A DISCUSSÃO SOBRE **ARMAZENAMENTO DE PORTAS LÓGICAS** À LUZ DO MARCO CIVIL DA INTERNET

BAPTISTA LUZ
ADVOGADOS

A DISCUSSÃO SOBRE ARMAZENAMENTO DE PORTAS LÓGICAS À LUZ DO MARCO CIVIL DA INTERNET

/ Pedro Henrique Ramos

/ Renato Leite Monteiro

/ Fernanda Foizer[1]

[1] Colaboraram com esse estudo também Davi Teófilo e Thais Muchon Schainberg.

BAPTISTA LUZ
ADVOGADOS

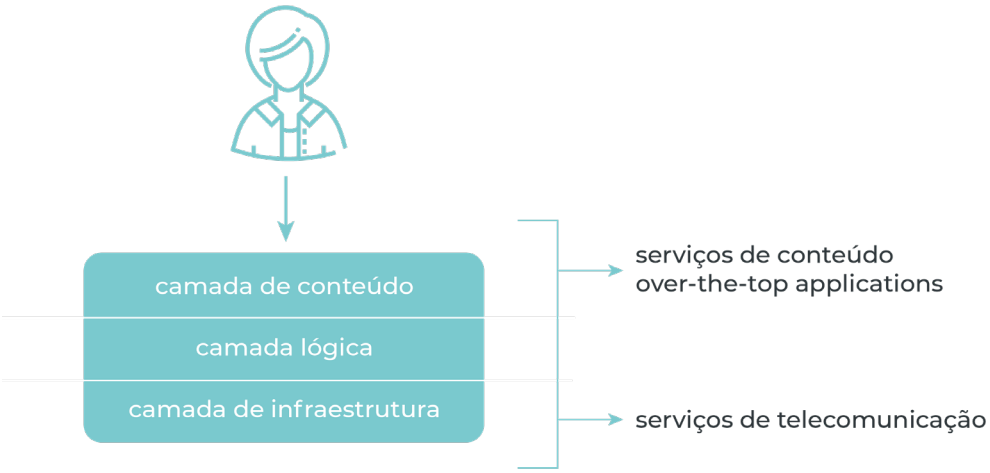
1/ INTRODUÇÃO

O objetivo deste trabalho é apresentar uma visão geral sobre a desobrigação de provedores de aplicação em armazenar portas lógicas de origem. Para melhor compreensão do tema, a análise será iniciada com uma descrição técnica sobre o conceito e a transição do IPV4 para o IPV6, que deu origem à presente discussão. Em seguida, será analisado como o Marco Civil da Internet abordou as discussões sobre portas lógicas. O objetivo será demonstrar que foi consciente e fundada a escolha do legislador por não atribuir o armazenamento de portas lógicas como obrigação legal, mostrando-se imprescindível restringir o rol de dados a serem armazenados por provedores de aplicações, mostrando ainda as consequências adversas que uma interpretação diversa, em contrassenso à legislação nacional e internacional, pode causar, em especial para a proteção de dados pessoais e para o fomento à inovação no país.

2/ MAS O QUE SÃO PORTAS LÓGICAS?

Portas lógicas são elementos importantes na eletrônica e, no contexto da internet, representam uma construção de sistemas e protocolos que especificam o término de uma linha de comunicação, e possuem relação com um conjunto de protocolos lógicos fundamental para o funcionamento da rede, o TCP/IP.

Gráfico 1. Modelo Teórico de Funcionamento de Redes [2]



O TCP/IP é o principal protocolo de funcionamento da internet, responsável pelo transporte dos pacotes de dados na rede[3]. O conjunto TCP *(Transmission Control Protocol)* e IP *(Internet Protocol)* possui, individualmente, funções específicas. Enquanto o TCP encarrega-se do transporte dos pacotes de dados, o IP identifica esses pacotes para os receptores, por meio de uma sequência de números únicos, como se fosse uma espécie de endereço[4]. A primeira versão do IP ficou conhecida como IPv4, e foi desenvolvida nos anos 1970, com sua numeração possibilitando uma quantidade máxima de aproximadamente 4.3 bilhões de endereços IP.

Com o crescimento do número de usuários da rede a partir

[2] O gráfico baseia-se na versão simplificada do modelo ISO/IEC 7498-1, criada por Yochai BENKLER (in From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. Fed. Comm. LJ, v. 52, p. 561, 1999), servindo como ferramenta metodológica para trabalhos sobre a regulação da internet e seus efeitos para os usuários.

[3] Conforme aponta RAMOS (RAMOS, P. H., Neutralidade da Rede: a regulação da arquitetura da internet no Brasil, Ed. IASP, São Paulo, 2018), a internet é um conjunto de redes particulares, interconectadas a partir de um mesmo protocolo (o TCP/IP) e seguindo os mesmos padrões técnicos, o que permite a comunicação entre diferentes localidades. Cada uma dessas redes é administrada por entes privados ou públicos, como governos, universidades e provedores de conexão (tanto provedores de acesso como provedores de trânsito), e são denominadas Sistemas Autônomos – grupo de redes de comutação por pacotes sob o protocolo TCP/IP, abaixo de uma única gerência técnica e que compartilham uma mesma política de roteamento, sendo autônoma em relação à tomada de decisões sobre interconexões com os demais Sistemas Autônomos.

dos anos 1990, o número de endereços IP disponíveis para identificação começa a reduzir rapidamente. Com a previsão de esgotamento, o IETF[5] desenvolveu, em 1998, o padrão RFC[6] 2460, que passou a ser a nova versão do IP: o IPv6. Esta nova versão tem quatro dígitos hexadecimais que permitem uma quantidade praticamente inesgotável de endereços. Se por um lado o IPv4 comportava 4.3 bilhões de endereços, por outro o IPv6 prevê um total de 3.4x1038 endereços.

O processo de transição do IPV4 para o IPV6 é lento e gradual, em razão dos investimentos técnicos que devem ser feitos por provedores de conexão e outras empresas que atuam na camada lógica da rede. Neste momento de transição, para que o acesso à internet não seja comprometido, tem sido adotada a técnica "NAT" *(Network Address Translation)*, que viabiliza o compartilhamento do mesmo número de IP por mais de um usuário, de forma simultânea. Ou seja, diferentes usuários podem trafegar na internet utilizando um único endereço IP, ao mesmo momento.

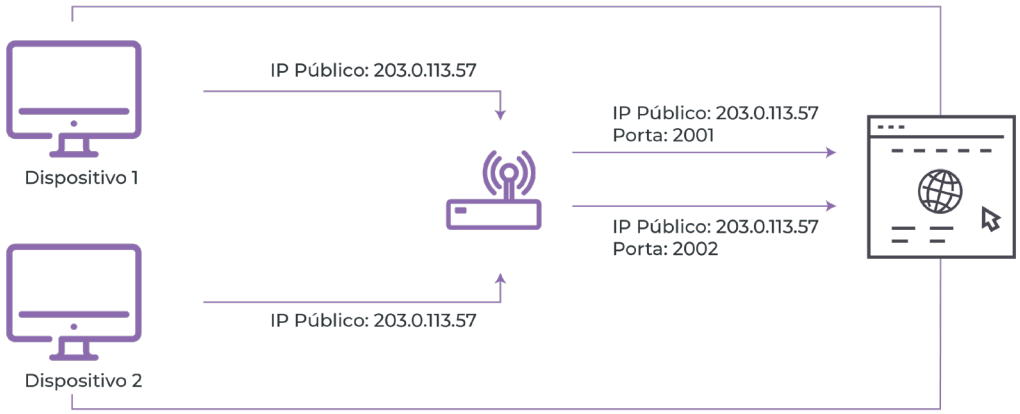
A técnica NAT ocorre no âmbito das operações de roteamento da conexão de rede e, entre outras funções, acrescenta às comunicações uma função adicional ao endereço de IP, que é a atribuição de **portas lógicas adicionais**, que também são numeradas e adicionadas ao final do endereço, para auxiliar na identificação da origem do pacote de dados quando dois dispositivos compartilharem um mesmo número de endereço IP.

Em uma comparação bastante simplista, é como se o serviço de correios recebesse duas cartas diferentes, de um mesmo endereço remetente, mas sem a identificação do nome da pessoa. Para garantir que o destinatário responderá a carta original para a pessoa certa, o serviço de correios cria uma marcação em cada um dos envelopes, garantindo que, na resposta, o remetente original (e agora destinatário da resposta) irá saber qual carta responde a primeira mensagem enviada.

A explicação aqui trazida é propositalmente despretensiosa e superficial, mas didática e suficiente para os fins aqui propostos. Em geral, a maioria das redes privadas possui mais de dois dispositivos conectados, sendo que cada um deles se abre para uma porta lógica a partir do roteamento. Todavia, a atribuição de portas lógicas não é uma constante e, logo, não são todos os dispositivos que necessariamente terão em seus IPs uma atribuição específica, em especial pelo uso de diversas técnicas para roteamento e conexão praticadas pelos provedores de conexão para dar eficiência ao uso da rede, o que significa que um mesmo dispositivo, ainda que com o mesmo IP, pode se conectar a várias diferentes portas ao longo de uma mesma sessão de uso da rede.

Assim, embora a porta seja importante para garantir o correto envio e recebimento das informações trafegadas, essa informação não é o mecanismo mais adequado para identificar um dispositivo, e há várias outras formas para essa identificação acontecer, haja vista a possibilidade de rotatividade constante de portas lógicas ao mesmo usuário.

Gráfico 2. Modelo Didático da técnica NAT



[4] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (Brasil) (Org.). CURSO IPv6 BÁSICO. São Paulo: Nic, 2012. 314 p.

[5] Internet Engineering Task Force (IETF): é uma instituição que de tempos em tempos organiza foros mundiais e abertos, onde se definem os padrões de arquitetura e as especificações técnicas que estruturam a internet. https://tools.ietf.org/html/rfc791

[6] Request for Comments, em português, "pedido de comentários", são documentos técnicos desenvolvidos e mantidos pelo IETF (Internet Engineering Task Force).

3/ INTERPRETAÇÕES À LUZ DO MARCO CIVIL DA INTERNET

Aprovado em 2014, o Marco Civil da Internet é uma referência no mundo sobre regulação da internet. Esta legislação estabeleceu princípios, garantias, direitos e deveres dos usuários da internet e tratou de forma específica as relações jurídicas estabelecidas na internet, visando conferir maior segurança aos agentes envolvidos nessas relações.

Dentre os diversos direitos e garantias dos usuários segundo o MCI, destacamos, para os fins deste trabalho:

(i) inviolabilidade da intimidade e da vida privada (Art. 7o, I);

(ii) preservação do sigilo das comunicações privadas transmitidas ou armazenadas (Art. 7o, II, III);

(ii) proteção contra o fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do titular (Art. 7o, VII);

(iv) direito a informações claras e completas sobre o tratamento de dados pessoais (Art. 7o, VIII); e

(v) prerrogativa do consentimento expresso e destacado sobre o tratamento destes (Art. 7o, XI).

Retenção de dados segundo o **Marco Civil da Internet**
(Lei nº 12.965, de 23 de abril de 2014)

	Provedor de conexão	Provedor comercial de aplicações	Provedor não comercial de aplicações
Tipos de dados a serem retidos	Registros de conexão à internet	Registros de acesso a aplicações	
Obrigatoriedade de retenção dos dados	Obrigatório		Mediante requisição sem ordem judicial
Período de retenção dos dados	1 ano	6 meses	
Aumento do período de retenção	Mediante requisição sem ordem judicial		
Acesso aos dados obtidos	Mediante ordem judicial		

fonte: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm

Ao mesmo tempo em que o MCI buscou garantir esses direitos, a Lei também buscou segurança jurídica ao tema da responsabilidade de provedores na guarda de registros, tema antes bastante debatido na jurisprudência brasileira. Esses registros foram divididos em dois tipos, quais sejam, **registros de conexão** e **registros de acesso à aplicação:**

> **(i) registros de conexão (art. 5º, VI):** 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;
>
> **(ii) registros de acesso a aplicações de internet (art. 5º, VIII):** conjunto de informações referentes **à data e hora** de uso de uma determinada aplicação de internet a partir de um **determinado endereço IP.**

Enquanto provedores de aplicações (sites, aplicativos e outras empresas que atuam na camada de conteúdo da rede) são obrigados a armazenar os registros de acesso a aplicações por, no mínimo, seis meses (art. 15), os provedores de conexão (as operadoras de internet) são obrigados a armazenar os registro de conexão por, no mínimo, um ano (art. 13), sendo certo que tal período poderá ser estendido mediante requisição das autoridades competentes (policial ou administrativa ou, ainda, o Ministério Público). A retenção dos registros é obrigatória, bem como a sua divulgação, mediante ordem judicial. **O texto legal em nenhum momento cita expressamente a necessidade de armazenamento de portas lógicas.** A não inserção da obrigação de retenção das portas lógicas por provedores também tem um objetivo teleológico, sendo **opção consciente do legislador,** conforme a análise da construção histórica da Lei.

O Marco Civil da Internet é um produto de uma realidade social, sendo um dos primeiros casos bem sucedidos de um processo legislativo amplo, com participação popular intensa, com três consultas públicas, um anteprojeto e quatro substitutivos ao projeto de lei original, contando com mais de **2 mil comentários e sugestões** enviadas por usuários, empresas e organizações da sociedade civil[7], além de um processo de consulta pública ao seu regulamento (Decreto 8.771/16) que contou com mais de **1.500 comentários e contribuições** dos diversos setores.

Os debates envolvendo a elaboração do texto do MCI e a sua posterior regulação foram intensos e perpassaram por diversos temas polêmicos, **inclusive, o armazenamento de portas lógicas.** Nas consultas públicas sobre o regulamento do MCI, alguns atores defenderam a ampliação, via decreto, do conceito de registros de acesso e registros de conexão previstos no MCI. O Ministério Público Federal argumentou que[8]:

> O novo protocolo denominado IPv6, mais complexo e extremamente custoso, ainda não foi adotado por todos os Provedores de Acesso à Internet nem de Aplicação, Governo, Universidades e centros de pesquisa, dentre outros. Como solução paliativa e provisória, até a plena migração para o novo protocolo IPv6, foi acordado entre os Provedores de Acesso (todas as empresas de telecomunicações) a adoção do compartilhamento de endereços IPv4 públicos por meio da implantação de plataformas CGNAT (Carrier Grade Network Address Translation), mais comumente conhecida como CG-NAT 44.
>
> (...)
> Sugere-se, assim, que o regulamento estabeleça de forma clara que a guarda e disponibilização de registros prevista no artigo 10 deve incluir elementos (IP, data, horário, fuso e porta de origem), que permitam a identificação inequívoca de usuário enquanto não for efetivada a completa migração do padrão IPv4 para IPv6.

[7] "Marco civil da internet: construção e aplicação"; Carlos Affonso Souza e Ronaldo Lemos, Juiz de Fora: Editar Editora Associada Ltda, 2016.

[8] Ministério Público Federal (Org.). Nota técnica conjunta nº 01/2015: Regulamentação do Marco Civil da Internet. São Paulo: Mpf, 2015. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/notas-tecnicas/nota-tecnica-mci-mpf>. Acesso em: 19 jul. 2019.

Posição semelhante foi apresentada pela Ordem dos Advogados do Brasil – Seccional Santa Catarina[9]:

> Tendo isso em vista, pede-se que sejam guardados adicionalmente os dados relativos à **porta lógica** utilizada. Essa medida possibilitará a individualização de suspeitos enquanto não for implementada a nova versão de IP (IPv6). Além da porta lógica, a OAB/SC também defende a criação de obrigação de guarda do endereço MAC (media access control), numeração produzida pelo roteador de redes domésticas ou profissionais que permitiria identificar ao certo o dispositivo ligado à atividade investigada.

Ambas posições traziam inconsistências técnicas e um grave problema de legalidade (ainda que o decreto pudesse regulamentar, não caberia a este instrumento expandir o conceito original da lei), e foram, ainda, minoritárias durante o debate da consulta pública. Logo, **a escolha do legislador por não criar tal obrigação legal foi fundamentada, consciente, baseada em um debate popular e democrático,** na medida em que a questão já era discutida quando da elaboração do texto de lei e de sua regulamentação. Nesse sentido, Francisco Brito Cruz[10] destaca que:

> O Marco Civil da Internet **não obriga a retenção de portas lógicas** assim como não determinou explicitamente a guarda de diversos tipos de informação que poderiam complementar ou auxiliar na identificação de outros usuários. **A escolha foi por cobrir alguns aspectos técnicos que tornam possível a identificação de usuários, mas não obrigar que provedores retivessem qualquer tipo de informação útil para identificação.** O percurso para identificar algum usuário de Internet pode encontrar outros obstáculos para além do compartilhamento de um IP e nem por isso o legislador se preocupou em cobrir tais casos (como, por exemplo, o compartilhamento de redes wi-fi por um grande número de pessoas). (...) **A identificação da conexão ou acesso já é possível com a numeração IP, data e hora (pois é pouco provável que dois indivíduos iriam conectar e desconectar exatamente na mesma hora, minuto e segundo).**

Os Tribunais brasileiros, em face dessa questão, também têm se posicionado no sentido de que, **se nem mesmo o decreto regulamentador, que poderia ter ampliado o conceito de registro de conexão para incluir portas lógicas, entendeu que caberia uma ampliação do conceito, muito menos ao Judiciário caberia alterar esse quadro.**

O Instituto de Referência em Internet e Sociedade (IRIS)[11] desenvolveu pesquisa e análise técnica de dados colhidos em processos judiciais versando sobre pedidos de acesso a **portas lógicas** em Tribunais de Justiça Estaduais e Tribunais de Justiça Federais de todo o país, concluindo que somente em 35% dos casos o Judiciário entende que há obrigação de fornecer a porta lógica[12], sendo o entendimento majoritário dos Tribunais brasileiros de que os p**rovedores de aplicação não têm a obrigação legal de fornecer a porta lógica de origem.** Nesse sentido, destacamos:

[9] INTERNETLAB (Org.). O que está em jogo na regulamentação do Marco Civil da internet? Relatório final sobre o debate público promovido pelo Ministério da Justiça para a regulamentação da lei 12.965/2014. São Paulo, 2015. 50 p.

[10] CRUZ, Francisco. Porta lógica e provedores de aplicação. Disponível em <http://www.omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/> Acesso em: 19, Julho de 2019.

[11] O Instituto de Referência em Internet e Sociedade é um centro de estudos independente fundado em Belo Horizonte, Minas Gerais. Sua missão é explorar, investigar e entender os desdobramentos da Internet sobre a sociedade contemporânea.

[12] INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Brasil) (Org.). Portas lógicas e registros de acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. Belo Horizonte: Iris, 2017.

> AGRAVO DE INSTRUMENTO. AÇÃO DE INDENIZAÇÃO. Determinação de apresentação de dados, notadamente da porta lógica de origem. Afastamento em parte. **Ré que figura como provedora de aplicação. Necessidade apenas do fornecimento dos dados previstos no artigo 5º, VIII, da Lei nº 12.965/14. Precedentes desta Câmara. Decisão reformada neste tópico.**
> RECURSO PROVIDO. (TJSP, 3ª Câmara de Direito Privado, Agravo de Instrumento n. 2102827-94.2019.8.26.0000, Comarca: São Paulo, Agravante: Facebook Serviços Online do Brasil Ltda. Agravada: Associação Brasileira de Direitos Reprográficos, **julgado 05/07/2019).**
>
> AGRAVO DE INSTRUMENTO. AÇÃO DE OBRIGAÇÃO DEFAZER.TUTELA ANTECIPADA. INTERNET. FORNECIMENTO DE DADOS. Agravante que pretende afastar tão somente a sua **obrigação de apresentação da "porta lógica de origem".** Cabimento. **Inexistência de obrigação legal de fornecimento da referida informação. O Marco Civil da Internet determinou apenas o dever de armazenar os dados concernentes às datas e horários de acesso.** Inteligência do art. 5º, VIII, e art. 15, da Lei nº 12.965/14. Agravante, ademais, que é mero provedor de aplicação de internet (Facebook). Obrigação que somente pode ser imposta a um provedor de conexão. Precedentes jurisprudenciais. Decisão reformada. RECURSO PROVIDO. (TJSP, Agravo de Instrumento nº: 2240522-27.2018.8.26.0000, Agravante: Google Brasil Internet LTDA. Agravada: Associação Brasileira de Direitos Reprográficos, Comarca: São Paulo Foro Central Cível, **julgado em 18/06/2019).**

Portanto, o legislador pátrio, nas várias oportunidades que teve para incluir a obrigação da retenção das portas lógicas, não o fez de forma deliberada, apesar das manifestações nessa direção de atores de diferentes contextos. Tal vontade tem sido reconhecida, majoritariamente, pelas cortes nacionais, sob um viés da leitura positiva da lei posta num contexto de impossibilidade de imposição de obrigação além daquela prevista na norma vigente. Ainda, o eventual mandamento de retenção das portas lógicas pode ter impacto nos direitos e princípios que regem a moldura regulatória de proteção à privacidade e aos dados pessoais.

4/ CONSEQUÊNCIAS NO CONTEXTO DE PROTEÇÃO DE DADOS PESSOAIS

O decreto 8.771/16 estabeleceu o conceito de dados pessoais no contexto do uso da internet no Brasil, sendo este qualquer *"dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa"* (art. 14, I). A definição deste conceito amplo, bem como a aprovação recente da Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados ("LGPD") – e que traz uma definição semelhante de dado pessoal –, traz importantes consequências para a presente discussão, visto que os dados sobre porta lógica são considerados dados pessoais e, logo, diversos direitos dos usuários podem ser afetados com a adoção da exigência.

A LGPD coloca o Brasil no rol dos países que possuem uma legislação específica sobre proteção de dados pessoais. A legislação surge em um momento de expansão do uso e processamento intenso de dados pessoais, aliado a uma agenda econômica global que objetiva estabelecer padrões mínimos para a coleta e o processamento de dados pessoais de forma adequada, com o objetivo de proteger direitos e liberdades fundamentais, além de desenvolver a economia e promover a inovação. A Lei, que entra em vigor em agosto de 2020, traz a Autoridade Nacional de Proteção de Dados como responsável por fiscalizar a aplicação da legislação e garantir que os direitos e garantias postulados na Lei estejam sendo respeitados.

Nesse contexto, tanto o MCI (art. 7°, VII e art. 16, II) quanto a LGPD (art. 6°) estabeleceram o **princípio da necessidade**[13] para uso de dados pessoais que, em

[13] Art. 6°, III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

suma, estipula que a coleta de dados deve se dar de maneira restritiva, considerando para o tratamento apenas os dados pessoais estritamente necessários ao atendimento da finalidade pretendida, sendo vedada, então, a coleta excessiva.

A criação dessa obrigação iria na contramão do fomento ao ecossistema de proteção de dados, incentivando que os provedores armazenem mais dados que o essencial para exercer suas atividades, além de determinar a retenção de mais dados do que os estritamente necessários para finalidade de identificação almejada por meio da análise de registros de conexão. Tendo em vista a preocupação da legislação brasileira em limitar a coleta e o tratamento de dados pessoais com o intuito de proteger a privacidade do usuário titular do dado, **exigir judicialmente o armazenamento e a entrega de um dado pessoal cuja obrigação não se encontra prevista no MCI ou em qualquer outra lei, e que não é estritamente necessária, significa não só criar uma obrigação de fazer excessiva e sem baliza legal, mas também criar, via Judiciário, uma obrigação que viola outros princípios da legislação.**

Trata-se de uma posição coerente com o cenário internacional. Em 2014, o Tribunal de Justiça da União Europeia ("TJUE") proferiu um julgado em que declarou inválida a Diretiva 2006/24/EC14, conhecida como diretiva de retenção de dados, e que obrigava provedores a reterem dados de comunicação eletrônica com o objetivo harmonizar as obrigações de provedores de internet no que tange à retenção de dados para fins de investigação e persecução criminal. A corte concluiu que a retenção dos dados listados na Diretiva 2006/24/EC era uma obrigação excessiva, pois, embora o seu artigo 5º (que listava as categorias de dados a serem armazenados) não incluísse o conteúdo das comunicações, o simples fato de mapear todos os dados listados no rol do referido artigo gerava risco para o usuário de violação de seus direitos à privacidade, à proteção de dados pessoais e outras liberdades fundamentais, dada a quantidade de dados excessivamente e desproporcionalmente armazenados.

Dessa forma, o princípio da necessidade, assim como o da adequação, que determina que os dados pessoais devem ser tratados levando em consideração o contexto do tratamento e as finalidades legítimas almejadas, em conjunto, restringem a lógica de que quanto mais dados se coletar, melhor. O princípio da necessidade prescreve, ainda, que na ocasião de mais de um tipo de dado pessoal ser necessário para atingir a mesma finalidade, deve-se escolher por àquele que seja menos intrusivo, ou que não demande uma maior coleta de dados. No caso das portas lógicas, há outros tipos de dados já existentes, como o endereço IP, data e hora, já permitem um amplo atingimento da finalidade de identificação. Determinar a coleta de mais dados seria uma violação expressa a este princípio regente da lógica de proteção dos dados pessoais e das liberdades fundamentais.

Em um julgado seguinte, a Corte de Justiça da União Europeia, partindo da lógica do caso que invalidou a diretiva de retenção de dados, determinou que "os Estados-Membros não podem impor a provedores uma obrigação genérica de reter dados relativos a serviços de comunicação eletrônica"[15]. Em suma, como dito pela corte em seu julgamento, a coleta de dados da forma almejada "excede os limites do que é estritamente necessário e não pode ser considerada justificada dentro de uma sociedade democrática"[16].

Desta forma, forçar provedores a coletarem e armazenarem mais dados que os estritamente necessários na concretização de suas atividades violam os princípios de proteção de dados do MCI e da LGPD, indo na contramão de leis, princípios e diretrizes de proteção de dados pessoais no mundo.

5/ DESENVOLVIMENTO TECNOLÓGICO

Parece-nos claro que qualquer decisão que obrigue provedores a armazenar um dado que não é exigido, por lei, consubstancia-se em direta afronta ao princípio da legalidade (art. 5º, II, da Constituição Federal), além de um perigoso precedente para ampliar cada vez mais o escopo de exigências de armazenamento para provedores.

Esse ciclo vicioso é ruim para todo o modelo de inovação, gerando incertezas que podem ter um grande impacto econômico e social, e que podem gerar ao menos duas consequências negativas para a internet no Brasil.

A primeira delas é a redução de espaços para experimentação tecnológica. Conforme sugerem Wernick e Picot[17] (2007), do ponto de vista de provedores de conexão e de aplicações, segurança jurídica e estabilidade do marco regulatório são em geral fatores mais relevantes para a decisão sobre a realização ou não de investimentos do que o próprio conteúdo da regulação em si. Uma jurisprudência que altere conceitos já definidos em lei e gere margem de dúvidas sobre quais dados devem ou não ser guardados por provedores faz com que não sejam criados incentivos para inovações tecnológicas tanto na fase de transição do IPv6, quanto após a sua consolidação, afastando inclusive a entrada de investimentos no setor. Perceba-se, assim, a incerteza que essa situação pode gerar

[14] Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others. PRESS RELEASE No 54/14. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

[15] Tradução livre: "The Members States may not impose a general obligation to retain data on providers of electronic communications services", Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och, telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf>.

[16] Tradução livre: "exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society", idem.

para a criação de novas tecnologias que possam vir a substituir ou aprimorar o sistema NAT, o uso de portas lógicas e o próprio padrão TCP/IP.

A segunda consequência é o próprio custo regulatório[18]. Embora este seja um tema pouco explorado na literatura nacional, houve uma preocupação do Marco Civil em aplicar a ideia de neutralidade tecnológica[19], isto é, restringir ao mínimo possível as questões técnicas relacionadas com a regulação da rede, evitando assim criar situações de rigidez que poderiam impedir a inovação tecnológica, caducar rapidamente ou, ainda, criar custos excessivos para a aplicação da lei. Logo, questões técnicas que dependem unicamente do Judiciário para serem resolvidas demandam um enorme período de tempo para que sejam pacificadas, consomem recursos importantes, como contratação de peritos e advogados, e dificilmente um caso específico seria suficientemente vinculante a outros casos semelhantes[20] (Magill, 2004), além de potencialmente privilegiar atores com mais recursos financeiros, prejudicando usuários e startups[21] (Sunstein, 1995).

Sobre startups, é importante ressaltar este ponto, já que este custo regulatório sem dúvidas atingiria de forma mais dura as pequenas empresas, que dependem de um ambiente regulatório equilibrado, seguro e previsível, para lidar com os altos riscos relacionados ao investimento no desenvolvimento de produtos e serviços de caráter inovador. A ampliação das obrigações de retenção de dados abalaria a livre concorrência e a liberdade de iniciativa e, portanto, a possibilidade de inovação que atualmente se observa no mercado de tecnologia, em especial pela evidente diferença de recursos financeiros e operacionais que existe entre startups e grandes empresas, o que geraria uma barreira de entrada ainda maior dessas pequenas empresas no mercado, favorecendo a concentração da inovação, e prejudicando a distribuição de riqueza.

A inovação também precisa ser um direcionamento institucional para decisões judiciais. A capacidade de um país em gerar inovações deve ser vista não como uma política de governo, mas sim como um mandamento de Estado, reforçado pela própria Constituição (art. 218), envolvendo todos os Poderes. Nesse sentido, Celso Furtado pontua que uma das características centrais do desenvolvimento de um determinado país está na capacidade deste em produzir inovações tecnológicas: “Nada é mais característico da civilização industrial do que a canalização da capacidade inventiva para a criação tecnológica, ou seja, para abrir caminho ao processo de acumulação”[22].

[17] WERNICK, C.; PICOT, A. Strategic Investment Decisions in Regulated Markets: Relationship Between Infrastructure Invest. and Regulation in European Broadband. Wiesbaden: Deutscher Universitätsverlag, 2007.

[18] Nesse sentido, ver KAPLOW, L. General Characteristics of Rules. Encyclopedia of Law and Economics. Northampton: Edward Elgar Publishing, 1999, e PIERCE, R. Administrative Law Treatise. 5. ed. New York: Aspen Publishers, 2010.

[19] RAMOS, op. cit.

[20] MAGILL, J. Agency Choice of Policymaking Form. The University of Chicago Law Review, v. 71, n. 4, 2004.

[21] SUNSTEIN, C. R. Problems with rules. California Law Review, p. 953-1026, 1995.

6/ CONCLUSÃO

A definição acerca do armazenamento de portas lógicas por provedores de aplicação é importante para a segurança jurídica, proteção de dados pessoais e fomento à inovação no Brasil. Destarte, partindo dos diversos argumentos trabalhados neste documento, entendemos que é inexistente a obrigação de armazenamento das portas lógicas por provedores de aplicação, seja em razão da aplicação gramatical ou teleológica no MCI, seja em razão das consequências que uma decisão no sentido contrário pode trazer.

As portas lógicas não são as únicas e determinantes informações para conseguir a identificação de um indivíduo – mesmo com o sistema NAT, os dados que o MCI previu como dados essenciais (IP, data e hora) já são suficientes para identificação, uma vez que é praticamente impossível que dois usuários se conectem e desconectem em um mesmo horário, além do fato de que tais dados podem ser cruzados com outros presentes no contexto do cenário identificado, como informações de login e outros identificadores únicos.

Dessa forma, estender a interpretação do artigo 15 do MCI, para apenas facilitar a identificação, além de configurar violação a princípios constitucionais, impacta a segurança jurídica e, como consequência, também viola deveres do Estado de promoção da inovação e do respeito à intimidade e privacidade dos usuários.

Sendo assim, parece nos claro que:

(i)Não deve ser estabelecida a obrigação de armazenamento de portas lógicas aos provedores de aplicação;

(ii) a obrigação de armazenamento das portas lógicas de origem por provedores de aplicação é uma imposição **sem amparo legal** e **com consequências adversas sérias** ao ecossistema de inovação brasileiro;

(iii) desde a elaboração do Marco Civil da Internet, o esgotamento do IPV4 jáhavia sido pautado como questão de relevância social, e mesmo assim **o legislador conscientemente optou por não mencionar no texto legal a obrigação de armazenamento das portas lógicas;**

(iv) o entendimento majoritário dos Tribunais consubstancia a tese contrária ao armazenamento de portas lógicas por provedores de aplicação, alegando não haver previsão legal que ampare a obrigação;

(v) a imposição de armazenamento levaria a **relativização do princípio da legalidade,** com a exigência de obrigação impossível aos provedores de aplicação;

(vi) a obrigação de armazenamento das portas lógicas levaria a construir entendimento jurisprudencial que vai **na contramão dos princípios de proteção de dados pessoais,** tanto nacionais quanto internacionais, colocando em xeque o princípio da proteção à privacidade; e

(vii) esta imposição também traria **onerosidade excessiva** às empresas de tecnologia, gerando um fundado risco ao setor de inovação brasileiro.


BAPTISTA LUZ
ADVOGADOS
WWW.BAPTISTALUZ.COM.BR