RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

RELATOR	**:**	**MINISTRO MARCO AURÉLIO BELLIZZE**
RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578 CAMILLA DO VALE JIMENE - SP222815 JULIANA ABRUSIO FLORÊNCIO - SP196280 CAMILA MACEDO MARTINS - SP285568 PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179 RENATO GOMES DE MATTOS MALAFAIA - SP368020 ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534 EDUARDO LUIZ BROCK - SP091311 FABIO RIVELLI - SP297608 RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487 JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

EMENTA

RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.

1. O recurso especial debate a extensão de obrigação do provedor de aplicações de guarda e fornecimento do endereço IP de terceiro responsável pela disponibilização de conteúdo ilícito às informações acerca da porta lógica de origem associada ao IP.

2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os provedores de conexão e os provedores de aplicações, em observância aos direitos à intimidade e à privacidade.

3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial.

4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita.

5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.

6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.

7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.

8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.

9. Recurso especial provido.

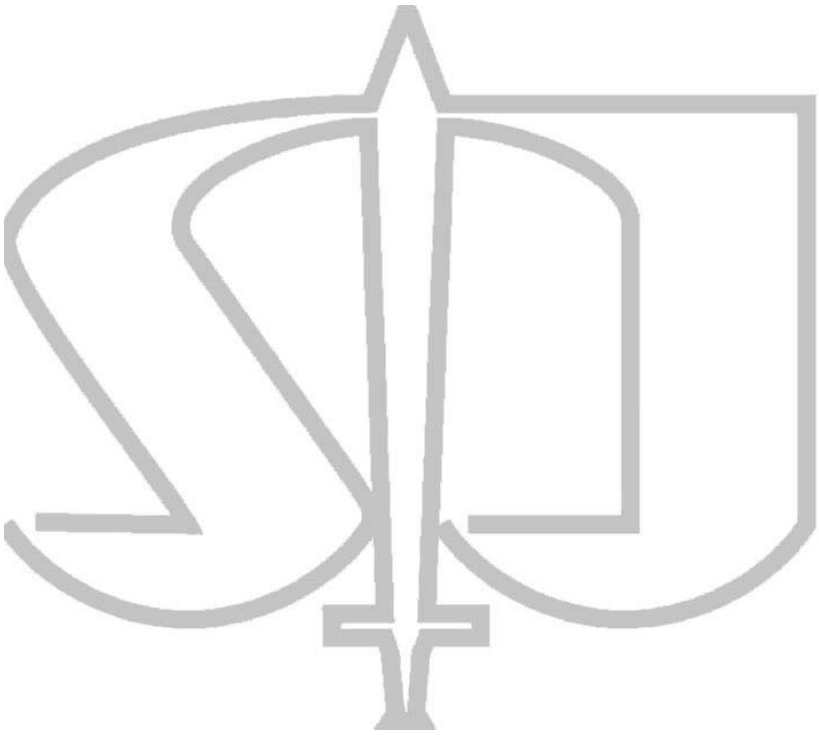
ACÓRDÃO

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da Terceira Turma do Superior Tribunal de Justiça, por unanimidade, dar provimento ao recurso especial, nos termos do voto do Sr. Ministro Relator.

Os Srs. Ministros Moura Ribeiro (Presidente), Nancy Andrighi, Paulo de Tarso Sanseverino e Ricardo Villas Bôas Cueva votaram com o Sr. Ministro Relator.

Brasília, 05 de novembro de 2019 (data do julgamento).

MINISTRO MARCO AURÉLIO BELLIZZE, Relator



RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

RELATÓRIO

O SENHOR MINISTRO MARCO AURÉLIO BELLIZZE:

Cuida-se de recurso especial interposto por Tim Celular S.A., com fundamento nas alíneas *a* e *c* da Constituição Federal.

Compulsando os autos, verifica-se que a recorrente propôs ação de obrigação de fazer, pelo rito sumário, contra Google Brasil Internet Ltda., com o fim de obter os dados de cadastro e registros eletrônicos que identificassem o responsável pela oferta de meios irregulares para adesão ao plano TIM BETA.

A recorrente esclareceu que o referido plano tinha por alvo o público jovem, que deveria participar de um jogo oferecido pelo sítio eletrônico da recorrente, como condição para adesão. No entanto, a recorrente tomou conhecimento de *blog* e página, ambos hospedados pela recorrida, que proporcionavam a adesão ao referido plano, independente da participação no jogo, o que deu ensejo à propositura desta demanda.

Em sentença, a ação foi julgada parcialmente procedente, para determinar que a recorrida, além de remover o *blog* e o perfil indicados na petição inicial, fornecesse os dados que possuísse acerca dos terceiros responsáveis pelo conteúdo.

Interposta apelação pela recorrente, o Tribunal de origem negou provimento ao recurso, nos termos da seguinte ementa (e-STJ, fl. 591):

> Obrigação de fazer. Remoção do ar de 'blog' e de perfil hospedados em URL. Fornecimento de dados cadastrais disponíveis e registros eletrônicos, inclusive porta lógica, com datas e horários, no padrão UTC. Apelada é somente provedora de aplicação e não de conexão. Ausência de respaldo legal para a exigência de fornecimento de origem dos IPs com a respectiva porta lógica. Devido processo legal observado. Desnecessidade de outras provas. Marco Civil da Internet não apresenta previsão legal para que o recorrido colete e armazene dados de porta lógica de usuário das páginas indicadas. Sucumbência observou as peculiaridades da demanda, ou seja, o objeto da lide, e não itens isolados pedidos. Apelo desprovido.

Opostos embargos de declaração, foram eles rejeitados.

Nas razões do apelo extremo, alega a insurgente violação dos arts. 5º, VIII,

10, § 1º, e 11, § 2º, da Lei n. 12.965/2014; 21, 85 e 86, parágrafo único, do CPC/2015; 2º e 17 do CDC; e 9º da LINDB, além de dissídio jurisprudencial. Sustenta, em síntese: *i)* cerceamento de defesa pelo julgamento antecipado da lide sem o deferimento de produção das provas requeridas, as quais tinham o condão de demonstrar que a liminar não foi devidamente cumprida pela empresa ré, inclusive no que diz respeito à remoção do conteúdo ilícito do ar; *ii)* obrigação do provedor de aplicação de internet de fornecer a porta lógica utilizada pelo usuário da aplicação, tendo em vista que essa informação "é elemento de suma importância para a exata identificação do responsável pelo ilícito, posto que na ausência desse dado, poder-se-á não encontrar ninguém ou, ainda, encontrar dezenas ou, até mesmo, centenas de usuários conectados ao mesmo endereço IP, o que inviabiliza a investigação" (e-STJ, fl. 619); *iii)* a obrigação dos provedores de aplicação de internet de tomar providências no sentido de indisponibilizar o conteúdo infringente em todo o território nacional; e *iv)* a necessidade de condenação da recorrida a arcar integralmente com os ônus sucumbenciais.

Contrarrazões apresentadas (e-STJ, fls. 681-707).

É o relatório.

RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

VOTO

O SENHOR MINISTRO MARCO AURÉLIO BELLIZZE (RELATOR):

Cinge-se a controvérsia a determinar a extensão da obrigação dos provedores de aplicação de fornecimento de dados de terceiros responsáveis pela disponibilização de conteúdos contestados.

1. Obrigação de identificação de terceiros

As obrigações e a responsabilidade civil de empresas atuantes no ambiente da internet, após tratamento jurisprudencial, teve seus contornos legais delimitados na Lei n. 12.965/2014. O Marco Civil da Internet, além de reconhecer a essencialidade do acesso à internet para o exercício da cidadania, posicionou no vértice principiológico da regulamentação o cuidado com a intimidade e a privacidade.

Decorrente dessa orientação, a necessária proteção aos registros, dados pessoais e comunicações privadas foi disciplinada de modo a restringir sua guarda por provedores de conexão e de acesso a aplicações. De outro lado, resultante da ponderação de interesses legítimos conflitantes, também se assegurou o acesso aos dados necessários à identificação de autores de crimes ou causadores de danos civis, obrigando-se, pela via judicial, os provedores à eventual disponibilização dos dados por eles guardados.

É o que se extrai do art. 10 e seu § 1º (sem destaques no original):

> Art. 10. 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.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam **contribuir para a identificação do usuário ou do terminal**, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

Essa obrigação de guarda de dados do acesso foi ainda repartida entre os

provedores de conexão e os provedores de aplicações. Evidenciando a preocupação constante com o respeito à privacidade no ambiente virtual, vedou-se a guarda dos dados de acessos a aplicações aos provedores de conexão. Noutros termos, aos provedores de conexão somente cabe a guarda dos dados de conexão (IP, data e horário), tornando impossível, apenas com esses dados, se conhecer a atividade completa do internauta, enquanto efetivamente conectado à rede mundial (art. 14 da Lei n. 10.965/2014). Do mesmo modo, cada provedor de aplicação somente poderá – e deverá – manter registros de acesso e de cadastro (quando houver) daquele que esteve conectado a sua aplicação, sendo igualmente vedado manter os dados da navegação, salvo consentimento do titular dos dados (art. 16 da Lei n. 10.965/2014).

Nesse cenário, tem-se, na prática, uma repartição das informações de navegação: *i)* o provedor de conexão, ao habilitar um terminal para envio e recebimento de dados, atribui a ele um IP e registra o momento em que iniciada, interrrompida e encerrada a conexão, e *ii)* cada provedor de aplicação registra o acesso dos IPs, momento de início e final, à sua própria aplicação. Desse modo, a totalidade da navegação da cada internauta dependerá da remontagem de cada uma das aplicações acessadas ao longo de uma única conexão.

O IP, portanto, embora inicialmente atribuído pelo provedor de conexão, segue sendo sucessivamente registrado por cada um dos provedores de aplicação por onde transita o internauta ao longo de sua conexão com a rede mundial de computadores, o que, a princípio, permitia a correta identificação de quem fosse o responsável pela disponibilização de conteúdo ofensivo em ambiente virtual.

Contudo, esse código atribuído no momento em que iniciada a conexão, em razão da expansão e do crescimento da internet, esgotou sua capacidade e, por isso, se encontra em fase de transição. Até que seja efetivamente concluída a implantação da nova versão do padrão IP (IPv6), adotou-se o compartilhamento de um mesmo número IP por vários usuários (dispositivos), o que dificulta sensivelmente o rastreamento dos registros e a identificação do usuário final, conforme conclusão da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos (relatório final disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%253D%253E+RCP+10/2015>, acesso em 10/4/2019).

Essa situação fática é esclarecida pela recorrida, em suas contrarrazões (e-STJ, fl. 693):

> com o esgotamento dos endereços de IPv4 e a necessidade de implementação da tecnologia IPv6, os provedores de conexão passaram a utilizar a tecnologia de transição denominada "IP NAT" em detrimento da segurança de seus clientes.
> Ou seja, ao contrário do que tenta fazer crer a Recorrente TIM - por sua vez, provedor de conexão -, a tecnologia "IP NAT" passou a ser utilizada pelos provedores de conexão, e não pelos os provedores de aplicações como a Recorrente.
> Tal tecnologia a funciona, em linhas gerais, como se fosse um enorme roteador caseiro. Ou seja, permite com que inúmeros usuários acessem a internet, ao mesmo tempo, pelo mesmo endereço IP.

De fato, embora seja apenas uma solução transitória, o Comitê Gestor da Internet no Brasil autorizou o compartilhamento de endereços de IP do IPv4 entre mais de um usuário da internet. Isso porque é imprescindível a utilização de IP para o estabelecimento de conexão de um dispositivo à rede mundial e, como já referido, o acesso à internet tem sua essencialidade reconhecida pelo legislador nacional.

Outrossim, a despeito do compartilhamento, há uma solução tecnológica que viabiliza a individualização da conexão e da navegação mesmo que mais de um dispositivo se encontre simultaneamente conectado à internet com o mesmo número IP: são as portas lógicas. Uma vez que são os provedores de conexão os responsáveis por atribuir a cada usuário um número IP, é intuitivo que eles serão também os responsáveis pela organização da relação entre usuários, endereços de IP e portas lógicas.

Todavia, daí não se extrai nenhuma consequência jurídica para a impossibilidade de conhecimento e armazenamento desses mesmos dados pelos provedores de aplicações, tampouco é suficiente para definir a extensão da obrigação legal estabelecida no art. 10 do Marco Civil da Internet.

Isso porque, de tudo quanto foi exposto, não há dúvidas de que o intuito do legislador ao regulamentar os dados que deveriam ser guardados, o sigilo e as hipóteses de seu levantamento, foi o de viabilizar a identificação dos causadores de danos ou, ao menos, dos dispositivos por eles utilizados. Esse é, portanto, o norte para interpretação conjunta dos arts. 15 e 5º, VIII, da Lei n. 12.965/2014.

Noutros termos, ainda que o legislador, ao estabelecer a obrigação de guarda dos dados de acesso à aplicação tenha se referido apenas aos respectivos

registros de acesso (art. 15 da Lei n. 12.965/2014), os quais, por sua vez, conforme a definição do art. 5º, VIII, se restringe à data e hora de uso "a partir de um determinado endereço IP", enquanto não se restabelecer a relação de individualidade dos IPs é preciso que se entenda incluída no endereço IP a correspondente porta lógica de origem, em razão da indissociabilidade entre as duas teconologias para o efetivo acesso individualizado à internet e às aplicações. Do contrário, a adoção da tecnologia paliativa resultaria no esvaziamento da lei, tornando inviável a identificação e responsabilização desses sujeitos.

Acrescenta-se que a questão da identificação de causadores de danos nesse cenário de transição foi objeto de intenso debate pelo Grupo de Trabalho da Agência Nacional de Telecomunicações – Anatel para implantação do protocolo IP Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações. Em seu relatório final, o referido Grupo de Trabalho assinalou a imprescindibilidade do fornecimento das portas lógicas por provedores de aplicações, constatando a necessidade de adaptação tecnológica para armazenagem de todas as informações de acesso, nas quais se inclui a porta lógica, sempre que se tratar de endereço IPv4 (disponível em <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=325769.pdf>, acesso em 16/4/2019, p. 14-15):

> Tanto no Grupo de Trabalho do NIC.br como no Grupo de Trabalho da ANATEL foi intensamente discutida a questão da identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado. Em ambos os Grupos de Trabalho foi consenso que a única forma das prestadoras 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 da conexão" que estava sendo utilizada durante a conexão. Dessa forma, **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"**.
>
> .....
>
> Diante do exposto, é importante reforçar que durante o período de utilização da solução paliativa do CG-NAT44, para que o processo de apuração de ilícitos na Internet não fique prejudicado, **é necessário que, não só provedores de acesso, como também provedores de conteúdo e serviços de internet (bancos e sites de comércio eletrônico, por exemplo) adaptem seus sistemas para possibilitar a armazenagem dos registros de aplicação (provedores de aplicação) ou registros de conexão (provedores de acesso) com a informação da "porta lógica de origem" utilizada**.

Com efeito, tão intuitiva quanto a percepção de que os provedores de conexão detêm as portas lógicas, é a compreensão de que os provedores de aplicações também as conhecem – na medida em que são elas que possibilitam a individualização da navegação e que o envio de dados entre dois pontos da comunicação depende intrinsecamente da localização virtual dos dispositivos conectados. Por consequência, é faticamente possível o arquivamento dessas informações, ainda que para tanto fosse necessária adaptação teconológica dos provedores de aplicações, como bem enfatiza trecho do relatório acima.

Desse modo, sempre que se tratar de IP ainda não migrado para a versão 6, torna-se imprescindível o fornecimento da porta lógica de origem por responsável pela guarda dos registros de acesso como decorrência lógica da obrigação de fornecimento do endereço IP.

2. Cerceamento de defesa e necessidade de dilação probatória

É de fundamental importância se ter em consideração que a presente demanda foi proposta em agosto de 2015, quando a adesão ao IPv6 era ainda irrisória no País. Segundo dados do Núcleo de Informação e Coordenação do Ponto BR – NIC.br (núcleo criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil), em janeiro de 2015, apenas 0,1% (um décimo por cento) de usuários de Internet no Brasil utilizavam IPv6. Até 2018, após 10 anos de sua criação, esse protocolo havia sido adotado para apenas um terço dos usuários da internet (dados disponíveis em <http://ipv6.br/post/forum-10anos/>, acesso em 16/4/2019).

Nesse contexto, foram expressamente pleiteados pela recorrente, em sua petição inicial, os dados de cadastro disponíveis e os registros de acesso, fazendo-se referência expressa aos "IPs de origem, com sua respectiva porta lógica, datas e horários, com fuso-horário no padrão UTC) atrelados à criação e demais acessos administrativos ao Blog e perfil do Google Plus" (e-STJ, fl. 21).

No entanto, a sentença e o acórdão de primeiro grau entenderam pela inexistência de previsão legal para a obrigação de fornecimento da porta lógica para os provedores de aplicações, ao fundamento de que este dado deveria ser informado tão somente pelo provedor de conexão.

O acórdão ainda registrou em sua fundamentação que a obrigação de fornecimento de portas lógicas de origem também não seria possível, do ponto de vista prático, conforme o seguinte trecho (e-STJ, fl. 593):

> Assim, deve ser reiterado que a apelada não possui dados de porta lógica, já que não os cadastra, por conseguinte, não os armazena, portanto, não tem possibilidade de fornecer, ressaltando, ainda, a ausência de disposição legal para tanto.

Sobre esse ponto, a recorrente aduz ter ocorrido também cerceamento de defesa, uma vez que o Judiciário não teria expertise necessária para aferir a real possibilidade para o fornecimento dos dados requeridos. Acrescenta que, na hipótese dos autos, não houve sequer despacho saneador, tendo sido surpreendido pelo julgamento de mérito, que expressamente afastou a obrigação de indicação de portas lógicas.

A despeito do esforço argumentativo quanto ao ponto, deve-se esclarecer que o acórdão recorrido foi expresso em afastar a necessidade de dilação probatória por entender que o processo se encontrava suficientemente instruído, o que atrai a Súmula n. 7/STJ. Além disso, os fundamentos do voto deixam claro que a *ratio decidendi* decorreu da ausência de obrigação legal, e não da impossibilidade fática, de modo que, *a priori*, não havia mesmo a necessidade de dilação probatória, não havendo, pois, que se cogitar de cerceamento de defesa.

Todavia, uma vez reconhecida a obrigação legal de fornecimento dos dados de acesso às aplicações, nos termos deste voto, o que inclui a porta lógica de origem sempre que o IP em questão não estiver ajustado à versão 6 – como decorrência da necessidade de identificação do dispositivo de origem –, é de se assegurar que, no caso dos autos, seja efetivamente oportunizada a dilação probatória. Isso porque uma eventual impossibilidade fática por desajuste tecnológico, o que resultaria na conversão da obrigação de fazer em perdas e danos, é matéria que refoge ao conhecimento do homem médio, e sua apreciação sem abertura de dilação atentaria contra o princípio do contraditório substancial.

Com esses fundamentos, dou provimento ao recurso especial para cassar a sentença e fixar o entendimento de obrigatoriedade de fornecimento da porta lógica associada a endereço IPv4 para fins de identificação de autor/dispositivo utilizado para causar danos a outrem. Por consequência, determino o retorno dos autos à origem para

que, em obediência ao princípio do contraditório, seja concedido às partes dilação probatória acerca de sustentada impossibilidade técnica de cumprimento da obrigação, bem como do efetivo cumprimento da decisão que determinou a retirada do conteúdo ilícito.

Julgo prejudicados os demais pedidos recursais.

É como voto.

CERTIDÃO DE JULGAMENTO
TERCEIRA TURMA

Número Registro: 2018/0322140-0 **PROCESSO ELETRÔNICO** **REsp 1.784.156 / SP**

Números Origem: 10786606020158260100 20170000423509 20180000209328

PAUTA: 11/06/2019 JULGADO: 11/06/2019

Relator
Exmo. Sr. Ministro **MARCO AURÉLIO BELLIZZE**

Presidente da Sessão
Exmo. Sr. Ministro MOURA RIBEIRO

Subprocuradora-Geral da República
Exma. Sra. Dra. MARIA IRANEIDE OLINDA SANTORO FACCHINI

Secretário
Bel. WALFLAN TAVARES DE ARAUJO

AUTUAÇÃO

RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578
		CAMILLA DO VALE JIMENE - SP222815
		JULIANA ABRUSIO FLORÊNCIO - SP196280
		CAMILA MACEDO MARTINS - SP285568
		PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179
		RENATO GOMES DE MATTOS MALAFAIA - SP368020
		ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	EDUARDO LUIZ BROCK - SP091311
		FABIO RIVELLI - SP297608

ASSUNTO: DIREITO CIVIL - Responsabilidade Civil

SUSTENTAÇÃO ORAL

Dr(a). ETTORE TARCISIO ZAMIDI, pela parte RECORRENTE: TIM CELULAR S.A

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Após o voto do Sr. Ministro Relator, dando provimento ao recurso especial, pediu vista antecipada a Sra. Ministra Nancy Andrighi. Aguardam os Srs. Ministros Moura Ribeiro, Paulo de Tarso Sanseverino e Ricardo Villas Bôas Cueva.

RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

RELATOR	:	MINISTRO MARCO AURÉLIO BELLIZZE
RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578 CAMILLA DO VALE JIMENE - SP222815 JULIANA ABRUSIO FLORÊNCIO - SP196280 CAMILA MACEDO MARTINS - SP285568 PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179 RENATO GOMES DE MATTOS MALAFAIA - SP368020 ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534 EDUARDO LUIZ BROCK - SP091311 FABIO RIVELLI - SP297608 RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487 JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

VOTO-VISTA

A EXMA. SRA. MINISTRA NANCY ANDRIGHI:

Cuida-se de recurso especial interposto por TIM CELULAR S.A., com fundamento nas alíneas "a" e "c" do permissivo constitucional, contra acórdão do TJ/SP.

Ação: de obrigação de fazer, ajuizada pela recorrente em face de GOOGLE BRASIL INTERNET LTDA., em que pleiteia a obtenção de dados cadastrais e registros de acesso que permitam a identificação do responsável pela oferta de meios irregulares para a adesão ao um plano de serviços. Isso porque a recorrente descobriu que, em blogs hospedados pela recorrida, havia a informação de como aderir a esse plano – TIM BETA – sem o cumprimento de todas as condições para sua adesão.

Sentença: julgou parcialmente procedente o pedido, para condenar a recorrida a remover os conteúdos indicados na petição inicial e fornecer os dados

que possuísse acerca dos responsáveis pela publicação dos conteúdos mencionados. No entanto, negou as informações relacionadas às portas lógicas utilizadas pelos números IP.

Acórdão: em apelação interposta pela recorrente, o Tribunal de origem negou provimento ao recurso, afirmando não existir fundamento legal para a obrigatoriedade de apresentação das informações vinculadas às portas lógicas do IP, conforme a ementa abaixo:

> Obrigação de fazer. Remoção do ar de 'blog' e de perfil hospedados em URL. Fornecimento de dados cadastrais disponíveis e registros eletrônicos, inclusive porta lógica, com datas e horários, no padrão UTC. Apelada é somente provedora de aplicação e não de conexão. Ausência de respaldo legal para a exigência de fornecimento de origem dos IPs com a respectiva porta lógica. Devido processo legal observado. Desnecessidade de outras provas. Marco Civil da Internet não apresenta previsão legal para que o recorrido colete e armazene dados de porta lógica de usuário das páginas indicadas. Sucumbência observou as peculiaridades da demanda, ou seja, o objeto da lide, e não itens isolados pedidos. Apelo desprovido.

Embargos de declaração: opostos pela recorrente, foram rejeitados pelo Tribunal de origem.

Recurso especial: alega violação aos arts. 5º, VIII, 10, § 1º e 11, § 2º, da Lei 12.965/2014 (Marco Civil da Internet), aos arts. 21, 85 e 86, parágrafo único, do CPC/2015; aos arts. 2º e 17 do CDC; e ao art. 9º da LINDB. Sustenta, ainda, a existência de dissídio jurisprudencial.

O recurso especial foi admitido na origem.

Na sessão de julgamento da Terceira Turma do dia 11/06/2019, o i. relator, Min. Bellizze, apresentou voto no sentido de dar provimento ao recurso especial, para tornar obrigatório o fornecimento das informações relacionadas à porta lógica associada ao endereço IPv4. Após, solicitei vistas, para melhor exame

da matéria.

É o relatório.

O propósito recursal consiste em definir a obrigatoriedade de guarda e apresentação, por parte da provedora de aplicação de internet, dos dados relacionados à porta lógica de origem associada aos endereços IPs indicados pela recorrente. A recorrente também suscita eventual cerceamento de defesa, bem como um possível descumprimento da decisão judicial que determinou a retirada de conteúdos ilícitos da internet.

A questão da guarda e fornecimento da chamada porta lógica de origem do IP, como bem ressaltado pelo i. Ministro relator, está diretamente relacionada ao esgotamento da versão 4 do IP (IPv4), a implementação de sua versão 6 (IPv6) e o compartilhamento de IPs como solução transitória. É interessante notar que isso reflete a relação entre a arquitetura da internet, seus aspectos técnicos, e matérias de política pública, relativas ao acesso e à operabilidade da internet, com consequências jurídicas, para as hipóteses de requisição de registros de acesso em investigações criminais e processos judiciais.

A rigor, o termo "porta lógica" seria mais corretamente utilizado no campo da eletrônica como um dispositivo que opera logicamente um circuito. O termo mais correto seria simplesmente “porta” ou “porta de origem”, utilizada no compartilhamento dos endereços IPs (YANDRA, B. A responsabilidade do provedor de aplicação pelo armazenamento e fornecimento da porta de origem do endereço IP, sob a ótica do Marco Civil da Internet. In: CV, IDP, Volume 2, n. 43, 2019, jan-fev-mar 2019). Contudo, a expressão mais comumente utilizada pelo Poder Judiciário é “porta lógica” e será usado sem distinção com o

termo “porta de origem”.

É fato que não há uma regulação consolidada sobre a coleta e o armazenamento das portas de origem, necessária à dinâmica atual como solução transitória ao processo de implementação do IPv6. Também não existe qualquer menção à expressão no Marco Civil da Internet. Dessa forma, como mencionado pelo Instituto de Referência em Internet e Sociedade - IRIS, cumpre ao Poder Judiciário esclarecer se: “*(i) Existe uma obrigação legal de armazenamento dos dados referentes à “porta lógica? (ii) Se sim, de quem a responsabilidade pelo armazenamento e disponibilização desses dados às autoridades competentes: dos provedores de conexão, de aplicação, ou de ambos? E (iii) O dado de porta lógica é necessário para identificação de usuários que acessam à internet por meio de IPs compartilhados (fornecidos pelos provedores de conexão)*?” (IRIS. Portas Lógicas e Registros de Acesso. Belo Horizonte, 2017).

1. A IMPORTÂNCIA DOS ENDEREÇOS IPS

Os endereços IPs são fundamentais na arquitetura da internet, que permite a bilhões de pessoas e dispositivos se conectarem à rede, permitindo que trocas de volumes gigantescos de dados sejam operadas com sucesso. Nesses termos, a doutrina define que “*o endereço IP (internet protocol) é a cédula de identidade de cada terminal, somente sendo admitido um terminal para cada número IP disponível, de modo que seja impossível a conexão de dois dispositivos à rede com o mesmo número, o que gera conflitos na transmissão e recepção de dados e, comumente, faz com que a própria rede derrube o acesso de todos os dispositivos com números colidentes*”. (HAIKAL, V.A. Da significação jurídica dos conceitos integrantes do art. 5º. In: LEITE, G.S.; LEMOS, R. (Coords.). Marco Civil da Internet. São Paulo: Atlas, 2014, p. 320)

Quando se trata de investigações civis ou criminais que necessitam identificar a autoria de ilícitos ocorridos na Internet, trata-se de informação essencial, a fim de permitir localizar o terminal e, por consequência, a pessoal que o utilizava para a realização de ilícitos. Por isso, determinou-se um dever de guarda e armazenamento de um conjunto de informações utilizadas pelos usuários na internet, entre eles, o número IP.

2. DA PERDA DA UNIVOCIDADE DO ENDEREÇO IP NA TRANSIÇÃO ENTRE AS VERSÕES 4 E 6

Para o próprio funcionamento da internet, é essencial que todos identificadores sejam realmente únicos. Em especial, os números IPs ainda são utilizados para a identificação dos usuários da internet que tenham cometido atos ilícitos de qualquer natureza.

No entanto, os números IPs – assim como outros recursos críticos da internet – são finitos, necessitando de adaptações e novas versões que permitam sua expansão. Aqui, a analogia pode ser feita com números de telefone celular, que tiveram um número nove acrescentado a seu início.

Atentos ao esgotamento dos números de IP, especialistas propuseram uma nova versão para o protocolo, que é o chamado Protocolo de Internet Versão 6, ou IPv6. Essa versão utiliza quatro dígitos hexadecimais que permitem uma quantidade virtualmente inesgotável de endereços (HINDEN, R. M.; DEERING, S. E. Internet Protocol, Version 6 (IPv6). Internet Engineering Task Force – IETF. RFC2460. Dezembro de 1998. Disponível em: https://www.ietf.org/rfc/rfc2460.txt).

Para se ter uma comparação, o IPv4 previa um total de 4.3 bilhões de endereços, já o IPv6 prevê um total de 3.4×10^{38} – algo em torno de 340 milhões de

trilhões de trilhões, valor mais elevado que total estimados de estrelas existentes no universo.

Historicamente, os números IPs da versão 4 foram distribuídos de forma irregular entre as diversas regiões mundo. Os números alocados para a América Latina e do Caribe se esgotaram em 2014. Em outras regiões do globo, os IPs se esgotaram ainda mais rapidamente.

Na tentativa de resolver esse problema, diversas ferramentas foram desenvolvidas para permitir que provedores de conexão continuassem expandindo o acesso em suas regiões de atuação. Uma delas é oferecida pelo sistema de Tradução de Endereço de Rede (*Network Address Translation* – NAT), que permite o mesmo número IP seja utilizado por diversos terminais.

Esse compartilhamento de números, como bem pontuou o i. Ministro relator, pode acarretar alguns problemas na esfera judicial, em razão da possibilidade de dificultar a identificação de usuários na internet. Nos termos da doutrina:

> Ocorre que os endereços IP, cuja função nas investigações sempre se prestou à identificação da localização do terminal de onde partiu a conexão, não mais poderão ser considerados como fonte segura para fins de identificação de autoria. Todos que se conectam à internet recebem necessariamente um endereço IP, único para determinada data e horário. Também durante a navegação na internet, o número do IP é registrado por provedores de aplicações. No entanto, os endereços IP que historicamente foram concebidos para uso individual, enfrentam hoje um cenário de esgotamento, de modo que vêm sendo compartilhados entre pessoas ou organizações distintas, de forma simultânea. Esta realidade já se faz presente hoje também em redes compartilhadas dentro de empresas ou condomínios, com estabelecimento de um IP e NAT, ou ainda, em redes abertas de wi-fi. Assim, enquanto o sistema estiver calcado no atual protocolo de internet chamado IPV4 e não houver a substituição pela versão IPV6, continuará a ocorrer o compartilhamento de IP e, por conseguinte, a impossibilidade de identificação de autorias com base em tal informação. (BRAUN, Caroline; MARTINS, Rafael D'Enrrico; ARTESE, Gustavo (coord.). O Marco Civil da Internet, a guarda e fornecimento de

> registros por provedores de conexão e de acesso a aplicações de internet. São Paulo: Quartier Latin, 2015, p. 132)

3. ENTENDENDO A PORTA LÓGICA DE ORIGEM

Para a correta compreensão do que seja a porta lógica de origem associada ao número IP, é necessário ter em mente que, na expansão do IPv4, uma quantidade determinada de endereços foi reservada para "IPs privados", que seriam utilizados em redes não conectadas à internet. Além desses, um número de IPs públicos ou globais também foi designado, e são esses IPs públicos os utilizados para realizar a maioria das conexões na Internet.

Como mencionado acima, é utilizado o sistema NAT (*Network Address Translation*) a fim de permitir que múltiplos IPs privados sejam conectados à internet global por meio de um único IP público. Para esse compartilhamento, o sistema NAT cria uma tabela de correspondência entre os diversos IPs privados e o IP público comum, por meio do acréscimo de um número ao final do endereço IP. Esse número adicional é a chamada porta lógica de origem. Conforme detalhado pelo Instituto IRIS:

> Para que o compartilhamento ocorra, o roteador, seja o doméstico, seja aquele utilizado por um provedor de conexões de maior porte, faz o trabalho de intermediário entre a rede interna a ele conectada e a internet. Por meio de associação entre os IPs privados utilizados na rede interna e um ou mais IPs públicos designados àquele roteador, o sistema de NAT direciona os pacotes de dados entrando e saindo através dele, utilizando-se de portas que o permitem identificar qual dispositivo se conecta com qual endereço externo. As portas são um número acrescentado ao final do endereço de IP, que permitem ao NAT criar uma tabela de associações e viabilizar seu função. (Instituto Referência em Internet e Sociedade. Portas Lógicas e Registros de Acesso. Belo Horizonte, 2017. Disponível em http://irisbh.com.br/wp-content/uploads/2017/11/Portas-L%C3%B3gicas-e-Registros-de-Acesso_PT.pdf)

A título de ilustração, abaixo se encontra um exemplo de tabela de

tradução gerado pelo sistema NAT, sendo a coluna à esquerda os múltiplos IPs privados e à direita o IP público usado para conexão à internet e, entre eles, a equivalência é feita pela porta lógica de origem:

IP privado	IP público
192.168.1.103:3663	152.238.154.3:3663
192.168.1.101:4554	152.238.154.3:4554
192.168.1.105:2882	152.238.154.3:2882

Fonte: IRIS, 2017.

Portanto, como é possível perceber, o IP Público usado pelos três endereços internos é o mesmo. Há uma diferença, contudo, na porta lógica existente ao final.

Este ponto é de extrema relevância para o deslinde deste julgamento, pois é possível perceber que a univocidade do número IP será apenas restabelecida – enquanto não for finalizada a transição para o IPv6 – por meio da associação desse número adicional, a chamada porta lógica de origem.

4. DOS DEVERES DE GUARDA E ARMAZENAMENTO: REGULAÇÃO NO MARCO CIVIL DA INTERNET

Feitos os esclarecimentos técnicos acima, passa-se a discutir sobre a obrigatoriedade de guarda dos dados relacionados à porta lógica de origem. Para esse fim, é necessário afirmar o seguinte sobre o tema de guarda e armazenamento de informações cadastrais dos usuários, conforme a doutrina:

> Entre nós, como cediço, não há norma específica, opinando Marcel Leonardi que é dever dos provedores de internet, no momento de fazer a contratação com um usuário, colher todos os seus dados, principalmente nome, endereço e números de documentos pessoais válidos, e em alguns casos, os números de IP atribuídos e utilizados pelo usuário, os números de telefone utilizados para estabelecer a conexão e o endereço físico de instalação dos equipamentos informáticos utilizados para conexões de alta velocidade. A hipótese de os dados fornecidos pelo usuário não correspondem à realidade, não permitindo a sua identificação ou

> localização, para Marcel Leonardi sujeita os provedores a responder de forma solidária pelo ato ilícito cometido pelo terceiro que não puder ser identificado ou localizado. A proposta do autor, na verdade corresponde ao modelo pretendido e superado em sede de Direito Comparado, que configuraria o provedor de internet como solidariamente responsável por eventuais danos causados por usuários anônimos ou sem recursos para custear eventual condenação em uma demanda por danos. E deve ser enfatizado que o fato de a arquitetura da internet permitir o acesso anônimo e não identificável é uma realidade intransponível, ao menos por ora, valendo mencionar o brocardo jurídico impossibilium nulla obligatio est (não há obrigação de coisas impossíveis).
> Para aceder à internet e obter uma conta de correio eletrônico (e-mail), basta dirigir-se a um cybercafé, ou até mesmo a outros locais, como as redes abertas em aeroportos e centros comerciais, apenas munido de um computador portátil, sem qualquer possibilidade efetiva de um provedor host ter controle sobre a real identidade do usuário em geral. Obviamente, em muitos casos o usuário perpetrador de uma difamação, por exemplo, não terá como ser identificado ou alcançado. Para que esse ônus existisse, o formato atual da rede deveria ser reformulado (o que parece ser impensável ou impraticável) ou as cautelas exigidas de um provedor de conteúdo de terceiros seriam tantas que tornariam o serviço lento e excessivamente oneroso. A internet e seus serviços tiveram sua grande expansão em função da interatividade e da possibilidade de transações eletrônicas, não podendo ser aceitável a imputação de um ônus demasiado para os provedores, como o de garantir a real identidade de seus usuários. Contudo, cabe ao provedor de acesso conservar os dados existentes de seus usuários, apenas fornecendo-os por ordem judicial específica, sempre com um olhar em face de não poder ser exigido um dado impossível de ser informados. (PAULO ROBERTO BINICHESKI. Responsabilidade civil dos provedores de internet: direito comparado e perspectivas de regulamentação no direito brasileiro. Curitiba: Juruá, 2011, p. 236)

No Marco Civil da Internet, há duas categorias de dados que devem ser obrigatoriamente armazenados: os registros de conexão e os registros de acesso à aplicação. A previsão legal para guarda desses dados objetiva facilitar a identificação de usuários da internet pelas autoridades competentes e mediante ordem judicial, porque a responsabilização dos usuários é um dos princípios do uso da internet no Brasil, conforme o art. 3º, VI, da mencionada lei.

Segundo o Marco Civil da Internet, os registros de conexão são definidos como "*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".

Por sua vez, os provedores de aplicação constituídos "*na forma de pessoa jurídica e que exerçam essa atividade de forma organizada, profissionalmente e com fins econômicos*", tem a obrigação de armazenar, por seis meses o "*conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP*", conforme o art. 5º, VIII, do Marco Civil da Internet.

Essa distinção entre as duas categorias de agentes, provedores de conexão e de aplicação, visa garantir a privacidade e a proteção da vida privada dos cidadãos usuários da Internet. Diminui-se, assim, a quantidade de dados pessoais que cada um dos atores da internet possui, como forma de prevenção ao abuso da posse dessas informações. Como bem pontuado pelo i. Ministro relator:

> Nesse cenário, tem-se, na prática, uma repartição das informações de navegação: i) o provedor de conexão, ao habilitar um terminal para envio e recebimento de dados, atribui a ele um IP e registra o momento em que iniciada, interrompida e encerrada a conexão, e ii) cada provedor de aplicação registra o acesso dos IPs, momento de início e final, à sua própria aplicação. Desse modo, a totalidade da navegação de cada internauta dependerá da remontagem de cada uma das aplicações acessadas ao longo de uma única conexão.

Nesse momento, é necessário voltar a atenção ao disposto no art. 10, *caput* e § 1º, do Marco Civil da Internet, que está redigido da seguinte maneira:

> Art. 10. 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.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na

> forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

Assim, pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, *caput* e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem, como bem pontuou o i. Ministro relator.

Como afirmado acima, apenas esse número da porta de origem é capaz de fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais.

Nesse sentido, é de amplo conhecimento que esta Corte Superior firmou entendimento de que as prestadoras de serviço de internet, como as demais empresas, estariam sujeitas a um dever legal de escrituração e registro de suas atividades durante o prazo prescricional de eventual ação de reparação civil, dever que tem origem no art. 10 do Código Comercial de 1850, e atualmente encontra-se previsto no art. 1.194 do Código Civil, abaixo transcrito:

> Art. 1.194. O empresário e a sociedade empresária são obrigados a conservar em boa guarda toda a escrituração, correspondência e mais papéis concernentes à sua atividade, enquanto não ocorrer prescrição ou decadência no tocante aos atos neles consignados.

Conjugando esse dever de escrituração e registro com a vedação constitucional ao anonimato, nos termos do art. 5º, IV, da CF/88, os provedores de acesso à internet devem armazenar dados suficientes para a identificação do usuário, conforme os seguintes julgados desta Corte:

> (...) 2. Reconhecimento pela jurisprudência de um dever jurídico dos

> provedores de acesso de armazenar dados cadastrais de seus usuários durante o prazo de prescrição de eventual ação de reparação civil. Julgados desta Corte Superior. 3. Descabimento da alegação de impossibilidade fática ou jurídica do fornecimento de dados cadastrais a partir da identificação do IP. Julgados desta Corte Superior. 4. Considerações específicas acerca da aplicabilidade dessa orientação ao IP dinâmico consistente naquele não atribuído privativamente a um único dispositivo (IP fixo), mas compartilhado por diversos usuários do provedor de acesso. (...) (REsp 1622483/SP, Terceira Turma, DJe 18/05/2018)
>
> (...) 5. Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, 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 in omittendo. 6. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço. (...) (REsp 1398985/MG, Terceira Turma, DJe 26/11/2013)
>
> (...) 5.- É juridicamente possível o pedido à empresa de telefonia de exibição do nome do usuário de seus serviços que, utiliza-se da internet para causar danos a outrem, até por ser o único modo de o autor ter conhecimento acerca daqueles que entende ter ferido a sua reputação. (...) (REsp 879.181/MA, Terceira Turma, DJe 01/07/2010)

Da mesma forma que com as informações mencionadas acima, é imperioso o reconhecimento da necessidade da guarda da porta lógica. Afirmar que não há obrigação de guarda ou fornecimento da porta de origem consiste em fechar os olhos deliberadamente para os mecanismos essenciais que fazer a internet funcionar. Ressalte-se, nesse ponto, o que i. Ministro relator afirmou:

> Noutros termos, ainda que o legislador, ao estabelecer a obrigação de guarda dos dados de acesso à aplicação tenha se referido apenas aos respectivos registros de acesso (art. 15 da Lei n. 12.965/2014), os quais, por sua vez, conforme a definição do art. 5º, VIII, se restringe à data e hora de uso "a partir de um determinado endereço IP", enquanto não se restabelecer a relação de individualidade dos IPs é preciso que se entenda incluída no endereço IP a correspondente porta lógica de origem, em razão da indissociabilidade entre as duas tecnologias para o efetivo acesso

> individualizado à internet e às aplicações. Do contrário, a adoção da tecnologia paliativa resultaria no esvaziamento da lei, tornando inviável a identificação e responsabilidade desses sujeitos.

Reafirmada a obrigação de guardar e fornecer as informações relacionadas à porta lógica de origem, cumpre investigar a quem incumbe tal obrigação, se apenas aos provedores de conexão ou se, igualmente, aos provedores de aplicação de internet.

Neste ponto, tal como feito pelo i. Ministro relator, é necessário destacar a importância do relatório produzido pelo Grupo de Trabalho sobre a transição para a versão 6 do IP, no âmbito da Agência Nacional de Telecomunicações – Anatel, em cujas conclusões é possível verificar a necessidade de guarda e do posterior fornecimento das portas lógicas, conforme se verifica nos trechos abaixo:

> CG-NAT44 e a quebra de sigilo nos casos previstos em lei: Com relação à guarda da porta, requisito necessário para que se viabilize a quebra de sigilo nos casos previstos legalmente, foi apontado pelas prestadoras a necessidade de padronização do LOG de registros de conexão, da forma que os pedidos de quebra de sigilo são gerados pelos demandantes e a conscientização dos provedores de conteúdo/aplicações para também guardar a porta de origem da conexão além das prestadoras. Ademais, a Anatel ponderou que a redução da proporção dos endereços IPv4 público/privado adotada no CG-NAT44 ajudaria na redução de problemas neste cenário. (ANATEL, p. 7)

> Tanto no Grupo de Trabalho do NIC.br como no Grupo de Trabalho da ANATEL foi intensamente discutida a questão da identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado. Em ambos os Grupos de Trabalho foi consenso que a única forma das prestadoras 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 da conexão" que estava sendo utilizada durante a conexão. Dessa forma, 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".
> Em uma Conexão à Internet, para cada sessão aberta pelo usuário, é utilizada uma "porta lógica" para sua comunicação com outras redes e equipamentos. Assim, mesmo quando dois usuários fazem o uso

> compartilhado de um mesmo IPv4, eles usarão portas distintas para a sua comunicação.
> Será com base na informação da "porta lógica de origem" que as identificações judiciais para fins de quebra de sigilo e interceptação legal continuarão sendo possíveis de serem realizadas de forma unívoca. Portanto, torna-se necessário que na solicitação de quebra de sigilo seja informada, além dos atributos atuais (endereço IP de origem, data, hora e fuso da conexão), a porta de origem da comunicação.
> As obrigações das prestadoras com relação às suas responsabilidades sobre a quebra de sigilo de identificação, comunicação ou interceptação telemática de um usuário permanecem sem qualquer alteração. Contudo, para que a identificação unívoca de usuário seja possível a partir da implantação do CG-NAT44, será necessário que as entidades com poder requisitório informem, além do (1) endereço IPv4 de origem e (2) do período de tempo em que foi realizado o acesso (acompanhado do fuso horário aplicável), passem também a informar (3) a porta de origem.
> Em obediência ao que está estabelecido no Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), as prestadoras estão adaptando seus sistemas e equipamentos para permitir a identificação unívoca no cenário de compartilhamento, passando a registrar também a porta de origem, além de todos os parâmetros atuais de conexão à internet (endereço IP de origem, período da conexão e fuso horário aplicável).
> Diante do exposto, é importante reforçar que durante o período de utilização da solução paliativa do CG-NAT44, para que o processo de apuração de ilícitos na Internet não fique prejudicado, é necessário que, não só provedores de acesso, como também provedores de conteúdo e serviços de internet (bancos e sites de comércio eletrônico, por exemplo) adaptem seus sistemas para possibilitar a armazenagem dos registros de aplicação (provedores de aplicação) ou registros de conexão (provedores de acesso) com a informação da "porta lógica de origem" utilizada. (p. 14)

Como visto a partir da recomendação do grupo de trabalho criado no âmbito da agência reguladora das telecomunicações, da mesma forma que ressaltado pelo i. Ministro relator, tanto os provedores de conexão quanto os provedores de aplicação necessitam desse número adicional, a porta de origem, para realizarem suas atividades na internet.

De fato, apenas com as duas pontas da informação – conexão e aplicação – é possível resolver a questão da identidade de usuários na internet, que estejam utilizam um compartilhamento da versão 4 do IP. Portanto, é inegável que ambas as categorias de provedores de que dispõe o Marco Civil da Internet

possuem a obrigação de guarda e fornecimento das informações da porta lógica de origem associada ao endereço IP.

Ademais, cumpre ressaltar que este é um problema que tende a se extinguir, pois, à medida em que a transição para IPv6 for efetuada, haverá menor necessidade de compartilhamento do IP por meio de porta lógica de origem.

Por fim, quanto á alegação de cerceamento de defesa, considerando que, como indicado pelo Ministro relator, haverá a necessidade de retorno dos autos ao Juízo de 1º grau de jurisdição para a correta instrução processual, deixa-se igualmente de apreciar a questão.

Quanto à discussão sobre o possível descumprimento da ordem judicial, a recorrente alega que a remoção não ocorreu de forma integral, que, com a utilização de endereços IP com origem mascarada, o conteúdo seria acessível, pois disponível para usuários da internet georreferenciados em outros países.

Contudo, considerando que os autos deverão retornar à ao Juízo de 1º grau de jurisdição, deixa-se de apreciar o mérito desta questão neste momento, considerando que ainda poderá haver mais instrução processual sobre as alegações, a fim de amadurecer este ponto do litígio, pois ausente do acórdão recorrido.

Forte nessas razões, louvando o voto do i. Ministro relator, acompanho suas conclusões para CONHECER e DAR PROVIMENTO ao recurso especial "*para cassar a sentença e fixar o entendimento de obrigatoriedade de fornecimento da porta lógica associada a endereço IPv4*" com o consequente retorno dos autos à origem.

CERTIDÃO DE JULGAMENTO
TERCEIRA TURMA

Número Registro: 2018/0322140-0 **PROCESSO ELETRÔNICO** **REsp 1.784.156 / SP**

Números Origem: 10786606020158260100 20170000423509 20180000209328

PAUTA: 11/06/2019 JULGADO: 25/06/2019

Relator
Exmo. Sr. Ministro **MARCO AURÉLIO BELLIZZE**

Presidente da Sessão
Exmo. Sr. Ministro MOURA RIBEIRO

Subprocuradora-Geral da República
Exma. Sra. Dra. MARIA SOARES CAMELO CORDIOLI

Secretário
Bel. WALFLAN TAVARES DE ARAUJO

AUTUAÇÃO

RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578
		CAMILLA DO VALE JIMENE - SP222815
		JULIANA ABRUSIO FLORÊNCIO - SP196280
		CAMILA MACEDO MARTINS - SP285568
		PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179
		RENATO GOMES DE MATTOS MALAFAIA - SP368020
		ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534
		EDUARDO LUIZ BROCK - SP091311
		FABIO RIVELLI - SP297608
		RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487
		JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

ASSUNTO: DIREITO CIVIL - Responsabilidade Civil

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Prosseguindo no julgamento, após o voto-vista da Sra. Ministra Nancy Andrighi, acompanhando o Relator, dando provimento ao recurso especial, pediu vista, antecipadamente, o Sr. Ministro Ricardo Villas Bôas Cueva. Aguardam os Srs. Ministros Moura Ribeiro e Paulo de Tarso Sanseverino.

RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

RELATOR	:	MINISTRO MARCO AURÉLIO BELLIZZE
RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578 CAMILLA DO VALE JIMENE - SP222815 JULIANA ABRUSIO FLORÊNCIO - SP196280 CAMILA MACEDO MARTINS - SP285568 PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179 RENATO GOMES DE MATTOS MALAFAIA - SP368020 ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534 EDUARDO LUIZ BROCK - SP091311 FABIO RIVELLI - SP297608 RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487 JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

VOTO-VISTA

O EXMO. SR. MINISTRO RICARDO VILLAS BÔAS CUEVA: Pedi vista dos autos para melhor compreensão da controvérsia.

Trata-se de recurso especial interposto por TIM CELULAR S.A., com fulcro no art. 105, inciso III, alíneas "a" e "c", da Constituição Federal, contra acórdão prolatado pelo Tribunal de Justiça do Estado de São Paulo assim ementado:

> "*Obrigação de fazer. Remoção do ar de 'blog' e de perfil hospedados em URL. Fornecimento de dados cadastrais disponíveis e registros eletrônicos, inclusive porta lógica, com datas e horários, no padrão UTC. Apelada é somente provedora de aplicação e não de conexão. Ausência de respaldo legal para a exigência de fornecimento de origem dos IPs com a respectiva porta lógica. Devido processo legal observado. Desnecessidade de outras provas. Marco Civil da Internet não apresenta previsão legal para que o recorrido colete e armazene dados de porta lógica de usuário das páginas indicadas. Sucumbência observou as peculiaridades da demanda, ou seja, o objeto da lide, e não itens isolados pedidos. Apelo desprovido*" (e-STJ fl. 591).

Ao relatório apresentado pelo Ministro Marco Aurélio Bellizze, acrescenta-se apenas que o feito foi levado a julgamento, pela Terceira Turma, em 11/6/2019, oportunidade em que, após a prolação do voto de Sua Excelência, dando provimento ao recurso para cassar a sentença de primeiro grau, fixar o entendimento de obrigatoriedade de fornecimento da porta lógica associada a endereço IPv4 por provedores de aplicação de internet e determinar o retorno dos autos à origem, pediu vista antecipadamente a Ministra Nancy Andrighi.

Acrescenta-se, ainda, a informação de que, na sessão de 25/6/2019, a Ministra

Nancy Andrighi apresentou seu voto-vista, acompanhando integralmente as conclusões do Relator do feito, oportunidade em que, também de forma antecipada, pedi vista dos autos e ora apresento meu voto.

É o relatório.

O cerne da controvérsia recursal reside em definir se constitui obrigação dos provedores de aplicações de *internet* armazenar, para fins de eventual necessidade de identificação dos terceiros usuários de seus serviços, informações relativas às portas lógicas de origem eventualmente associadas aos IPs a eles atribuídos.

Cuida-se, na origem, de ação cominatória ajuizada por TIM CELULAR S.A. (renomada empresa provedora de conexão), ora recorrente, em desfavor de GOOGLE BRASIL INTERNET LTDA. (renomada empresa provedora de aplicações de *internet*), ora recorrida, com o propósito de vê-la obrigada a (i) remover o conteúdo alegadamente ilícito por ela hospedado e que teria sido publicado por um terceiro usuário não identificado por meio de dois URLs específicos: o primeiro de um blog (http://www.convites timbeta.blogspot.com.br/) e o segundo de um perfil na rede social Google Plus (https://plus.google.com/117787748233817825419/posts), e (ii) fornecer *"os dados de cadastro disponíveis e os registros eletrônicos (IPs de origem, com sua respectiva porta lógica, datas e horários, com fuso-horário no padrão UTC) atrelados à criação e demais acessos administrativos ao Blog e perfil do Google Plus acima apontados"* (e-STJ fl. 21 - grifou-se).

O juízo de primeiro grau deferiu a antecipação dos efeitos da tutela para determinar a ré que promovesse tanto a remoção do conteúdo apontado na inicial quanto o fornecimento dos dados e registros solicitados pela parte autora para fins de identificação do efetivo responsável por sua publicação (e-STJ fl. 81).

Devidamente citada, a ré opôs embargos de declaração à decisão antecipatória e apresentou contestação. Mais tarde, peticionou nos autos (e-STJ fls. 111/146), informando o cumprimento da ordem de remoção e de fornecimento dos dados e registros que possuía, ressaltando a impossibilidade de fazê-lo (e a inexistência de obrigação legal nesse sentido) apenas no tocante ao apontamento das portas lógicas de origem eventualmente atreladas aos IPs fornecidos.

Ao sentenciar o feito, julgando antecipadamente a lide, o magistrado singular concluiu pela procedência parcial do pedido inicial, pelo que tornou "*parcialmente definitiva a tutela antecipada, determinando que a ré, como já o fez, remova o 'blog' e o perfil indicados na petição inicial e forneça os dados que possua a respeito*" (e-STJ fl. 317 - grifou-se).

Por entender configurada a reciprocidade sucumbencial, determinou que autora e

ré dividissem o pagamento de custas e despesas processuais e que arcassem com os honorários advocatícios dos patronos umas das outras, que foram fixados em 10% (dez por cento) do valor atribuído à causa. Assim o fez, por ter considerado descabida a pretensão de indicação de registros relativos às portas lógicas de origem a partir da seguinte fundamentação:

> "*(...) Quanto ao pedido de disponibilização dos dados cadastrais e de utilização dos aplicativos por parte do usuário, não há que se exigir a apresentação, tampouco o armazenamento, dos dados de porta lógica do usuário das páginas em questão, diante da inexistência de previsão legal para tanto, desse modo, deve a ré apenas disponibilizar os registros de conexão do usuário responsável pelas publicações, o que já foi feito, cabendo à autora, posteriormente, as medidas judiciais que entender pertinentes.*
>
> *Caberia ao provedor de conexão e não ao de aplicação, como a ré, o fornecimento dos dados atinentes à "porta lógica de origem*" (e-STJ fl. 316).

A referida sentença foi mantida íntegra pela Corte local que, ao negar provimento ao apelo interposto pela autora da demanda, ora recorrente, concluiu que os provedores de aplicações de *internet* não têm a obrigação legal de armazenar e, consequentemente, de fornecer dados relativos às portas lógicas eventualmente associadas aos IPs utilizados pelos terceiros usuários de seus serviços.

Daí a interposição do recurso especial que ora se apresenta, no qual a recorrente aponta, além da existência de dissídio pretoriano, a violação dos arts. 7º, 9º 85 e 86 do Código de Processo Civil de 2015 e dos arts. 5º, inciso VIII, 10, § 1º, e 11, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet).

Em suas razões recursais (e-STJ fls. 598/645), insiste a recorrente na tese de que constitui obrigação legal do provedor de aplicações armazenar (e disponibilizar por ordem judicial) os registros relativos às portas lógicas, pois, embora tal registro "*não esteja expressamente previsto no art. 5º do Marco Civil da Internet, não é menos verdade que o rol não é taxativo, especialmente em função da disposição contida no art. 10, §1º*" (e-STJ fl. 620) da referida lei.

Tece, ainda, considerações a respeito da suposta nulidade da sentença de primeiro grau por cerceamento de defesa, do não cumprimento da ordem judicial de remoção e do equívoco das instâncias de origem no reconhecimento da reciprocidade sucumbencial.

Diante desse cenário fático-processual, a solução mais adequada para a controvérsia é justamente aquela já apresentada no laborioso voto lançado pelo Relator, Ministro Marco Aurélio Bellize, que reconheceu ser obrigação legal imposta também aos

provedores de aplicações de internet, enquanto não concluída no país a implementação da tecnologia IPv6, o apontamento da porta lógica de origem eventualmente associada a endereço IPv4 para fins de identificação de terceiros usuários de seus serviços que, eventualmente, os tenham utilizado para a prática de atos ilícitos.

Como consabido, o Internet Protocol (ou simplesmente IP) é o protocolo de comunicação sobre o qual se baseia a rede mundial de computadores como a conhecemos hoje. Tal protocolo funciona, resumidamente, por meio da veiculação de pacotes de dados encapsulados que podem ser transmitidos por diversos meios de telecomunicação, servindo, também para definir mecanismos de endereçamento para identificação desses pacotes.

O protocolo IP poderia ser comparado a um sistema de correios capaz de identificar o destinatário e o remetente desses pacotes de dados fazendo tudo quanto o necessário para que a informação remetida por um usuário do sistema chegue ao outro.

Esses rementes/destinatários são identificados a partir do que se denomina, de forma popular, "endereço IP", que, na versão IPv4 (a predominantemente utilizada em todo o mundo desde a popularização da internet) é representado por um conjunto de quatro números de até três dígitos (exemplo: 192.168.1.101).

Ocorre que essa versão (IPv4) conta com número limitado de endereços, que se esgotaram em virtude da revolução digital que testemunhamos ao longo das últimas décadas.

Para contornar esse problema técnico e assegurar o acesso à internet a todos enquanto não promovida a implementação da tecnologia IPv6 (que permitirá a individualização de mais de trezentos e quarenta undecilhões de endereços distintos) optou-se pela utilização de um método paliativo, mais especificamente, pela adoção do sistema de Network Adress Translation (NAT) pelos provedores de conexão.

As primeiras aplicações desse sistema NAT foram pensadas para redes domésticas (as chamadas Local Area Networks - LANs), nas quais cada cliente de um provedor de conexões recebia seu próprio IP público e o compartilhava entre os dispositivos (computadores) conectados a sua rede residencial ou de trabalho que eram identificados pelas chamadas portas lógicas.

O progressivo esgotamento dos IPs (da versão IPv4) fez com que o referido sistema fosse utilizado em larga escala pelos próprios provedores de conexão, recebendo assim a denominação de Carrier Grade NAT (CGNAT) ou Lage Scale NAT (LSN).

Essa nova realidade fez com que aquilo que conhecemos como endereço IP (na versão IPv4), ou seja, aquela sequência representada por um conjunto de quatro números de

até três dígitos (exemplo: 192.168.1.101), não seja sempre suficiente para a exata identificação de um usuário da internet.

Isso porque, a partir do momento em que os provedores de conexão passaram a se valer do sistema CGNAT ou LSN, tornou-se recorrente a atribuição simultânea de um mesmo IP público a uma pluralidade de usuários distintos, que são individualizados apenas pela representação daquilo que se denomina serem suas respectivas portas lógicas de origem (representadas pela adição de outro número de até quatro dígitos acrescido ao final do endereço IP - ex: 192.168.1.101:3663).

A questão jurídica que se põe à apreciação desta Corte Superior é resultado do choque desse cenário fático (em que a simples indicação do endereço IP de um determinado usuário, por si só, pode ser ineficaz para sua identificação) com a literalidade das disposições insertas nos arts. 5º, inciso VIII, e 15 do denominado Marco Civil da Internet (Lei nº 12.965/2014).

Com efeito, o art. 15 do referido diploma legal estabelece que o provedor de aplicações de internet "*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*", ao passo em que o art. 5º, inciso VIII, da mesma lei dispõe que pela expressão "*registros de acesso a aplicações da internet*" se deve considerar "*o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP*".

A interpretação literal das normas legais em comento justificaria a conclusão esposada pelas instâncias de origem na hipótese em exame, no sentido de que não seriam obrigações legalmente impostas aos provedores de aplicação o armazenamento e, consequentemente, o fornecimento de informações relativas às específicas portas lógicas de origem que estariam atreladas aos endereços de IP (IPv4) utilizados por terceiros na eventual prática de ilícitos por meio de seus serviços.

Essa, todavia, não parece ser a melhor interpretação a ser dada à norma em comento e, menos ainda, a que traduz a adequada solução do caso em apreço.

Nesse aspecto, tenho por impossível não perfilhar a orientação de que a interpretação teleológica de todo o conjunto de disposições do Marco Civil da Internet leva à conclusão de que, independentemente da referência expressa, no inciso VIII do art. 5º da referida lei, apenas à expressão "endereço de IP", é inegável a existência do dever de guarda e fornecimento - tanto pelos provedores de aplicação quanto pelos de conexão - das informações relacionadas às respectivas portas de origem a ele

atreladas em virtude da utilização do sistema NAT como solução alternativa e paliativa à não conclusão da implementação do sistema IPv6 no país.

Como bem anotou a Ministra Nancy Andrighi, no voto-vista que proferiu ao somar seu ponto de vista ao do Relator do presente feito, "*apenas esse número da porta de origem é capaz de fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela*" (pag. 11).

É de se dizer também que não se pode engessar a própria inteligência da lei em virtude do emprego de uma expressão específica, especialmente quando essa expressão é própria da ciência da computação, área do conhecimento humano relativamente recente, dinâmica e que se encontra em processo de constante e acelerada evolução.

Primeiro porque a interpretação cega e literal do referido art. 5º, inciso VIII, acaba por ceder diante do que estabelece o § 1º do art. 10 da própria Lei nº 12.965/2014, segundo o qual, o provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e aplicações de internet por ele mantidos, "*de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial".*

Além disso, acaso considerada a mera literalidade da norma, tal interpretação representaria verdadeira negação da lei ao irrefreável desenvolvimento tecnológico, consistindo na imposição de uma espécie de prazo de validade à norma jurídica, pois seria completamente absurdo exigir que, ao advento de cada nova tecnologia, fosse necessária a promulgação de lei para alterar a vigente redação das disposições do Marco Civil da Internet.

Merecem destaque, ainda, as conclusões constantes do relatório final de atividades do Grupo de Trabalho para implantação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações (GT-IPv6) - que contou com a participação da ANATEL, do Ministério das Comunicações e dos maiores provedores de conexão com atuação no país -, que apontaram para a necessidade de que os provedores de conteúdo e serviços de internet (que receberam da Lei nº 12.965/2014 a denominação de provedores de aplicações de internet) adaptassem seus sistemas para possibilitar a armazenagem dos registros de suas respectivas aplicações com a informação relativa à porta lógica de origem eventualmente relacionada ao endereço de IP de seus usuários durante o período de utilização da solução paliativa CG-NAT44 (que está em uso no Brasil):

"*(...).*

Tanto no Grupo de Trabalho do NIC.br como no Grupo de Trabalho da ANATEL foi intensamente discutida a questão da identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado. Em ambos os Grupos de Trabalho foi consenso que a única forma das prestadoras 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 da conexão' que estava sendo utilizada durante a conexão. Dessa forma, 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'.

Em uma Conexão à Internet, para cada sessão aberta pelo usuário, é utilizada uma 'porta lógica' para sua comunicação com outras redes e equipamentos. Assim, mesmo quando dois usuários fazem o uso compartilhado de um mesmo IPv4, eles usarão portas distintas para a sua comunicação.

Será com base na informação da 'porta lógica de origem' que as identificações judiciais para fins de quebra de sigilo e interceptação legal continuarão sendo possíveis de serem realizadas de forma unívoca. Portanto, torna-se necessário que na solicitação de quebra de sigilo seja informada, além dos atributos atuais (endereço IP de origem, data, hora e fuso da conexão), a porta de origem da comunicação.

As obrigações das prestadoras com relação às suas responsabilidades sobre a quebra de sigilo de identificação, comunicação ou interceptação telemática de um usuário permanecem sem qualquer alteração. Contudo, para que a identificação unívoca de usuário seja possível a partir da implantação do CG-NAT44, será necessário que as entidades com poder requisitório informem, além do (1) endereço IPv4 de origem e (2) do período de tempo em que foi realizado o acesso (acompanhado do fuso horário aplicável), passem também a informar (3) a porta de origem.

Em obediência ao que está estabelecido no Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), as prestadoras estão adaptando seus sistemas e equipamentos para permitir a identificação unívoca no cenário de compartilhamento, passando a registrar também a porta de origem, além de todos os parâmetros atuais de conexão à internet (endereço IP de origem, período da conexão e fuso horário aplicável).

Diante do exposto, é importante reforçar que durante o período de utilização da solução paliativa do CG-NAT44, para que o processo de apuração de ilícitos na Internet não fique prejudicado, é necessário que, não só provedores de acesso, como também provedores de conteúdo e serviços de internet (bancos e sites de comércio eletrônico, por exemplo) adaptem seus sistemas para possibilitar a armazenagem dos registros de aplicação (provedores de aplicação) ou registros de conexão (provedores de acesso) com a informação da 'porta lógica de origem' utilizada.

Caso contrário, será inviável a identificação unívoca de um usuário que está fazendo uso de um determinado IP compartilhado. Este é um risco que necessita ser compartilhado com todos os elos da cadeia de investigação para garantir o correto funcionamento do processo de investigação.

Este tema foi amplamente discutido nas reuniões do grupo, sendo que as prestadoras, por meio do Sinditelebrasil, enviaram uma carta à ANATEL e órgãos responsáveis pela apuração de ilícitos na Internet detalhando esta questão.

> *Ademais, como a proporção de endereços IPv4 Privado/Público impacta diretamente na quantidade de portas possíveis de alocação para os clientes e nos arquivos de logs necessários para garantir a quebra de sigilo, definiu-se que as prestadoras devem implementar o CG-NAT44 de forma a minimizar o impacto na quebra de sigilo, ou seja, com a menor taxa de compartilhamento possível*" (https://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769 - págs. 14/15 - grifou-se).

Desse modo, resulta inequívoco que a irresignação recursal merece mesmo prosperar, como bem apontou o Ministro Relator, sendo certo, ainda, que, em virtude da necessidade de retorno dos autos, para que seja concedida às partes a oportunidade de produzirem as provas que acharem convenientes a respeito da eventual impossibilidade técnica de cumprimento da obrigação e do suposto cumprimento da ordem de remoção do conteúdo objeto da controvérsia, fica prejudicada a discussão a respeito da distribuição dos ônus sucumbenciais, que será refeita quando da prolação de nova sentença.

Ante o exposto, acompanhando integralmente o voto do Relator, dou provimento ao recurso especial.

É o voto.

CERTIDÃO DE JULGAMENTO
TERCEIRA TURMA

Número Registro: 2018/0322140-0 **PROCESSO ELETRÔNICO** **REsp 1.784.156 / SP**

Números Origem: 10786606020158260100 20170000423509 20180000209328

PAUTA: 11/06/2019 JULGADO: 05/11/2019

Relator
Exmo. Sr. Ministro **MARCO AURÉLIO BELLIZZE**

Presidente da Sessão
Exmo. Sr. Ministro MOURA RIBEIRO

Subprocurador-Geral da República
Exmo. Sr. Dr. ANTÔNIO CARLOS ALPINO BIGONHA

Secretário
Bel. WALFLAN TAVARES DE ARAUJO

AUTUAÇÃO

RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578
		CAMILLA DO VALE JIMENE - SP222815
		JULIANA ABRUSIO FLORÊNCIO - SP196280
		CAMILA MACEDO MARTINS - SP285568
		PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179
		RENATO GOMES DE MATTOS MALAFAIA - SP368020
		ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534
		EDUARDO LUIZ BROCK - SP091311
		FABIO RIVELLI - SP297608
		RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487
		JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

ASSUNTO: DIREITO CIVIL - Responsabilidade Civil

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Prosseguindo no julgamento, após o voto-vista do Sr. Ministro Ricardo Villas Bôas Cueva, a Turma, por unanimidade, deu provimento ao recurso especial, nos termos do voto do Sr. Ministro Relator. Os Srs. Ministros Moura Ribeiro (Presidente), Nancy Andrighi, Paulo de Tarso Sanseverino e Ricardo Villas Bôas Cueva votaram com o Sr. Ministro Relator.