Entrave tecnológico provoca impasse sobre Marco Civil e anonimato

A vedação ao anonimato prevista na Constituição Federal encontra novos desafios desde a disseminação da internet. Nas hipóteses em que o exercício da liberdade de manifestação do pensamento por uma pessoa ofenda direitos fundamentais de outra, é necessário identificar o responsável. Antes da entrada em vigor do Marco Civil da Internet (Lei 12.965/14), os tribunais já tratavam de diversos aspectos dessa identificação, mas a nova lei procurou sistematizá-los de forma coerente.

A partir da leitura do Marco Civil, inferem-se duas providências que, em regra, devem ser tomadas para essa identificação: primeiro, pede-se ao provedor de acesso à aplicação o endereço IP[1] do terminal[2] de onde partiu o ato investigado, bem como informações referentes à data e hora do acesso à aplicação; descoberto o provedor de conexão vinculado a esse IP, pode-se pedir ao provedor de conexão descoberto a identificação do usuário que utilizava o IP naquele exato momento.

Todavia, o aumento do número de usuários trouxe como consequência uma maior dificuldade na identificação. O atual Protocolo de Internet, chamado de IPv4, encontra-se em estágio de esgotamento, isto é, não há mais números de IP disponíveis para atender a todos os novos terminais conectados à rede.

Para solucionar o problema, foi criado um novo protocolo, chamado de IPv6, ainda relativamente pouco utilizado no Brasil. Neste momento de transição, para que a difusão da internet não fique impossibilitada, utiliza-se um novo protocolo de rede denominado "NAT" (*Network Adress Translation*), que viabiliza o compartilhamento do mesmo número de IP por mais de um usuário, de forma simultânea.

Segundo Relatório da Anatel de 2014, sobre o "Grupo de Trabalho para implantação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações", foi consenso nas reuniões desse grupo que deveria ser implementada uma "solução paliativa para evitar a estagnação da Internet no País, com suspensão das vendas, congelamento do crescimento da base de usuários e a interrupção dos programas de massificação da Internet no Brasil"[3].

O chamado "NAT" consiste numa técnica que permite o compartilhamento de IPs entre vários usuários. A partir da adoção dessa tecnologia, há uma série de discussões na doutrina e na jurisprudência acerca da necessidade de os provedores de aplicações guardarem informações referentes não apenas ao IP, mas também em relação à "porta lógica de origem" utilizada por cada usuário. Segundo especialistas e a própria Anatel, apesar de não estar prevista na lei, essa informação é indispensável para que se identifique de forma unívoca o usuário infrator.

No entanto, não é consenso entre os provedores a definição de quem deve guardar essas informações. Os provedores de conexão, como pode ser visto no relatório da Anatel, defendem que, além deles, os provedores de aplicações também devem guardar informações referentes às portas lógicas dos usuários. Os provedores de aplicações alegam, porém, que não possuem essa obrigação, apresentando os argumentos expostos a seguir.

O argumento principal utilizado por estes provedores toma como base o princípio da legalidade. Isto é, não haveria previsão em nosso ordenamento jurídico quanto à guarda e fornecimento de informações

relacionadas a “portas lógicas de origem” por parte deles. A definição de “registros de acesso a aplicações de internet” encontra-se prevista no inciso VIII do artigo 5°[4], não abrangendo a porta lógica.

Segundo os provedores, tal norma, assim como o artigo 15[5], não pode ser interpretada extensivamente para abranger outros registros não expressamente previstos. Trata-se de uma interpretação predominantemente literal dos dispositivos do Marco Civil. Se não há previsão de guarda das portas lógicas, os provedores de aplicações não poderiam sofrer sanções por não as guardarem.

Além da literalidade, essa interpretação se caracteriza por priorizar a segurança jurídica: se os provedores forem obrigados a guardar dados não previstos expressamente no Marco Civil, cada juiz poderia determinar a apresentação de dados diferentes, o que causaria insegurança.

Outro ponto levantado é que tal assunto foi abordado nas discussões sobre a regulamentação do Marco Civil, mas a edição final do Decreto n8.771/16 não tratou disso expressamente[6]. Ou seja, utiliza-se uma interpretação histórica para mostrar que a presidente deixou de incluir a questão da “porta lógica de origem” no decreto justamente porque não pretendia ampliar as hipóteses de guarda de registro já previstas no Marco Civil.

Em contribuição ao debate público sobre a regulamentação do Marco Civil, o ITS Rio (Instituto de Tecnologia e Sociedade) alegou que a interpretação extensiva das normas sobre guarda de registros “pode acabar por gerar uma grande quantidade de armazenamento de dados desnecessários, trazendo um ônus econômico exagerado, especialmente se considerarmos pequenos provedores de serviços e produtos na Internet”[7].

O entendimento favorável aos provedores de aplicações foi acolhido pelo Tribunal de Justiça de São Paulo no julgamento do Agravo de Instrumento 2150710-76.2015.8.26.0000[8]. O acórdão deu provimento a um recurso da Google, considerando que a guarda das informações referentes às portas lógicas caberia apenas aos provedores de conexão.

Defensores da tese contrária aos provedores de aplicações baseiam-se não na interpretação literal do Marco Civil da Internet, e sim em uma interpretação finalística, evolutiva e sistemática. Renato Ópice Blum, por exemplo, entende que é natural que o Marco Civil não tenha previsto todos os improvisos do mercado, tal qual a técnica utilizada para compartilhamento de IPs. Todavia, nas palavras dele, “a obrigatoriedade de identificação existe, é patente e está entre as finalidades da lei. Portanto, se a quebra dessa sistemática ocorreu, é preciso aplicar ao novo contexto a mesma lógica da lei”[9].

Como o objetivo da previsão de guarda de registros é a identificação precisa de usuários, essa corrente defende que o Marco Civil precisa ser interpretado de acordo com essa finalidade, em atenção ao artigo 6° da lei[10]. Dessa forma, a interpretação da Lei não poderia ser engessada, pois a tecnologia muda constantemente.

O esgotamento do IPV4 trouxe uma nova situação, não prevista na época em que o Marco Civil foi editado; assim, o não fornecimento de determinadas informações prejudica os objetivos da lei, pois impossibilita a correta identificação de autores de ilícitos. Fazem parte dessa corrente, por exemplo, Caio Cesar Carvalho Lima[11], Fabio Nori[12] e Giuliano Giova[13].

Provedores de conexão alegam que seria inútil que eles registrassem qual usuário se utilizou de cada porta lógica de origem se os provedores de aplicações não identificassem qual foi a porta lógica de origem que realizou o acesso, pois os provedores de conexão não podem guardar informações sobre o acesso. O relatório da Anatel segue a mesma linha.

Nos grupos de trabalho realizados para discutir a transição do IPv4 para IPv6, chegou-se à conclusão de que a única forma de as provedoras de conexão fornecerem o nome do usuário que faz uso de um IP compartilhado em um determinado instante seria com a informação da "porta lógica de origem". Assim, "os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a 'porta lógica de origem'"[14].

O entendimento de que cabe aos provedores de aplicações a obrigação de guarda dos dados referentes às portas lógicas é acolhido de forma majoritária pelo Tribunal de Justiça de São Paulo. No julgamento do Agravo de Instrumento 2206954-25.2015.8.26.0000[15], os desembargadores entenderam que o fornecimento apenas do IP é insuficiente para identificação dos usuários. Além disso, o não apontamento da porta lógica levaria ao anonimato, deixando impunes as pessoas que se utilizam da internet para a prática de ilícitos.

Os argumentos que procuram atribuir obrigação de guarda das portas lógicas aos provedores de aplicações não merecem prosperar. Como visto anteriormente, a adoção do NAT para compartilhamento de IPs entre vários usuários foi, nas palavras da própria Anatel, uma solução paliativa adotada pelos teles enquanto o protocolo IPv6 não estivesse totalmente difundido no país. Uma opção de natureza econômica, portanto, que buscou diminuir os custos dessas empresas durante o período de transição.

A solução proposta pelos provedores de conexão, em conjunto com a Anatel, de transferir os ônus dessa opção aos provedores de aplicação e aos usuários não se mostra adequada. Em relação aos provedores de aplicação, isso representaria um aumento dos custos, o que pode prejudicar pequenos prestadores de serviço na internet, e uma insegurança jurídica, pois nada impede que no futuro surjam novas exigências de guardas de registros que não estão previstas em nosso ordenamento.

Já do ponto de vista do usuário, abrir essa exceção quanto à porta lógica de origem pode representar um aumento da vigilância e uma restrição de sua privacidade. Pois a interpretação extensiva do Marco Civil pode, no futuro, ir além das portas lógicas, abrangendo cada vez mais informações.

O próprio NIC.br (Núcleo de Informação e Coordenação do Ponto BR) não recomenda a adoção do NAT. Segundo Frederico Neves, "não estimulamos nem recomendamos nenhum tipo de NAT. O que resolve o problema de falta de endereços é a introdução do IPv6. Há quem aposte que vai conseguir viver com NAT e IPv4 para sempre, mas o risco é muito grande"[16]. Assim, a melhor interpretação a ser adotada é no sentido de que os provedores de aplicações não são obrigados a guardar dados de acesso além daqueles já previstos pelo Marco Civil (data e hora de uso de uma determinada aplicação a partir de um determinado endereço IP).

Caso a identificação de um usuário se torne impossível em decorrência da ausência da informação referente à porta lógica de origem, o provedor de aplicações não pode ser responsabilizado, pois não tem obrigação de guardar esse dado. Todavia, caso se constate que a ausência dessa informação deve-se a ato

ou omissão do provedor de conexão, este pode ser responsabilizado.

O artigo 18 do Marco Civil[17] não pode socorrer os provedores de conexão neste caso. Isso porque sua aplicação pressupõe que o provedor cumpra todos os seus deveres. Se o provedor de conexão adota uma atitude que inutiliza seus próprios registros e os dos provedores de aplicação, descumpre deveres previstos pelo Marco Civil.

Assim, se o provedor de conexão não cumpre seu dever no sentido de identificar o responsável pelo ato ilícito, pode ser responsabilizado por "fato do serviço", nos termos do artigo 14 do Código de Defesa do Consumidor[18]. O usuário que sofre as consequências do ato ilícito, sendo impossível a localização daquele que cometeu a ilicitude, pode ser considerado "consumidor por equiparação", nos termos do artigo 17 do Código de Defesa do Consumidor[19]. Por isso, é possível, em tese, que o provedor de conexão seja responsabilizado pelos danos causados.

Enquanto o Marco Civil permanecer como está, os usuários e os provedores de aplicações não podem ser prejudicados por uma opção dos provedores de conexão. Ao longo desse tempo, ou enquanto não for completamente adotado o IPv6, aqueles que são responsáveis pela tecnologia NAT (provedores de conexão) devem arcar não apenas com os bônus, mas também com os ônus dessa opção.

[1] Art. 5°, inc. III da Lei n° 12.965/14: "endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".

[2] Art. 5°, inc. II: "terminal: o computador ou qualquer dispositivo que se conecte à internet".

[3] Disponível em < http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoP >.

[4] VIII – registros de conexão: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[5] 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.

[6] Os diferentes posicionamentos acerca do tema são expostos por relatório do Internet Lab sobre os debates públicos realizados antes da regulamentação da Lei. Disponível em http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-ptbr.pdf

. Acesso em 12 de dezembro de 2016.

[7] Comentário ao artigo 11° da primeira minuta do Decreto n° 8.771/16. Disponível em < http://pensando.mj.gov.br/marcocivil/texto-em-debate/minuta/>. Acesso em 09 de dezembro de 2016.

[8] BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento n° 2150710-76.2015.8.26.0000. Agravante: Google Brasil Internet Ltda.; Agravada: Tim Celular S.A. Relator Desembargador Alexandre Marcondes. São Paulo, 31 de agosto de 2015.

[9] BLUM, Renato Ópice. **Portas Lógicas de Origem: identificação e caos jurídico**. 2016. Disponível em <http://jota.info/artigos/direito-digital-portas-logicas-de-origem-dificuldade-de-identificacao-e-o-caos-juridico-26102016 >. Acesso em 08 de dezembro de 2016.

[10] Art. 6°. Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

[11] LIMA, Caio César Carvalho. Garantia da Privacidade e Dados Pessoais à Luz do Marco Civil da Internet. In: LEMOS, Ronaldo; LEITE, George Salomão (Org.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 153.

[12] NORI, Fabio. A Guarda dos Registros de Conexão e dos Registros de Acesso às Aplicações no Marco Civil. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III – Tomo II**. São Paulo: Quartier Latin, 2015. p. 180.

[13] GIOVA, Giuliano. **Marco Civil e endereços na Internet inviabilizam produção de provas**. Disponível em: http://www.conjur.com.br/2014-jul-12/giuliano-giova-marco-civil-enderecos-internet-inviabilizam-provas. Acesso em 08 de dezembro de 2016.

[14] Disponível em < http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoP >. p. 14.

[15] BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento 2206954-25.2015.8.26.0000. Agravante: Google Brasil Internet Ltda.; Agravado: Itaú Unibanco S.A. Relator Desembargador Paulo Alcides. São Paulo, 12 de maio de 2016.

[16] Disponível em http://nic.br/noticia/na-midia/esgotamento-dos-enderecos-ipv4-acirra-tensoes-entre-teles-e-nic-br/

. Acesso em 13 de dezembro de 2016.

[17] Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiro.

[18] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

[19] Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.

Date Created
17/12/2016