REVISTA
CADERNO
VIRTUAL

Tema Geral "Atualidades do Direito e da Gestão Pública Contemporânea"

A RESPONSABILIDADE DO PROVEDOR DE APLICAÇÃO PELO ARMAZENAMENTO E FORNECIMENTO DA PORTA DE ORIGEM DO ENDEREÇO *IP,* SOB A ÓTICA DO MARCO CIVIL DA INTERNET

THE RESPONSIBILITY OF THE INTERNET APPLICATION PROVIDER FOR THE STORAGE AND SUPPLY OF THE IP ADDRESS PORT NUMBER FROM THE PERSPECTIVE OF BRAZILIAN CIVIL RIGHTS FRAMEWORK FOR THE INTERNET

Barbara Fernanda Ferreira Yandra[1]
Aluna do Curso de Graduação em Direito do
Instituto Brasiliense de Direito Público

Resumo: O presente artigo de iniciação científica tem por objetivo analisar em que medida o não fornecimento e armazenamento dos dados referentes à porta de origem dos registros de IP pelos provedores de aplicação violaria o disposto no Marco Civil da Internet. Buscou-se examinar se os provedores de aplicação são responsáveis pela guarda de dados adicionais ao endereço IP, que possibilitem a identificação inequívoca dos indivíduos na rede, mesmo após a inserção de políticas de compartilhamento. Para tanto, foi necessário recorrer ao método de pesquisa bibliográfica, a partir da revisão de literatura de textos jurídicos e não jurídicos. Analisando-se as disposições do Marco Civil da Internet, a recente Lei Geral de Proteção de Dados Pessoais e os entendimentos jurisprudenciais fixados sobre o tema, bem como o diagnóstico técnico proposto pela Agência Nacional de Telecomunicações. Assim, partindo de todo este aporte teórico chegamos a conclusão, em uma análise sistemática do Marco Civil da Internet, que os provedores de aplicação deveriam preservar as portas de acesso, juntamente aos provedores de conexão, com o propósito de garantir a privacidade dos usuários, por não permitir o controle total dos dados de navegação pelo provedor de conexão, e a identificação inequívoca dos indivíduos que se conectam à rede. Porém, responsabilizar os provedores de aplicação baseado em um cenário ideal pode colocar em risco a segurança jurídica, bem como tornar inacessível a internet para provedores de pequeno porte, sem condições de arcar com o ônus de tal armazenamento. Dessa forma, propõe-se uma resposta proporcional, a contemplar os aspectos técnicos, jurídicos e econômicos, caminhando por novas possibilidades.

[1] http://orcid.org/0000-0003-4350-9707

Palavras-chaves: Portas de origem. Endereço IP. Marco Civil da Internet. Privacidade. Anonimato.

Abstract: This article aims to analyze the extent to which the non-provision and storage by the internet application provider of the IP address port number could violate the Brazilian Civil Rights Framework for the Internet. We sought to investigate whether it would be the responsibility of the internet application providers to store data additional to the IP address that would allow the unambiguous identification of the individuals in the network. Therefore, it was necessary to use the method of bibliographic research, based on a legal and non-legal texts. In order to investigate the provisions contained in the Brazilian Civil Rights Framework for the Internet, some of the established jurisprudential understandings on the subject, as well as the proposed technical analysis by the National Telecommunications Agency and, lastly, a brief analysis of the recent General Law on Protection of Personal Data. Thus, starting from such premises we conclude that the internet application provider should store the port number, in order to guarantee the privacy of the users, by not allowing the connection provider to have total control of the data, while at the same time curbing virtual anonymity, by unequivocally identifying individuals who connect to the network. But blaming application providers based on an ideal scenario can compromise legal security as well as make the Internet inaccessible to small internet providers who could not afford the burden of such storage. In this way, a proportional response is proposed, considering the technical, legal and economic aspects, going through other possibilities.

Keywords: Port number. IP address. Brazilian Civil Rights Framework for the Internet. Privacy. Anonymity.

INTRODUÇÃO

Com o advento das novas tecnologias e, consequentemente, o crescimento exponencial do número de usuários conectados à *internet*, a atual arquitetura de rede não foi capaz de suportar o seu "superpovoamento".

Nesse cenário, enquanto se buscavam novas políticas de gerenciamento dessa rede "superpovoada", foi necessário a utilização de uma

solução transitória para a sua estruturação, a saber, o compartilhamento de IPs públicos.

Apesar dessa resposta provisória possibilitar o acesso de todos à *internet*, a identificação dos usuários, os quais não mais se identificam apenas pelo número do endereço IP, acabou ficando comprometida, haja vista o compartilhamento de tal endereço entre diversos usuários.

Se a própria estrutura da rede não conseguiu acompanhar a sua evolução, a produção legislativa padeceu do mesmo sintoma. O Marco Civil da Internet não previu a transição de protocolos IP e, consequentemente, a inserção de plataformas de compartilhamento, a qual identifica os usuários pela porta de origem[2] e não somente pelo registro de IP.

Assim, a entrada cada vez maior de usuários trouxe, em contrapartida, o ônus da regulação da rede "superpovoada". Quando ajuizadas ações requerendo a identificação de usuários que supostamente cometeram algum tipo de ilícito na rede, passou-se a questionar em algumas demandas a insuficiência de dados fornecidos pelos provedores de aplicação, sendo necessário além do previsto no Marco Civil da Internet, o fornecimento das portas de origem dos endereços IP. Em diversos casos, atualmente, a identificação não é possível, frustrando investigações penais e a reparação de diversas vítimas.

Salienta-se aqui a existência de certo tipo de consenso doutrinário e jurisprudencial, pelo qual os provedores de conexão devem armazenar as portas de acesso, uma vez que eles operacionalizam o compartilhamento de IPs públicos. Por isso, foi proposto averiguar a responsabilidade do provedor de aplicação no fornecimento dessas portas, sob a perspectiva do Marco Civil da Internet, além da análise de estudos técnicos e entendimentos jurisprudenciais.

Para tanto, utilizamos como premissas princípios fundamentais do Marco Civil, como a vedação ao anonimato e a proteção da privacidade, a fim de se realizar uma leitura contextual da norma, apta a chegar a uma conclusão adequada sobre a proteção de dados e a guarda de registros.

[2] Sequência numérica adicional utilizada em conjunto com número IP para identificar a localização de dispositivos conectados à *internet*.

Insta ressaltar que apesar de existir nova regulamentação quanto à proteção de dados pessoais, nos concentramos no Marco Civil da Internet, dado que o presente trabalho busca analisar os requisitos para fornecimento dos registros de acesso e conexão. A Lei geral de Proteção de Dados, por sua vez, preocupa-se primordialmente com a coleta de dados não obrigatórios para o acesso à rede, por isso não dispõe sobre a guarda obrigatória de registros de acesso e aplicação, continuando o regulado pelo Marco.

Assim, partindo dessa investigação bibliográfica, buscamos averiguar se a responsabilidade pelo armazenamento e disponibilização desses dados é apenas dos provedores de conexão ou também dos provedores de aplicação.

1 A GUARDA DE REGISTROS NO MARCO CIVIL DA INTERNET

Antes de adentrarmos efetivamente no problema central desse trabalho, precisamos, em primeiro lugar, compreender a lógica interna do Marco Civil da Internet[3] - MCI - quanto à guarda de registros de acesso e conexão[4] pelos provedores de *internet*[5].

O Marco Civil ao instituir a guarda de registros primou por dois aspectos essenciais a governabilidade da rede, quais sejam: (i) a vedação ao anonimato e (ii) a privacidade dos dados dos usuários.

Portanto, passemos a investigar tais premissas.

1.1 A LIBERDADE DE EXPRESSÃO E A VEDAÇÃO AO ANONIMATO NOS AMBIENTES VIRTUAIS

[3] BRASIL. *Marco Civil da Internet*. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: nov. 2018.

[4] Conceitos a serem explanados em tópico pertinente: *1.2 A privacidade e a proteção de dados pessoais*.

[5] Os provedores de *internet* podem ser divididos em provedores de aplicação e conexão. De acordo com o Marco Civil da Internet, o provedor de conexão é uma categoria que corresponde ao provedor de acesso, em geral as empresas de telecomunicação. O provedor de aplicação alcança os provedores de correio eletrônico, de hospedagem e de conteúdo, ou seja, os responsáveis pelas páginas da internet.

A Constituição Federal de 1988[6] elegeu a liberdade de expressão - vedado o anonimato - como um dos nossos maiores fundamentos constitucionais. O artigo 5º, inciso IV, expressamente estabelece que "é livre a manifestação do pensamento, sendo vedado o anonimato" e, o inciso IX, "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença".

O texto constitucional passou a outorgar aos indivíduos o direito de expor as suas ideias e os seus pensamentos, sem o crivo prévio ou interesse do Estado. Isto é,

> por liberdade de pensamento e de manifestação entendemos a tutela (proteção) constitucional a toda mensagem passível de comunicação, assim como toda opinião, convicção, comentário, avaliação ou julgamento sobre qualquer temática, seja essa relevante ou não aos olhos do interesse público, ou mesmo dotada - ou não - de valor[7].

Conforme Daniel Sarmento, "a liberdade de expressão permite que a vontade coletiva seja formada através do confronto livre de ideias, em que todos os grupos e cidadãos devem poder participar, seja para exprimir seus pontos de vista, seja para ouvir os expostos por seus pares[8]", haja vista o desenvolvimento de um estado democrático de participação popular[9].

---

[6] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: jul. 2018.

[7] FERNANDES, Bernardo Gonçalves. *Curso de Direito Constitucional*. 9 ed. Salvador: Jus podivm, 2017, p. 354.

[8] SARMENTO, Daniel. A liberdade de expressão e o problema do "Hate Speech". *In:* SARMENTO, Daniel. *Livres e iguais*: estudos de Direito Constitucional. Rio de Janeiro: Lumen Juris, 2006, p. 67.

[9] Cf. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 9 ed. São Paulo: Saraiva, 2014, p. 264.

Se a Constituição de 1988 já conferiu vasto suporte jurídico para o exercício de ampla liberdade de manifestação, com o surgimento das novas tecnologias de comunicação, ficou ainda mais fácil de expressarmos nossas ideias e opiniões. Pois, a *internet* possibilitou as pessoas, mesmo estando em locais diferentes, a conexão direta umas às outras, facilitando consideravelmente a nossa comunicação e o nosso acesso à informação.

No entanto, da mesma forma que as novas tecnologias promovem o exercício da liberdade de expressão, elas acabam, muitas vezes, oportunizando o desenvolvimento de um grande campo de batalha, político e social, em razão dos indivíduos se sentirem mais livres e protegidos pela rede em virtude da falsa crença no anonimato virtual, na medida em que não precisam mais expor seus rostos, sendo traduzidos operacionalmente como números na *web*.

O Marco Civil da Internet, principal fonte normativa para a regulação dos ambientes virtuais, no artigo 2º, *caput*, estabelece como seu fundamento o respeito à liberdade de expressão. Todavia, conforme dispõe a Constituição brasileira, apesar de a liberdade de expressão ser uma garantia fundamental, não é absoluta, encontrando limites, além de outros fundamentos[10], na vedação ao anonimato. Em última análise, todos estão livres para manifestar as suas ideias e opiniões, desde que sejam identificáveis.

O princípio da vedação ao anonimato cumpre dois objetivos. O primeiro está relacionado ao exercício do direito de resposta, assegurado pelo artigo 5º, inciso V[11], da Constituição, visto que para o efetivo exercício deste direito é necessário identificar quem proferiu a ofensa. O segundo se dá em virtude da necessidade de identificar os responsáveis por excessos no uso da liberdade de expressão, sendo devidamente responsabilizados pela violação de direitos de terceiros, como a privacidade, a honra e a imagem. Nesse sentido,

> para a corrente majoritária de viés axiológico, a liberdade de manifestação é limitada por outros direitos e garantias fundamentais como a vida, a igualdade, a integridade física, a liberdade de locomoção. Assim

[10] A exemplo da vedação a discursos de ódio e da proteção à intimidade.

[11] É assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem.

> sendo, embora haja liberdade de manifestação, essa não pode ser usada para manifestações que venham a desenvolver atividades ou práticas ilícitas (antissemitismo, apologia ao crime e etc).
>
> Por isso mesmo, o texto constitucional consagra a liberdade de pensamento, mas veda o anonimato, uma vez que é por meio do conhecimento da autoria que se faz possível a utilização do direito de resposta, proporcional ao agravo, bem como o pleito judicial por indenização por danos materiais e morais que atinjam a imagem (art. 5°, IV da CR/88) ou, até mesmo, ações penais para as tipificações dos crimes contra a honra. O direito de resposta pode ser definido como uma reação ao uso indevido dos meios de comunicação, tendo a perspectiva de um desagravo (art. 5°, V da CR/88)[12].

No âmbito digital, principalmente por ser mais atrativa a ideia do anonimato, surge-se a necessidade de uma regulação efetiva, de modo a garantir a identificação de todos os usuários da rede, evitando-se o anonimato.

Nas redes sociais ou em outros espaços digitais, as pessoas conseguem expressar mais facilmente a sua opinião. Geralmente, o ofensor cria coragem para manifestar os seus posicionamentos lesivos à honra e à integridade de outros indivíduos, se tornando cada vez mais necessário a imposição de limites a esses atos e a inibição de um sentimento de impunidade. Logo, a identificação dos usuários responsáveis pela manifestação se faz primordial.

Pontua-se aqui que, apesar de no âmbito internacional existirem teorias[13] a defender a não regulação da *internet*, em razão da rede estar supostamente em um ambiente "extraespacial" não sujeito a gerência do

[12] FERNANDES, Bernardo Gonçalves. *Curso de Direito Constitucional*. 9 ed. Salvador: Jus podivm, 2017, p. 427-428.

[13] Liberalismo cibernético. Cf. BARLOW, John Perry. *A Declaration of the Independence of Cyberspace*. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: ago. 2018.

Estado[14], a jurisprudência brasileira já fixou o entendimento de que "a internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer[15]".

A ideia de governança digital não deve ser entendida como um controle abusivo do Estado, mas como a defesa e a proteção de direitos assegurados constitucionalmente, os quais, sem a intervenção estatal, estariam provavelmente em um estado de vulnerabilidade.

Em perspectiva, da mesma forma que um indivíduo tem o direito de se manifestar, a sociedade, em contrapartida, tem a garantia de identificar quem proferiu o discurso, se este for ilícito[16]. Isso porque, tal discurso, quando externalizado, sai da instância particular do transmissor e passa a alcançar a instância pública, atingindo diretamente outras esferas jurídicas, como é o caso de ofensas à honra, à imagem e à privacidade.

Nesse sentido, embora a liberdade de expressão seja um direito de perfil majoritariamente negativo[17], o Estado não pode permitir aos indivíduos a exposição de sua opinião de forma absoluta, tendo por encargo coibir os excessos advindos dela, sem recorrer, entretanto, à censura.

Salienta-se que

> censura, no texto constitucional, significa ação governamental, de ordem prévia, centrada sobre o conteúdo de uma mensagem. Proibir a censura significa impedir que as ideias e fatos que o indivíduo pretende

[14] Cf. TSESIS, Alexander. *Hate in Cyberspace*: Regulating Hate Speech On the Internet. Loyola University Chicago, School of Law, 2001.

[15] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1117633/RO. Segunda Turma. Relator Ministro Herman Benjamin. Julgado em 26/03/2010. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=1117633&b=ACOR&p=true&l=10&i=5>. Acesso em: ago. 2018.

[16] Não há direito à identificação se o discurso for lícito, a fim de assegurar o pleno gozo da liberdade de expressão. A Constituição assegura a privacidade e o Código Civil permite o uso do pseudônimo, o que, na prática, impede a identificação do autor da mensagem se esta não extrapolar os limites da liberdade de expressão.

[17] Cf. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 9 ed. São Paulo: Saraiva, 2014.

> divulgar tenham de passar, antes, pela aprovação de um agente estatal. A proibição de censura não obsta, porém, a que o indivíduo assuma as consequências, não só cíveis, como igualmente penais, do que expressou[18].

Logo, como o Estado está impedido de exercer um controle prévio e preventivo sobre as manifestações de seus sujeitos de direito, este deve agir de forma, no mínimo, a assegurar a identificação e a responsabilização daqueles que abusam do seu direito.

A identificação do usuário é importante para a repressão da ação estatal ser posterior e não prévia. Um ambiente em que se permite o anonimato, em qualquer situação, pode servir de desculpa para a defesa do controle prévio do teor do discurso, sem ser oportunizada ampla defesa ou contraditório, ou seja, a promoção da censura. Vejamos,

> ao defendermos que a liberdade de expressão não é um direito absoluto, enfatizamos que as restrições à mesma não podem ser impostas de antemão, sob pena de configuração de censura, pois tal restrição prévia configuraria a tentativa de limitação da cidadania, de instauração de uma tutela, considerando-nos assim não livres para pensar e agir como quisermos, ou seja, não capazes de decidir sobre nosso próprio destino e de assumirmos responsabilidade pelo mesmo. Trata-se então de lidar com a pretensa dimensão estabilizadora do direito sem negar o espaço inovador e inesperado das ações políticas, ou seja, uma tentativa de trabalhar os limites da liberdade sem destruir a potencialidade criativa que a mesma possui[19].

[18] Cf. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 9 ed. São Paulo: Saraiva, 2014, p. 265.

[19] TORRES, Ana Paula Repolês. Pensando a liberdade de "expressão" com Hannah Arendt. *Prometeus Filosofia em Revista*. Sergipe, ano 5, nº. 10, 2012, p. 51.

De outra parte, a vedação ao anonimato não é um princípio capaz de alterar a "ordem espontânea[20]" desenvolvida no meio digital, mas apenas permitir a circulação dos conteúdos de forma a torná-los rastreáveis, pelas razões já expostas, e em nome da convivência social harmônica.

Deve-se ter em vista ainda a proteção dos direitos fundamentais ante à prática de atos desmesurados ou desproporcionais. Tais direitos possuem uma esfera de aplicabilidade positiva pelo Estado, "tem-se, inequivocamente, a identificação de um dever deste de tomar todas as providências necessárias para a realização ou concretização dos direitos fundamentais[21]".

Assim sendo, depreende-se que a liberdade de expressão é um direito fundamental, tanto para o desenvolvimento social quanto individual, porém não é um direito absoluto, devendo ser ainda regulado de acordo com as especificidades dos novos cenários digitais.

1.2 A PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

Do mesmo modo que se desenvolveu a liberdade de expressão, o direito à privacidade ganhou destaque em nosso texto constitucional. A Constituição, de natureza igual, consolidou tal previsão em seu artigo 5º, inciso X, ao dispor: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Na atualidade, ao passo que os avanços tecnológicos revolucionaram a forma como nos comunicamos, propiciaram a existência de maiores riscos à privacidade, trazendo novos desafios aos intérpretes da Carta da República. "O direito à privacidade é explicado como um direito que um indivíduo tem de se destacar (se separar) de um grupo, isolando-se da observação dele ou

[20] O desenvolvimento natural da rede, sem qualquer tipo de intervenção regulatória. Cf. VOLKMER, André; et. al. *A liberdade na era digital.* Série Pensamentos Liberais. Volume XV. Porto Alegre: Instituto de Estudos Empresariais, 2011. p. 183.

[21] MENDES, Gilmar Ferreira. *Direitos fundamentais e controle de constitucionalidade*: estudos de direito constitucional. 4 ed. São Paulo: Saraiva, 2012, p. 122

como, ainda, o direito ao controle das informações veiculadas sobre si mesmo[22]". Ademais,

> Uma questão importante é a referente à restrição ao direito de privacidade a partir do consentimento do próprio indivíduo, já que os direitos fundamentais, mesmo não sendo passíveis de renúncia plena, comportam formas de autolimitação. Se a restrição é feita espontaneamente, com o seu titular falando sobre sua intimidade como em uma entrevista, o caso é de mais fácil problematização. Todavia, um cuidado maior deve ser dispensado quando ocorre o chamado consentimento tácito na divulgação da matéria ou da imagem[23].

De tal maneira, o acesso gratuito à serviços na *internet* está intrinsecamente ligado à coleta tácita de dados e, por isso, requer atenção. Quando o usuário trafega na *web*, nas redes sociais, usa o *email*, automaticamente, acaba fornecendo dados pessoais. Nota-se que

> A utilização sempre mais ampla de dados pessoais para as mais variadas atividades identificação, classificação, autorização e tantas outras - faz com que esses dados se tornem elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores da Sociedade da Informação. Os dados pessoais acabam por identificar ou mesmo representar a pessoa em uma série de circunstâncias nas quais a sua presença física não é possível ou conveniente. São elementos centrais,

[22] FERNANDES, Bernardo Gonçalves. *Curso de Direito Constitucional*. 9 ed. Salvador: Jus podivm, 2017, p. 487.

[23] *Ibid*, p. 487.

portanto, da construção da identidade em nossa sociedade[24].

O uso cada vez mais frequente de dispositivos conectados à *internet* e, consequentemente, de usuários praticando inúmeras operações na rede, desde o acesso até a publicação de conteúdo, implica a coleta de mais dados e informações dos clientes pelas empresas gerenciadoras do meio ambiente digital.

O Marco Civil da Internet - MCI, nessa acepção, reconhece como princípio fundamental a proteção da privacidade e dos dados pessoais. Tal norma reproduziu o mandamento do texto constitucional sobre a proteção à privacidade em seu inciso I, artigo 7º[25], bem como estabeleceu na redação do seu artigo 3º, inciso VIII[26], a liberdade dos modelos de negócio promovidos na *internet* não conflitem com princípios como a proteção à privacidade e aos dados pessoais, dispostos nos incisos II e III[27] deste mesmo artigo.

A Lei Geral de Proteção de Dados Pessoais - LGPD[28], em seu artigo 2º, concebeu como fundamentos da proteção de dados pessoais: "I - o respeito à privacidade; (...) III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; (...)". Definiu ainda em seu artigo 10, parágrafo 1º: "quando o tratamento for baseado no legítimo interesse do controlador, somente os

[24] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães. *Direito privado e Internet*. São Paulo: Editora Atlas, 2014, p. 61.

[25] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; (...).

[26] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei; (...)".

[27] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; (...)".

[28] BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: nov. 2018.

dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados".

Isto posto, a fim de proteger a vida privada dos usuários da rede, o MCI instituiu diferenças de obrigações relativas à guarda de dados entre as suas principais categorias de agentes econômicos, a saber, os provedores de conexão[29] e de aplicação[30], vez que "a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade[31]".

Nessa via, foram estabelecidas duas categorias de dados a serem armazenados obrigatoriamente, a saber: (i) os registros de conexão, de acordo com o artigo 5º, inciso VI, do MCI, são compreendidos pelo "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"; e (ii) os registros de acesso à aplicação, conforme o artigo 5º, inciso VIII, do MCI, podem ser entendidos pelo "conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP"[32].

Por este ângulo, foi estabelecido ainda no artigo 14 do MCI que aos provedores de conexão é vedado armazenar dados de registro de acesso a aplicações de internet. O tipo de dado a ser armazenado pelo agente econômico é limitado ao tipo de serviço prestado, de modo a impossibilitar a um só agente controle total e irrestrito dos dados que circulam na rede, salvaguardando a privacidade e os dados pessoais do usuário.

O MCI inovou nesse aspecto, pois

[29] De acordo com o Marco Civil da Internet, o provedor de conexão é uma categoria que corresponde ao provedor de acesso, em geral as empresas de telecomunicação.

[30] O provedor de aplicação da internet alcança os provedores de correio eletrônico, de hospedagem e de conteúdo, ou seja, os responsáveis pelas páginas da internet.

[31] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães. *Direito privado e Internet*. São Paulo: Editora Atlas, 2014, p. 63.

[32] IP (Internet Protocol) é uma sequência numérica usada para identificar um dispositivo conectado à internet, representado atualmente por conjunto de quatro números de até três dígitos (e.g. 192.168.1.100)

> Até a aprovação da lei, os provedores de conexão à internet em banda larga podiam guardar os registros de conexão e de navegação por prazo indeterminado, mas não havia obrigatoriedade. O provedor de conexão podia coletar não só quando e por quanto tempo o usuário ficou conectado (registro de conexão) mas também quais sítios haviam sido acessados.
>
> Na nova lei, os provedores de conexão à internet deverão guardar os registros de conexão por 1 ano e não poderão guardar os registros de navegação do usuário.[33]

Observemos que o armazenamento e a manipulação em massa de dados pessoais, em um mesmo banco de dados[34], geram constantemente informações preciosas aos novos modelos negociais, tendo em vista que "a informação pessoal é o elemento fundamental em uma série de novos modelos de negócios típicos da Sociedade da Informação[35]".

Nesse seguimento, a depender do cruzamento dos dados nos bancos de dados empresariais, pode-se extrair inúmeras informações sobre indivíduos, de maneira a diminuir significativamente a sua privacidade, "a qual, em grande parte, pode ser entendida como o direito de alguém controlar e estabelecer limites sobre o fluxo de informações sobre si próprio[36]".

Por isso, é importante definir limites aos dados coletado por aqueles que empresariam a rede, a fim de estipular quais informações pessoais

---

[33] NAZARENO, CLAUDIO. *Marco civil da internet*: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

[34] É o conjunto de dados estruturados de modo que se possa extrair dele informações específicas. A Lei Geral de Proteção de Dados, Lei nº 13.709/18, prevê em seu artigo 5º, inciso IV que banco de dados é o "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico".

[35] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães. *Direito privado e Internet*. São Paulo: Editora Atlas, 2014, p. 62.

[36] SANKIEVICZ, Alexandre. *Direito ao esquecimento e sobre fatos e circunstâncias dos trópicos que devemos especialmente ponderar*. Cadernos Aslegis, n. 48. Brasília: Aslegis, 2015, p. 88.

poderão ser acessadas por estes. O controle sobre como os dados são coletados e manipulados é fundamental, pois

> Os bancos de dados que contém dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos sobre as informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo[37].

Note-se ainda,

> O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento[38].

[37] DONEDA, op. cit., p. 66.

[38] SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 37 ed. São Paulo: Malheiros Editores, 2014, p. 211-212.

É importante esclarecer que os registros armazenados pelos provedores de conexão e aplicação, os quais, a princípio, têm a capacidade de identificar o usuário na rede, devem ser tratados como dados pessoais, pois conceituamos a informação pessoal, em sentido *lato*, como capaz de identificar alguém, revelando algum elemento pessoal objetivo.

De acordo com a Lei 13.709/18, LGPD, em seu artigo 5º, inciso I, dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável[39]".

Por outro lado, encontramos concepções mais técnicas em que o dado, na verdade, é uma forma mais primitiva da informação, isto é, apenas a potencialidade de se transformar em informação[40].

Nesse sentido, os registros de IP, armazenados pelos provedores de *internet*, são considerados dados pessoais, pois deles se é capaz de se extrair uma informação pessoal, mesmo representando apenas uma sequência numérica, a qual por si só não possui um conteúdo pessoal, e sim uma potencialidade ou uma "chave de acesso" ao conteúdo informacional pretendido.

O Tribunal de Justiça da União Européia[41], por exemplo, entendeu, em sede de precedente, que endereços de IP são dados pessoais, pois possibilitam a identificação do usuário.

De outro modo, além da quebra da privacidade, a guarda pelos provedores de conexão dos registros de aplicação poderia inclusive comprometer a neutralidade de rede, regulada pelo artigo 9º[42] do MCI,

[39] Anteriormente, o Decreto nº 8.771, definia em seu artigo 14, inciso I, como dado pessoal o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".

[40] DONEDA, Danilo. *O direito fundamental à proteção de dados pessoais*. *In*: MARTINS, Guilherme Magalhães. Direito privado e Internet. São Paulo: Editora Atlas, 2014, p. 63.

[41] Cour de justice de l'Union européenne. *Patrick Breyer v. Bundesrepublik Deutschland*: Case C-582/14. 19 Outubro de 2016. Disponível em: <http://bit.ly/2gsdqaf>. Acesso em: 10 set. 2018.

[42] Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

"entendida de forma simplificada como a necessidade de que a rede não favoreça uma aplicação sobre a outra[43]".

Os provedores de conexão a partir do armazenamento dos registros de aplicação poderiam identificar qual o conteúdo estaria sendo mais acessado pelo usuário e estabelecer por acordos informais ordens de preferência dos conteúdos a serem enviados, prejudicando a proteção saudável do meio ambiente digital[44]. Assim,

> Como se percebe, contamos, agora, com um conjunto de disposições legais que busca proteger, com razoável detalhamento, as operações de coleta e armazenamento de dados, os registros de conexão, bem como os conteúdos acessados, baixados ou transmitidos. Cabe destacar como ponto positivo entre as medidas adotadas, a expressa exigência de autorização judicial para qualquer forma de acesso a esses dados, preservando-se, com isso, a privacidade do usuário[45].

Em linhas gerais, por todo o exposto, vemos que o "Direito Digital tem o desafio de equilibrar a difícil relação existente entre interesse comercial, privacidade, responsabilidade e anonimato, gerada pelos novos veículos de comunicação[46]".

---

[43] COLNAGO, Cláudio de Oliveira Santos. Provedores de conexão e guarda de registros de acesso a aplicações de internet: o art. 14 do marco civil no contexto do dever fundamental de preservação do meio ambiente digital. In: LEITE, George Salomão; LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014, p. 767.

[44] Cf. *Ibid*, p. 767.

[45] MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; P. COELHO, Alexandre Zavaglia. *Direito, inovação e tecnologia*. Vol. 1. São Paulo: Saraiva, 2015, p. 243.

[46] PINHEIRO, Patrícia Peck. *Direito digital*. 2 ed. São Paulo: Saraiva, 2007, p. 43.

2 A TRANSIÇÃO DO PROTOCOLO IPV4 PARA IPV6 E A INSUFICIÊNCIA DAS DISPOSIÇÕES SOBRE A GUARDA DE REGISTROS ESTABELECIDAS NO MCI

Por ser de difícil previsão o número de indivíduos[47] que teriam hoje acesso à rede, políticas públicas de tráfego e registro dos novos usuários não foram implementadas antecipadamente.

Atualmente, o protocolo de registro dos endereços IPs[48] - IPv4 - não é suficiente para atender a todos os usuários. A versão 4 do protocolo IP "mostrou-se muito robusta, e de fácil implantação e interoperabilidade, entretanto, seu projeto original não previu alguns aspectos como: – O crescimento das redes e um possível esgotamento dos endereços IP"[49].

A versão 4 do IP[50] tornou-se obsoleta, de modo a demandar a implementação da versão 6 - IPv6[51]. Enquanto o IPv4 possui 32 bits, possibilitando a combinação de 4 bilhões de endereços, o IPv6, por sua vez, com 128 bits, pode fornecer 340 undecilhões de combinações.

Devemos lembrar ainda que

[47] Durante o desenvolvimento do IPv6, o número de usuários conectados à Internet saltou de 30.000.000, em 2000, para aproximadamente 732.000.000, em 2010. Cf. SANTOS, Rodrigo Regis dos; et. al. *Curso IPv6 básico*. São Paulo: Núcleo de Informação e Coordenação do ponto BR, 2010. Disponível em: <http://ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf>. Acesso em: nov. 2018.

[48] Versão atual do protocolo IP, o qual irá permitir o número de combinações possíveis para a utilização de diferentes endereços IPs.

[49] SANTOS, op. cit., p. 7.

[50] Utilizada desde o início da internet comercial, década de 1990, composto por quatro sequências de três dígitos (8 bits), o campo do cabeçalho reservado para o endereçamento possui 32 bits (4x8=32 bits), prevê um total de 4.294.967.296 (2 elevado a 32) endereços distintos. Sendo que os endereços IPv4 foram distribuídos de forma irregular entre as macrorregiões do globo. Os IPs delegados ao órgão responsável pela macrorregião da América Latina e do Caribe - LACNIC - ficaram escassos em 2011, promovendo-se políticas de alocação de IP para esgotamento suave. Cf. SANTOS, op. cit.

[51] Os endereços IPs desse protocolo utilizam oito sequências de quatro dígitos hexadecimais (16 bits) que permitem a combinação de uma quantidade exorbitante de endereços (8x16=128 bits). Com 128 bits é possível a combinação de 340.282.366.920.938.463.463.374.607.431.768.211.456 de endereços (2 elevado a 128). Cf. SANTOS, op. cit.

> O IPv4 e o IPv6 não são diretamente compatíveis, já que o IPv6 não foi projetado para ser uma extensão, ou complemento, do IPv4, mas sim, um substituto que resolve o problema do esgotamento de endereços. Embora não interoperem, os protocolos podem funcionar em paralelo nos mesmos equipamentos, possibilitando realizar a transição de forma gradual[52].

Entretanto, durante esta transição entre os protocolos, considerando não ser possível implementar o IPv6 antes da escassez do IPv4, foi necessário estabelecer como solução transitória o compartilhamento entre vários usuários de um mesmo IP público, em sua versão 4.

A partir deste compartilhamento foi preciso adotar outro critério, além do endereço IP, para possibilitar o compartilhamento e diferenciar os usuários na rede. Optou-se por diferenciá-los de acordo com a sua porta de origem[53], denominada posteriormente pelos juristas como "porta lógica de origem[54]".

A porta de origem é o que, neste momento, irá identificar inequivocamente o usuário na rede, caso esteja compartilhando o seu IP público no protocolo IPv4, porque pelo IP extrai-se apenas a informação de quais são os usuários a compartilhar aquele endereço, só sendo possível sua individualização pela porta de acesso. Dessarte,

> Ocorre que os endereços IP, cuja função nas investigações sempre se prestou à identificação da localização do terminal de onde partiu a conexão, não mais poderão ser considerados como fonte segura para fins de identificação de autoria. Todos que se conectam à internet recebem necessariamente um endereço IP, único para determinada data e horário. Também durante

[52] *Transição*. Disponível em: <http://ipv6.br/post/transicao/>. Acesso em: 03 nov. 2018.

[53] Sequência numérica adicional utilizada em conjunto com número IP para identificar a localização de dispositivos conectados à *internet*.

[54] O termo "porta lógica" é utilizado no campo da eletrônica como um dispositivo que opera logicamente um circuito, enquanto a "porta", utilizada no compartilhamento dos endereços IPs, é o número que identifica um terminal que se comunica com outros na rede. Assim há um equívoco na utilização da expressão "porta lógica de origem".

> a navegação na internet, o número do IP é registrado por provedores de aplicações. No entanto, os endereços IP que historicamente foram concebidos para uso individual, enfrentam hoje um cenário de esgotamento, de modo que vêm sendo compartilhados entre pessoas ou organizações distintas, de forma simultânea. Esta realidade já se faz presente hoje também em redes compartilhadas dentro de empresas ou condomínios, com estabelecimento de um IP e NAT, ou ainda, em redes abertas de wi-fi. Assim, enquanto o sistema estiver calcado no atual protocolo de internet chamado IPV4 e não houver a substituição pela versão IPV6, continuará a ocorrer o compartilhamento de IP e, por conseguinte, a impossibilidade de identificação de autorias com base em tal informação[55].

A Europol[56], no relatório "*The Internet Organised Crime Threat Assessment*" – IOCTA[57], entendeu que o uso de IPs compartilhados significava um importante problema de governança da internet, especialmente quando relacionado aos crimes cibernéticos.

Segundo o relatório, é inviável tentar solucionar o problema aguardando a transição completa para o IPv6, pois se trata de um procedimento de longa duração ante a falta de incentivos comerciais e a necessidade de inúmeros investimentos na estrutura do IPv4.

---

[55] BRAUN, Caroline; MARTINS, Rafael D'Enrrico; ARTESE, Gustavo (coord.). *O Marco Civil da Internet, a guarda e fornecimento de registros por provedores de conexão e de acesso a aplicações de internet*: limites legais e questões probatórias relevantes in Marco Civil da Internet – Análise Jurídica sob uma Perspectiva Empresarial. São Paulo: Quartier Latin, 2015, p. 132.

[56] A "European Police Office" (Europol), é uma agência da União Européia - UE, sem poderes executivos, que busca promover a coordenação entre as polícias civis dos membros da UE. Seu foco de atuação está no combate a crimes internacionais como cibercrimes, terrorismo, lavagem de dinheiro, entre outros. Cf. EUROPOL. "About Europol". Disponível em:<http://bit.ly/2jWsUV8>. Acesso em: jun. 2018.

[57] EUROPOL. IOCTA 2016 - Internet Organised Crime Threat Assessment. Disponível em: <http://bit.ly/2fCum7o>. Acesso em: jun. 2018.

Na Austrália, de acordo com o "Telecommunications Act" exige-se adicionalmente o armazenamento da porta de acesso, a fim de assegurar o acesso aos dados relativos à origem de uma comunicação[58]. A regulação, porém, é feita pela esfera executiva.

Todavia, não há no Brasil uma regulação estatal consolidada sobre a coleta e o armazenamento das portas de acesso, necessárias à dinâmica atual como solução transitória ao processo de implementação do IPv6.

Como visto em capítulo anterior, o MCI estabeleceu regras de registro de dados, tanto para os provedores de conexão quanto de aplicação. O artigo 5º do MCI, o qual apresenta o conceito de registros de conexão e de acesso às aplicações, em seus incisos VI e VIII, respectivamente, afirma ser necessário apenas a guarda da data e hora de início e término de uma conexão ou de uma aplicação a partir de um endereço IP, não falando nada sobre as portas de origem.

Contudo, em virtude da acelerada evolução tecnológica, em contraposição ao lento processo legislativo e a obsolência das leis reguladoras do campo digital, parte da doutrina e dos tribunais brasileiros vem conferindo interpretação ampliativa ao artigo 5º do Marco Civil para consignar a obrigatoriedade do armazenamento da "porta lógica" pelos provedores, além das informações expressamente exigidas.

Nesse sentido,

> Havendo compartilhamento dos endereços IPv4 entre vários usuários e na ausência de informação da porta, não será possível identificar univocamente uma pessoa associada a uma conexão, deixando esse registro, ao menos formalmente, de ser uma informação pessoal, perdendo sua utilidade prática se individualmente considerado. (...) Por isso os conteúdos de informação

[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. Communications Access Co-ordinator. Publicado em julho de 2015. Disponível em: <http://m.tio.com.au/__data/assets/pdf_file/0005/188753/INDUSTRY-FAQs-V1.1-JULY-2015.pdf>. Acessado em: jul. 2018, p. 21.

> dos registros descritos nesses incisos têm caráter meramente exemplificativo e devem receber o complemento necessário para que o registro mantenha sua utilidade na identificação segura de uma pessoa ou terminal[59].

Do mesmo modo, o Tribunal de Justiça do Estado do Amazonas consignou na ementa do acórdão que

> 1. Ao exigir a identificação das "portas lógicas de origem" o juízo a quo não excedeu os limites do pedido, mas apenas adotou providência necessária à obtenção do resultado prático perseguido pela demandante. 2. A ordem de revelação da "portas lógicas de origem" consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP. 3. As "portas lógicas de origem" integram os "registros de acesso" cujo dever de guarda/exposição é consagrado pelo artigo 22 do Marco Civil da Internet (Lei n. 12.965/14). Interpretação contextualizada e voltada ao fim social da norma, em atenção ao artigo 5º da LINDB. 4. Fosse insuficiente, vale destacar que a Agência Nacional de Telecomunicações - ANATEL, em estudo pertinente ao tema, consignou que os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a "porta lógica de origem".[60]

---

[59] NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coordenadores). *Direito & Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo II. São Paulo: Quartier Latin, 2015, p. 179 a 180.

[60]BRASIL. Tribunal de Justiça do Amazonas. *Agravo de Instrumento nº 4004023-74.2016.8.04.0000*. 2ª Câmara Cível. Relator Maria do Perpétuo Socorro Guedes Moura. Publicado em 19.06.17. Disponível em:<https://consultasaj.tjam.jus.br/cposgcr/show.do?processo.foro=900&processo.codigo=P00002NQM0000&uuidCaptcha=sajcaptcha_30df6002199e4b2f90f5356bb0db3528#?cdDocumento=22>. Acesso em: set. 2018.

Neste julgado, atribui-se à finalidade da norma, qual seja, a identificação inequívoca do usuário, legitimidade para determinar o fornecimento de outros dados não previstos no dispositivo legal, na medida em que o comando normativo não possuiria mais força sem esta inclusão. Veja-se também fragmento do voto proferido pela 2ª Turma Cível do Tribunal de Justiça do Distrito Federal:

> Em que pese em um dos julgados ter se considerado como satisfatório o fornecimento do registro do número do IP dos computadores utilizados para cadastramento de contas na internet para a identificação dos usuários, necessário levar em consideração, conforme consignado na decisão agravada, que no atual estágio da tecnologia, tais dados não são suficientes para a identificação do usuário que cometeu os atos ilícitos narrados na inicial, de modo que é decorrência lógica do fornecimento dos números de IPs que o provedor de aplicações forneça igualmente as portas lógicas de conexão dos IPs, sob pena de inviabilizar a identificação daqueles que se utilizam da internet, com o anonimato, para fins de propagação de diversos ilícitos, sem que possam ser devidamente fiscalizados e até responsabilizados. Nesse sentido, transcrevo trechos do relatório final de atividades GT-IPv6 - Grupo de Trabalho para implantação do protocolo IPVersão 6 nas redes das Prestadoras de Serviços de Telecomunicações realizado pela ANATEL em dezembro de 2014, que dispõe que a única forma das prestadoras fornecerem o nome do usuário que faz uso de um IP compartilhado em um determinado instante seria com a informação da "porta lógica de origem da conexão" que estava sendo utilizada durante a conexão. Dessa forma, os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a "porta lógica de origem", sendo que somente com base nessa informação que as identificações

> judiciais para fins de quebra de sigilo e interceptação legal continuarão sendo possíveis de serem realizadas de forma unívoca[61].

Nessa via, considera-se ainda a capacidade técnica dos provedores em armazenar os dados adicionais requeridos para a precisa localização do usuário. Confira-se o seguinte julgado:

> Cinge-se a questão jurídica à possibilidade de a agravante, provedora de aplicação, fornecer os dados relativos à "porta lógica de origem".
>
> Conquanto a agravante impute a responsabilidade pelo fornecimento e armazenamento de tal dado ao provedor de conexão, não comprova, como lhe competia, a impossibilidade técnica de fazê-lo.
>
> Por outro lado, a Lei nº 12.965/14, que regula o Marco Civil da Internet, não traz limitação de responsabilidade quanto ao fornecimento do referido dado.
>
> Não é razoável supor que uma empresa do porte da agravante não possua mecanismo para rastreamento de seus usuários, o que aliás, iria de encontro ao objetivo legislativo regulamentador da matéria, o qual, ao atribuir à agravante, provedora de aplicação, a responsabilidade pelo "conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (Lei nº 12.965/14, art. 5º, inc. VIII), buscou a individualização do usuário do IP responsável por veicular as informações na internet.

[61] BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. *Agravo de Instrumento nº 07086665020188070000.* 2ª Turma Cível. Relator Cesar Loyola. Publicado em 10/10/2018. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: nov. 2018

Em razão do avanço tecnológico (transição do IPv4 para o IPv6) houve a necessidade de compartilhamento do IP, razão pela qual os provedores de internet, incluindo a agravante, devem se acautelar para buscar a referida individualização que, no caso, ocorre por meio da porta lógica de origem.

Caso assim não se proceda, os usuários ficarão à mercê de ataques anônimos, situação que põe em xeque as garantias previstas na Carta Magna vigente.

Aliás, para evitar o anonimato, a ANATEL, no relatório de implantação do novo protocolo IP "Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações" http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=325769.pdf), entendeu que "a única forma das prestadoras fornecerem o nome do usuário que faz uso de um IP compartilhado em um determinado instante seria com a informação da 'porta lógica de origem da conexão' que estava sendo utilizada durante a conexão. Dessa forma, os provedores de aplicação devem fornecer não somente o IP de origem utilizado para usufruto do serviço que ele presta, mas também a "porta lógica de origem".

Logo, a responsabilidade da agravante pelo fornecimento da porta lógica de origem é patente, não podendo se eximir da obrigação, sob a mera e cômoda alegação de inviabilidade técnica para o cumprimento da ordem[62].

[62] BRASIL. Tribunal de Justiça de São Paulo. *Agravo de Instrumento nº 2257879-25.2015.8.26.0000*. Relator J.L. Mônaco da Silva. 5ª Câmara de Direito Privado. Publicado em 14/03/2016. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=9264245&cdForo=0>. Acesso em: set. 2018.

Por outro lado, da mesma forma que a ampliação dos conceitos de registros de conexão e de aplicação, baseado na finalidade da norma, pode beneficiar os usuários, também pode ser um motivo para invasão da privacidade destes, pois os provedores guardariam mais dados para poderem se prevenir de eventuais responsabilizações.

Contudo, se os provedores cumprirem estritamente a finalidade da guarda de registro, dificilmente existiria uma invasão à privacidade das pessoas conectadas à rede. Nesse sentido, a Lei Geral de Proteção de Dados Pessoais, estabelece como princípio das atividades de tratamento de dados pessoais o da finalidade, conforme artigo 6º, inciso I[63], bem como da boa-fé no *caput*.

No mesmo ângulo, o decreto regulamentador do Marco Civil da Internet nº 8.771, prevê em seu artigo 13, algumas diretrizes aos provedores de conexão e de aplicações quanto ao armazenamento e ao tratamento de dados pessoais, afirmando no parágrafo 2º que "os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I - tão logo atingida a finalidade de seu uso".

Superado este óbice, pode-se ainda indagar se seria possível incluir tal exigência no comando normativo por um critério interpretativo, porquanto a inserção de nova obrigação implica na responsabilização dos provedores de internet, os quais não teriam condições de prever esta exigência, pautando-se por uma interpretação restritiva da norma. Pois, dispõe a Constituição Federal em seu artigo 5º, inciso II, que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Ou seja, "só a lei cria direitos e impõe obrigações positivas ou negativas[64]".

---

[63] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[64] SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 37 ed. São Paulo: Malheiros Editores, 2014, p. 424.

No mesmo sentido: Tribunal de Justiça de São Paulo. Agravo de Instrumento n. 2183584-17.2015.8.26.0000, Des. Rel. Mauro Conti Machado, 9ª Câmara de Direito Privado, p. 15/12/2015.

Nessa linha, o Tribunal de Justiça de São Paulo, em seus recentes julgados, vem se manifestando no seguinte sentido:

> De acordo com o Marco Civil da Internet (Lei nº 12.965/2014), observa-se que, realmente, a lei não impõe aos provedores de aplicação o armazenamento dos registros referente à "porta lógica de origem", mas tão somente armazenar registros de acesso a aplicações de Internet consistentes no conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet, a partir de um determinado endereço IP (artigos 5°, inciso VIII, e 15).
>
> (...)
>
> Ademais, por se tratar de uma questão transitória, até o implemento total da rede "IPv6" no Brasil, cuida-se de matéria não expressamente regulada na Lei nº 12.965/2014, principalmente quanto à responsabilidade dos provedores de conexão e de aplicação pelo armazenamento e fornecimento de dados. Oportuna a transcrição de GIULIANO GIOVA que "a identificação de origem e autoria não poderá mais se basear apenas no endereço IP, será necessário preservar também registros sobre qual foi a porta de comunicação utilizada em cada acesso, elemento que diferenciará as conexões feitas por empresas ou pessoas diferentes que utilizam simultaneamente um mesmo endereço IP válido na Internet" (in "Marco Civil da Internet Análise Jurídica sob uma Perspectiva Empresarial", Coordenador GUSTAVO ARTESE, Ed. Quartier Latin, 2015, p. 132).
>
> Entretanto, embora recomendada a guarda de tais informações nesse período de transição de modelos, não há qualquer dispositivo legal a impor às agravadas a obrigação de coletar e armazenar os dados da "porta lógica de origem".
>
> Nesse sentido, diversos precedentes deste Egrégio Tribunal de Justiça em casos bastante semelhantes:

(...)[65]

O art. 15 da Lei n. 12.965/14 determina que o provedor de aplicações de internet que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos, deve manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses.

Por registros de acesso a aplicações de internet entende-se o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (art. 5º, VIII, da Lei n. 12.965/14).

No caso, verifica-se que a agravante se insurgiu quanto ao indeferimento do pedido de identificação das portas lógicas de acesso das conexões apontadas a fs. 31.

Sem razão, contudo.

Os dados relativos às portas lógicas de acesso devem ser obtidos junto ao provedor de conexão com a internet, que é o responsável pelo armazenamento das informações, sobretudo porque a Lei n. 12.965/14 não atribui expressamente tal responsabilidade aos provedores de aplicação.

A questão já foi decidida em inúmeros casos envolvendo o mesmo provedor de aplicações: AI.n. 2225928-76.2016.8.26.0000, rel. Des. Moreira Viegas, j.

[65] BRASIL. Tribunal de Justiça de São Paulo. *Agravo de Instrumento nº. 2064240-08.2016.8.26.0000*. Relator J.B. Paula Lima. 10ª Câmara de Direito Privado. Publicado em 19/12/2016. Disponível em: <https://esaj.tjsp.jus.br/cposg/search.do?conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=2064240-08.2016&foroNumeroUnificado=0000&dePesquisaNuUnificado=2064240-08.2016.8.26.0000&dePesquisa=&uuidCaptcha=#?cdDocumento=33>. Acesso em: set. 2018.

1º.2.2017, AI. n. 2225114-64.2016.8.26.0000, rel. Des. Grava Brazil, j. 23.1.2017, AI. n. 2251294-54.2015.8.26.0000, rel. Des. Miguel Brandi, j. 21.9.2016 e AI.n. 2027881-59.2016.8.26.0000, rel. Des. Elcio Trujillo, j. 28.6.2016.

Nessas condições, se os dados fornecidos pelo agravado são insuficientes para a correta identificação dos autores das postagens ofensivas, deverá a agravante requerer o fornecimento das informações relativas às portas lógicas de acesso junto ao respectivo provedor de conexão[66].

Por outro lado, a guarda das informações relativas aos dados pessoais do responsável pela criação do perfil e das alegadas ofensas vinculadas ao número de IP fornecido pela agravante, são de responsabilidade dos provedores de conexão à internet, por meio do registro de conexão, nos termos dos artigos 5º, V e VI c.c. art. 13, do Marco Civil da Internet. Através do número de IP fornecido pela agravante, é possível identificar a empresa provedora de acesso à internet, responsável pelos dados e informações relacionadas ao IP[67].

---

[66]BRASIL. Tribunal de Justiça de São Paulo. *Agravo de Instrumento nº. 2062855-88.2017.8.26.0000*. 4ª Câmara de Direito Privado. Relator Hamid Bdine. Publicado em 30/05/2017. Disponível em: <https://esaj.tjsp.jus.br/cposg/show.do?processo.codigo=RI003XPJR0000&conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=1070451-05.2015&foroNumeroUnificado=0100&dePesquisaNuUnificado=1070451-05.2015.8.26.0100&dePesquisa=&uuidCaptcha=#?cdDocumento=23>. Acesso em: set. 2018.

No mesmo sentido: Tribunal de Justiça de São Paulo. Agravo de Instrumento n° 2012094-24.2015.8.26.0000. Relator Egidio Giacoia. 3ª Câmara de Direito Privado. p. 28/04/2015. Tribunal de Justiça do Amazonas. Agravo de Instrumento n.º 4002988-45.2017.8.04.0000. 1ª Câmara Cível. Pub. 12/12/17. Relator Ernesto Anselmo Queiroz Chíxaro.

[67] BRASIL. Agravo de Instrumento 2018874-72.2018.8.26.0000. Relator Pedro de Alcântara da Silva Leme Filho. 8ª Câmara de Direito Privado. Data de publicação: 07/06/2018. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=11520452&cdForo=0&uuidCaptcha=sajcaptcha_548d15df36f14c759917da02c2d2958f&vlCaptcha=WnKQ&novoVlCaptcha=>. Acesso em: set. 2018.

Outrossim, o artigo 10, § 1º, do MCI prevê que

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

Sobre tal dispositivo há julgado do Tribunal de São Paulo, posicionando-se da seguinte forma:

> A Recorrente tem o dever de levar ao conhecimento do Magistrado todas as informações que possuir; se por al não detiver mais, que informe ao r. Juízo da impossibilidade, e o local de armazenamento dos dados, geralmente colocados no exterior. A desoneração, neste momento, de a Agravante apresentar a "porta lógica de origem" e número de telefone usado na conexão pode frustrar o escopo da lide[68].

Porém, em sentido inverso, e mais adequado:

> No mais, o artigo 10, § 1º, do Marco Civil da Internet não faz referência sobre a pretensão da recorrente, uma

No mesmo sentido: Agravo de Instrumento nº 2225114-64.2016.8.26.0000. 8ª Câmara de Direito Privado. Relator Grava Brazil, p. 23/01/2017. Agravo de Instrumento n.º 2.012.094-24.2015.8.26.0000. Relator Egídio Giacoia. 3ª Câmara Direito Privado. p. 28/04/2015; Agravo de Instrumento nº 2225928-76.2016.8.26.0000. Relator Moreira Viegas. 5ª Câmara de Direito Privado. p.: 01/02/2017.

[68] BRASIL. Tribunal de Justiça de São Paulo. *Agravo de Instrumento nº 2254100-62.2015.8.26.0000*. Relator Giffoni Ferreira. 2ª Câmara de Direito Privado. Publicado em 19/02/2016. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=9186093&cdForo=0>. Acesso em: set. 2018.

> vez que os provedores são obrigados apenas a disponibilizar os registros de acesso de forma autônoma ou associados a dados pessoais, porém, mediante ordem judicial, logo, não abrange dados envolvendo a porta lógica, mas somente armazenamento de IP. Assim, deve ser reiterado que a apelada não possui dados de porta lógica, já que não os cadastra, por conseguinte, não os armazena, portanto, não tem possibilidade de fornecer, ressaltando, ainda, a ausência de disposição legal para tanto[69].

Portanto, ante a divergência doutrinária e jurisprudencial, para se entender que existe uma obrigatoriedade no armazenamento da porta de origem, deveríamos conceber a natureza principiológica e finalística do Marco Civil, tendo em vista a falta de obrigação legal expressa.

Adotando tal entendimento, existiria um dever legal em relação ao armazenamento dos dados referentes à "porta lógica". Entretanto, seria necessário investigar, com mais precisão, de quem seria a responsabilidade pelo armazenamento e disponibilização desses dados, a saber, dos provedores de conexão, de aplicação, ou de ambos.

3 O DEVER DE ARMAZENAMENTO DAS PORTAS DE ORIGEM PELO PROVEDOR DE APLICAÇÃO E OUTRAS POSSIBILIDADES TÉCNICAS

Caso entendêssemos que o art. 5º do MCI possui o caráter meramente exemplificativo, sendo justificável, portanto, o fornecimento obrigatório da porta de origem vinculada ao endereço IP, restaria ainda investigar de quem seria a responsabilidade pela guarda de tais portas, a saber, do provedor de conexão ou de aplicação.

[69] BRASIL. Tribunal de Justiça de São Paulo. *Apelação nº 1078660-60.2015.8.26.0100*. Relator Natan Zelinschi de Arruda. 4ª Câmara de Direito Privado. Publicado em 13/06/2017. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=10515872&cdForo=0>. Acesso em: out. 2018.

A jurisprudência, apesar de heterogênea, como visto em tópico anterior[70], caminha no sentido de que a responsabilidade pelas "portas lógicas de origem"[71] devem ser dos provedores de conexão: "o eventual compartilhamento do IP, em face de usuários da rede IPv4, e a atribuição de uma porta lógica de acesso, constitui informação a, se caso, ser solicitada ao provedor de conexão"[72].

No mesmo sentido, voto do Tribunal de Justiça do Ceará:

> No presente caso, não me parecem razoáveis e relevantes as alegações da recorrente. Isso porque, em que pese a matéria em questão não está expressamente regulamentada no Marco Civil da Internet (Lei nº 12.965/14), a jurisprudência pátria possui julgados atribuindo responsabilidade de armazenamento e fornecimento da porta lógica de origem aos provedores de conexão, caso em que se enquadra a agravante[73].

[70] Cf. também REsp 1696546; REsp 1695974; AREsp 1291668; REsp 1734636.

[71] A exemplo do Tribunal de Justiça de São Paulo, no Agravo de Instrumento nº 20188747220188260000, p. 07/06/2018 e do Tribunal de Justiça do Ceará no Agravo de Instrumento nº 06204377820178060000, p. 03/05/17.

[72] BRASIL. Tribunal de Justiça de São Paulo. Agravo de Instrumento nº 2028047-28.2015.8.26.0000. Segredo de Justiça.

[73] BRASIL. Tribunal de Justiça do Ceará. *Agravo de Instrumento nº 0620437-78.2017.8.06.0000*. Relator Carlos Alberto Mendes Forte. Julgado em 03/05/2017. Disponível em: <http://esaj.tjce.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=3123206&cdForo=0&uuidCaptcha=sajcaptcha_3e537481d14f40989637b9782300edc6&g-recaptcha-response=03ADlfD19WVu1unih2pt9ItoTIagF3vtuQKSDNeO_Ce_AngHAdzs_3hJCpboivSpPDwxAdSHVpTkm7yaddmamoXX-zQL4mcCWby0ikEeIbawEPSpMWWE_zwJBxPI01H36COUF6ULKxQg8iSHU4bhwtqBbsci22kvpU6j66bGiGzYJ_WZcBlz4ZeSEKGsuEIB_c2ICJr123s7Eq769bS_pS9rP0WkK22XMt36UMLH2FiqYBu6sduuFJXWPuI-T8h4NPCBtzivJkH5aShnnm3IqFg_9Fg3l1FDjduQ>. Acesso em: nov. 2018

Os provedores de conexão, por sua vez, vêm ajuizando ações para indicar a impossibilidade de identificar o usuário de IP em razão da falta de informação sobre a "porta lógica" pelos provedores de aplicação[74].

Como já admitido pela empresa de telecomunicação TIM, em consulta pública[75] realizada pelo Ministério da Justiça ao decreto regulamentador do Marco Civil da Internet, "(...) 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[76]". Porém, segundo ela, o dever de informação deveria ser de ambos os provedores, haja vista ser necessário o cruzamento de dados para se identificar inequivocamente o usuário.

A exemplo, em ação ajuizada no âmbito do Superior Tribunal de Justiça - STJ, a empresa TIM já argumentou que, durante o período de transição entre modelos de rede, a informação a respeito da "porta lógica" utilizada pelo usuário da aplicação é elemento importante para a exata identificação do responsável pelo ilícito. A ausência desse dado, pode-se encontrar uma infinidade de usuários conectados ao mesmo endereço IP.

Por esse caráter técnico e diante de premissas jurídicas, como a proteção da privacidade e da vedação ao anonimato, para que o fornecimento da porta de origem seja adequado, ambos os provedores devem a armazenar, em consequência do provedor de conexão, pelas normas já expostas em capítulo pertinente, não poder guardar registros de aplicação. Rememoramos que

> Para o governo e para os detentores de direitos, o importante é que essas informações sejam guardadas pelos provedores, de modo a facilitar o trabalho das

[74] REsp nº 1.734.636/CE, Rel. Min. Moura Ribeiro, p. 30/04/18.

[75] Plataforma de debate do Marco Civil da Internet. O Projeto Pensando o Direito é uma iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), e foi criado em 2007 para promover a democratização do processo de elaboração legislativa no Brasil.

[76] *Armazenamento da porta lógica de origem pelos provedores de aplicação*. Secretaria de Assuntos Legislativos do Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/marcocivil/pauta/armazenamento-da-porta-logica-de-origem-pelos-provedores-de-aplicacao-2/>. Acesso em: 03 nov. 2018.

> autoridades judiciais e investigativas. A versão aprovada, bem como a proposta original, proíbe os provedores de conexão de guardar dados acerca da navegação do usuário e, com isso, dificulta a mitigação de crimes cibernéticos, pois não haverá nenhuma entidade com a responsabilidade de armazenar todos os dados de navegação do usuário (apenas os provedores de conteúdo teriam esses dados, mas de maneira isolada). Certamente essa é uma solução de boa receptividade entre aqueles que advogam pelas liberdades individuais, embora embuta a premissa de que o monitoramento pelos provedores de conteúdo seja aceitável[77].

Dessa forma, caso os provedores não armazenem as portas de origem da mesma forma da guarda de registros de dados prevista no MCI corre-se o risco de violar a privacidade dos usuários.

Segundo a TIM, o provedor de serviços da internet responsável pela guarda dos registros de acesso à aplicação é obrigado a fornecer a "porta lógica[78]", nos termos do artigo 10, § 1º, da Lei 12.965/14, a disponibilizá-los associados a outras informações aptas a contribuir para a identificação do usuário ou terminal[79].

Entretanto, como analisado em tópico anterior, o artigo supracitado apenas faculta ao juiz requerer outros dados que possibilitem a localização do usuário, mas não impõe aos provedores o dever de fornecer os dados requeridos, pois não possuem a obrigação legal de armazená-los.

O IOCTA, objeto de análise deste trabalho, utiliza como fonte técnica o memorando "*Request for Comments 6302 - Logging Recommendations for*

---

[77] NAZARENO, CLAUDIO. *Marco civil da internet*: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

[78] REsp nº 1.714.702/SP, Rel. Minª. Nancy Andrighi, p. 06.08.18

[79] AREsp nº 1.011.826/SP, Rel. Minª. Nancy Andrighi. p. 09.03.18.

Internet-Facing Server[80]", o qual sugere aos provedores de conexão e de aplicação armazenarem as portas de acesso, indicando também a necessidade de mudanças legislativas para garantir o adequado armazenamento dos dados adicionais.

Assim, retomamos a questão de ser tecnicamente mais adequado o fornecimento da porta de origem por ambos provedores, mas se juridicamente também seria a melhor decisão, visto que não há previsão legal expressa nesse sentido.

Por outra via, embora tenhamos verificado ser necessário o armazenamento da porta de origem para inequívoca identificação do usuário na internet, há outras possibilidades de solução técnica para o problema da transição entre os protocolos.

Em primeiro lugar, devemos entender que durante o processo de transição dos protocolos foi implementada a plataforma *Carrier Grade Network Address Translation* - CG NAT, a qual permite o compartilhamento de endereços IPv4 públicos.

Inicialmente as aplicações *Network Address Translation* - NAT[81] - eram utilizadas em redes domésticas[82]. O responsável por uma rede local recebia do provedor de conexão determinado número IP e o compartilhava entre os terminais da sua rede privada. Contudo, com a crescente utilização dos endereços de IPs públicos, o NAT começou a ser estendido também a estes endereços, passando a ser compartilhado entre milhares de usuários.

Ou seja, nesse novo sistema, o IPv4 público é compartilhado entre usuários da rede, de modo similar ao já realizado em IPs privados compartilhados em redes domésticas. Os usuários, assim, acabam convivendo com duas camadas de NAT, utilizada na rede doméstica e pública.

---

[80] Internet Engineering Steering Group. *Request for Comments 6302*: Logging Recommendations for Internet-Facing Servers. 2011. Disponível em: <http://bit.ly/2kgwjye>. Acesso em: jul. 2018.

[81] "Compartilhamento" de um IP único entre diversos computadores (roteador - doméstico ou do provedor de conexão), 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.

[82] 'Local Area Networks - LANs': redes domésticas.

Salienta-se, por oportuno, que a proposta de estudo deste trabalho não se aplica a redes domésticas, pois sempre existiu a falta de individualização dos dispositivos singulares conectados a uma rede local. Procuramos, portanto, compreender esse novo cenário desenvolvido em redes públicas, o qual representa um grande problema de governabilidade da internet.

Assim, a utilização das técnicas de compartilhamento dos endereços de IP, denominadas NAT, ficaram a cargo dos provedores de conexão. Isto porque, caso sejam atribuídos a um provedor de conexão determinado número de endereços IPs inferior a sua demanda, será imprescindível a utilização do sistema de NAT 44 para permitir a todos os seus clientes se comunicarem com redes externas.

No entanto, mesmo o NAT 44 sendo uma ferramenta importante na transição do protocolo IPv4 para IPv6, o seu uso deve ser evitado, pois não atende ao princípio de comunicação direta "fim a fim"[83], deixando os seus usuários mais vulneráveis[84]. Deve-se priorizar, quando possível, a utilização de redes IPv6, assim como devemos evitar a menor taxa de compartilhamento possível pela plataforma CG NAT.

Nesse sentido, foi proposta nova alternativa no VIII Fórum de Internet no Brasil[85], promovido pelo Núcleo de Informação e Coordenação do Ponto br - NIC.br - e pelo Comitê Gestor da Internet - CGI.br -, para os provedores de conexão fossem limitados a compartilhar cada endereço IP com no máximo 64 (sessenta e quatro) usuários.

De acordo com o Fórum, o número seria razoável para investigações judiciais e tecnicamente viável aos provedores de conexão, de modo a afastar o problema da guarda das portas de acesso e minimizar a questão relativa à privacidade de usuários que, embora não tenham nenhuma relação com o crime objeto da investigação, acabam por ter o seu cadastro fornecido para as autoridades policiais.

---

[83] Comunicações diretas entre terminais.

[84] *Transição*. Disponível em: <http://ipv6.br/post/transicao/>. Acesso em: 03 nov. 2018.

[85] Realizado entre os dias 04 a 07 de novembro de 2018, na cidade de Goiânia. Disponível em: <https://www.youtube.com/watch?v=LLZ8rsRp7Gk>. Acesso em: 10 nov. 2018.

Todavia, o não fornecimento da porta de acesso ainda continuaria a implicar a invasão de privacidade dos 63 (sessenta e três usuários), os quais não teriam envolvimento com o caso, mas apenas estavam compartilhando o mesmo endereço IP com o autor do ilícito.

É possível identificar erroneamente o titular dos dados[86], ou seja, buscar dados pessoais dos não participantes da relação conflituosa. Contudo, deve haver uma ponderação, vendo a prevalência ou não do direito à privacidade sobre o interesse público. Ainda mais, não estamos falando aqui de dados pessoais sensíveis, mas de dados cadastrais, os quais revelam outro nível de invasão à privacidade.

Da mesma maneira que a liberdade de expressão pode ser relativizada, a privacidade também poderá. "O desafio é como equacionar tudo isso em uma internet que seja viável, acessível e justa para todos[87]".

Deve-se lembrar, por fim, de não utilizar o direito como inibidor de inovações. Vejamos

> No debate público, especialmente no que respeita à inovação tecnológica, o direito vigente é muitas vezes rotulado como inibidor da inovação. Isso é muito unilateral: o direito pode assumir muitas formas e afetar muitos dos resultados, seja o da promoção, ou do efeito inibidor, dependendo da natureza do direito a partir da pesquisa científica. A pesquisa em inovação na ciência jurídica analisa os modos de ação do direito que permitam inovações ou que as estimulem, a esta função de signo de "abertura do direito" às inovações. O direito também é instituído para defender valores e interesses e proteger bens jurídicos que possam ser colocados em risco. Nesse sentido, o direito incide na realização do bem comum e este pode ser favorecido pela inovação, mas igualmente pode ser posto em risco. Portanto, para

[86] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães. *Direito privado e Internet*. São Paulo: Editora Atlas, 2014, p. 61.

[87] NAZARENO, CLAUDIO. *Marco civil da internet*: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

> a cautela relativamente à compatibilidade do comportamento inovador, juridicamente marcado pelo bem comum, denomino "responsabilidade pela inovação[88]".

Assim, deve-se adotar uma solução que seja proporcional, pois

> O princípio da proporcionalidade esclarece a necessidade de avaliações e da escolha adequada entre as diferentes opções: se deve eleger a opção que é a mais conveniente não somente para resolver o problema, mas também a menos desvantajosa para outros interesses. Para uma avaliação adequada, os operadores do direito devem também levar em conta as alterações das condições do cenário econômico, tecnológico, político ou cultural. Também exige uma disposição para aprendizagem[89].

Dessa forma, propõe-se uma resposta proporcional, a contemplar os aspectos técnicos, jurídicos e econômicos, caminhando por novas possibilidades.

CONSIDERAÇÕES FINAIS

Do exposto, podemos perceber que, atualmente, não há um consenso doutrinário e jurisprudencial sobre o tema. Desse modo, precisamos recorrer igualmente a análise direta das fontes legais e técnicas, em especial do Marco Civil da Internet.

Da análise do Marco Civil, conclui-se, *a priori*, ser de obrigação tanto do provedor de aplicação quanto de conexão o fornecimento das portas de

---

[88] HOFFMANN-RIEM, Wolfgang. Direito, tecnologia e inovação. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; P. COELHO, Alexandre Zavaglia. *Direito, inovação e tecnologia*. Vol. 1. São Paulo: Saraiva, 2015, p. 15

[89] Ibid, p. 28

origem, tendo em vista a preservação da privacidade dos usuários, bem como a vedação do anonimato e a finalidade da norma quanto à localização inequívoca do usuário.

Contudo, em outra perspectiva, não há nenhuma previsão expressa na norma indicando se a guarda desses dados deveria ser realizada pelos provedores, correndo-se o risco de instituir obrigações a particulares não previstas em lei, em clara violação à segurança jurídica.

Salienta-se aqui, no entanto, não ser coerente parte da jurisprudência que estabelece a obrigação somente ao provedor de conexão, pois a medida se tornaria efetiva apenas se o armazenamento fosse realizado por ambos os provedores, haja vista a limitação de cada um dos provedores em poder armazenar apenas os dados vinculados a sua prestação de serviço, nos mesmos termos da guarda de registros de conexão e de aplicação.

Diante dessas perspectivas, são propostas três soluções opostas: (i) a de realizar uma interpretação principiológica e finalística do Marco Civil, afirmando ser de responsabilidade de todos os provedores de *internet* o armazenamento das portas de origem, em vista da lógica interna do MCI quanto à guarda de dados; (ii) propor uma mudança legislativa de efeitos prospectivos, de forma a delimitar expressamente como deveria ser realizada a guarda das portas de acesso pelos provedores; e (iii) propor outras soluções técnicas, preservando a legislação vigente, como a limitação do compartilhamento dos endereços IPs a 64 (sessenta e quatro usuários).

Entretanto, como já visto, a primeira solução pode vulnerar a segurança jurídica, sendo necessário ainda avaliar a capacidade técnica dos provedores de aplicação em fornecer tais dados, pois poderia representar um ônus excessivo a estes, principalmente para os pequenos provedores e inviabilizar a sua manutenção na rede.

A segunda resposta ao problema das portas de acesso, por sua vez, soluciona o problema da falta de segurança jurídica, mas fica ao alvedrio do processo legislativo, não apresentando uma solução para os problemas atuais. Ademais, por se tratar de um problema de cunho transitório, questiona-se a necessidade de uma mudança legislativa.

Na terceira hipótese o principal problema é o não cumprimento da finalidade da norma de maneira satisfatória, isto é, a identificação inequívoca

do usuário. Ainda há quem justifique um dano à privacidade dos usuários que estariam compartilhando o endereço IP. Contudo, apesar do acesso ser Dados pessoais violaria a privacidade ou apenas dados pessoais sensíveis.

Portanto, sabendo que todas as soluções apresentam uma relação de custo-benefício aos direitos fundamentais em jogo, a solução de se responsabilizar todos os provedores de *internet* o armazenamento das portas de origem, é a que possibilita a inequívoca possibilidade de identificação e o menor risco à privacidade de terceiros.

Contudo, o presente trabalho não tem o objetivo de esgotar o tema, ainda é necessário maiores investigações técnicas para avaliarmos qual resposta contemplaria de modo mais adequado os aspectos jurídicos, econômicos e sociais, os quais, em um cenário ideal deveria ficar a cargo do legislador, mas ante a mora legislativa, muitas vezes a escolha fica sob a responsabilidade do magistrado, o qual deverá fundamentar a sua decisão de modo proporcional e razoável.

REFERÊNCIAS

NAZARENO, CLAUDIO. **Marco civil da internet** [recurso eletrônico]: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Série legislação; n. 164. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

IESG. **Request for Comments 6302:** Logging Recommendations for Internet-Facing Servers. 2011. Disponível em: <http://bit.ly/2kgwjye>. Acesso em: jun. 2018.

Transição. Comitê Gestor da Internet no Brasil. Disponível em: <http://ipv6.br/post/transicao/>. Acesso em: 03 nov. 2018.

MARTINS, Guilherme Magalhães. **Direito privado e Internet**. São Paulo: Editora Atlas, 2014.

BARRETO, Alesandro Gonçalves; SILVEIRA, Beatriz. **Manual de Investigação Cibernética: à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016.

Grupo de Trabalho para Implantação do Protocolo IP: Versão 6 nas Redes das Prestadoras de Serviços de Telecomunicações, publicado pela Agência Nacional de Telecomunicações - ANATEL, em 2014. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=325769.pdf>. Acesso em: ago. 2018

POLIDO, Fabrício B. Pasquot; ANJOS, Lucas Costa dos. **Portas lógicas e registros de acesso**: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. Instituto de Referência em Internet e Sociedade. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/11/Portas-Lo%CC%81gicas-e-Registros-de-Acesso.pdf>. Acesso em: abr. 2018.

Armazenamento da porta lógica de origem pelos provedores de aplicação. Secretaria de Assuntos Legislativos do Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/marcocivil/pauta/armazenamento-da-porta-logica-de-origem-pelos-provedores-de-aplicacao-2/>. Acesso em: 03 nov. 2018.

Plataforma de debate do Marco Civil da Internet. O Projeto Pensando o Direito é uma iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), e foi criado em 2007 para promover a democratização do processo de elaboração legislativa no Brasil.

EUROPOL. IOCTA 2016 - **Internet Organised Crime Threat Assessment.** Disponível em: <http://bit.ly/2fCum7o>. Acesso em: jun. 2018.

Cour de justice de l'Union européenne. **Patrick Breyer v. Bundesrepublik Deutschland**:Case C-582/14. 19 Outubro de 2016. Disponível em: <http://bit.ly/2gsdqaf>. Acesso em: 10 set. 2018.

SANKIEVICZ, Alexandre. **Direito ao esquecimento e sobre fatos e circunstâncias dos trópicos que devemos especialmente ponderar**. Cadernos Aslegis, n. 48. Brasília: Aslegis, 2015.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** São Paulo: Atlas, 2014.

VOLKMER, André; et. al. **A liberdade na era digital.** Série Pensamentos Liberais. Volume XV. Porto Alegre: Instituto de Estudos Empresariais, 2011.

SARMENTO, Daniel. **Livres e iguais**: estudos de Direito Constitucional. Rio de Janeiro: Lumen Juris, 2006.

TSESIS, Alexander. **Hate in Cyberspace**: Regulating Hate Speech On the Internet. Loyola University Chicago, School of Law, 2001.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: ago. 2018.

TORRES, Ana Paula Repolês. Pensando a liberdade de "expressão" com Hannah Arendt. **Prometeus Filosofia em Revista.** Sergipe, ano 5, nº. 10, 2012, p.51.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9 ed. Salvador: Jus podivm, 2017.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: nov. 2018.

BRASIL. Marco Civil da Internet. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: nov. 2018.

BRASIL. Decreto regulamentador do Marco Civil da Internet. Decreto nº 8.771, de 11 de maio de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: jun. 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. 2 ed. São Paulo: Saraiva, 2007.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; P. COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia**. Vol. 1. São Paulo: Saraiva, 2015.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 37 ed. São Paulo: Malheiros Editores, 2014, p. 211-212

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: jul. 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 9 ed. São Paulo: Saraiva, 2014,

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.117.633/RO**. Segunda Turma. Relator Ministro Herman Benjamin. Julgado em 26/03/2010. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=1117633&b=ACOR&p=true&l=10&i=5>. Acesso em: ago. 2018.

SANTOS, Rodrigo Regis dos; et. al. **Curso IPv6 básico**. São Paulo: Núcleo de Informação e Coordenação do ponto BR, 2010. Disponível em: <http://ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf>. Acesso em: nov. 2018.

AUSTRALIAN GOVERNMENT. Attorney-General's Department. **Data retention**: frequently asked questions for industry. Communications Access Co-ordinator. Publicado em julho de 2015. Disponível em: <http://m.tio.com.au/__data/assets/pdf_file/0005/188753/INDUSTRY-FAQs-V1.1-JULY-2015.pdf>. Acessado em: jul. 2018.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coordenadores). **Direito & Internet III**: Marco Civil da Internet (Lei n. 12.965/2014). Tomo II. São Paulo: Quartier Latin, 2015.

BRASIL. Tribunal de Justiça do Amazonas. **Agravo de Instrumento nº 4004023-74.2016.8.04.0000**. 2ª Câmara Cível. Relator Maria do Perpétuo Socorro Guedes Moura. Publicado em 19.06.17. Disponível em:<https://consultasaj.tjam.jus.br/cposgcr/show.do?processo.foro=900&processo.codigo=P00002NQM0000&uuidCaptcha=sajcaptcha_30df6002199e4b2f90f5356bb0db3528#?cdDocumento=22>. Acesso em: set. 2018.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Agravo de Instrumento nº 07086665020188070000**. 2ª Turma Cível. Relator Cesar Loyola. Publicado em 10/10/2018. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: nov. 2018.

BRASIL. Tribunal de Justiça de São Paulo. **Agravo de Instrumento nº 2257879-25.2015.8.26.0000**. Relator J.L. Mônaco da Silva. 5ª Câmara de Direito Privado. Publicado em 14/03/2016. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=9264245&cdForo=0>. Acesso em: set. 2018.

BRASIL. Tribunal de Justiça de São Paulo. **Agravo de Instrumento nº. 2064240-08.2016.8.26.0000.** Relator J.B. Paula Lima. 10ª Câmara de Direito Privado. Publicado em 19/12/2016. Disponível em: <https://esaj.tjsp.jus.br/cposg/search.do?conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=2064240-08.2016&foroNumeroUnificado=0000&dePesquisaNuUnificado=2064240-08.2016.8.26.0000&dePesquisa=&uuidCaptcha=#?cdDocumento=33>. Acesso em: set. 2018.

BRASIL. Tribunal de Justiça de São Paulo. **Agravo de Instrumento nº. 2062855-88.2017.8.26.0000**. 4ª Câmara de Direito Privado. Relator Hamid Bdine. Publicado em 30/05/2017. Disponível em: <https://esaj.tjsp.jus.br/cposg/show.do?processo.codigo=RI003XPJR0000&conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=1070451-05.2015&foroNumeroUnificado=0100&dePesquisaNuUnificado=1070451-05.2015.8.26.0100&dePesquisa=&uuidCaptcha=#?cdDocumento=23>. Acesso em: set. 2018.

BRASIL. Agravo de Instrumento 2018874-72.2018.8.26.0000. Relator Pedro de Alcântara da Silva Leme Filho. 8ª Câmara de Direito Privado. Data de publicação: 07/06/2018. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=11520452&cdForo=0&uuidCaptcha=sajcaptcha_548d15df36f14c759917da02c2d2958f&vlCaptcha=WnKQ&novoVlCaptcha=>. Acesso em: set. 2018.

BRASIL. Tribunal de Justiça de São Paulo. **Agravo de Instrumento nº 2254100-62.2015.8.26.0000**. Relator Giffoni Ferreira. 2ª Câmara de Direito Privado. Publicado em 19/02/2016. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=9186093&cdForo=0>. Acesso em: set. 2018.

BRASIL. Tribunal de Justiça de São Paulo. **Apelação nº 1078660-60.2015.8.26.0100**. Relator Natan Zelinschi de Arruda. 4ª Câmara de Direito Privado. Publicado em 13/06/2017. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=10515872&cdForo=0>. Acesso em: out. 2018.

BRASIL. Tribunal de Justiça do Ceará. **Agravo de Instrumento nº 0620437-78.2017.8.06.0000**. Relator Carlos Alberto Mendes Forte. Julgado em 03/05/2017. Disponível em: <http://esaj.tjce.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=3123206&cdForo=0&uuidCaptcha=sajcaptcha_3e537481d14f40989637b9782300edc6&g-recaptcha-response=03ADlfD19WVu1unih2pt9ItoTIagF3vtuQKSDNeO_Ce_AngHAdzs_3hJCpboivSpPDwxAdSHVpTkm7yaddmamoXX-zQL4mcCWby0ikEeIbawEPSpMWWE_zwJBxPI01H36COUF6ULKxQg8iSHU4bhwtqBbsci22kvpU6j66bGiGzYJ_WZcBlz4ZeSEKGsuEIB_c2ICJr123s7Eq769bS_pS9rP0WkK22XMt36UMLH2FiqYBu6sduuFJXWPuI-T8h4NPCBtzivJkH5aShnnm3IqFg_9Fg3l1FDjduQ>. Acesso em: nov. 2018