os acessos que aquele usuário faz, porém não o pode fazê-lo por vedação do art. 14 do Marco Civil. Isso seria considerado invasão de privacidade, uma vez que o provedor de acesso centralizaria todo o histórico de navegação dos seus usuários. Entretanto, o art. 13 determina a guarda dos registros de conexão por um ano.<sup>4</sup>

## 2. Compartilhamento de Wi-Fi

Considerando que atualmente é muito normal se compartilhar o acesso à Internet, por Wi-Fi em empresas, escolas, lojas de varejo, academias e até mesmo nas residências, pode-se questionar: aquele que é proprietário de um estabelecimento ou residência que fornece a *chave/senha* do Wi-Fi pode ser considerado sistema autônomo para fins de aplicação das regras do Marco Civil? Vale lembrar que alguns sequer se utilizam de chave, o acesso é simplesmente livre. A resposta vai depender se há o enquadramento no conceito de sistema autônomo. Normalmente estabelecimentos

empresariais e residências não o são, portanto, num primeiro olhar não poderiam ser responsabilizados como tal. Mas, para uma resposta mais precisa, precisaremos de uma análise mais apurada das questões que envolvem o tema.

Visando trazer luz à questão, entendemos ser válida uma breve explicação de como o acesso à Internet chega até o usuário residencial ou empresarial, bem como a definição de quem exerce qual função no processo de conexão com a Internet, além das formas de conexão, via cabo ou sem fio, dentro do ambiente local do usuário.

A ICANN - *Internet Corporation for Assigned Names and Numbers* (em português, Corporação da Internet para Atribuição de Nomes e Números) é a entidade americana responsável, a nível mundial, por zelar pela estabilidade operacional da Internet, pela alocação do espaço de endereços IP, pela atribuição de identificadores de protocolo e a administração do sistema de nomes de domínio. A ICANN, por meio de entidades regionais (como o Comitê Gestor da Internet no Brasil - CGI.br), atribui endereços IP aos provedores de acesso (muitas vezes ligados ao setor de telecomunicações) ou aos "usuários finais" (grandes instituições que administram blocos de IP exclusivamente). Utilizando-se dos provedores de backbones (detentores da estrutura de cabeamento de altíssima velocidade capazes de interligar redes de cidades, nações e continentes entre si), os provedores de acesso podem conectar-se aos servidores gerenciados pela ICANN.

Entre o usuário (residencial, empresarial, governamental ou não) e o provedor de acesso pode haver a figura de outro provedor que denominamos como provedor intermediário (ou provedor de serviço<sup>5</sup>), que identifica o usuário (por exemplo, via um e-mail e senha de conexão) e assim conecta-o à rede do provedor de acesso, para aí alcançar a Internet. O provedor intermediário não desenvolve necessariamente a mesma atividade do provedor de acesso, pois é um autenticador que não é indispensável para a conexão do usuário à Internet (como determina a Res. Anatel 614/2013, art. 6.º c/c os arts. 10, 4.º, VII e 3.º, *caput*, do Regulamento do Serviço de Comunicação Multimídia - Anexo I da referida Resolução.<sup>6</sup> Essa temática já era objeto de decisão judicial). Isso ocorre, por exemplo, no caso de operadoras que oferecem conexão de banda larga à Internet via cabo a qual dispensa o serviço do provedor intermediário.

Visando deixar um pouco mais clara a diferença entre o provedor de acesso e o provedor intermediário, vamos fazer uma analogia. José foi convidado para ir à festa de um amigo, que colocou seu nome em uma lista de convidados. Quando José chega à festa, há um recepcionista a quem ele diz o seu nome. O recepcionista confere se o nome do José está na lista. Se não estiver, ele não entrará na festa; estando na lista, o recepcionista diz para o coordenador da festa que José é um convidado legítimo e que pode entrar. O coordenador da festa entrega para José uma credencial daquele lugar e libera sua entrada na festa.

Em nosso contexto: o provedor intermediário é o "recepcionista da festa", que confere se o usuário pode utilizar aquele serviço. O "coordenador da festa" é o provedor de acesso a quem o usuário precisa ser conectado para acessar a Internet. "José" representa o modem do usuário. Assim, a atitude do recepcionista em informar ao coordenador da festa que José é um autêntico convidado é a efetivação da conexão com a Internet. A "credencial" é o endereço IP e a "festa" a rede mundial de computadores.

Por isso é que a Internet é conhecida como a "rede das redes de computadores" ou "rede mundial de computadores". Isso pois, a rede de computadores do usuário (ou mesmo que seja apenas um terminal) se conecta à rede do provedor de acesso (podendo haver a autenticação de um provedor intermediário), que, por sua vez, se conecta via backbone à rede dos servidores gerenciados pela

ICANN.

A tarefa de conectar uma rede à outra ao longo deste processo é feita por um aparelho chamado roteador (dispositivo que encaminha pacotes de dados entre redes de computadores), cujo porte adequado varia conforme o seu ambiente. O roteador utilizado na residência ou empresa do usuário é muito mais simples do que aquele utilizado para interligar um provedor de acesso à rede administrada pela ICANN, mas todos possuem a mesma função essencial: permitir a comunicação bidirecional (ou interoperabilidade) entre diferentes redes computacionais.

Até aqui procuramos explicar o que acontece com o modem do usuário para fora. Dentro da residência ou do estabelecimento do usuário ocorre um processo similar: conecta-se um aparelho roteador ao modem de Internet, sendo o roteador configurado (de fábrica ou pelo usuário) para formar uma rede local com e/ou sem fio (conforme o modelo do roteador) capaz de acessar a Internet por meio do modem a ele conectado. O roteador atribuirá um endereço IP (interno) para cada dispositivo a ele conectado. Neste caso estará formada a rede local do usuário, que permitirá o acesso tanto entre os dispositivos e recursos locais (como, por exemplo, um computador acessando o conteúdo de outro ou impressoras etc.) quanto à Internet.

Para todos os efeitos, independentemente do número de internautas que estejam acessando a Internet pelo roteador Wi-Fi de um usuário, para o provedor de acesso será considerada uma única conexão identificada pelo mesmo IP. Assim, a identificação no provedor será unicamente a do número do IP atribuído àquele roteador. Por isso, compartilhar o acesso à web por Wi-Fi nada mais é do que fazer o compartilhamento do IP atribuído pelo provedor de acesso.<sup>7</sup> Entretanto, o roteador Wi-Fi atribui “IPs” internos que podem ser utilizados pelo usuário titular do modem para individualização dos internautas.

Dessa forma, quando quaisquer destes dispositivos desejarem acessar a Internet, o roteador entende qual dispositivo pediu o acesso e o que ele deseja, e assim guarda seu endereço IP. Em seguida, transmite o pedido ao modem que, por já estar conectado ao provedor de acesso, tem condições de acessar os servidores da ICANN para descobrir em qual computador do mundo (desde que conectado à rede) está a informação desejada. Assim, o modem “vai” até aquele computador e “traz” de volta a resposta solicitada, repassando essa resposta ao roteador que a entregará para aquele dispositivo que a solicitou. De forma sintética, esse fenômeno é o que acontece quando um internauta se conecta à Internet. Tudo isso pode acontecer em milésimos de segundos.

Dito isto, percebemos que o usuário empresarial ou doméstico não é responsável pela conexão à Internet em si, pois ele depende de um provedor que forneça a ele um endereço IP que permita seu modem acessar à rede mundial de computadores. Lembrando que o “receptionista”, ou seja, o provedor intermediário, não é necessariamente obrigatório.

Tão importante é o fato de que, quando o internauta utiliza em seu ambiente um dispositivo que se conecta a uma rede, usando fios ou não, ele não está se conectando diretamente à Internet. Isso porque o roteador, de acordo com as configurações de segurança que foram realizadas, pode exigir uma senha para conectar aquele dispositivo à rede local sem fio por ele formada para atribuir a ele um endereço IP válido naquela rede específica. Contudo, a conexão aqui não é feita à Internet, mas apenas à rede local, sendo que os endereços IP disponibilizados pelo roteador do usuário para os dispositivos (com ou sem fio) não permitem “por si só” o acesso à Internet.

### **3. Riscos e atribuição de responsabilidade**

Tomadas todas as considerações realizadas até aqui, concluímos que “administradores de sistemas autônomos” são os provedores de acesso e as grandes instituições cadastradas no CGL.br para administrar blocos de IP; não contemplando, a princípio, os provedores de backbones ou intermediários, nem os meros usuários (residenciais, empresariais, governamentais ou não) que se conectam à Internet via provedor de acesso. Isso porque são os provedores de acesso (e as grandes instituições) que “administram blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrados no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País [CGL.br]”, conforme o art. 5.º, IV e V, e art. 13, *caput*, do Marco Civil da Internet. Consequentemente, como tratam da “provisão de conexão à Internet”, a estes provedores de acesso (e grandes instituições) cabe o dever de manter os registros de conexão efetuados por seu intermédio.

Importante ressaltar que o usuário, a princípio, não pode ser caracterizado como administrador de sistema autônomo, uma vez que ele, por si mesmo, não é responsável por prover conexões à Internet, pois depende de um provedor de acesso e/ou um provedor intermediário para ter sua conexão estabelecida. Isso vale tanto à pessoa física que cede o acesso de sua conexão sem fio (Wi-Fi) a seus amigos como à pessoa jurídica que oferece o benefício de conexão sem fio à Internet por meio de sua rede local aos seus clientes e colaboradores.

Além disso, poderíamos colocar a questão sob o prisma de não ser a “atividade-fim” do usuário, o que o diferencia do provedor cuja finalidade é a provisão de acesso à Internet. Assim, se alguém tiver isto como atividade-fim ele poderá ser caracterizado como provedor de acesso, devendo neste caso ser registrado “no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País”. Essa seria uma hipótese em que tal usuário poderia ser equiparado a administrador de sistema autônomo. Um risco, portanto. Contudo, uma pessoa física ou jurídica que, tendo contratado o serviço de conexão junto a um provedor para seus propósitos particulares (doméstico ou empresarial), querendo compartilhar o acesso à Internet, não tem a obrigação de se sujeitar ao crivo do CGL.br e/ou da Anatel, seja para utilizar a Internet seja para criar uma infraestrutura local de acesso com ou sem fio (Wi-Fi), ainda que esta infraestrutura local permita acessar a Internet.

Outro risco relevante está na atribuição de responsabilidade quando alguém utiliza o acesso à Internet via Wi-Fi disponibilizado pelo usuário (doméstico ou empresarial) e acaba cometendo um ilícito. Haveria alguma implicação o fato de a chave/senha do Wi-Fi ter sido compartilhada ou obtida por invasão ou outros meios não cordiais? Para o provedor de acesso o endereço IP que ficará registrado em seus controles é o atribuído ao modem daquele usuário titular da rede local.

De toda sorte, o fato de o usuário não ser caracterizado como administrador de sistema autônomo não deveria eximi-lo da observância dos procedimentos de segurança adequados ao uso de rede com ou sem fio. Isso porque evita problemas relacionados à segurança de informações em sua própria rede local (como invasão de sistemas, roubo de senhas, acesso indevido a arquivos e informações confidenciais etc.), bem como evita o uso indevido de sua conexão à Internet por pessoas estranhas ao seu conhecimento e/ou interesse. Para todos os usuários é recomendado recorrer ao auxílio de um especialista para configurar corretamente o acesso à rede sem fio. Sobretudo no caso de usuários que sejam empresas, e demais organizações, também é sugerido solicitar os serviços periódicos de uma consultoria em segurança de informações a fim de verificar os meios mais adequados para minimizar os riscos de incidentes desagradáveis.

Assim, aqueles que compartilham para terceiros o acesso à Internet por Wi-Fi até poderiam ser equiparados a provedores de acesso em sentido amplo, mas não o são (assim como as *lan houses*

também não o são), sobretudo porque não podem ser tidos como “sistema autônomo”. Dessa forma, as regras do art. 13 do Marco Civil são direcionadas àqueles provedores que se enquadrem como sistema autônomo, ou seja, os provedores de conexão em sentido estrito e as grandes instituições que administram blocos de IP e são cadastradas no CGI.br (provedor em sentido amplo).

Contudo, aqueles que compartilham a senha/chave do Wi-Fi, em regra, não são responsáveis se a lei e/ou o contrato não o obrigam. Do contrário, haveria um grande ônus para efeitos de cadastramento de todos aqueles que pretendam utilizar-se do Wi-Fi daquele fornecedor, ou mesmo do proprietário de uma residência. E, sendo isso inviável, o compartilhamento de Wi-Fi gratuito simplesmente tornar-se-ia escasso devido ao risco que isso possa representar.

Tal como no caso de uma empresa que empresta a linha telefônica para um cliente fazer uma ligação, e este acaba utilizando esse canal telefônico para prática de um crime, a empresa não pode ser responsabilizada por isso, salvo conivência. Em caso de eventual responsabilização pelo fornecimento de Wi-Fi, isso deve ser apurada mediante a teoria da culpa (responsabilidade subjetiva) e não pela teoria do risco (responsabilidade objetiva).

Vale ter em conta que os provedores de conexão à Internet não são responsáveis pelos atos danosos de seus usuários, cujo raciocínio aplica-se plenamente ao usuário (residencial, empresarial, governamental ou não) que compartilha Wi-Fi (desde que não seja um sistema autônomo).

Caso fosse atribuída responsabilidade a quem compartilha Wi-Fi pelos atos daqueles que se utilizam do acesso sem fio para praticar algum ilícito, a este deveria ser dado o direito de vigiar o conteúdo do que está sendo acessado, postado, enviado, recebido etc. pelo usuário. Isso seria inconcebível na relação fornecedor-cliente, exemplificativamente, além da violação da privacidade.

A título comparativo, no caso de o *empregador* monitorar o conteúdo do que é acessado pelo seu *colaborador* ao utilizar-se dos equipamentos da empresa, sendo que neste caso não haveria privacidade a ser preservada. Nos casos em que o empregado utiliza-se dos equipamentos e ferramentas da empresa (como o e-mail corporativo), ele acaba por abrir mão de sua privacidade, na medida em que a empresa tem o direito de vigiar o seu funcionário para preservar o seu negócio, bem como sua responsabilidade. Isso porque, conforme o Código Civil, art. 932, III, o empregador é responsável pelos atos de seus colaboradores.

Entretanto, uma empresa que compartilha Wi-Fi, que pode ser usado inclusive pelos seus colaboradores, não poderá monitorar os internautas (sejam empregados, clientes etc.) se estes estiverem utilizando seus equipamentos particulares, como smartphones ou tablets. Nesse caso, estas empresas que compartilham o Wi-Fi estão livres de responsabilidade pelos atos daqueles que utilizam a Internet para a prática de ilícitos (da mesma forma que os provedores de acesso não são responsáveis pelos atos de seus usuários e vendedores de chips de celular não podem ser responsabilizados pelos atos dos compradores). Essa isenção de responsabilidade se dá tanto na esfera civil como na penal. De toda sorte, nunca se deverá perder de vista a teoria geral da responsabilidade civil, sobretudo a questão do nexo de causalidade entre a ação/omissão e o dano.

Afirmamos isso porque criar regras muito rígidas, desprendidas da teoria geral, pode implicar rápida obsolescência ou injustiça. Vejamos duas hipóteses praticadas por um funcionário durante sua jornada de trabalho na empresa. Na primeira, ele pratica um ilícito por meio do seu e-mail corporativo denegrindo a imagem de alguém. Já na segunda, ele posta na sua página do Facebook uma foto que ofende moralmente outra pessoa. Ambas as situações foram praticadas no ambiente de trabalho utilizando os computadores das empresas. Se, por um lado, a empresa é responsável na primeira hipótese, por outro, não o será na segunda. Isso porque, nos termos do art. 932, III, do CC, a

responsabilidade do empregador pelos atos de seus prepostos se dá quando estes estão “no exercício do trabalho que lhe compete ou razão dele”. Assim, no primeiro caso, o funcionário utiliza o e-mail corporativo “em razão do seu trabalho”, por isso a empresa poderá responder pelo uso inadequado da ferramenta fornecida (até porque carrega o seu nome de domínio da empresa na descrição do e-mail). Já no segundo caso, a foto poderia ser postada de qualquer equipamento com acesso à Internet, da casa do usuário, do local onde estuda etc., o que implica a falta denexo causal e, conseqüentemente, a irresponsabilidade do empregador.

Realizadas tais considerações, cabe ao administrador de sistema autônomo (normalmente um provedor de conexão) o dever de manter os registros de conexão por um ano. Frise-se que 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. Os registros devem ser mantidos em sigilo, em ambiente seguro e sob o controle do administrador, conforme regulamento a ser editado.

Do ponto de vista jurídico, “administrador” não foi a melhor expressão empregada pelo Marco Civil, isso porque administrador significa o responsável técnico pela empresa, aquele que organiza e dirige a atividade. A depender do tipo associativo (sociedade, associação etc.) o administrador pode ser sócio ou não, cabendo a ele a representação da pessoa jurídica, pois é por meio do administrador que uma pessoa jurídica assume seus direitos e obrigações.

De qualquer forma, o desrespeito à regra do art. 13 do Marco Civil, conforme sua própria redação, implica responsabilidade para o “administrador” de sistema autônomo, ou seja, a pessoa física ou jurídica que administra blocos de endereços IP específicos, cadastrada no CGI.br. É importante destacar que a responsabilidade pela guarda dos registros de conexão não pode ser cedida a terceiros, sendo essa uma regra imperativa e qualquer disposição contratual diversa não tem efeitos jurídicos.

A guarda por prazo superior a um ano pode ser requerida pelo Ministério Público, Delegado de Polícia ou autoridade administrativa (por exemplo, da Receita Federal), os quais deverão ingressar dentro do prazo de 60 dias com pedido de autorização judicial para poder ter acesso aos registros requeridos. O responsável pela guarda dos registros deve manter de forma sigilosa o requerimento, que, por sua vez, perderá o efeito se for indeferido o pedido judicial ou protocolado fora do prazo de 60 dias. De qualquer forma, o responsável pelos registros somente pode fornecê-los ao requerente (Ministério Público ou autoridade policial) após receber a ordem judicial autorizadora.

Caso ocorra infração às regras do art. 13, que acabamos de apontar, deverá o aplicador da sanção considerar a natureza e a gravidade da falta, os danos provocados por ela, vantagem auferida pelo infrator e seus antecedentes, circunstâncias agravantes e reincidência (repetição da mesma infração). Acontece que o art. 13 não prevê sanção específica para o seu descumprimento. De acordo com o referido dispositivo, ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento. Ou seja, não há pena expressa prevista para o caso de infração ao art. 13, dependendo, portanto, da regulamentação do dispositivo, que ora encontra-se em consulta pública promovida pelo Ministério da Justiça com o fim de regulamentar o Marco Civil da Internet. Entretanto, isso a princípio não impede a aplicação de multa judicial.

## Considerações finais

Por fim, quem compartilha Wi-Fi não pode ser responsabilizado pelos atos daqueles que utilizam o



acesso à Internet ora disponibilizado; porém, é prudente que guarde os registros de conexão pelo prazo de um ano (nos termos do art. 13 do Marco Civil). Isso porque não será difícil haver entendimentos de que aquele que compartilha o acesso via Wi-Fi deve agir com diligência em relação aos dados daqueles que se utilizam do acesso, tendo em vista eventual necessidade de identificação de quem praticou um ilícito a partir daquele meio de conexão.

Em julgamentos que envolvem responsabilidade de provedores de conteúdo por postagens em suas redes sociais na Internet, o STJ tem aplicado o critério da “diligência média”, como nos Recursos Especiais 1.193.764-SP, 1.186.616-MG e 1.308.830-RS. A diligência média é um dever de conduta relacionado a um padrão de comportamento esperado pela sociedade, ou seja, um grau de diligência comum. Nos casos julgados pelo STJ tem-se decidido que, sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa omissiva. Mesmo que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o IP dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet.<sup>8</sup>

Assim, aquele que compartilha o acesso à Internet via Wi-Fi, a princípio, não se sujeita à regra do art. 13. Todavia não nos surpreenderemos ao receber notícias de decisões (sob o mesmo raciocínio do STJ quanto à diligência média) que sejam favoráveis às vítimas de ilícitos e responsabilizando às pessoas físicas ou jurídicas que compartilharam acesso via Wi-Fi com alguém que praticou a infração. Seria uma responsabilidade indireta por ato de outrem. A fundamentação da decisão poderá estar no fato de o usuário que compartilhou o Wi-Fi não ter guardado por certo período (por exemplo, um ano) os registros de conexão que permitissem identificar o infrator, realizando assim numa aplicação analógica do art. 13. Este dispositivo se aplicaria no que couber a essa situação, não somente ao *caput*, mas também aos seus parágrafos referentes à não terceirização da guarda, ao atendimento das ordens judiciais para prolongamento do período de guarda etc.

Para afastar qualquer chance de ser responsabilizado pelo ato de outrem que se utilizou do acesso à Internet via Wi-Fi, é prudente manter os registros de conexão que permitam identificar o usuário da rede interna que a utilizou para se conectar e assim praticar o ilícito.<sup>9</sup>

Se pensarmos em uma possível responsabilidade a quem fornece acesso via Wi-Fi, estaremos pensando em equiparar tal pessoa, via analogia, a um provedor de conexão, pois não deixa de ser um conector para uma rede interna (local), que a partir daí seu usuário possa alcançar a Internet. Essa responsabilidade ficaria restrita à falta de guarda dos dados de conexão, pois atribuir responsabilidade pelo fato de outrem contrariaria o que prevê o art. 18 do Marco Civil: “O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”. Um entendimento diverso deste, que pretenda atribuir responsabilidade a quem compartilha Wi-Fi pelos atos de outrem, acabaria impondo uma responsabilidade maior do que a dos próprios provedores de conexão, o que sem dúvida é descabido.

Contudo, os registros de conexão devem incluir informações sobre dia e horário de início e término de uma conexão à Internet, bem como outros dados que permitam identificar o computador utilizado e, de preferência, a pessoa (internauta). Por isso, o oferecimento de Wi-Fi deve ser muito bem pensado, quanto ao seu custo-benefício, pois se em alguns tipos de atividades já não se admite o não fornecimento de Wi-Fi visando ao conforto dos clientes, como hotéis, academias, escolas etc., em outros, o fornecimento não é tão relevante para a atração e manutenção de clientes, a exemplo de

consultórios médicos e fisioterapêuticos.

## Bibliografia

BINICHESKI, Paulo Roberto. *Responsabilidade civil dos provedores de Internet: direito comparado e perspectivas de regulamentação no direito brasileiro*. Curitiba: Juruá, 2011.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Ed. Juarez de Oliveira, 2005.

LORENZETTI, Ricardo Luis. *Comércio eletrônico*. São Paulo: Ed. RT, 2004.

MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico)*. São Paulo: Ed. RT, 2004.

POCH, Miquel Peguera. *La exclusión de responsabilidad de los intermediarios en Internet*. Granada: Comares, 2007.

REINALDO FILHO, Demócrito Ramos. *Responsabilidade por publicações na Internet*. Rio de Janeiro: Forense, 2005.

TEIXEIRA, Tarcisio. *Curso de direito e processo eletrônico: doutrina, jurisprudência e prática*. 3. ed. São Paulo: Saraiva, 2015.

\_\_\_\_\_. *Comércio eletrônico – conforme o Marco Civil da Internet e a regulamentação do e-commerce no Brasil*. São Paulo: Saraiva, 2015.

\_\_\_\_\_. *Direito empresarial sistematizado: doutrina, prática e jurisprudência*. 4. ed. São Paulo: Saraiva, 2015.

\_\_\_\_\_. *Compromisso e promessa de compra e venda: distinções e novas aplicações dos contratos preliminares*. 2. ed. São Paulo: Saraiva, 2015.

\_\_\_\_\_. Os interesses das empresas e dos empregados no uso do e-mail. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coords.). *Direito e Internet – aspectos jurídicos relevantes*. São Paulo: Quartier Latin, 2008. vol. 2.

\_\_\_\_\_; LOPES, Alan Moreira (coords.). *Direito das novas tecnologias: legislação eletrônica comentada, mobile law e segurança digital*. São Paulo: Ed. RT, 2015.

### Pesquisas do Editorial

- COMÉRCIO ELETRÔNICO, de Carla Andreatta Sobbé Moraes - RDC 97/2015/255
- RESPONSABILIDADE CIVIL NA INTERNET, de Geraldo Frazão de Aquino Júnior - RDCI 86/2014/451
- GUARDA DE DADOS PESSOAIS E REGISTROS ELETRÔNICOS PELOS PORTAIS DE COMÉRCIO ELETRÔNICO À LUZ DO MARCO CIVIL DA INTERNET, de Caio César Carvalho Lima - RT 958/2015/63

