Instituto de Referência em Internet e Sociedade

PORTAS LÓGICAS E REGISTROS DE ACESSO

DAS POSSIBILIDADES TÉCNICAS AOS ENTENDIMENTOS DOS TRIBUNAIS BRASILEIROS

IRIS
Instituto de Referência em Internet e Sociedade

Instituto de Referência em Internet e Sociedade

PORTAS LÓGICAS E REGISTROS DE ACESSO

DAS POSSIBILIDADES TÉCNICAS AOS ENTENDIMENTOS DOS TRIBUNAIS BRASILEIROS

Conselho científico
Fabrício B. Pasquot Polido
Lucas Costa dos Anjos

Autoria
Iara Vianna Lima
Luiza Couto Chaves Brandão
Odélio Porto Júnior
Pedro Vilela Resende Gonçalves
Victor Barbieri Rodrigues Vieira

Como citar em ABNT
LIMA, Iara Vianna et al. **Portas lógicas e registros de acesso**: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: http://bit.ly/36bdDTC. Acesso em: DD mmm. AAAA

SUMÁRIO

1. Introdução 4

2. Alguns esclarecimentos técnicos necessários 5

O sistema NAT (Network Address Translation) 6

Implementação do IPv6 no Brasil 8

3. O Marco Civil da Internet e Portas Lógicas 9

4. Sistemas NAT e Portas Lógicas na União Europeia e na Austrália 11

Marco Legal na União Européia 11

Austrália 15

5. Metodologia de coleta e análise dos dados dos tribunais brasileiros em tema de acesso a portas lógicas 18

Método de varredura 18

Marco temporal 19

Variáveis - Banco de Dados 01 19

Variáveis - Banco de Dados 02 22

6. Análise dos resultados Perfil das decisões judiciais 23

Perfil das decisões 23

Decisões e fundamentos 26

7. Considerações finais 30

8. Referências 31

9. Anexos 35

1. Considerações iniciais[1]

"A ligação entre questões técnicas e de política pública é de particular importância para a governança da internet."[2] O esgotamento da versão 4 do IP (IPv4), a implementação de sua versão 6 (IPv6) e o compartilhamento de IPS como solução transitória refletem a relação entre a arquitetura da internet, sua camada técnica[3], e aquela de política pública, relativa ao acesso e à operabilidade da internet. Esse problema ainda se traduz em consequências jurídicas nos casos em que registros de acesso são requisitados em investigações criminais e processos judiciais de natureza variada, com a finalidade de identificar um usuário específico.

Um endereço de IP (*Internet Protocol*) é uma sequência numérica usada para identificar um dispositivo conectado à internet, e para orientar os pacotes de dados que chegam e saem daquele dispositivo. No processo de transição das versões de IP, o problema de esgotamento dos blocos de IPv4s tem sido solucionado por meio do compartilhamento entre vários usuários de um mesmo IP público. Essa foi a solução técnica escolhida no Brasil, e em diversos outros países, a fim de que a expansão da internet não fosse interrompida no período de transição de protocolos. Assim ficou a cargo dos provedores de conexão a implementação das técnicas de compartilhamento denominadas *Network Address Translation* - NAT. Com essas técnicas, surgiram dificuldades adicionais para identificação de usuários online que utilizam IP compartilhados. Nesse sentido, os tribunais estão sendo demandados quanto ao fornecimento das chamadas "portas lógicas", que designam uma sequência numérica adicional utilizada em conjunto com número IP para identificar a localização de dispositivos conectados à internet.

Como o termo "porta lógica" não está previsto expressamente no texto do Marco Civil da Internet (Lei 12.965/2014), o Poder Judiciário brasileiro tem sido demandado a responder se:

- Existe uma obrigação legal de armazenamento dos dados referentes à "porta lógica?
- Se sim, de quem a responsabilidade pelo armazenamento e disponibilização desses dados às autoridades competentes: dos provedores de conexão, de aplicação, ou de ambos?
- 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)?

Com base nesses questionamentos, este estudo busca integrar questões técnicas, opções regulamentadoras e interpretações judiciais sobre a responsabilidade de guarda de registros e os pedidos que chegam ao Poder Judiciário relacionados ao período de transição do IPv4 para o IPv6 no Brasil.

1 Estudo realizado sob a coordenação de Fabrício B. Pasquot Polido e Lucas Costa dos Anjos, Membros do Conselho Científico do **Instituto de Referência em Internet e Sociedade - IRIS**, tendo contribuído na qualidade de coautores para este trabalho as pesquisadoras e os pesquisadores Iara Vianna Lima, Luiza Couto Chaves Brandão, Odélio Porto Júnior, Pedro Vilela Resende Gonçalves, Victor Barbieri Rodrigues Vieira.

2 WEBER, Rolf H. *Shaping internet governance: Regulatory challenges.* Springer Science & Business Media, 2010, p. 187.

3 Para um maior compreensão deste artigo é necessário ter um conhecimentos básicos de como se dá o funcionamento da internet. Para isso recomendamos que o leitor veja a série de vídeos animados "Como funciona a Internet", produzida pelo NIC.br. Disponível em: <http://bit.ly/2frAF03>

O estudo aborda, primeiramente, os aspectos técnicos envolvidos na guarda de registros de portas lógicas, seja por provedores de aplicação, seja por provedores de conexão, e como o tema tem sido abordado na União Europeia e na Austrália. Em seguida, é apresentada a metodologia de análise e varredura das decisões, aplicação das variáveis e coleta dos dados. Por fim, são apresentados os resultados da pesquisa de decisões judiciais sobre a temática, de modo a delinear as características das decisões, seus dispositivos e fundamentos. Dessa forma, o estudo se propõe a compreender argumentos e as soluções dadas pelos tribunais brasileiros.

2. Alguns esclarecimentos técnicos necessários

O IP, ou *Internet Protocol*,[4] é o principal protocolo de comunicação sobre o qual se baseia a internet como a conhecemos hoje. O IP funciona por meio de pacotes de dados encapsulados que podem ser transmitidos via diversos meios de telecomunicação. Ele também define os mecanismos de endereçamento para a identificação da origem desses pacotes. Uma analogia comum em relação ao IP é aquela que compara os pacotes de dados a envelopes de carta contendo um determinado conteúdo. O Protocolo IP seria comparado ao sistema de correios que identifica tanto o destinatário como o remetente e faz tudo o que seja necessário para levar a carta de um usuário do sistema para o outro.

O IP identifica seus destinatários e remetentes a partir do chamado "**endereço IP**", representado por conjunto de quatro números de até três dígitos (*e.g.* 192.168.1.100) que permitem que pacotes de dados sejam transmitidos entre terminais conectados a uma rede. Atualmente, a versão predominante do protocolo é a quarta, o **IPv4**, utilizada amplamente pela internet comercial desde seu início, na década de 1990. O IPv4, entretanto, conta com um número limitado de endereços, que se esgotaram após o aumento da demanda por acesso à internet nas décadas seguintes a sua implementação.

Já prevendo o **esgotamento dos números de IP**, especialistas propuseram ainda na década de 1990 uma nova versão para o protocolo. O Protocolo de Internet Versão 6, ou IPv6,[5] utiliza quatro dígitos hexadecimais que permitem uma quantidade virtualmente inesgotável de endereços. Enquanto o IPv4 previa um total de 4.3 bilhões de endereços (menos de um para cada pessoa no planeta), o IPv6 prevê um total de 3.4×10^{38} endereços (mais que o total estimado de estrelas no universo conhecido!).

Os endereços IPv4 foram distribuídos de forma irregular e arbitrária entre macrorregiões do globo, ainda nas décadas de 1980 e 1990. Os IPs delegados ao órgão responsável pela macrorregião da América Latina e do Caribe (LACNIC) se esgotaram em 2014. Em outras regiões de maior penetração da internet, os IPs se esgotaram mais rapidamente. Ainda diante de assimetrias características da regulação global da Internet, a demanda por novas conexões - e consequentemente de IPs - continuou crescendo. Para contornar o problema, diversas ferramentas foram desenvolvidas para permitir que provedores de conexão continuassem expandindo o acesso em suas regiões de atuação. Uma delas é oferecida pelosistema de *Network Address Translation* - NAT, que

4 Defense Advanced Research Projects Agency, "Internet Protocol: DARPA Internet Program Protocol Specification". *IETF*, RFC791. Setembro de 1981. Disponível em: <https://tools.ietf.org/html/rfc791> Acesso em 20 de Setembro de 2017.

5 HINDEN, Robert M. e DEERING, Stephen E. "Internet Protocol, Version 6 (IPv6)". *IETF*. RFC2460. Dezembro de 1998. Disponível em: <https://www.ietf.org/rfc/rfc2460.txt> Acesso em 20 de Setembro de 2017.

permite o "compartilhamento" de um IP único entre diversos computadores, como forma de mitigar o esgotamento do IPv4 até a implementação completa do IPv6.

O sistema NAT (Network Address Translation)

Durante o desenvolvimento do IPv4, uma quantidade determinada de endereços foi reservada aos "IPs privados", que seriam utilizados em redes privadas não conectadas à internet como um todo. Além dos IPs privados, um número de IPs públicos (ou globais) também foi designado, e esses IPs são utilizados para realizar a maior parte das conexões na Internet. O sistema NAT[6] contorna o problema do esgotamento de IPs ao permitir que vários dispositivos em uma rede de IPs privados compartilhem um único IP público quando desejarem se conectar a uma rede externa, a internet.

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.

IP Privado	IP Público/Global
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

Tabela 1. Exemplo de tabela de vinculação de endereços

Segundo a tabela acima, é possível perceber- que o IP Público usado pelos três endereços internos é o mesmo: o que os difere, contudo, é a porta lógica ao final. Nesse caso, a porta lógica permite uma espécie de variabilidade aos endereços. Os IPs Privados, por sua vez, já eram diferentes entre si, e mesmo assim têm uma porta lógica a eles adicionada a fim de ajudar o sistema de NAT a associá-los ao IP Público. A equivalência entre a porta adicionada ao IP Privado e àquela adicionada ao IP Público, embora prática predominante, não é absoluta.

Por exemplo, se foram atribuídos a um provedor de conexão certo número de IPs, mas esse provedor atende a um número muito maior de clientes e dispositivos do que tem de IPs, será necessário um sistema de NAT para permitir que os dispositivos de seus clientes se comuniquem com a rede externa. Por meio do **gerenciamento das portas lógicas**, poderá compartilhar um IP global entre vários dispositivos conectados, sabendo a origem e destino de cada pacote endereçado ao roteador. Mesmo que todos os pacotes sejam destinados a um mesmo IP, serão diferenciados pelo roteador do provedor, por meio da tabela de vinculação e das portas lógicas a eles anexadas.

Suponhamos que João deseja obter de um determinado website ou aplicativo a previsão do tempo para Belo Horizonte. Ao enviar um pacote de dados contendo a pergunta "Qual a previsão do tempo para Belo Horizonte?", esse pacote deixará seu dispositivo marcado com um endereço de origem e um de destino. Por estar conectado

6 SRISURESH, Pyda & HOLDREGE, Matt. "IP Network Addres Translator (NAT) Technology and Considerations. *IETF*, RFC2663. Agosto de 1999. Disponível em: <https://tools.ietf.org/html/rfc2663> Acesso em 20 de Setembro de 2017.

a um roteador (que pode conectar apenas dispositivos de uma mesma residência, ou pode conectar dezenas de clientes de um provedor de conexão), o endereço de origem será um IP Privado daquela rede interna (por exemplo, 192.168.1.2), e o de destino será o IP Público do servidor hospedando o website, ou aplicação (por exemplo, 40.41.42.43). O pacote, então, partiria do computador de João da seguinte forma:

De: 192.168.1.2

Para: 40.41.42.43

"Qual a previsão do tempo para Belo Horizonte?"

Como existem outros dispositivos conectados àquele roteador, o sistema de NAT terá que ser acionado para conectar o dispositivo de João ao servidor de onde a informação virá. Para isso, adicionará uma porta ao endereço privado (por exemplo, 192.168.1.2:3662) e associará esse endereço privado a um endereço público, que será utilizado para posteriormente receber a resposta (por exemplo, 10.11.12.13:3662). Para o roteador, o pacote seria então endereçado desta forma:

De: 192.168.1.2:3662

Para: 40.41.42.43:80

"Qual a previsão do tempo para Belo Horizonte?"

Como o servidor de destino não conseguirá se conectar ao IP e à porta acima designados, por se tratar de um IP Privado, o sistema de NAT do roteador então redirecionará esse pacote ao destino por meio de um IP Público. Para a internet, qualquer que seja o destinatário, os dados parecem ter vindo do próprio roteador. O pacote então deixaria o roteador endereçado desta forma:

De: 10.11.12.13:3662

Para: 40.41.42.43:80

"Qual a previsão do tempo para Belo Horizonte?"

Por meio do IP Público associado, o servidor de aplicação de previsão do tempo poderá responder ao pedido. Enquanto isso, o roteador ao qual o dispositivo de João está ligado terá inserido a seguinte associação em sua tabela:

192.168.1.2:3662 = 10.11.12.13:3662

O servidor contendo a informação sobre a previsão do tempo então retornaria um pacote endereçado desta forma ao roteador:

De: 40.41.42.43:80

Para: 10.11.12.13:3662

"Mínima de 15 graus e máxima de 24"

No entanto, endereço em questão não identifica o dispositivo de João para a rede externa, apenas para o roteador responsável por intermediar a comunicação. Ao receber esse pacote, ele consultará sua tabela para descobrir qual endereço da rede interna foi associado ao endereço 10.11.12.13:3662 e, então, o redirecionará para o dispositivo de João.

Utilizando-se da analogia das cartas já mencionada acima, o sistema NAT funcionaria como o funcionário de um prédio em que moram várias famílias, responsável por redistribuir as correspondências que chegam para aquele endereço. Se Ana da Silva, que mora no apartamento 303 do Condomínio Solar, Rua dos Guajajaras, n. 13, envia uma correspondência para a Prefeitura de Belo Horizonte, Av. Afonso Pena, n. 1212, ela deixará o endereço com este destinatário, mas seu remetente seria algo como: Rua dos Guajajaras, n. 13, 303. Qualquer resposta da prefeitura que for enviada para Rua dos Guajajaras, n. 13, 303, passará primeiro pelas mãos do funcionário, que saberá que o apartamento 303 é a residência de Ana da Silva, e, então, a entregará.

NAT e *Carrier-Grade* NAT

As primeiras aplicações do NAT foram realizadas para **redes domésticas** (**'Local Area Networks - LANs'**), quando cada cliente de um provedor de conexões recebia seu próprio e IP e o compartilhava entre os dispositivos de sua residência ou trabalho. Com o progressivo esgotamento dos IPs, o NAT passou a ser usado também pelos provedores de conexão: de um sistema para compartilhar endereços entre meia dúzia de dispositivos, desenvolveu -se um sistema que atendia às necessidades de milhares de usuários dos provedores de conexão.

O NAT utilizado em larga escala pelos provedores de conexão é chamado de NAT444, *Carrier-Grade* NAT (CGN)[7] ou *Large Scale* NAT (LSN). Esse último termo é considerado o mais preciso, porque se trata apenas de uma versão em larga escala do mesmo sistema utilizado por redes locais ou de pequeno porte.

Implementação do IPv6 no Brasil[8]

Com o esgotamento do bloco de IPv4 ao redor do mundo, como mencionado acima, diversos países e agentes envolvidos têm buscado implantar o IPv6 em suas redes e serviços. A empresa americana Akamai Technologies Inc. executa medições periódicas sobre uso do IPv6 no mundo, com base no tráfego em suas redes. Para o Brasil, a empresa estima que há um adoção de 19,8% de IPv6, colocando o país na 9º posição global:[9]

[10]

7 JIANG, Sheng, GUO, Dayong & CARPENTER, Brian. "An incremental Carrier-Grade NAT (CGN) for IPv6 Transition". *IETF*, RFC6264. Junho de 2011. Disponível em <https://tools.ietf.org/html/rfc6264> Acesso em 20 de Setembro de 2017.

8 Para mais fontes de informação sobre o IPv6 no Brasil e no mundo, consulte a página do Núcleo de Informação e Coordenação do Ponto BR - NIC.br em <http://ipv6.br/>.

9 Tabela disponível em: <http://bit.ly/2kzWeRD>. Acessado em: 09/10/2017.

10 Tabela disponível em: <http://bit.ly/2kzWeRD>. Acessado em: 09/10/2017.

A empresa Google aponta dados semelhantes de adoção do IPv6 no Brasil. Ela calcula que 20,17% de tráfego de dados no Brasil são em IPv6, classificando-o como um país com nível alto implementação e no qual são apresentados poucos problemas de conexão com os sites da Google:[11]

Como observado no gráfico, a situação do Brasil, em termos de adoção do IPv6 é similar a de países com considerável penetração da internet e pertencentes ao grupo de países desenvolvidos do hemisfério norte e países em desenvolvimento do hemisfério sul. Em estimativa semelhante, o Asia-Pacific Network Information Centre aponta uma capacidade de 20,97% de IPv6 para o Brasil, o que posiciona o país em 14º lugar no ranking desse tipo de conexão[12].

3.0 Marco Civil da Internet e portas lógicas

O Marco Civil da Internet estabelece duas categorias de dados que devem ser armazenados, obrigatoriamente: 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 (art. 10[13], porque a responsabilização dos usuários é um dos princípios do uso da internet no Brasil, conforme o art 3º, VI[14], da mesma lei. Esses registros também podem ser utiliza-

11 Google IPv6. 2017. Disponível em :<http://bit.ly/2yazwEE>. Acessado em: 09/10/2017.

12 Ranking produzido pela Asia-Pacific Network Information Centre. Informações disponíveis em: <https://stats.labs.apnic.net/ipv6>. Também disponibilizadas pelo site do ipv6.br: <http://ipv6.br/>.

13 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.

14 Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] VI - responsabilização dos agentes de acordo

dos para fins comerciais, desde que com "consentimento livre, expresso e informado" (art. 7º, VII)[15].

Segundo o Marco Civil, 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". Sua guarda cabe ao administrador de sistema autônomo[16], que deve zelar por sua proteção, pelo prazo de 1 (um) ano (art. 13)[17].

Já os provedores de aplicação[18] 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 6 meses[19] 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[20] do Marco Civil da Internet.

Essa diferença de obrigações entre as duas categorias de agentes, provedores de conexão e de aplicação, almeja garantir a consecução de outros princípios: a privacidade e a proteção da vida privada do cidadãos usuários da Internet. Afinal, para que o usuário de uma aplicação seja identificado, uma das técnicas possíveis de serem utilizadas é a realização do cruzamento dos dados de registros de ambos provedores.

Suponhamos um caso em que qual João utiliza um email criado com informações de cadastro falsas para venda ilegal de passagens áreas. Se uma autoridade policial busca identificar quem está usando esse email, ela requisita da empresa de e-mails os registros de aplicação que informam qual o IP está sendo utilizado para o acesso à aplicação. Com esse IP, a autoridade investigativa entra em contato com o provedor de conexão que forneceu aquele IP a um de seus consumidores para conexão à internet. Dessa forma, em um cenário no qual a cada usuário é atribuído um único IP para conexão à internet, a técnica explicada não encontra dificuldades para identificar uma pessoa.

Com o uso de sistemas NAT, todavia, o IP armazenado em um registro de aplicação pode levar a uma lista com diversos usuários do provedor de conexão, que utilizaram aquele IP de forma compartilhada. Assim, há casos apreciados pelo Poder Judiciário brasileiro em que a parte que busca identificar um usuário (geralmente, o Ministério Público) tem requerido, além dos registros explicitados na Lei, o número de "porta lógica" associado ao IP compartilhado. Como o termo técnico "porta lógica" não é mencionado no texto legal do Marco Civil da Internet, discute-se judicialmente se essa lei permite a interpretação extensiva ou ampliativa de que provedores de conexão e/ou aplicação devem também armazenar dados referentes às portas lógicas.

---

com suas atividades, nos termos da lei;

15 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

16 "Art. 5º - Para os efeitos desta Lei, considera-se: [...]: IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;". Lei. 12.965/2014.

17 Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

18 Art. 5º - Para os efeitos desta Lei, considera-se: [...] VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; "

19 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.

20 Art. 5º Para os efeitos desta Lei, considera-se: VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

4. Sistemas NAT e porta lógicas na União Europeia e na Austrália

Além do Brasil, outros países também têm enfrentado problemas semelhantes com a identificação de usuários de internet que se conectam por meio de compartilhamento de IPs. Com o propósito de oferecer **viés comparativo de análise**, em termos de **perfis regulatórios e jurisdicionais**, o trabalho investiga como o tema do compartilhamento de IPs e portas lógicas é similarmente discutido na União Europeia e na Austrália (representantes de sistemas legais em que o IPv6 é amplamente implantado) .

Os casos que serão demonstrados a seguir objetivam, pois, fornecer maior contextualização ao debate, extrapolando as visões meramente domésticas sobre compartilhamento de IPs e identificação de usuários no ambiente brasileiro. O estudo ressalva, entretanto, que os casos foram selecionados devido à maior facilidade de acesso às informações, e não representam, nesse estágio de análise exploratória, a defesa de determinado modelo regulatório para o Brasil.

Marco legal da União Europeia

A União Europeia aplicava a Diretiva 2006/24/EC[21], sobre retenção obrigatória de dados, que somente dava diretrizes gerais, as quais os Estados membros deveriam seguir para implementar em suas legislações nacionais. No art. 5º, a Diretiva estabelecia quais eram as categorias de dados que os Estados-membros deveriam assegurar a conservação, definindo-os como os "dados necessários para encontrar e identificar a fonte de uma comunicação" e para "identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento". Em nenhum momento a norma utiliza o termo "porta lógica" ou *port.* Contudo, é necessário uma análise mais aprofundada de cada país para se verificar como cada regulação nacional trata do tema, e se há menção expressa ou não à guarda de portas lógicas.

Em 2014, a Corte de Justiça da União Europeia (CJUE), nos casos conjuntos *Digital Rights Ireland Ltd* e *Kärntner Landesregierung*[22], consideroua Diretiva 2006/24 inválida por contrariar os artigos 7º (direito de proteção à vida privada) e 8º(direito de proteção de dados pessoais) da Carta dos Direitos Fundamentais da União Europeia.[23] Em 2016, ainda em um contexto de *vacatio legis (*no sentido de regulação aplicada a todos os membros da EU) deixado pela invalidação da Diretiva, a Corte julgou dois casos conjuntos nos quais estabeleceu quais proteções gerais os Estados-membros deveriam aplicar para estarem em conformidade com a Diretiva de Privacidade Eletrônica (2002/58/CE) e com Carta de Direitos Fundamentais da UE .

Nos casos *Tele2 Sverige* e *Home Secretary v. Watson*[24] o CJUE julgou que os Estados Membros não podem impor uma obrigação geral de retenção de dados para os serviços de telecomunicações eletrônicas (*electronic telecommunications services*)[25], em relação à

21 UE - "*Directiva 2006/24/CE do Parlamento Europeu e do Conselho*, de 15 de Março de 2006 , relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE". Disponível em: <http://bit.ly/2fPZOWg>. Acessado em: 04/10/2017

22 CJEU. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources Ireland and others and Kärntner Landesregierung.* Joined cases C-293/12 and C-594/12, Grand Chamber, 8 de abril de 2014. Disponível em: <https://goo.gl/fjqymW>. Acesso em: 04/10/2017.

23 CJEU. The Court of Justice of the European Union. *Press Release Nº 54 /14*. Luxemburgo, 8 de Abril de 2014. Disponível em: <http://bit.ly/2tBS4IV>. Acessado em: 04/10/2017.

24 CJUE. *Tele2 Sverige AB contra Post- och telestyrelsen e Secretary of State for the Home Department contra Tom Watson*. C-203/15.2016. Disponível em <http://bit.ly/2yxxiNR>. Acessado em: 18/10/2017

25 European Union Agency for Fundamental Rights (FRA). *Data retention across the EU*. Disponivel em: <http://bit.ly/2zhJIZu>.

tráfego de dados e localização dos usuários. A decisão, contudo, não chegou a banir a possibilidade de retenção de dados, desde que utilizada para finalidades específicas (p. ex. no caso de um suspeito específico de uma criminal específica). O julgado também afirma que são necessários critérios de contra peso ao armazenamento e acesso de dados armazenados. Afirmou-se que é necessário haver limitações ao armazenamento de determinadas categorias de dados, buscando-se somente aqueles estritamente necessárias a determinado caso; foi exposto a necessidade de se limitar de forma clara quais pessoas têm acesso aos registros; e de se limitar a retenção a um período proporcional de tempo.[26]

Apesar dos julgados do CJUE, os Estados não possuem obrigação legal estrita de implementação das recomendações, sendo que somente quatro Estados membros fizeram alterações em suas legislações após os julgados.[27]

É importante mencionar também o julgamento do caso *Breyer*[28], realizado pela CJUE em 2016, o qual buscava responder se endereços de IP são dados pessoais, e se seu armazenamento seria permitido somente para os casos previstos na antiga Diretiva de retenção de dados, ou se eles também poderiam ser armazenados pela justificativa de um interesse legítimo (*legitimate interest*). A CJUE entendeu que endereços de IP são, sim, qualificados como dados pessoais, desde que seja possível identificar o indivíduo associado ao seu uso; mesmo que os dados necessários para a identificação estejam na posse de um terceiro. E estabeleceu que provedores de serviços de mídia online (*online media service providers*) podem armazenar os dados pessoais de seus usuários, como o endereço de IP, desde que sejam utilizados para um fim legítimo específico.[29]

O Regulamento Geral de Proteção de Dados - *General Data Protection Regulation* (2016/679), que será aplicada a partir de 2018, não trata especificamente sobre o tema de retenção obrigatória de dados eletrônicos[30]. Assim a regulação na União Europeia ainda carece de uma uniformização geral, tendo cada país leis específicas sobre o tema. A Agência da União Europeia para Direitos Fundamentais avaliou em 2017 que:

> De modo geral, o progresso dos Estados-Membros na questão continua limitada. , desde a invalidação pelo TJUE da Diretiva de retenção de dados. Isto pode dever-se, em parte, à ausência de regras harmonizadas a nível da UE. A Eurojust, agência da UE para a cooperação judiciária em matéria penal, afirmou que, embora os sistemas de retenção de dados sejam considerados instrumentos necessários na luta contra crimes graves, é necessário criar um regime legal ao nível da UE para que sejam cumpridas as salvaguardas estabelecidas pelo TJUE. De qualquer forma, seja a nível europeu ou nacional, enquanto normas de retenção de dados continuem a ser implementadas, medidas de proteção adequadas devem ser implementadas o mais rápido possível a fim de se prevenir violações a direitos fundamentais.[31]

Acessado em: 18/10/2017.

26 European Union Agency for Fundamental Rights (FRA). *Fundamental Rights Report 2017*. 2017. p.162-165. Disponível em: <http://bit.ly/2yvAxoY>. Acessado em: 18/10/2017.

27 Ibid, p. 164.

28 CJUE. *Patrick Breyer v. Bundesrepublik Deutschland*. Case C-582/14. 19 Outubro de 2016. Disponível em: <http://bit.ly/2gsdqaf>. Acessado em: 18/10/2017.

29 European Union Agency for Fundamental Rights (FRA). Op. cit. p. 163

30 Por exemplo, o termo *retention* é mencionado somente duas vezes ao longo do texto da lei.

31 Tradução livre de: "All in all, Member States' progress on the issue since the CJEU's invalidation of the Data Retention Directive remains limited. This may partly be due to the absence of harmonised rules at EU level. Eurojust, the EU agency for judicial cooperation in criminal matters, has stated that, while data retention schemes are considered necessary tools in the fight against serious crime, there is a need to create an EU regime on data retention that complies with the safeguards laid down by the CJEU.133 In any event, regardless of whether at European or national level: as long as data retention measures continue to be deployed, adequate protection measures must soon be implemented to prevent fundamental rights violations.". Ibid, p. 164.

Portas lógicas e as instituições europeias de investigação criminal

A Europol[32], órgão policial internacional da União Europeia, é um dos agentes estatais europeus que alerta sobre o problema da identificação de usuários online que utilizam o compartilhamento de IP por meio de sistemas *Carrier-Grade* NAT (CGN). Em 2016, foi publicado pela instituição o relatório *The Internet Organised Crime Threat Assessment* (IOCTA), que reconheceu com um dos principais problemas de governança da internet daquele ano o uso de CGNs por provedores de conexão.[33] O relatório avalia que o uso de CGN tem levado as polícias europeias a dificuldades para associar um usuário online investigado com um único endereço de IP. Tentando medir a extensão do problema, a Europol cita questionário realizado pelo *European Cyber Crime Centre* alegando que 90% dos investigadores policiais de cybercrimes, consutlados na pesquisa, afirmam encontrar regularmente problemas de identificação de usuários devido a tecnologias CGN.[34]

O relatório também aponta que esperar pela transição do IPv6 seria inviável, porque avalia-se que o processo ainda levará vários anos devido à falta de incentivos comerciais para a implementação do novo protocolo, e à necessidade de inúmeros investimentos na estrutura do IPv4. Assim, recomenda-se que as forças policiais que estão em investigações envolvendo CGN requisitem, por meio das vias legais: 1) os endereços IP de Origem e Destino; 2) a porta lógica de origem; e 3) o horário exato da conexão (inclusive segundos).[35]

O IOCTA utiliza como uma de suas fontes especializadas as recomendações do memorando técnico *Request for Comments 6302 - Logging Recommendations for Internet-Facing Servers*[36], produzido pela Força Tarefa de Engenharia de Internet - *Internet Engineering Task Force* - designado em 2011. Este memorando sugere que:

> É recomendado como uma das melhores práticas que servidores voltados à Internet registrando endereços de IP advindos de tráfego de IP também guardem: o número da porta lógica de origem; uma etiqueta de marcação de tempo, preferencialmente em tempo universal (UTC), com menção de segundos, de uma fonte de rastreável (Por exemplo, NTP [RFC5905]); o protocolo de transporte (Geralmente TCP ou UDP) e o número de porta lógica de destino, quando a aplicação de servidor está configurada para usar múltiplos transportes ou múltiplas portas[37] [38]

Por fim, o IOCTA conclui que:

32 A "European Police Office" (Europol), é uma agência da UE, sem poderes executivos, que busca promover a coordenação entre as polícias civis dos 28 membros da UE. Seu foco de atuação está no combate a crimes internacionais como cibercrimes, terrorismo, lavagem de dinheiro, entre outros. EUROPOL. "About Europol". Disponível em:<http://bit.ly/2jWsUV8>. Acessado em: 29/09/2017.

33 EUROPOL. "IOCTA 2016 - Internet Organised Crime Threat Assessment". Disponível em: <http://bit.ly/2fCum7o>. p. 57 e 58. Acessado em: 25/09/2017.

34 *Ibidem*.

35 *Ibidem*.

36 Um RFC é um documento que representa um consenso ao qual os membros da IEFT chegaram após um período de debate. O documento RFC 6302 recebeu uma revisão pública prévia e foi aprovado pelo Internet Engineering Steering Group (IESG) para publicação. IESG. "*Request for Comments 6302 - Logging Recommendations for Internet-Facing Servers*". 2011. Disponível em: <http://bit.ly/2kgwjye>. Acessado em: 02/10/2017.

37 *Ibidem*.

38 Tradução livre de: *'It is RECOMMENDED as best current practice that Internet-facing servers logging incoming IP addresses from inbound IP traffic also log: - The source port number. - A timestamp, RECOMMENDED in UTC, accurate to the second, from a traceable time source (e.g., NTP [RFC5905]). - The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports."*

> Mudanças regulatórias/legislativas são necessárias para garantir que os provedores de serviços de conteúdo online retenham sistematicamente os dados adicionais necessários (porta lógica de origem) para que as autoridades policiais possam para os usuários finais. Alternativamente, soluções práticas podem ser desenvolvidas através da colaboração entre os prestadores de serviços eletrônicos e as forças policiais. Alguns provedores eletrônicos da Europa armazenam as informações relevantes (porta de origem). Um website de toda a Europa poderia ser criado para manter uma lista atualizada desses provedores e uma lista de canais de contato para cooperação com forças policiais, para os casos em que uma investigação estiver emperrada por envolver CGN.[39]

Em janeiro de 2017 a Europol lançou um Grupo de Trabalho denominado *"European Network of Law Enforcement Specialists in CGN"* cujo objetivo principal é o de estudar soluções práticas para a questão do uso de IPs compartilhados e identificação de usuários. Em nota pública foram estabelecidos como objetivos do Grupo:

> Documentar casos de não atribuição de IP à usuários ligados ao uso de CGN na UE; documentar as melhores práticas para superar os problemas de atribuição relacionados à CGN atualmente em vigor em alguns Estados Membros; sensibilizar os formuladores de políticas europeus sobre o problema de atribuição ligado às tecnologias CGN; representar a voz das autoridades policiais, desenvolvendo uma narrativa comum e promovendo um modelo de cooperação voluntária, a nível da UE, para melhorar a rastreabilidade, engajando-se de forma coordenada com os provedores de conexão (ISPs) e provedores de conteúdo.[40]

Na mesma nota, a agência manteve o diagnóstico do IOCTA 2016 de que o uso de CGN tem dificultado a identificação de cibercriminosos, alertando que essa questão pode levar as forças de investigação a ter que recorrer a meios de investigação mais invasivos à privacidade[41]. Adicionalmente, a nota cita que ainda é elevado o uso de CGN pelos provedores de conexão no mundo, principalmente pelas operadoras de telefonia móvel, dando suporte à hipótese da Europol de que alguns anos serão necessários para a transição total para o IPv6:

> De acordo com uma pesquisa recente realizada entre 70 provedores de conexão [Internet Service Providers - ISPs] tradicionais (cabo, fibra e ADSL) em todo o mundo, 38% desses ISPs tradicionais têm CGN e 12% estão planejando implantá-lo[1]. Sendo a situação ainda pior para os provedores GSM [Global System for Mobiles]: de acordo com o mesmo estudo, 95% dos ISPs de internet móvel (ou seja, os endereços IP fornecidos pelos provedores GSM) usam as tecnologias CGN. [...] Isso significa que o CGN está aqui para ficar e que a política pública adotada anteriormente (ou seja, esperar a transição para o IPv6) não é a abordagem correta da perspectiva das vítimas. O uso do

39 Tradução livre de: "*Regulatory/legislative changes are required to ensure that content service providers systematically retain the necessary additional data (source port) law enforcement requires to identify end users. Alternatively, practical solutions can be developed through collaboration between the electronic service providers and law enforcement. Some electronic providers Europe do store the relevant information (source port). A European- wide portal could maintain an updated list of those providers and a list a contact points to address in case an investigation is stalled by CGN.*" *Idem*, p. 58.

40 "*On 31st January 2017 a European Network of law enforcement specialists in CGN will be established, the secretariat of which will be established/provided by? at Europol. The aim of this network is to: document cases of non-attribution linked to CGN in EU; document existing best practices to overcome CGN-related attribution problems currently in place in some Member States; raise awareness of European policy-makers about the problem of attribution linked to CGN technologies; represent the voice of law enforcement developing a common narrative and advocating for a voluntary scheme at EU level to improve traceability by engaging in a coordinated fashion with ISPs and content providers*". EUROPOL/EC3 - 5127/17. *"Carrier-Grade Network Address Translation (CGN) And the Going Dark Problem*". 16 de Janeiro de 2017. p. 7. Disponível em: <http://bit.ly/2hw37OX> e <http://bit.ly/2yDviCI>. Acesso em: 29/09/2017.

41 *Ibid*, p.4.

> CGN continuará a crescer apesar da transição para o IPv6, dificultando ainda mais a capacidade das forças policiais de identificar um usuário final por meio um endereço de IP.[42]

Na busca por soluções para o problema de **identificação de usuários online**, a Europol afirma que é necessário um maior debate e cooperação entre os atores envolvidos (ISPs, provedores de conteúdo, provedores de armazenamento de dados, e forças policiais) Em um cenário de ausência de uma regulamentação harmonizada de retenção de dados, entre os países europeus, a instituição afirma a necessidade urgente da busca de soluções:

> [...] podem ser buscadas soluções práticas mediante colaboração entre os provedores de serviços eletrônicos/Internet e os aplicadores da lei por meio de canais de cooperação já estabelecidos, como o *Fórum da Internet da UE*. O Fórum poderia fornecer excelente plataforma para discussão com os ISPs/provedores de conteúdo mais importantes, sobre a necessidade de se implementar a rastreabilidade dos números de portas lógicas de origem, e a necessidade de se fornecer esses números de forma voluntária quando solicitados (diretamente ou por processo legal), por autoridades policiais e judiciárias, a fim de facilitar a identificação de criminosos.[43]

Austrália

Em 2015, o Parlamento da Austrália aprovou uma lei de retenção de dados para o país, que foi emendada ao "Telecommunications (Interception and Access) Act" de 1979.[44] A lei obriga que determinados dados de serviços de telecomunicação[45] e de provimento de acesso à internet sejam armazenados por um período mínimo de 2 anos (contados da data de criação da informação), podendo-se ultrapassar esse período para fins de uso comercial.[46] A critério de comparação, a Diretiva 2006/24/EC da União Europeia estabelecia 2 anos como tempo máximo de armazenamento de dados de telecomunicação.

Primeiramente, é preciso esclarecer o **conceito de provedor de serviços** (*content provider)* conforme a lei australiana. Ele é gênero, que se divide em duas espécies: (a) *carriage service provider* e (b) *content service provider*.[47] Um *carriage service provider* fornece serviços de telecomunicações por meio de energia eletromagnética[48]. Já um *content*

42 "*According to a recent a survey carried out among 70 traditional ISPs (cable, fiber and ADSL) worldwide, 38% of these traditional ISPs have CGN in place and 12% are planning to deploy it*[1]*. The situation is even worse for GSM [Global System for Mobiles] providers: according to the same study, 95% of mobile ISPs (i.e. IP addresses provided by GSM providers) use CGN technologies. [...] This means that CGN is here to stay and that the old policy response (i.e. wait for the transition to IPv6) is not the right approach from the perspective of the victims. The use of CGN will continue to grow in spite of the transition to IPv6, further impeding the law enforcement ability to perform a trace back to an individual end-user of an IP address.*" *Ibid*, p. 5.

43 Tradução livre de: "*[...] practical solutions can be sought through collaboration between the electronic/Internet service providers and law enforcement using already established channels for cooperation such as the EU Internet Forum. The latter could provide an excellent platform for discussion with the most important ISPs/content providers the need to implement the traceability of source port numbers and to provide these numbers on a voluntary basis when requested (directly or by legal process) by law enforcement and judiciary authorities in order to facilitate the attribution of crime.*" *Ibid*, p.6.

44 AUSTRALIA, "Telecommunications (Interception and Access) Act" Nº 114, 1979, Compilation Nº. 96. Disponível em: <https://www.legislation.gov.au/Details/C2017C00308>. Acessado em: 05/10/2017.

45 "*What is telecommunications data? - Telecommunications data is information or documents about communications, but not the content or substance of those communications.*" AUSTRALIAN GOVERNMENT- Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p. 11 . Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017.

46 AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers* . Julho de 2015. P.4. Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017

47 Section 86. Telecommunications Act 1979.

48 Sections 7 e 87. Telecommunications Act 1979.

service provider fornece conteúdo online ao público (streaming de vídeos, jogos online, etc.), que trafega por meio da estrutura fornecida pelos *carriage service provides*.[49] A lei de retenção de dados se aplica somente aos *carriers*, *carriage service providers* e *internet service providers* (ISPs),[50] ou seja às empresas de telecomunicações e provedoras de conexão à internet.

O *Telecommunications Act* determina seis tipos de informação que devem ser armazenadas relativas a uma sessão de comunicação[51], que está associada a um serviço específico que os provedores oferecem[52]. Deve-se frisar que esses registros precisam ser criptografados e armazenados de forma segura, podendo ser requisitados por um número limitado de autoridades investigadoras. São exemplos de serviços o fornecimento de acesso à internet, serviços VoIP (*Voice Over Internet Protocol*), SMS, entre outros, tendo cada um certas especificidades na obrigação de retenção de dados. Os seis tipos de informações sujeitas À solicitação/requisição são:

> 1. Dados do assinante, as contas, serviços, dispositivos de telecomunicações e outros serviços, todos relacionados ao serviço relevante; 2. a origem de uma comunicação; 3. o destino de uma comunicação; 4. a data, hora e duração de uma comunicação, ou de uma conexão com um serviço relevante; 5. o tipo de comunicação, ou o tipo de um serviço relevante usado em conexão com uma comunicação; e 6. a localização do equipamento, ou linha, utilizada em conexão com uma comunicação.[53]

Há situações em que um provedor de serviço não é obrigado a armazenar todas as seis categorias. Por exemplo, os ISPs não podem armazenar dados de destino de uma comunicação, nem dados relativos ao histórico de navegação do usuário[54], no contexto de provimento de serviços de conexão à internet. Norma semelhante é estabelecida no art. 14[55] do Marco Civil da Internet, que veda aos provedores de conexão de armazenar dados de registro de acesso à aplicações de internet. No caso brasileiro, a vedação busca limitar a quantidade de dados que um só agente pode armazenar, almejando maior proteção da privacidade e dos dados pessoais do usuário. No limite, trata-se de uma regra que objetiva equilíbrio entre poder econômico detido pelos provedores de conexão e direitos de usuários relativos ao uso da internet.

Para efeitos de comparação, no Marco Civil da Internet há duas categorias de agentes que têm a obrigação de guarda de registros: os **provedores de conexão**, arts. 5º, IV, V, VI e 13; e os **provedores de aplicação**, arts. 5º, VII, e 15. O conceito de *content provider* se assemelha mais ao conceito brasileiro de provedor de aplicação. Serviços OTT (*over-the-top-content*) na lei brasileira, por exemplo, seriam classificados também como provedores de aplicação. Porém, na regulação australiana, alguns tipos de serviços

49 Sections 15 e 97. *Telecommunications Act 1979.*

50 *"Only carriers, carriage service provider and internet service providers (C/CSP/ISPs) have obligations under the data retention regime."* AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p. 11 . Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017.

51 *"The meaning of communication or session depends on each particular relevant service. For instance, for VoIP services, obligations are applied to each call scenario. For SMS, each SMS is a separate communication. For email, the session is the customer's log-in to the email service and the communications are each email. For internet access services, the session will typically be the period for which a private IP address is allocated." Ibid*, p.8.

52 AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers*. Julho de 2015. p.4.

53 *"The data to be retained is set out in six categories: 1. the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service; 2. the source of a communication; 3. the destination of a communication; 4. the date, time and duration of a communication, or of its connection to a relevant service; 5. the type of a communication or of a relevant service used in connection with a communication, and; 6. the location of equipment, or a line, used in connection with a communication.". Ibid,* p. 4.

54 *Ibid*, p. 12.

55 Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

OTT[56], como VoIP, chat e troca de mensagens online devem ter metadados armazenados, conforme o *Telecommunications Act*, se fornecidos por empresas de telecomunicações e por provedores de conexão à internet.[57]

Para os **dados relativos à origem de uma comunicação** (*source of a communication*), exige-se do ISPs o **armazenamento do endereço IP e da porta lógica** alocada para o assinante ou para o dispositivo conectado à internet, no momento da comunicação.[58] É importante ressaltar que o *Telecommunications Act* não cita o termo técnico *port number* (porta lógica), sendo essa uma regulação de esfera executiva, e não legislativa.

Outro ponto importante é que *Attorney-General's Department* australiano faz referência expressa aos agentes que utilizam sistemas NAT e a sua obrigação de armazenar as portas lógicas. Essa obrigação deriva da interpretação do termo legal "identificadores de conta ou serviço" (*identifier allocated to an account or service*), conforme Parágrafo *187AA*, do *Telecommunications (Interception and Access) Act*:[59]

> Para evitar dúvidas, o requisito de manter registros NAT será (no mínimo) aplicável ao [endereço IP interno; Porta Lógica Interna; Endereço IP externo; Porta Lógica externa] de uma Tabela NAT. Independentemente dos elementos que sejam mantidos como parte dos registros NAT de um provedor, deve ser possível identificar de forma única e associar o endereço IP Interno / Porta Lógica Interna a um endereço IP externo/Porta lógica Externa e vice-versa. Se as tabelas NAT de uma empresa também incluem elementos de endereço IP de destino e Porta Lógica de Destino (por exemplo, sob um *Symmetrical NAT model*), as obrigações de retenção de dados não serão aplicadas a esses elementos.[60]

Estranhamente, o *Telecommunication Act* é omisso quanto às obrigações de retenção de dados por parte de empresas que oferecem serviços OTT que não sejam ISPs.[61] Por conseguinte, não há previsão na lei australiana sobre armazenamento de

56 *O Body of European Regulators for Electronic Communications* define OTT como um conteúdo, um serviço ou um aplicativo que é fornecido ao usuário final por meio da internet pública. A disponibilização desse serviço, conteúdo ou aplicativo ocorre sem o envolvimento de quem fornece a conexão à internet. BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATION *Report on OTT services*. 2016. p. 14. Disponível em:<http://bit.ly/2yRFc3s>. Acessado em 08/10/2017.

57 "*Will off-shore over-the-top (OTT) providers that don't own or operate infrastructure in Australia be captured by the data retention obligations? The data retention obligations only apply where the service meets all three of the following criteria: 1. the service is for carrying or enabling communications to be carried by electromagnetic energy; 2. the service is operated by a C/CSP or an Internet Service Provider (ISP); and 3. the provider owns or operates infrastructure in Australia that enables provision of any relevant service. Criterion one captures a broad range of services including OTT services like VoIP and chat or other online/application messaging services. Criterion two acts as a limitation on the first criterion. That is, a person might host a website or an FTP server that facilitates communications via electromagnetic energy. But if that person does not have a carrier licence and does not meet the CSP or ISP definition, that person does not attract data retention obligations. Criterion three provides a further limitation by excluding providers that do not have any communications infrastructure in Australia. Infrastructure means any line or equipment used to facilitate communications across a telecommunications network. This includes servers that host websites or services furnished by OTT providers, as well as line links and network units.*". *Idem*, p. 18

58 "*What are the data retention obligations relating to a provider who only offers an internet access service (i.e. no additional OTT) services offered)? [...] all IP addresses and, where applicable, port numbers allocated to the subscriber during that session, including the associated dates and times*". AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p.21 . Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017.

59 *Idem*, p. 13

60 "*For the avoidance of doubt, the requirement to keep NAT records will (at minimum) apply to the [Internal IP address; Internal Port; External IP address; External Port] elements of a NAT table. Whatever elements are kept as part of a provider's NAT records, it must be possible to uniquely identify and associate the Internal IP address/Internal Port to an External IP address/External Port and vice versa. If a carrier's NAT tables also include [Destination IP address; Destination Port] elements (for example, under a Symmetrical NAT model), data retention obligations will not apply to those elements. Whether a carrier wishes to retain those additional elements is a decision for the carrier.*" *Ibidem*.

61 HURST, Daniel. *Telcos question data retention plans that exempt Facebook, Gmail and Skype*. The Guardian. 2015. Disponível em: <http://bit.ly/2xqggnn>. Acessado em: 08/10/2017.

porta lógicas para esses agentes, do que poderia resultar uma espécie de assimetria na alocação de obrigações para agentes econômicos atuantes nos segmentos de provimento de acesso e de aplicação:

> A maneira complexa com que os "*over the top services*" foram excluídos cria uma distinção incomum na Lei, na qual somente os serviços fornecidos pelos próprios ISPs australianos serão incluídos no âmbito das obrigações legais. Assim, por exemplo, se um assinante acessa um e-mail através de um provedor como o Google, ou faz uma ligação por serviço de VoIP como o Skype, estes são serviços *"over the top"*, porém eles não têm nenhuma obrigação de reter qualquer informação sobre o uso das aplicações. Mas, onde os serviços de e-mail ou VoIP são fornecidos pelo próprio ISP, é necessário armazenar qualquer informação sobre as comunicações que seus usuários fazem - incluindo os endereços aos quais os e-mails são enviados e para onde e são direcionadas as chamadas.[62]

5. Metodologia de coleta e análise dos dados dos tribunais brasileiros em tema de acesso a portas lógicas

Método de varredura

Os dados sobre **processos judiciais** que envolvam **pedidos de acesso a portas lógicas** analisados neste estudo foram coletados nos websites de todos os Tribunais de Justiça Estaduais brasileiros, nos Tribunais de Justiça Federais, bem como no Superior Tribunal de Justiça - STJ. A escolha dessas instâncias justifica-se pela disponibilidade das decisões, bem como de seus conteúdos, por meio dos mecanismos *online* de pesquisa jurisprudencial, diferentemente do que ocorre, por exemplo, na primeira instância. As buscas foram realizadas utilizando as expressões "porta lógica" e "portas lógicas". O estudo, portanto, não teve acesso a processos não constantes das bases de dados de jurisprudência em formato eletrônico, ou àqueles eventualmente existentes em formato de autos físicos.

Foram construídas, então, tabelas compartilhadas (na ferramenta do Google Drive) para que os pesquisadores envolvidos pudessem registrar as informações encontradas nas buscas e observações online. Isso permitiu que os dados fossem selecionados, identificados, analisados de forma conjunta (por todos os pesquisadores) e que as informações pudessem ser visualizadas de forma agregada em fase posterior de pesquisa. No primeiro banco de dados, estão reunidas as decisões que levaram os casos aos tribunais inferiores, ou ao STJ (Tabela 01). No segundo, encontram-se referências a Embargos de Declaração, quando interpostos, contra as decisões analisadas (Tabela 02).

62 Tradução livre de: "The complex way that 'over the top' services are excluded creates an unusual distinction in the Act where services that are provided by Australian ISPs themselves will actually be included within the scope of the obligation. So, for example, if a subscriber accesses email through a third party provider, like Google, or makes a call through a VoIP service like Skype, these are 'over the top' services, and the provider is under no obligation to retain any information about their use. But, where email or VoIP services are provided by the ISP itself, it is required to store any information about the communications its users make – including addresses to which emails are sent or calls placed." SUZOR, Nicolas; PAPPALARDO, Kylie; McINTOSH, Natalie. *The passage of Australia's data retention regime: national security, human rights, and media scrutiny*. Internet Policy Review- Journal on Internet Regulation.Volume 6, Edição 1. Março de 2017. Disponivel em: <http://bit.ly/2y4aUeB>. Acessado em: 08/10/2017.

Marco temporal

Esta pesquisa tem como marco temporal a vigência da Lei n. 12.965, de 23 de abril de 2014, o Marco Civil da Internet no Brasil[63]. Isso porque, em cenário anterior, não havia no Brasil legislação específica[64] que obrigasse agentes a guardar registros de acessos a aplicação de internet, ou dados cadastrais de usuários, mas apenas decisões esparsas e sem qualquer uniformidade pretendida por lei especial. Foram coletadas decisões a partir do ano de 2014 e que, portanto, já se inseriam no contexto de vigência do Marco Civil. OI termo final da pesquisa foi o dia 31 do mês de agosto de 2017. A escolha desse critério para marco temporal, apesar de desconsiderar dado grupo de decisões anteriores à entrada em vigor do Marco Civil da Internet, impondo obrigações de guarda de registros de acessos, permite estabelecer referência analítica para continuidade do monitoramento de decisões futuras sobre esse tema.

Variáveis - Banco de dados 01

As seguintes variáveis foram registradas (mensuradas) no esforço de coleta de informações:

1.Número do processo

Os processos colhidos foram identificados por meio dos números atribuídos pelos próprios tribunais. Esse campo serviu apenas para que os pesquisadores envolvidos tomassem como referência no preenchimento dos demais campos.

2.Estado Federado (UF)

O objetivo dessa variável é investigar o foro de processamento das demandas sobre portas lógicas no Brasil. Com o uso das palavras-chave eleitas para esta pesquisa, os resultados nos Tribunais Federais não acarretaram resultados efetivamente relevantes para o recorte temático inicialmente proposto pelo estudo. Dessa forma, na prática, este campo corresponde aos resultados obtidos nos Tribunais de Justiça de cada Estado da Federação, além do STJ, cujo campo foi assim preenchido, uma vez que se trata de instância superior não adstrita os Estados.

3.Ano

As pesquisas foram realizadas tendo como referência o marco temporal de decisões promulgadas a partir de 2014, e nas quais já se encontrava vigente Marco Civil da Internet. Desse modo, foram encontradas decisões em 2014, 2015, 2016 e 2017.

4.Polo ativo em sede recursal

Foram sistematizadas as partes envolvidas apenas na instância recursal e que integraram, especificamente, cada uma das decisões coletadas. Por "polo ativo", compreende-se não o autor da ação em primeira instância, mas aquele que interpôs o re-

63 A vigência da Lei n.12965 se deu 60 dias após sua publicação,em 23 de junho de 2014.

64 Precedentes anteriores ao Marco Civil da Internet justificavam a obrigação de fornecer dados de acesso por meio da legislação consumerista. Nesse sentido, os provedores, por exercerem atividade lucrativa utilizando-se da internet, assumiam a obrigação de fornecer, por exemplo, IPs e dados cadastrais. Nesse sentido, *c.f.* STJ, *REsp nº 1403749/GO,* Ministra Nancy Andrighi, Terceira Turma. Data de julgamento: 22/10/2013. Importa para a pesquisa, contudo, o período e que tais obrigações são discutidas à luz da Lei n. 12.965/14.

curso. Na Tabela 01, os “polos ativos” são os agravantes, apelantes ou recorrentes, a depender do recurso, e, na Tabela 02, são os embargantes.

As partes foram categorizadas a fim de permitir o processamento gráfico dos dados. Foram utilizadas as seguintes categorias:

- **PA**: empregada quando a parte é um **provedor de aplicação**;
- **PC**: empregada quando a parte é um **provedor de conexão**;
- **PJ**: refere-se à **pessoa jurídica que não seja um provedor de aplicação ou de conexão**;
- **PN**: utilizada nos casos em que a parte é **pessoa natural**;
- **NI**: refere-se aos casos em que as **partes não foram identificadas**, em razão da anonimização dos dados

5. Polo passivo em sede recursal

Considerado o mesmo sistema de identificação e categorização do polo ativo, a variável de polo passivo buscou considerar quem eram, na Tabela 01, os agravados, apelados e recorridos e, na Tabela 02, os embargados.

6. Multa

O objetivo da variável “multa” foi identificar quantos recursos que alcançaram os Tribunais tratavam da cominação de multas, tanto de caráter interlocutório, quanto em decisão terminativa de mérito. O campo foi preenchido com as opções “sim”, “não” e “não identificado”, quando a análise era inconclusiva.

7. Valor da Multa

Nos casos em que se identificou o arbitramento de multa, os pesquisadores também buscaram discriminar o valor definido.

8. Tutela provisória

Buscou-se identificar quais decisões representaram o questionamento sobre tutela provisória. Isso porque a obrigação de fornecer porta lógica pode ser definida em decisão interlocutória, na primeira instância, e contra ela as partes se insurgirem, levando o caso à análise dos tribunais.

9. Dispositivo legal

O campo sobre dispositivo legal colheu informações sobre os instrumentos citados ou invocados na decisão. Eles foram identificados pela Equipe de Pesquisa por meio de siglas. Por exemplo, “MCI” refere-se ao Marco Civil da Internet, enquanto “CR” à Constituição da República Federativa do Brasil.

10. Argumento estritamente processual

O objetivo dessa variável foi verificar quantas das decisões sobre a obrigação, pelos provedores de aplicação, de fornecer a porta lógica de origem para identificação de um usuário, discutiram materialmente a controvérsia ou limitaram-se a questões adjetivas e regras processuais. A variável, de modo secundário, também permite aferir em que medida certas decisões interlocutórias ou terminativas de mérito deixam de estabelecer qualquer contribuição, em termos de formação de precedentes materialmente consistentes, sobre a interpretação de regras substantivas do Marco Civil.

11. Citação ao Marco Civil da Internet

Considerando que o Marco Civil da Internet é o instrumento normativo, no Brasil, que trata da guarda de dados pelos provedores, necessário se fez investigar quantas decisões sobre porta lógica o consideravam em sua fundamentação.

12. Dispositivo do Marco Civil citado ou invocado

Nos casos em que o Marco Civil da Internet foi citado, procurou-se distinguir os dispositivos, a fim de analisar sua pertinência à matéria debatida.

13. Obrigação de fornecer porta lógica

A "obrigação de fornecer porta lógica" corresponde ao dispositivo da decisão, ao resultado da recurso interposto. Essa obrigação refere-se, especificamente, aos **provedores de aplicação**, uma vez que figuram no centro das controvérsias sobre a responsabilidade de guarda e entrega das portas lógicas. O campo foi preenchido com "sim", "não" e "NI", nos casos em que não ficou clara a definição da obrigação.

14. Citação de precedente

Em razão da crescente importância dos precedentes no ordenamento brasileiro, sobretudo a partir da entrada em vigor do Novo Código de Processo Civil, a pesquisa considera a frequência em que as decisões citam soluções anteriores sobre a matéria controversa. Foram preenchidos como "sim", os campos em que são apresentados julgados relativos à obrigação dos provedores de aplicação de fornecerem porta lógica de origem.

15. Citação de parecer técnico

Os aspectos técnicos são relevantes para a decisão sobre a guarda e entrega de portas lógicas. Por esse motivo, foi verificado se as decisões citavam, pareceres técnicos ou relatórios em sua fundamentação. Foram considerados pelos pesquisadores, como parecer técnico, tanto relatórios de agências estatais e organizações da sociedade civil, quanto a citação, na decisão, de literatura especializada e opiniões legais sobre o tema.

16. Interpretação teleológica do Marco Civil da Internet

Nos casos em que o Marco Civil da Internet foi citado, verificou-se que tipo de interpretação foi realizada pelo tribunal sobre a lei. A interpretação teleológica, para os fins da presente pesquisa, foi compreendida como aquela que fundamenta a decisão

com base na *finalidade* da lei, discutindo qual seria ela e como deve ser assegurada. Assim, quando a decisão estabelece a obrigação, por exemplo, com a finalidade de o Marco Civil da Internet identificar usuários acusados de atos ilícitos, o campo foi preenchido como "sim". Quando a interpretação foi distinta da finalidade, o resultado foi "não" e ainda, quando, apesar de a lei ser citada, sua interpretação não foi clara, completou-se o campo com "NI - não identificável".

17. Interpretação literal do Marco Civil da Internet

Outra interpretação possível do Marco Civil da Internet como variável de pesquisa, segundo a metodologia adotada pela Equipe, foi a interpretação literal. Quando identificado que a fundamentação da decisão a partir da lei representa sua transcrição literal e se limita ao que os artigos citados definem, foi preenchido como "sim" o campo "interpretação literal". Quando houve interpretações diversas, "não", e nos casos em que não ficou claro, "NI".

Variáveis - Banco de dados 02

Correspondentes ao banco de dados 01

A tabela 02 reúne o grupo dos Embargos de Declaração e conta com as seguintes variáveis também apresentadas na tabela 01, sob justificativa idêntica:

- Número do processo - e também da decisão recorrida, apenas para fins de identificação.
- Estado;
- Ano;
- Polo ativo;
- Polo passivo.

Argumento estritamente processual

Nesse campo, pretende-se verificar se os Embargos servem como meio de revisão material das decisões, ou se restringem a argumentos processuais relativamente à função do recurso interposto, ou da identificação de ânimo protelatório de uma das partes.

Revisão da decisão recorrida

O objetivo é investigar a efetividade do recurso para a reforma das decisões embargadas. O campo foi preenchido, novamente, com "sim" e "não" nos casos em que é claro o dispositivo, ou com "não identificado" quando a decisão recorrida não foi localizada pelas buscas, de modo que a variável acerca da revisão restou inconclusa para os pesquisadores.

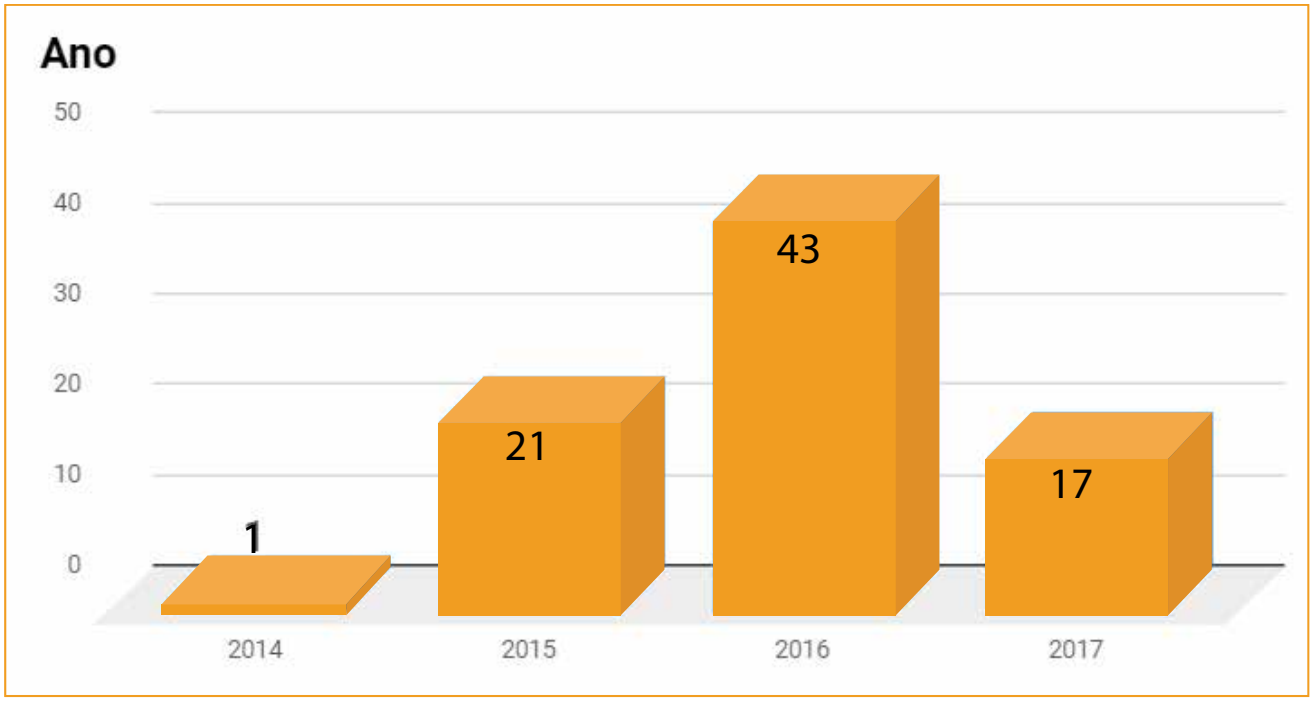
6. Análise dos resultados Perfil das decisões judiciais

Perfil das decisões

Considerada a opção por investigar os casos a partir da segunda instância, em primeiro momento, foram analisados 80 (oitenta) recursos de Agravo de Instrumento, de Apelação e de Suspensão de Execução, todos identificados e selecionados a partir da base dos Tribunais de Justiça. No Superior Tribunal de Justiça, foram encontrados apenas dois Agravos em Recurso Especial[65] que, em sede de decisão monocrática, não discutiram a matéria de portas lógicas e, portanto, não serviram para orientar a pacificação da controvérsiada controvérsia e formar entendimentos jurisprudenciais sobre o tema. Em ambos, na verdade, foram utilizados argumentos processuais que impediram a apreciação da matéria de fundo pelo STJ.

No caso Agravo em Recurso Especial nº 897.089 - SP, o motivo apontado foi a superveniência de Apelação, que suspende recursos interpostos anteriores a ela. Por sua vez, a justificativa para que não fosse discutido o Agravo em Recurso Especial nº 1011826 - SP encontra-se na interpretação de que ele demandaria análise de fatos ou provas, finalidades a que essa espécie de recurso não se presta[66].

Considerados os recursos apresentados nos Tribunais de Justiça, nos quais se trata efetivamente da obrigação, pelo provedor de aplicação, de fornecer porta lógica, entre os anos de 2014 e agosto de 2017, percebe-se maior concentração em 2016:



Uma primeira observação levaria à impressão de que o número de demandas têm aumentado[67]. Pode-se esperar, contudo, que esse crescimento não se mantenha,

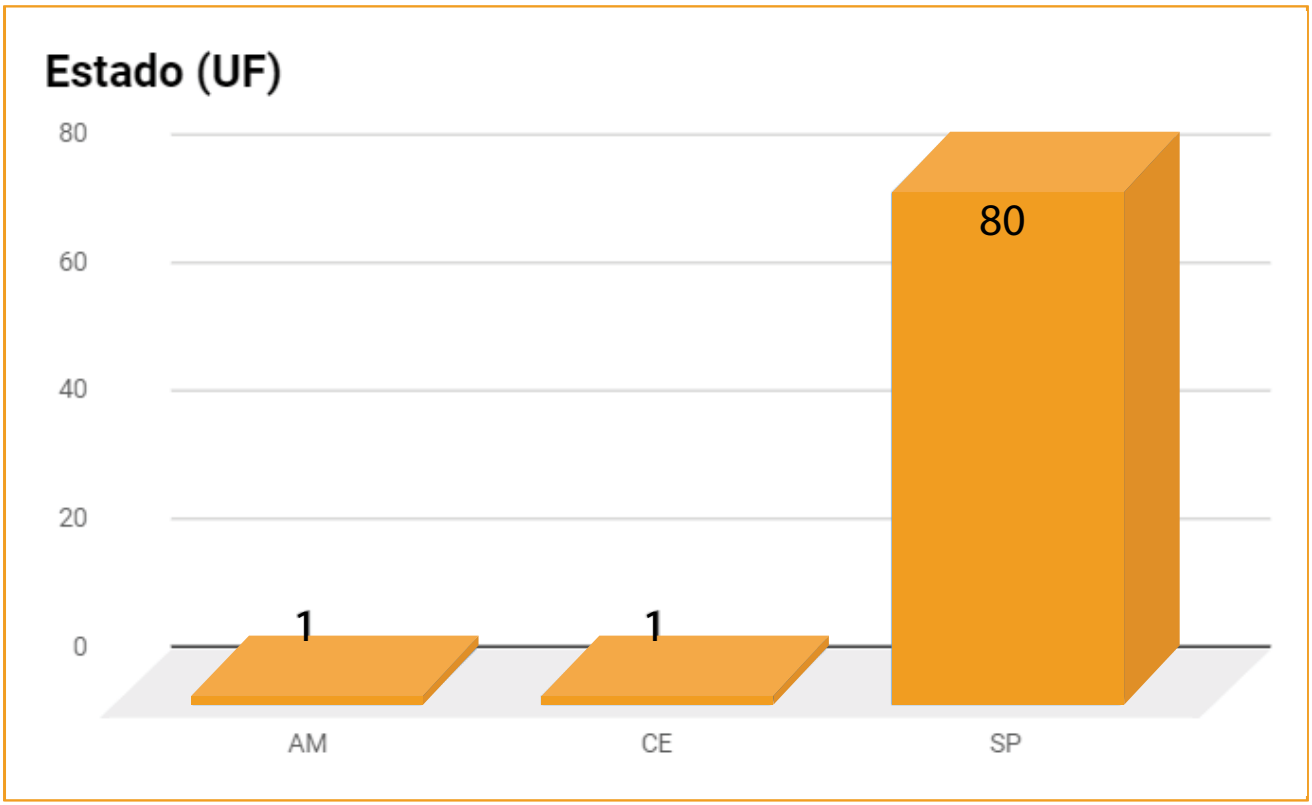
65 STJ, *AResp nº 897.089 - SP (2016/0087515-0)*, Decisão Monocrática, Ministro Moura Ribeiro, Data de julgamento: 16/09/2016 e STJ, *AREsp nº 1011826 - SP (2016/0293419-7)*, Decisão Monocrática, Ministra Nancy Andrighi, data de julgamento: 28/06/2017.

66 Devido às fundamentações estritamente processuais, sem análise material do objeto deste estudo, os casos encontrados no STJ não foram incluídos na Tabela 01, que serviu de base para as variáveis explicadas nas Notas Metodológicas.

67 É importante reforçar que a varredura do ano de 2017 terminou em 31/08/2017, como apresentado na sessão sobre o marco temporal da pesquisa.

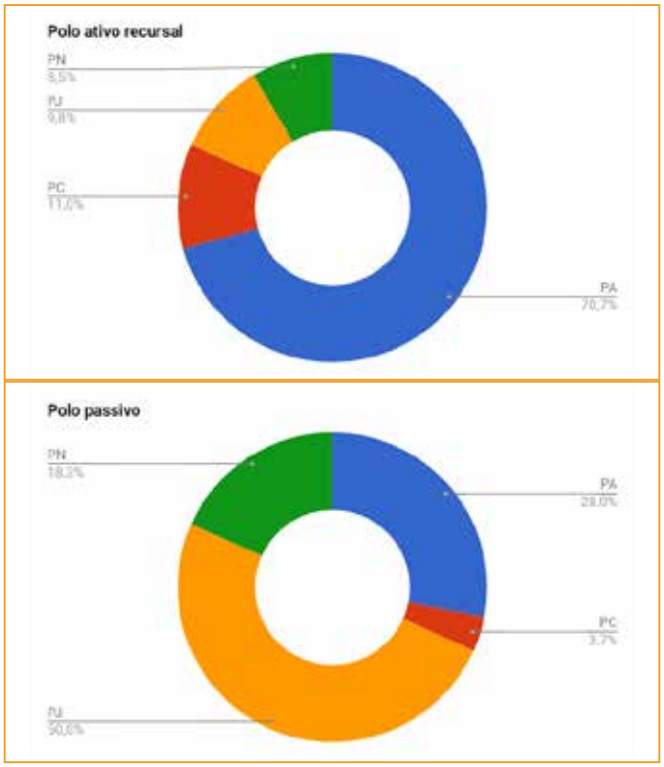
caso o processo de implementação do IPv6 no país se acelere (considerando que não haja uso de sistemas NAT em um cenário de IPv6) , levando à diminuição do uso de portas lógicas. Mesmo que ainda incipiente, a utilização do IPv6 no Brasil está entre as mais expressivas do mundo, conforme demonstram os dados do sub-título "Implementação do IPv6 no Brasil" deste estudo. Apesar disso, o ritmo é lento e, ainda que a utilização de portas lógicas seja medida transitória, as controvérsias ainda alcançarão os tribunais enquanto a transição não tiver sido completada.

Observou-se que o Tribunal de Justiça de São Paulo concentra alto grau de litigiosidade em demandas sobre a obrigação, por provedores de aplicação, de fornecer portas lógicas[68]. A expressiva maioria dos casos que atingem a segunda instância, no Brasil, está no Estado:



Em relação aos litigantes, as partes são tanto pessoas naturais, quanto pessoas jurídicas. Entre estas, foram destacados os provedores de conexão e aplicação. Afinal, a discussão sobre portas lógicas e a definição da obrigação de um, de outro, ou de ambos de fornecê-las os afeta diretamente. Especificamente, a polêmica acerca de provedores de aplicação fornecerem ou não as portas lógicas pode ser apontado como o motivo pelo qual eles são a maioria das partes, tanto como recorrente, quanto recorrida.

68 Algumas das hipóteses para a concentração de demandas envolvendo a responsabilidade pelo fornecimento de portas lógicas no TJSP seriam a localização dos escritórios de grandes provedores de aplicação, como Facebook e Google, o que facilitaria possíveis procedimentos de execução ou coação contra eles, e a concentração de escritórios de advocacia especializados nessas demandas.



Além de os provedores de aplicação figurarem como maioria dos recorrentes, eles também são a maioria das partes recorridas. A justificativa para tanto pode estar ligada ao fato de que as decisões analisadas não serem homogêneas. Uma parte ou outra pode impetrar diferentes recursos a fim de reformarem, por exemplo, decisões interlocutórias a elas contrárias. Tudo dependerá, portanto, do instrumento recursal possibilitado pelo direito brasileiro.

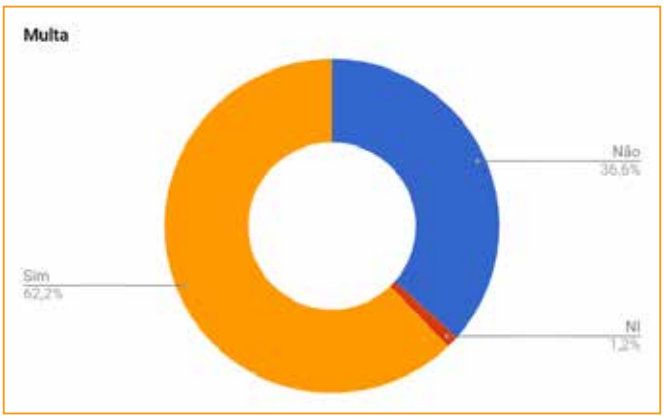
A maioria da amostragem das decisões analisadas é formada por acórdãos em recursos contra decisões interlocutórias. Deles, 82%[69] referem-se a agravos de instrumento impetrados para questionar decisão de primeira instância que deferiu ou não tutela provisória para a entrega de informações sobre portas lógicas. A tutela provisória é instrumento processual utilizado para proteger tanto o direito material objeto da demanda quanto o processo judicial em si, em razão da urgência ou dos prejuízos que podem ser causados pelo decurso do tempo. Busca-se obter a porta lógica que permita identificar um usuário inequivocamente antes do fim do processo, quando pode ser que essa função tenha se perdido. É importante destacar que a tutela de emergência ocorre em cognição sumária, sem que as provas sejam esgotadas, ou que a solução seja definitiva. Apesar disso, obriga as partes a cumprirem a decisão e, por isso, podem ser observadas como a causa da maior parte dos recursos envolvendo o fornecimento de portas lógicas pelos provedores de aplicação.

As decisões que definem obrigação de fazer, como é o caso de "entregar porta lógica", contam com instrumentos para constranger o devedor a cumprí-las. Um deles é conhecido como "astreinte". Prevista no art. 537 do CPC[70], trata-se de multa determinada judicialmente, em geral diária, que incide enquanto a obrigação não for cumprida. Sua fixação pode ocorrer tanto em sentença, quanto em tutela provisória, bem como na fase de execução do processo. Nos casos analisados, as multas foram estabelecidas a fim de impelir os provedores de aplicação a fornecerem a porta lógica de origem, caso

69 Isso representa 68 das 82 decisões analisadas.

70 Art. 537. A multa independe de requerimento da parte e poderá ser aplicada na fase de conhecimento, em tutela provisória ou na sentença, ou na fase de execução, desde que seja suficiente e compatível com a obrigação e que se determine prazo razoável para cumprimento do preceito.

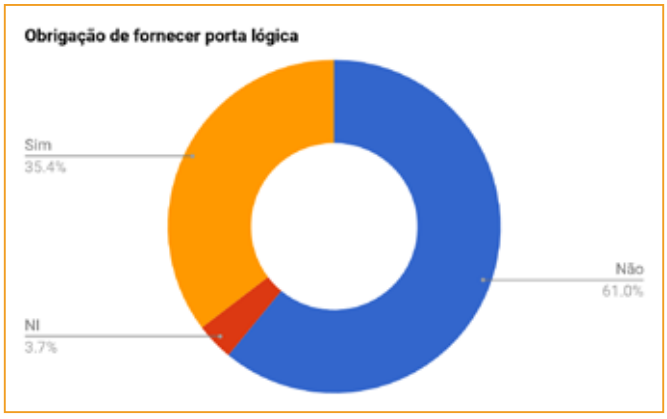
não o façam até o prazo fixado[71]. Observa-se que a maioria das decisões tratou de multas fixadas em primeira instância:



Nos casos em que se identificou o arbitramento de multa, percebe-se que o montante estabelecido é muito variado. Há multas diárias de R$100,00[72] e outras que alcançam os R$10.000,00[73]. Algumas decisões impõem limites de dias, ou de montante a ser pago[74], e outras não definem teto[75]. Tecnicamente, não há um padrão para fixação das multas por astreintes, de modo que, ao defini-las, o juiz deve considerar as especificidades dos casos, a fim de que a medida seja proporcional e suficiente. Apesar disso, a grande variação de valores e condições parece ser um sintoma da heterogeneidade com que o tema da obrigação de fornecer portas lógicas, pelo provedor de aplicação, tem sido tratado na justiça brasileira.

Decisões e fundamentos

A maioria das decisões analisadas, em segunda instância, não atribui aos provedores de aplicação a obrigação de fornecer portas lógicas:



Verificado o resultado das decisões, a pesquisa buscou identificar seus fundamentos. Para tanto, considerou como **variáveis** a presença de **referências** ao **Marco**

71 O Agravo de Instrumento nº 2120450-79.2016.8.26.0000/TJSP, por exemplo, trata de multa fixada em decisão de antecipação de tutela, caso o provedor não forneça a porta lógica em 05 dias, sob pena de multa diária de R$500,00 até o valor máximo de R$50.000,00. TJSP. *Agravo de Instrumento nº 2120450-79.2016.8.26.0000/TJSP.* Relator: Desembargador Costa Netto, Data de Julgamento: 13/12/2016, 9ª Câmara de Direito Privado, Data de Publicação: 19/12/2016.

72 TJSP. *Agravo de Instrumento nº 2108286-82.2016.8.26.0000*, Relator: Desembargador Alcides Leopoldo e Silva Júnior, Data de Julgamento: 13/09/2016, 1ª Câmara de Direito Privado, Data de Publicação: 13/09/2016.

73 TJSP. *Agravo de Instrumento nº 2175598-75.2016.8.26.0000.* Relator: Desembargador Beretta da Silveira, Data do julgamento: 08/12/2016, 3ª Câmara de Direito Privado, Data de publicação: 08/12/2016.

74 O Agravo de Instrumento nº 2185053-64.2016.8.26.0000/TJSP, por exemplo, limita a multa a noventa dias. Já o Agravo de Instrumento nº 2108074-61.2016.8.26.0000/TJSP define como teto o montante de R$10.000,00. TJSP. *Agravo de Instrumento nº 2185053-64.2016.8.26.0000.* Relator: Desembargador J.L. Mônaco da Silva, Data do julgamento: 16/11/2016, 5ª Câmara de Direito Privado, Data de publicação: 21/11/2016.

75 C.f.: TJSP. *Agravo de Instrumento nº 2158001-30.2015.8.26.0000/TJSP.* Relator: Desembargador Rui Cascaldi. Data do julgamento: 03/11/2015, 1ª Câmara de Direito Privado, Data de publicação: 04/11/2015.

Civil da Internet, que é a lei que estabelece a obrigação de guarda de dados, pelos provedores, a precedentes e a pareceres técnicos. Em geral, a discussão envolve aspectos da **capacidade dos provedores de aplicação** de armazenar e entregar a porta lógica, quando solicitados judicialmente. Os números que relacionam a presença desses fundamentos com o resultado sobre a obrigação pesquisada, contudo, não são suficientes para estabelecer um padrão de fundamentação das decisões, pois elas são muito variáveis.

A Lei n. 12.965/2014, o Marco Civil da Internet

A respeito dos fundamentos das decisões analisadas, a pesquisa identificou que nem todas[76] se baseiam no Marco Civil da Internet. Apesar de a Lei não tratar especificamente de portas lógicas, como já mencionado, ela disciplina o uso da internet no Brasil. É possível apontar, como uma das razões, o desconhecimento da lei pelo próprio Poder Judiciário, porque se verificou que, com o tempo e com a consolidação do Marco Civil, sua aplicação tem aumentado. Assim, enquanto em 2014 e 2015 o número de decisões que não citavam a lei era maior do que as que citavam, esse comportamento se inverte em 2016, e também no período de 2017 analisado. Percebe-se, portanto, que a lei tem sido mais aplicada nos casos envolvendo portas lógicas.

Não variam de modo significativo os dispositivos do Marco Civil da Internet, quando constam nas decisões[77]. De modo geral, aparecem com frequência os seguintes dispositivos: o art. 5º, VIII, que define, para os efeitos da lei, "registros de acesso"[78]; o art. 10, que trata da proteção de registros[79]; e o art. 15, que define a guarda de registros relativamente aos provedores de aplicação[80]. De modo menos frequente, são referidos outros incisos do art. 5º, como o inciso VII, no qual são definidas as aplicações da internet[81], o art. 19, a respeito da responsabilidade dos provedores[82] e o art. 22, sobre a requisição judicial dos registros[83].

Algumas decisões, apesar de citarem o Marco Civil da Internet, não se dedicam a interpretá-lo. Do total de decisões, o levantamento sobre a interpretação teleológica ou literal[84] da lei foi realizado apenas 46, em que foi possível identificar o esforço her-

76 Das 82 decisões analisadas, em 27 não se identifica nenhuma referência ao Marco Civil da Internet. Registra-se aqui a crítica de que os princípios, bem como as definições legais e responsabilidades definidas pela lei, em razão do contexto em que a demanda se desenvolve, deveriam, aos menos, ser considerados. Para mais informações quanto à aplicabilidade da lei, cf. a seção deste estudo sobre o Marco Civil.

77 C.f. Banco de dados 01, anexo.

78 Art. 5º Para os efeitos desta Lei, considera-se: [...] VI - registro de conexão: 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.

79 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.

80 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.

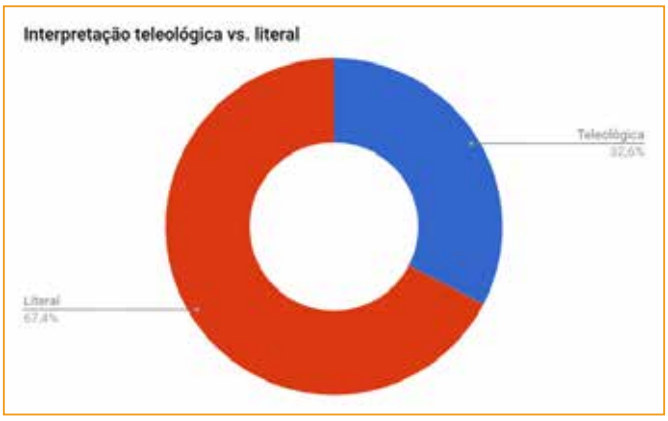
81 Art. 5º [...] VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

82 Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

83 Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

84 As duas formas de interpretação foram escolhidas em razão da frequência com que aparecem nos processos sobre o tema das portas lógicas. A teleológica está ligada à interpretação da norma conforme a finalidade do legislador ao editar a lei e busca estender a norma para além do texto em si. Já a interpretação literal atrela-se ao que foi prescrito na lei e baseia-se em leitura mais restrita,

menêutico sobre a lei. Nesse recorte feito entre as decisões, observa-se que a interpretação literal tem prevalecido:



De maneira geral, a **interpretação literal** baseia-se no fato de o Marco Civil da Internet não tratar de portas lógicas ao definir os registros de acesso (art. 5º) que os provedores de aplicação devem guardar ou fornecer mediante ordem judicial (art. 15). De acordo com essa perspectiva, não havendo outro diploma legal que regule a matéria discutida, o silêncio do Marco Civil da Internet a respeito das portas lógicas desobriga os provedores de aplicação quanto a seu armazenamento e entrega[85]. De modo diverso, a **interpretação teleológica** elege como finalidade das disposições sobre a guarda de registros de acesso no Marco Civil da Internet a identificação dos usuários de aplicação, quando isso for necessário judicial ou administrativamente, ou ainda à polícia ou ao Ministério Público (art. 15 e parágrafos). Ainda que a lei não faça menção expressa, as decisões que adotam essa interpretação consideram que, a fim de viabilizar a identificação do usuário, as portas lógicas podem ser incluídas nos **registros de acesso** de que trata o art. 5º da lei, cuja guarda é obrigatória pelos provedores de aplicação[86].

Precedentes

Frequentemente são utilizados precedentes para justificar tanto as decisões favoráveis, quanto as contrárias à **obrigação de fornecer porta lógica**. A maioria das decisões conta com outros julgados anteriores e que tratam do mesmo tema. Por serem citados julgamentos anteriores em ambas as direções, não se pode concluir que a existência de precedentes no julgado revele uma tendência de decisão, particularmente pela inconsistência das orientações estabelecidas.

Pareceres técnicos

Considerada a natureza da controvérsia, que envolve a infraestrutura necessária para que provedores de aplicação registrem e entreguem - ou não - a porta lógica, bus-

fundamentada na segurança jurídica. Este estudo não tem a pretensão de valorar a aplicação de uma ou outra interpretação, limitando-se, pois, a identificá-las.

85 Essa perspectiva pode ser encontrada, por exemplo, nas seguintes decisões: TJSP. *Agravo de Instrumento n. 2087441-29.2016.8.26.0000*. Relator: Desembargador Moreira Viegas, Data do julgamento: 23/11/2016, 5ª Câmara de Direito Privado, Data de publicação: 24/11/2016; TJSP. *Agravo de Instrumento n. 2083730-16.2016.8.26.0000*. Relator: Desembargador Vito Guglielmi, Data do julgamento: 14/07/2016, 6ª Câmara de Direito Privado, Data de publicação: 15/07/2016; e TJSP. *Agravo de Instrumento n. 2251294-54.2015.8.26.0000*. Relator: Desembargador Miguel Brandi, Data do julgamento: 21/09/2016, 7ª Câmara de Direito Privado, Data de publicação: 21/09/2016.

86 Verifica-se essa abordagem nos seguintes Agravos de Instrumento: TJSP. *Agravo de Instrumento n. 2149601-90.2016.8.26.0000*, Relator: Desembargador Ricardo Pessoa de Mello Belli, Data do julgamento: 05/12/2016, 19ª Câmara de Direito Privado, Data de publicação: 11/01/2017; TJSP. *Agravo de Instrumento n. 2120450-79.2016.8.26.0000*. Relator: Desembargador Costa Netto, Data do julgamento: 13/12/2016, 9ª Câmara de Direito Privado, Data de publicação: 19/12/2016; e TJAM. *Agravo de Instrumento n. 4004023-74.2016.8.04.0000*. Relatora: Desembargadora Maria do Rosário Perpétuo Socorro Guedes Moura, Data de julgamento: 05/06/2017, 2ª Câmara Cível.

cou-se analisar se as decisões dos Tribunais de Justiça consideraram também argumentos técnicos, constantes não apenas em relatórios propriamente dessa natureza, mas também compreendidos em referências bibliográficas referentes ao tema. Observou-se que apenas 17 das 82 decisões[87] consideraram esses argumentos. Entre elas, 11 decisões citaram pareceres técnicos que definiam a obrigação de fornecer portas lógicas, e 6 a negavam.

A **referência técnica** mais frequente nos julgados é o relatório final de atividades do Grupo de Trabalho para Implantação do Protocolo IP-Versão 6 nas Redes das Prestadoras de Serviços de Telecomunicações, publicado pela ANATEL em 2014. O grupo reuniu não apenas representantes da Anatel, como também de prestadoras de serviços de telecomunicações com o objetivo de discutir a implementação do IPv6 no país, seu período de transição e técnicas a serem utilizadas[88]. No Brasil, o relatório representa a discussão, em nível técnico, mais robusta sobre as técnicas NAT, compartilhamento de IPs e portas lógicas. Por isso, o documento é utilizado em parte das decisões como referência técnica. É curioso que referências ao Relatório são encontradas tanto para embasar a decisões favoráveis[89], quanto contrárias[90] à obrigação de o provedor de aplicação fornecer porta lógica.

Destaca-se que o relatório do grupo de trabalhos da ANATEL não é o único parecer publicamente disponível sobre o assunto. A provedora de conexão TIM Brasil, por exemplo, indica na consulta pública do Ministério da Justiça ao decreto regulamentador do Marco Civil da Internet, que: "(...) a porta lógica não se caracteriza como registro de acesso a aplicações de internet, nos termos da Lei. Ao contrário, a porta lógica está relacionada ao conceito de registro de conexão, pois é uma informação que complementa o endereço IP."[91] Observa-se, aqui, a inércia do Poder Judiciário em buscar outras fontes técnicas sobre a matéria discutida.

Embargos de Declaração

Algumas das decisões dos tribunais foram questionadas por Embargos de Declaração. O banco de dados 02 buscou reunir o perfil também desses recursos e verificar se houve revisão das decisões. Percebeu-se que eles se encontram apenas no Tribunal de Justiça de São Paulo. Assim como no banco de dados 01, provedores de aplicação são a maior parte dos polos ativo e passivo. Foi verificado que a maioria dos Embargos de Declaração não trata do objeto material da demanda[92], as portas lógicas, mas se concentram em argumentos estritamente processuais, como os requisitos dos Embargos de Declaração, sua natureza, ou finalidade. Algumas decisões identificam

87 Isso compreende 20,7% das decisões objeto deste estudo. Nota-se que em 79,3% das decisões a discussão não abrange, pelo menos em segunda instância, argumentos técnicos ou especializados.

88 "Art. 1º Constituir o Grupo de Trabalho para implantação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações – GT-IPv6, com a participação das prestadoras de serviços de telecomunicações e das Superintendências da Anatel envolvidas, com o objetivo de coordenar os trabalhos necessários à adoção do protocolo IP-Versão 6 nas redes das prestadoras de serviços de telecomunicações brasileiras.". ANATEL. *GT-IPv6: Grupo de Trabalho para implantação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações -Relatório Final de Atividades.* Brasília. 12/2014. Disponível em: <http://bit.ly/2vy4e9U>. Acesso em: 01/09/2017

89 Uma das decisões que definiram a obrigação dos provedores de aplicação de fornecer porta lógica e utilizaram o relatório da do GT-IPv6 foi o Agravo de Instrumento n. 2257879-25.2015.8.26.0000. TJSP. *Agravo de Instrumento n. 2257879-25.2015.8.26.0000.* Relator: Desembargador J.L. Mônaco da Silva, Data do julgamento: 14/03/2016, 5ª Câmara de Direito Privado, Data de publicação: 14/03/2016.

90 Como exemplo de decisão que não define a obrigação de fornecer porta lógica e cita o relatório, c.f. TJSP. *Agravo de Instrumento n. 2189710-83.2015.8.26.0000.* Relatora: Desembargadora Ana Lucia Romanhole Martucci, Data do julgamento: 27/11/2015, 6ª Câmara de Direito Privado, Data de publicação: 28/11/2015.

91 TIM BRASIL. *"Armazenamento da porta lógica de origem pelos provedores de aplicação".* Disponível em: <https://goo.gl/LDp7py>. Acesso em 10/10/2016.

92 80% das decisões baseiam-se em questões estritamente processuais. Cf. Banco de dados 02, anexo.

um propósito protelatório na interposição dos Embargos de Declaração. Por isso, outro dado importante referente aos Embargos de Declaração é que a maioria não altera as decisões agravadas:

7. Considerações finais

É possível identificar que a problemática a respeito das portas lógicas é polêmica não apenas no Brasil, em razão do esgotamento mundial do IP versão 4. Ao mesmo tempo em que se reconhece que a implementação do IPv6 restabelecerá a ligação direta com a internet, viabilizando a identificação inequívoca do usuário, também se admite que ela está atrasada e que a técnica pode continuar sendo usada, mesmo com a nova versão. A discussão sobre se (e quem) deveria armazenar e fornecer os dados necessários à identificação inequívoca deve persistir.

No Brasil, a análise das decisões coletadas nos tribunais reflete as incertezas sobre o tema, na medida em que são encontrados entendimentos diametralmente distintos, sem espaços para uniformização nessa fase de análise. A interpretação sobre os registros de acesso pelos provedores de aplicação não é pacífica, assim como não se vislumbra solução uniforme para as disposições do Marco Civil da Internet.

Ainda é preciso considerar que muitas das decisões analisadas não se tratam da solução final dos processos, e foram recorridas sem que todo o arcabouço probatório fosse esgotado. De qualquer maneira, devem ser objeto de acompanhamento, com o objetivo de analisar as provas apresentadas pelas partes e como elas serão consideradas na solução da controvérsia. Os resultados encontrados na pesquisa tratam-se, portanto, de perspectivas jurisprudenciais ainda não consolidadas e revelam-se bastante heterogêneos, ainda que *tenha prevalecido o entendimento de que os provedores de aplicação não têm a obrigação legal de fornecer a porta lógica de origem*.

Finalmente, é necessário observar que, na falta de políticas públicas e legislativas sobre a utilização da técnica NAT e sobre o uso de portas lógicas, o Poder Judiciário tem sido demandado a definir posicionamento a respeito do tema.

Nesse contexto, devem ser considerados, além dos aspectos técnicos, os impactos econômicos[93], de inovação e da viabilidade de pequenas empresas, sopesados em relação à necessidade de se identificar usuários que possivelmente tenham cometidos atos ilícitos, considerando os princípios definidos pelo Marco Civil da Internet para a governança das redes no Brasil.

93 Este estudo não teve como escopo os possíveis impactos das decisões sobre a obrigação de fornecer portas lógicas pelos provadores de aplicação em suas atividades econômicas. No entanto, é necessário considerar que a exigência de armazenar e entregar a porta lógica demanda infraestrutura, cujo custo pode afetar de forma mais impactante, ainda que não os grandes, os pequenos provedores de aplicações de internet.

8. Referências

Livros, artigos e teses

ANATEL . "GT IPv6: Grupo de Trabalho para implementação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações, *Relatório Final de Atividades*." Dezembro de 2014. Disponível em: <http://bit.ly/2zk0tTF>. Acesso em: 20/09/2017.

AUSTRALIA. "Telecommunications (Interception and Access) Act" Nº 114, 1979, Compilation Nº. 96. Disponível em: <http://bit.ly/2yTtp97>. Acessado em: 05/10/2017.

AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017.

AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers* . Julho de 2015. Disponível em: <http://bit.ly/2gOWCJG>. Acessado em: 06/10/2017

BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATION *Report on OTT services*. 2016. p. 14. Disponível em:<http://bit.ly/2yRFc3s>. Acessado em 08/10/2017.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. "Internet Protocol: DARPA Internet Program Protocol Specification". *IETF*, RFC791. Setembro de 1981. Disponível em: <http://bit.ly/2jy2SCa> Acesso em 20 de Setembro de 2017.

DURAN, Alan et al. "Logging Recommendations for Internet-Facing Servers". *IETF*, RFC6302. Junho de 2011. Disponível em: <http://bit.ly/2kgwjye>. Acessado em: 02/10/2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). *Data retention across the EU*. Disponivel em: <http://bit.ly/2zhJIZu>. Acessado em: 18/10/2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). *Fundamental Rights Report 2017*. 2017. p.162-165. Disponível em: <http://bit.ly/2yvAxoY>. Acessado em: 18/10/2017.

EUROPOL. *About Europol.* Disponível em:<http://bit.ly/2jWsUV8>. Acessado em: 29/09/2017.

EUROPOL/EC3 - 5127/17. "Carrier-Grade Network Address Translation (CGN) And the Going Dark Problem". 16 de Janeiro de 2017. p. 7. Disponível em: <http://bit.ly/2hw37OX> e <http://bit.ly/2yDviCI>. Acesso em: 29/09/2017.

EUROPOL. "*IOCTA 2016 - Internet Organised Crime Threat Assessment*". Disponível em: <http://bit.ly/2fCum7o>. p. 57 e 58. Acessado em: 25/09/2017.

HINDEN, Robert M. e DEERING, Stephen E. "Internet Protocol, Version 6 (IPv6)". *IETF.* RFC2460. Dezembro de 1998. Disponível em: <http://bit.ly/2iIJ4Xz> Acesso em 20 de Se-

tembro de 2017.

HURST, Daniel. *Telcos question data retention plans that exempt Facebook, Gmail and Skype*. The Guardian. 2015. Disponível em: <http://bit.ly/2xqggnn>. Acessado em: 08/10/2017.

JIANG, Sheng, GUO, Dayong & CARPENTER, Brian. "An incremental Carrier-Grade NAT (CGN) for IPv6 Transition". *IETF*, RFC6264. Junho de 2011. Disponível em <http://bit.ly/2gOo5ZQ> Acesso em 20 de Setembro de 2017.

SRISURESH, Pyda & HOLDREGE, Matt. "IP Network Addres Translator (NAT) Technology and Considerations. *IETF*, RFC2663. Agosto de 1999. Disponível em: <http://bit.ly/1FFjvRC> Acesso em: 20/09/2017.

SUZOR, Nicolas; PAPPALARDO, Kylie; McINTOSH, Natalie. *The passage of Australia's data retention regime: national security, human rights, and media scrutiny*. Internet Policy Review- Journal on Internet Regulation.Volume 6, Edição 1. Março de 2017. Disponivel em: <http://bit.ly/2y4aUeB>. Acessado em: 08/10/2017.

TIM BRASIL. *"Armazenamento da porta lógica de origem pelos provedores de aplicação".* Disponível em: <https://goo.gl/LDp7py>. Acesso em 10/10/2016.

UE. "*Directiva 2006/24/CE do Parlamento Europeu e do Conselho*, de 15 de Março de 2006 , relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE". Disponível em: <http://bit.ly/2fPZOWg>. Acessado em: 04/10/2017

WEBER, Rolf H. *Shaping internet governance: Regulatory challenges.* Springer Science & Business Media, 2010.

Casos

CJEU. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources Ireland and others and Kärntner Landesregierung.* Joined cases C-293/12 and C-594/12, Grand Chamber, 8 de abril de 2014. Disponível em: <https://goo.gl/fjqymW>. Acesso em: 04/10/2017.

CJEU. *Patrick Breyer v. Bundesrepublik Deutschland*. Case C-582/14. 19 Outubro de 2016. DIsponível em: <http://bit.ly/2gsdqaf>. Acessado em: 18/10/2017.

CJEU. T*ele2 Sverige AB contra Post- och telestyrelsen e Secretary of State for the Home Department contra Tom Watson*. Case C-203/15.2016. DIsponível em <http://bit.ly/2yxxiNR>. Acessado em: 18/10/2017.

CJEU. The Court of Justice of the European Union. *Press Release Nº 54 /14*. Luxemburgo, 8

de Abril de 2014. Disponível em: <http://bit.ly/2tBS4lV>. Acessado em: 04/10/2017.

STJ, *REsp nº 1403749/GO,* Ministra Nancy Andrighi, Terceira Turma, Data de julgamento: 22/10/2013.

STJ, *AResp nº 897.089 - SP (2016/0087515-0)*, Decisão Monocrática, Ministro Moura Ribeiro, Data de julgamento: 16/09/2016.

STJ, *AREsp nº 1011826 - SP (2016/0293419-7)*, Decisão Monocrática, Ministra Nancy Andrighi, Data de julgamento: 28/06/2017.

TJAM. *Agravo de Instrumento n. 4004023-74.2016.8.04.0000.* Relatora: Desembargadora Maria do Rosário Perpétuo Socorro Guedes Moura,Data de julgamento: 05/06/2017, 2ª Câmara Cível.

TJSP. *Agravo de Instrumento nº 2120450-79.2016.8.26.0000/TJS*P. Relator: Costa Netto, Data de Julgamento: 13/12/2016, 9ª Câmara de Direito Privado, Data de Publicação: 19/12/2016.

TJSP. *Agravo de Instrumento nº 2108286-82.2016.8.26.0000*, Relator: Desembargador Alcides Leopoldo e Silva Júnior, Data de Julgamento: 13/09/2016, 1ª Câmara de Direito Privado, Data de Publicação: 13/09/2016.

TJSP. *Agravo de Instrumento nº 2185053-64.2016.8.26.0000.* Relator: Desembargador J.L. Mônaco da Silva, Data do julgamento: 16/11/2016, 5ª Câmara de Direito Privado, Data de publicação: 21/11/2016.

TJSP. *Agravo de Instrumento nº 2158001-30.2015.8.26.0000/TJSP.* Relator: Desembargador Rui Cascaldi. Data do julgamento: 03/11/2015, 1ª Câmara de Direito Privado, Data de publicação: 04/11/2016.

TJSP. *Agravo de Instrumento n. 2087441-29.2016.8.26.0000*. Relator: Desembargador Moreira Viegas, Data do julgamento: 23/11/2016, 5ª Câmara de Direito Privado, Data de publicação: 24/11/2016.

TJSP. *Agravo de Instrumento n. 2083730-16.2016.8.26.0000.* Relator: Desembargador Vito Guglielmi, Data do julgamento: 14/07/2016, 6ª Câmara de Direito Privado, Data de publicação: 15/07/2016.

TJSP. *Agravo de Instrumento n. 2251294-54.2015.8.26.0000*. Relator: Desembargador Miguel Brandi, Data do julgamento: 21/09/2016, 7ª Câmara de Direito Privado, Data de publicação: 21/09/2016.

TJSP. *Agravo de Instrumento n. 2257879-25.2015.8.26.0000.* Relator: Desembargador J.L. Mônaco da Silva, Data do julgamento: 14/03/2016, 5ª Câmara de Direito Privado, Data de publicação: 14/03/2016.

TJSP. *Agravo de Instrumento n. 2189710-83.2015.8.26.0000*. Relatora: Desembargadora Ana Lucia Romanhole Martucci, Data do julgamento: 27/11/2015, 6ª Câmara de Direito Privado, Data de publicação: 28/11/2015.

9. Anexos

Banco de Dados 01

-	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Multa	Valor da Multa	Tutela provisória	Argumento est. processual	Cita o MC? *	Se Sim, qual dispositivo?	Obrigação de fornecer porta lógica (prov. apli.)	Cita precedentes sobre porta lógica	Cita parecer técnico	Interpretação teleológica MCI*	Interpretação literal MCI*
AI 2107751-27.2014.8.26.0000	SP	2014	PA	PA	Não	-	Sim	Sim	Não	-	Não	Não	Não	Não	Não
AI 2158001-30.2015.8.26.0000	SP	2015	PA	PN	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VI a VIII, e 15, caput	Não	Sim	Não	Não	Sim
AI 2205211-77.2015.8.26.0000	SP	2015	PA	PJ	NI	-	NI	Não	Não	-	Não	Não	Não	Não	Não
AI 2012094-24.2015.8.26.0000	SP	2015	PA	PC	Não	-	Sim	Não	Não	-	Não	Não	Não	Não	Não
AI 2250400-78.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2086530-51.2015.8.26.0000	SP	2015	PA	PA	Sim	-	Sim	Não	Sim	Art. 15	Sim	Não	Não	Sim	Não
AI 2228882-32.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2227540-83.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Não	Não	Não	-	Não	Não	Não	NI	NI
AI 2012094-24.2015.8.26.0000	SP	2015	PA	PC	Não	-	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2112160-12.2015.8.26.0000	SP	2015	PA	PA	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2028312-30.2015.8.26.0000	SP	2015	PJ	PA	Sim	Diária R$ 5.000 limitada à quantia de R$ 150.000.	Sim	Não	Sim	Art. 22	Sim	Não	Não	NI	NI
AI 2136055-02.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$1.000,00 a R$50.000,00	Sim	Sim	Não	-	Sim	Sim	Não	NI	NI
AI 2057480-77.2015.8.26.0000	SP	2015	PJ	PA	Sim	-	Sim	Não	Sim	Art. 22	Sim	Sim	Não	NI	NI
AI 2159146-58.2014.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	NI	Não	Não	NI	NI
AI 2092413-76.2015.8.26.0000	SP	2015	PA	PN	Sim	-	Sim	Não	Não	-	Não	Sim	Não	Não	Sim
AI 2203864-09.2015.8.26.0000	SP	2015	PA	PJ	Sim		Sim	Não	Sim	Art. 15	Não	Sim	Não	Não	Sim
AI 2150710-76.2015.8.26.0000	SP	2015	PA	PC	Sim	Diária - R$10.000,00 com valor máximo de R$500.000,00	Sim	Não	Sim	Art. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AI 2255280-16.2015.8.26.0000	SP	2015	PA	PJ	Sim	R$50.000,00/dia	Sim	Não	Sim	Art. 5º, VIII	Não	Sim	Não	Não	Sim
AI 2172692-49.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$2.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2189710-83.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Sim	Não	Sim
AI 2172692-49.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$ 2.000,00	Sim	Não	Sim	-	Não	Sim	Sim	Não	Sim
AI 2219.128-03.2014.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$ 2..500,00 sem teto	Sim	Não	Sim	Arts. 10, §2º, e 20	Não	Não	Não	NI	NI
AI 2040293-22.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00/dia até R$500.000,00	Sim	Não	Sim	Art. 22	Sim	Sim	Não	Sim	Não
AI 2274058-34.2015.8.26.0000	SP	2016	PN	PA	Não	-	Sim	Não	Sim	Arts. 10, § 1º; 13; 15; e art 22	Não	Sim	Não	Não	Não
AI 2254100-62.2015.8.26.0000	SP	2016	PA	PN	Não	-	Sim	Não	Não	-	Sim	Não	Não	Não	Não
AI 2072406-29.2016.8.26.0000	SP	2016	PA	PA	Sim	Diária - R$5000,00 sem teto	Sim	Não	Sim	Arts. 5º, VII, e 15	Sim	Sim	Não	Não	Não
AI 2061576-04.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Art. 5º, VI e VIII, e 15	Sim	Sim	Não	Sim	Não
AI 2061576-04.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VI e VIII, e 15	Sim	Sim	Não	Sim	Não
AI 2257879-25.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Sim	Art. 5º, VIII	Sim	Sim	Sim	Sim	Não
AI 2081265-34.2016.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Sim	Arts 6 e 10.	Sim	Sim	Sim	Sim	Não
AI 2185053-64.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 1.000,00 (limite 90 dias)	Sim	Não	Sim	Arts. 5º,VIII; 10, capu, e § 1º; e 15	Sim	Sim	Sim	Sim	Não
AI 2092101-03.2015.8.26.0000	SP	2016	PJ	PJ	Sim	Não especificado	Não	Não	Não	-	Não	Não	Não	NI	NI
AI 2136855-93.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 5.000,00	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2134739-17.2016.8.26.0000	SP	2016	PC	PN	Sim	Diária R$ 10.000,00.	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2108074-61.2016.8.26.0000	SP	2016	PA	PJ	Sim	R$ 1.000,00 limitado à R$ 10.000,00.	Sim	Não	Sim	Art. 5º, VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2004349-56.2016.8.26.0000	SP	2016	PC	PJ	Não	-	Não	Sim	Não	-	Não	Não	Não	NI	NI
AI 2057550-60.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Sim	Sim	Não	-	Não	Não	Não	NI	NI
AI 2139037-52.2016.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2039490-39.2016.8.26.0000	SP	2016	PJ	PA	Sim	Diária - R$1.000,00 sem teto	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2206954-25.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Não	Não	Sim	Art 5º, 6º, 10º, §1º	Sim	Sim	Sim	Sim	Não
AI 2258906-43.2015.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 50.000,00	Sim	Não	Sim	Art 5º, 6º, 10º, §1º	Sim	Sim	Sim	Sim	Não
AI 2175598-75.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$10.000,00 a R$310.000,00	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2109770-35.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$10.000,00 sem teto	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2108286-82.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$ 100.00, até no máximo R$ 2.000,00.	Sim	Não	Sim	Arts 5º, V,VI, VII e VIII; e 15	NI	Sim	Não	NI	NI
AI 2250177-28.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Não	Sim	Não	-	Não	Não	Não	NI	NI
AI 2057550-60.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Não	Sim	Não	-	NI	Não	Não	NI	NI
AI 2149601-90.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Sim	Não	Sim	Arts 5º, VII, 15, §§	Sim	Sim	Sim	Sim	Não
AI 2040105-29.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$1.000,00	Sim	Não	Sim	Art. 5º, VIII e 15	Não	Não	Não	Não	Sim
AI 2120450-79.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária R$500,00 - limite: R$50.000,00	Sim	Não	Sim	Arts. 5º, VIII; 10; 19; 22	Sim	Não	Não	Sim	Não
AI 2072406-29.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$ 5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VII e VIII, e 15	Não	Não	Não	Não	Sim
AI 2110716-07.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária R$ 1.000,00	Sim	Não	Sim	Art 5º, V e VII	Não	Não	Não	Não	Sim
AI 2251294-54.2015.8.26.0000	SP	2016	PA	PJ	Sim	-	Sim	Não	Sim	Arts 5°, VIII e 15, § 1°	Não	Não	Não	Não	Sim
AP 1088666-63.2014.8.26.0100	SP	2016	PN	PA	Sim	Não	Sim	Sim	Sim	Arts. 10 e 22	Não	Não	Não	Não	Sim
SE 2066773-37.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$10.000,00 (limite 10 dias)	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AP 1055250-07.2014.8.26.0100	SP	2016	PN	PA	Sim	-	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AP 1108368-58.2015.8.26.0100	SP	2016	PA	PJ	Não	-	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AI 2078865-47.2016.8.26.0000	SP	2016	PN	PA	Sim	Diária R$500,00.	Sim	Não	Sim	Arts. 5°, VIII, e 15.	Não	Sim	Não	Não	Sim

-	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Multa	Valor da Multa	Tutela provisória	Argumento est. processual	Cita o MC? *	Se Sim, qual dispositivo?	Obrigação de fornecer porta lógica (prov. apli.)	Cita precedentes sobre porta lógica	Cita parecer técnico	Interpretação teleológica MCI*	Interpretação literal MCI*
AI 2106771-12.2016.8.26.0000	SP	2016	PA	PJ	Sim	R$ 1.000,00.	Sim	Não	Sim	Arts 5º V, VI, VII e VIII, e 15	Não	Sim	Não	Não	Sim
AI 2064240-08.2016.8.26.0000	SP	2016	PC	PA	Sim	Diária R$ 500,00.	Sim	Não	Sim	Arts 5°, inciso VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2027881-59.2016.8.26.0000	SP	2016	PC	PA	Sim	Diária de R$ 500,00, limitada a R$25.000,00	Sim	Não	Sim	Arts 5°, VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2084529-59.2016.8.26.0000	SP	2016	PA	PN	Não	-	Sim	Não	Sim	Arts. 5º, VI e VIII e 22	Não	Sim	Não	Não	Sim
AI 2184364-20.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária R$ 5.000,00	Sim	Não	Sim	Arts 5°, VIII e 15.	Não	Sim	Não	Não	Sim
AI 2256281-36.2015.8.26.0000	SP	2016	PN	PA	Não	-	Sim	Não	Não	-	Não	Sim	Sim	Não	Sim
AI 2252527-86.2015.8.26.0000	SP	2016	PA	PJ	Sim	Diária de R$ 3.000,00	Sim	Não	Sim	Arts 5°, VIII, e 15.	Não	Sim	Sim	Não	Sim
AI 2083730-16.2016.8.26.0000	SP	2016	PA	PJ	Sim		Sim	Não	Sim	Arts 5º e 15	Não	Sim	Sim	Não	Sim
AI 2087084-15.2017.8.26.0000	SP	2017	PA	PA	Sim		Sim	Não	Sim	Art. 5º, VIII	Sim	Sim	Sim	Sim	Não
AI 2168151-36.2016.8.26.0000	SP	2017	PA	PJ	Não	-	Sim	Não	Sim	Art. 5º, III	Sim	Sim	Sim	Sim	Não
AI 2216048-60.2016.8.26.0000,	SP	2017	PA	PN	Sim	Diária - R$ 2.000,00 até R$ 20.000,00.	Sim	Não	Não	-	Não	Sim	Não	Não	Não
AI 2225114-64.2016.8.26.0000	SP	2017	PA	PN	Sim	DIária - R$ 2.000,00 até R$20.000,00	Sim	Não	Não	-	Não	Sim	Não	Não	Não
AI 0620437-78.2017.8.06.0000	CE	2017	PC	PJ	Sim	R$ 4.400,00.	Sim	Não	Sim	-	Não	Sim	Não	Não	Não
AP 0004132-12.2015.8.26.0411	SP	2017	PJ	PA	Não	-	Não	Não	Sim	Arts. 5º, VIII; 6º; 15; e 16, II	Sim	Sim	Sim	Sim	Não
AI 4004023-74.2016.8.04.0000	AM	2017	PA	PN	Sim	Diária - 1.000,00 limite até R$20.000	Sim	Não	Sim	Arts. 5º III, IV, V e VI, e 22	Sim	Sim	Sim	Sim	Não
AI 2034460-86.2017.8.26.0000	SP	2017	PN	PJ	Não	-	Não	Não	Sim	Arts. 7º, I, e 8º	Não	Não	Não	NI	NI
AI 2087441-29.2016.8.26.0000	SP	2017	PA	PN	Não	-	Sim	Não	Sim	Art 5º, VIII	Não	Sim	Não	Não	Sim
AI 2251999-18.2016.8.26.0000	SP	2017	PN	PA	Sim	Diária - R$500,00 a R$20.000,00	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2106758-13.2016.8.26.0000	SP	2017	PA	PJ	Sim	R$ 2.000,00/dia	Sim	Não	Sim	Art. 15	Sim	Não	Sim	NI	NI
AP 1078660-60.2015.8.26.0100	SP	2017	PC	PA	Não	-	Não	Não	Sim	Art. 10, §1º	Não	Sim	Não	Não	Sim
AI 2062855-88.2017.8.26.0000	SP	2017	PC	PA	Não	-	Não	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2062855-88.2017.8.26.0000	SP	2017	PC	PA	Não	-	Sim	Não	Sim	Arts 5º, V, VII e VIII; e 15	Não	Sim	Não	Não	Sim
AI 2225928-76.2016.8.26.0000	SP	2017	PC	PJ	Sim	Diária - R$500,00 a R$100.000,00	Sim	Não	Sim	Arts. 5º, V, VII e VIII; e 15	Não	Sim	Não	Não	Sim
AI 2203488-86.2016.8.26.0000	SP	2017	PA	PJ	Sim	Diária - R$500,00 a R$5.000,00	Sim	Sim	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2072869-68.2016.8.26.0000	SP	2017	PA	PJ	Sim	Diário - R$ 1.000,00	Sim	Não	Sim	Arts. 5º, inc. VIII, 6 e 15	Não	Sim	Sim	Não	Sim

Legenda
PA = provedor de aplicação
PC = provedor de conexão
PJ = pessoa jurídica que Não PA e PC
PN = pessoa natural
NI = Não identificável

Banco de Dados 02

Embargo	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Reforma da decisão agravada	Argumentação estritamente processual
ED 2168151-36.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2105786-43.2016.8.26.0000/50000	SP	2.016	PJ	PN	NI	Sim
ED 2107751-27.2014.8.26.0000/50000	SP	2.014	PJ	PA	Não	Sim
ED 2216048-60.2016.8.26.0000/50001	SP	2.017	PN	PA	Não	Sim
ED 0620437-78.2017.8.06.0000/50000	CE	2.017	PC	PJ	Não	Sim
ED 2250400-78.2015.8.26.0000/50000	SP	2.015	PA	PJ	Não	Não
ED 2228882-32.2015.8.26.0000/50001	SP	2.016	PA	PA	Não	Sim
ED 2081265-34.2016.8.26.0000/5000	SP	2.016	PJ	PJ	Não	Sim
ED 2108074-61.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2090609-73.2015.8.26.0000/50000	SP	2.015	PA	PA	NI	Sim
ED 2142453-62.2015.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2107751-27. 2014.8.26.0000/50000	SP	2.014	PA	PA	NI	Sim
ED 2087441-29.2016.8.26.0000/50000	SP	2.017	PN	PA	Não	Sim
ED 2139037-52.2016.8.26.0000/50000	SP	2.017	PA	PJ	Sim	Sim
ED 2039490-39.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Não
ED 2039490-39.2016.8.26.0000/50001	SP	2.016	PA	PJ	Não	Sim
ED 2039490-39.2016.8.26.0000/50002	SP	2.016	PA	PJ	Não	Sim
ED 2125513-85.2016.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2206954-25.2015.8.26.0000/50000	SP	2.016	PA	PJ	Não	Sim
ED 2258906-43.2015.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2106303-48.2016.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2131118-46.2015.8.26.0000/50000	SP	2.015	PN	PA	NI	Sim
ED 2149601-90.2016.8.26.0000/50000	SP	2.017	PA	PC	NI	Sim
ED 2040105-29.2016.8.26.0000 /50000	SP	2.016	PJ	PA	Não	Sim
ED 2120450-79.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2203864-09.2015.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2150710-76.2015.8.26.0000/50000	SP	2.016	PC	PA	Não	Não
ED 2078865-47.2016.8.26.0000/50001	SP	2.017	PN	PA	Não	Não
ED 2106771-12.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2064240-08.2016.8.26.0000/50000	SP	2.016	PC	PA	Sim	Não
ED 2027881-59.2016.8.26.0000/50000	SP	2.016	PC	PA	Não	Não
ED 2172692-49.2015.8.26.0000/50000	SP	2.015	PJ	PA	Não	Não
ED 2203488-86.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2057480-77.2015.8.26.0000/50000	SP	2.015	PA	PJ	Sim	Não
ED 2158001-30.2015.8.26.0000/50001	SP	2.016	PN	PA	Não	SIm
ED 2227540-83.2015.8.26.0000/50000	SP	2.016	PA	PJ	Não	Sim
ED 2012094-24.2015.8.26.0000/50000	SP	2.015	PC	PA	Não	Sim
ED 2090609-73.2015.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2172692-49.2015.8.26.0000/50000	SP	2.015	PJ	PA	Não	Sim
ED 2189710-83.2015.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2219.128-03.2014.8.26.0000/50000	SP	2015	PJ	PA	Não	Sim
ED 2225114-64.2016.8.26.0000/50000	SP	2017	PN	PA	Não	Sim
ED 2083730-16.2016.8.26.0000/50000	SP	2016	PJ	PA	Não	Sim
ED 2252527-86.2015.8.26.0000/50000	SP	2016	PJ	PA	Não	Não
ED 1055250-07.2014.8.26.0100/50000	SP	2016	PN	PA	Não	Sim

Legenda
PA = provedor de aplicação PC = provedor de conexão PJ = pessoa jurídica que Não PA e PC PN = pessoa natural NI = Não identificável