**Universidade de Brasília**
**Faculdade de Direito**

**Felipe Fonseca Coutinho**

# A guarda preventiva de logs no Marco Civil da Internet: uma análise comparada à jurisprudência europeia sobre proteção de dados pessoais

**Brasília**
**2016**

**FELIPE FONSECA COUTINHO**

# A guarda preventiva de logs no Marco Civil da Internet: uma análise comparada à jurisprudência europeia sobre proteção de dados pessoais

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, como requisito para a conclusão do curso de graduação em Direito, sob a orientação da Professora Laura Schertel Mendes.

**Brasília**
**2016**

# A guarda preventiva de logs no Marco Civil da Internet: uma análise comparada à jurisprudência europeia sobre proteção de dados pessoais

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, como requisito para a conclusão do curso de graduação em Direito, sob a orientação da Professora Laura Schertel Mendes.

Aprovada em 05/12/2016

_____

Prof. Dra. Laura Schertel Mendes
Universidade de Brasília

_____

Prof. Dr. Alexandre Kehrig Veronese Aguiar
Universidade de Brasília

_____

Prof. Me. Thiago Luís Sombra
Universidade de Brasília

BRASÍLIA- DF
2016

## RESUMO

O presente estudo tem como objetivo analisar a instituição no Marco Civil da Internet do dever de guarda de logs para os provedores de aplicação e de conexão, a partir da comparação dos fundamentos que balizaram os recentes julgados de tribunais europeus, quais sejam, o Tribunal de Justiça da União Europeia e o Tribunal Federal Constitucional Alemão, quanto a Diretiva 2006/24/EC e a Lei de Telecomunicações Alemã,no que se refere à proteção dos dados pessoais e da privacidade. Partindo do pressuposto de que a Constituição Federal de 1988 tem como fundamento a dignidade da pessoa humana e outros valores fundamentais, busca-se verificar de que forma foi sancionada a regulação e as medidas técnicas de segurança no Decreto 8.771/16 e, seda forma como foi posta, não extrapola o limite e se caracteriza em uma violação ao direitos fundamentais dos cidadãos que utilizam da rede em território nacional.



Palavras-chave: Marco Civil da Internet, Lei nº 12.965/2014, provedores, dados pessoais, direito à privacidade, Marco Civil da Internet, guarda, preventiva, logs, registros de conexão, registros de aplicação, jurisprudência europeia, princípio da proporcionalidade, regulação, Decreto 8.771/16.

ABSTRACT

This paper analyzes the duty of Internet Service Providers (ISPs) and Application Service Providers (ASPs) as a precautional measure to retain metadata, such as connection logs and application logs, for a certain period of time, imposed by the Brazilian Civil Rights Framework for Internet, specifically in the respect for private life and the protection of personal data. This intends to be done by comparing its shape to the legal fundaments exposed in recent decisions of European Courts about the Directive 2006/24/EC and the German Law that internalized the directive. Assuming the fact that the Brazilian Constitution is founded on the principle of human dignity and other fundamental values, the focus is to verify under which circumstances the regulation and the technical protection measures were sanctioned and if these configure a encroachment and a violation of fundamental rights of citizens that use the net in Brazilian national territory.

Key words: Brazilian Civil Rights Framework for the Internet, personal data, internet service providers, data retention, connection logs, comparison, analyses, european jurisprudence, regulation, Directive 2006/24/EC, proportionality principle, technical safety measures.

**SUMÁRIO**

# 1) Introdução

A forma como as sociedades se relacionam vem se alterando drasticamente nas últimas décadas, desde o fim do século XX até o presente momento do século XXI, em razão do contexto de rápido desenvolvimento tecnológico e de facilitação da comunicação, atingindo um nível de celeridade de troca de informações não sonhado anteriormente.

Em grande medida, a popularização da Internet, neste mesmo período, contribuiu como ponto crucial de transição, deixando de ser uma rede restrita a pesquisadores para se tornar amplamente comercial, ao preconizar como fundamento o fomento de um ambiente de livre expressão dos indivíduos e aberto a criações que contribuíssem para a otimização da comunidade em rede.

Além das inegáveis benesses advindas desse processo tecnológico irreversível, surgiram novas problemáticas, entre elas, como responsabilizar um indivíduo pela prática de ilícitos em um ambiente com uma arquitetura viabilizadora de infinitas possibilidades de anonimização de sua pessoa? Ou então, como um indivíduo pode manter o controle das informações sobre si que circulam na rede e que são coletadas e tratadas para fins diversos aos explicitados pelos provedores de serviço de internet, provedores de conteúdo, de correio eletrônico e outros?

Nesse intrincado jogo de poderes assimétricos, em que o refinamento qualitativo e quantitativo de informações passíveis de serem extraídas a partir dos dados gerados a todo momento se torna monetizável e extremamente rentável para tomada de decisões pelos mais diversos agentes estatais e privados, põe-se novamente à luz a necessidade de ser discutido qual a aplicação dos direitos e deveres dos usuários no âmbito da internet, especificamente quanto ao direito à privacidade e à proteção dos dados pessoais frente ao direito a segurança pública e a reparação e responsabilização de eventos danosos.

Com os desafios postos, ainda que a ideia tradicionalista de controlar por meio de uma legislação não seja mais tão eficaz para fazer frente às rápidas mudanças de códigos e protocolos, dependendo do tipo de regulamentação estatal realizada, esta torna-se em certo grau um dos meios viáveis de retomada da autodeterminação informativa, de proteção do sigilo dos dados, de combate à discriminação, promovendo um ambiente igualmente democrático.

Recentemente, foi promulgada no Brasil legislação noticiada pelos veículos de comunicação como a "Constituição da Internet do Brasil", a Lei 12.965/14, por ter definidos

princípios, conceitos, fundamentos, direitos e deveres dos usuários, que devem ser seguidos para a utilização democrática da internet.

Mas estes não foram os únicos pontos positivados, houve também o estabelecimento de proteções aos provedores de aplicação, como a responsabilização por veiculação de conteúdo gerado por terceiros apenas em caso de descumprimento de ordem judicial específica, em contraposição à teoria importada do *Notice and Take Down* (notificar e retirar), que vinha se firmando na jurisprudência brasileira[1].

No entanto, ponto de igual ou maior relevância, e que põe em xeque a inviolabilidade do direito à intimidade e vida privada, disposto no artigo 5º, inciso X da Constituição Federal de 1988, e a proteção dos dados pessoais, é a obrigação de que provedores de acesso e de aplicação retenham, por um período legalmente determinado, os logs de conexão e aplicação, isto é, registros de conexão e aplicação, no caso de eventual interesse no acesso a esses meta dados pelas autoridades estatais.

Tendo em vista que essa realidade brasileira se insere no contexto internacional de estabelecer por meio de regulamentos prazo e procedimentos para legitimar a retenção preventiva de logs, o objetivo da presente monografia é responder à seguinte pergunta:

Levando em consideração a análise feita pela jurisprudência europeia sobre esse tipo de retenção, o Marco Civil da Internet e o Decreto 8.771, ao estatuírem a guarda preventiva de dados por tempo determinado, atenderam aos padrões de segurança técnicos e procedimentos claros para a proteção em última medida da privacidade para o desenvolvimento da personalidade dos usuários da rede?

Fixando nosso objeto de estudo, o que se pretende mostrar, em verdade, é o que fez, afinal, o Marco Civil da Internet e o Decreto 8.771/16, que regulamentou medidas de segurança para a guarda de logs, para garantir que estas informações estejam protegidas em toda a cadeia de tratamento, da coleta até a exclusão ao fim do período legal. Mais do que isso, pretende-se mostrar quais foram os procedimentos adotados para o acesso a esses dados, quem pode acessá-los se as medidas de segurança atendem aos padrões de segurança internacionais.

Para tanto, iniciamos o trabalho fazendo uma breve síntese histórica do desenvolvimento das normas de proteção de dados pessoais na União Europeia até a edição da Diretiva de Retenção de Dados 2006/24/EC.

---

[1]SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou Retrocesso? A Responsabilidade Civil por Dano derivado do Conteúdo Gerado por Terceiro. Disponível em http://www.andersonschreiber.com.br/downloads/artigo-marco-civil-internet.pdf

A partir de então, questionar-se-á na mesma oportunidade a constitucionalidade da obrigação de retenção preventiva pelos provedores frente ao embate com os direitos a privacidade e proteção de dados pessoais, baseando-se na decisão emblemática da Corte Constitucional Alemã que declarou inconstitucional, com efeitos *ex tunc*, a norma que internalizou a diretiva naqueles moldes.

Ainda no primeiro capítulo será abordada a recente decisão de 2014 do Tribunal de Justiça da União Europeia, após os questionamentos feitos no reenvio prejudicial do tema pela Corte Austríaca e o Supremo Tribunal Irlandês, que indagaram acerca da validade da Diretiva 2006/24/EC em relação às limitações aos direitos fundamentais, assim disposto na Carta dos Direitos Fundamentais da União Europeia

Em sequência, no segundo capítulo, a partir da compreensão da jurisprudência europeia, marcada fundamentalmente por uma cultura de assegurar a efetividade do direito à proteção de dados pessoais e à privacidade, procuramos mostrar qual é a configuração atual do cenário brasileiro, no que se refere à análise do dever de retenção de registros de conexão e aplicação, tendo em vista que o tema foi tratado no Marco Civil da Internet e posterior regulamentação no decreto 8.771/16.

Observamos inicialmente que a Constituição brasileira de 1988 é classificada como dirigente e incorpora em seu texto valores emanados da comunidade política. O Estado, portanto, tem o dever de agir para cumprir os objetivos para o qual foi criado, como a construção de uma sociedade livre, justa e solidária.

Partindo do pressuposto de que a nossa Carta Constitucional tem como fundamento a dignidade da pessoa humana e outros valores fundamentais, pretende-se analisar se a legislação, na forma em que foi sancionada, não extrapola o limite e se configura em violação ao direitos fundamentais.

Desde já é necessário deixar claro que o debate não se limita apenas ao comumente associado, qual seja, direito à privacidade versus direito a segurança pública, mas amplia-se para o diálogo imprescindível entre segurança da informação e segurança pública.

O acesso a essas informações, contudo, não pode ocorrer ao sabor do Estado, sempre ávido por uma estrutura de poder para guiar a tomada de suas decisões e especificamente, no que se refere ao tema abordado, a responsabilização de ações ilícitas cíveis e penais. Por isso a análise perpassa tanto em que medida os órgãos estatais agem nos limites de poder que lhes é conferido, quanto se o procedimento de acesso garante que as

informações colhidas atendem ao princípio da finalidade e preservam a privacidade dos cidadãos.

O capítulo é iniciado abordando em que circunstâncias o Marco Civil da Internet foi promulgado, considerando que projetos semelhantes sobre o tema tramitavam a mais tempo.

A partir daí, analisar-se-á detalhadamente quais foram os pontos trazidos pelo novo regramento que fortaleceram a proteção dos dados e quais contribuíram negativamente, seja por manter-se silente sobre aspecto essencial ou pela ausência de clareza, possibilitando interpretações dúbias que não se coadunam com o texto constitucional.

No terceiro capítulo pretende-se apresentar soluções aos problemas oriundos do Marco Civil da Internet e pelo Decreto 8.771/16, para que o ordenamento jurídico brasileiro esteja em consonância com o direito a proteção dos dados pessoais, à privacidade e ao sigilo dos dados.

Será tratado brevemente também o novo paradigma que vem sendo construído, em especial, a Internet das Coisas e as implicações quanto à obrigatoriedade dos registros de conexão e aplicação dos novos dispositivos conectáveis.

Por fim, será abordada a importância de se construir uma cultura de proteção de dados no território nacional. Afinal, diante da atualidade da discussão acerca da proteção de dados pessoais, relegá-la tem diversas consequências econômicas, sociais, políticas e jurídicas, colaborando para a permanência em um ambiente de insegurança jurídica para todos os setores envolvidos, em especial, para o cidadão.

## 2) Sistema de Proteção de Dados Pessoais e a Jurisprudência Europeia

## 2.1)Breve panorama de Proteção de Dados Pessoais na União Europeia

Compreende-se dado pessoal como qualquer dado referente a uma pessoa singular identificada ou identificável, estando vinculadas a características e ações de um sujeito de direitos, ou seja, capazes de revelar elementos objetivos[2], por exemplo, a identidade física, psíquica, econômica, cultural ou social.

Considerando a importância dessas informações para o desenvolvimento da personalidade do indivíduo[3], sua tutela se mostra um dever para concretização dos mais diversos projetos de vida no plano de sociedades pluralistas alicerçadas sob a égide do Estado Democrático de Direito.

Foi sob essa perspectiva que se desenvolveu e consolidou-se uma base de proteção de dados pessoais na União Europeia, em relação ao tratamento e circulação de dados, estabelecida em 1995, com a aprovação da Diretiva 95/46/CE.

Conforme disposto no art. 1º, seu objetivo primordial era garantir a proteção às liberdades e direitos fundamentais dos cidadãos, especificamente quanto a dimensão do direito à privacidade, através da harmonização de leis entres os Estados Membros do bloco, voltando-se a prevenir abusos cometidos tanto pelo mercado quanto pelo Estado.

Para alcançar sua finalidade, foram definidos não só conceitos essenciais com vistas à melhor compreensão da matéria, tais como o que se entende por tratamento de dados pessoais, o consentimento, mas também princípios referentes à legitimidade do tratamento e a qualidade desses dados, além de um rol de garantias ao titular dos dados.

Como consequência da padronização, a transferência dos dados foi facilitada entre os Estados Membros, tendo em vista que o alinhamento no alto nível de proteção implementado adequou-se aos requisitos de segurança usualmente exigidos nas legislações nacionais. Deste modo, a restrição à livre circulação de dados nos países integrantes da União Europeia ocorreria em situações excepcionais previamente definidas.

Todavia, a introdução de novos serviços de comunicações eletrônicas e o acesso à *internet,* tendente a cada vez mais se massificar no modelo da sociedade da rede, tornou perceptível a necessidade de regulamentar este tipo de tratamento de dados pessoais em um

[2]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª. ed. Rio de Janeiro: Renovar, 2006. p. 157

[3]SCHREIBER, Anderson. Direitos da personalidade - São Paulo: Atlas, 2011. p. 131-132

instrumento legal específico, diante do alto grau de capacidade de processamento que as redes digitais possuem e a inerente possibilidade de violação aos direitos dos usuários.[4]

Assim, foi aprovada a Diretiva 2002/58/CE, que entre seus pontos fulcrais, estabeleceu no art. 6º que os dados de tráfego tratados e armazenados pelo provedor de uma rede pública de comunicações ou de um serviço de comunicações eletrônicas publicamente disponíveis deveriam ser eliminados ou tornados anônimos quando deixassem de ser necessários para efeitos da transmissão da comunicação.

A referida diretiva, em contraposição, também previu que excepcionalmente os Estados Membros poderiam editar disposições legislativas para restringir os direitos e obrigações supracitados. Isto ocorreria quando a medida fosse estritamente necessária para garantir a segurança nacional, a defesa, a segurança pública, a prevenção, a investigação, a detecção e a repressão de infrações penais, em consonância com o pilar basilar europeu de proteção de dados pessoais[5] e com o art. 52 (1) da Carta de Direitos Fundamentais da União Europeia, que estabelece:

> Art. 52 – Âmbito dos direitos garantidos
>
> 1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efectivamente a objectivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

É necessário ressaltar que em ambas as diretivas o âmbito de aplicação abarcou apenas questões de direito comunitário, não se expandindo a assuntos de cooperação de justiça e persecução criminal, que deveriam ser regulados por outros instrumentos legais[6] no contexto do bloco, razão pela qual alguns países já haviam adotado medidas para tal limitação.

Todavia, apenas após os ataques terroristas ocorridos em Madrid (2004) e Londres (2005) que a proposta de utilização de dados coletados por provedores de comunicações eletrônicas como ferramenta em investigações criminais e cooperação internacional tornou-se

---

[4] União Europeia. DIRETIVA 2002/58/CE. Exposição de motivosnº4. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT

[5] União Europeia. Diretiva 95/46/CE. Art. 13, nº 1. Disponível em http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf

[6] European Union Agency for Fundamental Rights. Council of Europe.Handbook on European Data Protection Law. 2014, pág 19, http://www.echr.coe.int/documents/handbook_data_protection_eng.pdf

pauta prioritária no Conselho Europeu[7], resultando na aprovação da Diretiva de Retenção de Dados (Diretiva 2006/24/EC).

A partir de então, os países tiveram um prazo de 2 anos para internalizar a diretiva em seus ordenamentos jurídicos, que impôs aos provedores de serviço de comunicação e internet o dever de guarda de logs dedados de todos os indivíduos e entidades legais por um período de seis meses até dois anos, para que, caso necessário, fossem utilizados pelas autoridades nacionais competentes, para efeitos de investigação, repressão de crimes graves tal como definidos no direito nacional de cada Estado.

Ao não definir o que constituiriam tais crimes, foi aberta a possibilidade de que os países ampliassem o escopo de condutas passíveis de acesso aos dados retidos, por meio de um conceito aberto e maleável por cada legislatura nacional[8],

No que diz respeito ao acesso à internet, aos serviços de e-mail e às comunicações telefônicas por meio da internet,foi delimitado o que o log de dados deveria abarcar e entre eles compreendiam[9]: o código de identificação do usuário, o nome e o endereço do assinante, a quem o endereço do protocolo de IP estava registrado ou ao número de telefone estavam atribuídos no momento da comunicação; a data e hora de início (*log-in*) e do fim (*log off*) de acesso a internet, juntamente com o endereço do protocolo de IP, dinâmico ou estático atribuído pelo provedor do serviço de acesso à internet, bem como o código de identificação de utilizador do subscritor ou do utilizador registrado; a data e hora do log in e log off do serviço de e-mail ou das comunicações telefônicas através da internet; etc.

De acordo com a Diretiva de Proteção de Dados, toda essa atividade estaria compreendida dentro de tratamento de dados pessoais, que é conceituado como qualquer operação ou conjunto de operações realizadas sobre dados pessoais, automatizadas ou não, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, bloqueio, destruição e outras.

Na seara do tratamento de dados, é imprescindível conceituar log de dados para aprofundar na discussão das implicações que essa retenção pode gerar. Bernard Jansen[10]

[7]POLI, SARA, The Legal Basis of Internal Market Measures With a Security Dimension. Comment on Case C-301/06 of 10/02/2009, pág 141

[8]TZANOU, Maria, Is Data Protection the same as privacy?An Analysis of Telecommunications Data Measures, Journal of Internet Law, September 2013, pág. 22

[9] União Europeia. Diretiva 2006/24/EC. Art. 5º. Disponível em http://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX:32006L0024&qid=1462090129997

[10]JANSEN, Bernard J. Search log analysis: What it is, what'sbeendone, howto do it.Library&Information Science Research 28 (2006) pág. 408

afirma que log de dados é caracterizado pelo arquivo de registro de determinadas atividades em um sistema computacional de um usuário deste sistema.

Com esses metadados armazenados, por exemplo, os provedores de acesso a internet são capazes de traçar o comportamento de determinado assinante de seu serviço de conexão, como em que período do dia usualmente ele se conecta, quantos dados gasta em determinado período para efeitos de emissão de fatura, em que local ocorre o acesso a partir do ip a ele denominado.

Constata-se que foi expressamente delimitada a inaplicabilidade da norma em relação ao acesso especificamente ao conteúdo das comunicações eletrônicas, pois, seria uma clara violação ao direito à privacidade e o direito a proteção de dados pessoais[11], definidos na Carta Europeia de Direitos Fundamentais.

Ainda assim, representantes do Parlamento Europeu, autoridades em proteção de dados e ONGs[12] como Electronic Frontier Foudantion (EFF) e European Digital Rights (EDRi)[13] se opuseram ao modelo de retenção desses metadados, por considerarem uma excessiva vigilância sopesada sob os cidadãos europeus.

Conforme constata Laura Schertel:

> Afinal, a tecnologia não se encontra em um vácuo, devendo ser compreendida a partir do meio social, econômico e político em que está inserida. Isso porque a própria tecnologia é criada pela sociedade para atingir determinados fins e o grau de sua regulação é estabelecido pela sociedade que a criou. Nesse sentido, é fundamental que o debate sobre proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a ideia de que ela é a responsável pela perda de privacidade pessoal da sociedade contemporânea. Isto é, não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia[14].

Tendo em vista as controvérsias apontadas na Diretiva de Retenção de Dados, serão abordados dois casos paradigmáticos e os fundamentos que parametrizaram as decisões do Tribunal Federal Constitucional Alemão (*Bundesverfassungsgericht),* em 2010, e posteriormente, da Corte de Justiça da União Europeia (CJEU), em 2014, quanto a guarda de logs por provedores de serviço de telecomunicação.

[11]União Europeia. Carta de Direitos Fundamentais da União Europeia. Art. 7º e 8º.
[12]Loideain Nora Ni.EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era Media and Communication, 2015, Volume 3, Issue 2
[13]Mandatory Data Retention.Disponívelem https://www.eff.org/issues/mandatory-data-retention
[14] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito do consumidor. 1ª Edição. São Paulo:Saraiva, 2014, p.35.

## 2.2) A emenda à Lei de Telecomunicações Alemã e a decisão do Tribunal Constitucional Federal Alemão

A Alemanha, país marcado desde a década de 70 pelo comprometimento com a proteção aos dados pessoais e ao direito à privacidade, contribuiu em grande medida para o desenvolvimento das discussões acerca do tema,sob o prisma de que aquelas constituem uma projeção da personalidade do indivíduo, nos termos do art. 2 I da Lei Fundamental Alemã.

Exemplificativamente reputa-se[15] ao julgamento da "Lei de Recenseamento de População, Profissão, Moradia e Trabalho", pelo Tribunal Constitucional Alemão em 1983, comoumdosmarcos referenciais da teoria de proteção de dados pessoais, ao reconhecer um direitosubjetivo fundamental que alçou o indivíduo ao patamar de protagonista no processo do tratamento de seus dados, o reconhecido direito à autodeterminação informativa.

O Parlamento Alemão cumpriu com suas obrigações perante o bloco europeu ao internalizar a diretiva em dezembro de 2007, com a promulgação da Lei de Vigilância das Telecomunicações e outras Medidas de Investigações Secretas (Gesetz zur Neuregelung der Telekommunikationsüberwachung *und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*), que emendou a Lei de Telecomunicações Alemã (Telekommunikationsgesetz - TKG) e também o Código de Processo Criminal (*Strafprozessordnung*– StPO).

Concretamente,requereu-se que os provedores de serviços de telecomunicações, aqui também incluídos os provedores de acesso a internet (PSIs), teriam de preventivamente armazenar, optando pelo mínimo requerido,durante6 meses, os já especificados registros de tráfego e localização de dados de seus usuários e assinantes.

Além disso, foi estabelecido em quais condições as autoridades poderiam ter acesso a esses registros: para a persecução de crimes; para repelir perigos substanciais à segurança pública; para execução dos deveres estatutários das autoridade da Federação e do Estados na proteção da Constituição, do Serviço Federal de Inteligência e do Serviço de Contra-Inteligência Militar; e, quando as autoridade competentes requeressem, na extensão das disposições estatutárias relevantes e a transmissão tenha sido ordenada em caso individual[16].

---

[15]MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito do consumidor. 1ª Edição. São Paulo:Saraiva, 2014, p.31

[16]ALEMANHA. Lei de Telecomunicações (Telekommunikationsgesetz), § 113a and § 113b.

No entanto,como Anna-Bettina Kaiser[17] afirma, para sociedade alemã a proteção de dados e da privacidade estaria simbolicamente no mesmo patamar valorativo de proteção à vaca sagrada para os indianos, razão pela qual, em março de 2008, a expressiva quantia de 34.000 reclamações constitucionais[18] foram submetidas visando questionar a emenda feita à Lei de Telecomunicações e à própria Diretiva 2006/24/EC.

A Corte considerou preenchidos os requisitos de admissibilidade dos reclamantes que alegaram que a emenda violaria o respeito ao direito de sigilo das correspondências e das telecomunicações, disposto no art. 10.1 da Constituição Alemã, mesmo que o dever de guarda não fossem a eles direta e pessoalmente direcionados como usuários, mas sim aos provedores, sendo desta forma partes legítimas para ajuizamento da reclamação.

E também considerou admissível os reclamantes no bojo dos provedores, como aqueles voltados para a anonimização de dados, pois, estas consideravam que tal obrigação violaria também a liberdade de exercício de profissão, consagrado no art. 12.1 da Lei Fundamental Alemã, na medida em que a partir de então criar-se-iam dificuldades de ordens técnicas e financeiras,suportadas como resultado do dever de retenção, sem que houvesse qualquer compensação clara por parte do Estado, podendo serem submetidas a sanções administrativas como multas pela não observância do dever legal.

A jurisprudência alemã entende que a proteção ao direito fundamental do sigilo das comunicações abrange não só o conteúdo destas, mas está intrinsecamente relacionada às circunstâncias do processo de comunicação, isto é, inclui-se os procedimentos e medidas técnicas de tratamento dos dados, a finalidade para acesso pelas autoridade estatais.

Inicialmente, a Corte Constitucional vislumbrou que os dispositivos questionados cumpriram formalmente[19] o requerimento de uma base legal disposto no art. 10.2 da Constituição Alemã, que admite a restrição ao sigilo das comunicações em casos como em que a limitação seja necessária para a defesa contra um perigo iminente para a existência ou ordem fundamental livre e democrática da Federação ou de um Estado federado, para a proteção da juventude contra abandono ou para a prevenção de delitos, etc:

---

[17] KAISER, Anna-Bettina.*German Federal Constitutional Court:* German Data Retention Provisions Unconstitutional In Their Present Form; Decisionof2March 2010, NJW 2010, p. 833.EuropeanConstitutional Law Review, Outubro 2010. Vol. 6, Iss. 3. Disponível em https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S1574019610300083

[18] ALEMANHA. Tribunal Constitucional Federal Alemão.,BvR 256/08 - §89 ,Julgadoem 02/03/2010disponívelem http://www.bverfg.de/e/rs20100302_1bvr025608en.html

[19] ALEMANHA.Tribunal Constitucional Federal Alemão.BvR 256/08 - §197 ,Julgadoem 02/03/2010disponívelem http://www.bverfg.de/e/rs20100302_1bvr025608en.html

> Lei Fundamental Alemã
> Artigo 10 [Sigilo da correspondência, da comunicação postal e da telecomunicação]
> (1) O sigilo da correspondência, assim como das comunicações postais e da telecomunicação é inviolável.
> (2) Limitações só podem ser ordenadas em virtude de lei. Se a limitação tiver por finalidade proteger a ordem fundamental livre e democrática ou a existência e segurança da Federação e de um Estado federado, a lei pode determinar que a limitação não seja levada ao conhecimento do indivíduo atingido e que, em vez de se seguir a via judiciária, o controle seja efetuado por órgãos principais e auxiliares, nomeados pelos representantes do povo.

Essas limitações são substancialmente constitucionais se atendem propósitos legítimos de interesse público e estejam em consonância com o princípio da proporcionalidade, isto é, se são adequados, necessários e apropriados para atender suas finalidades, de modo que não sejam por si só inconstitucionais e garantam a preservação do núcleo essencial dos direitos fundamentais.

Partindo desta ótica, o propósito de fazer com que a persecução criminal e a prevenção de danos a coletividade se torne mais efetivo é um objetivo legítimo, que a princípio pode justificar certa limitação ao sigilo das telecomunicações, afinal a guarda de logs não é vedada em qualquer circunstância, mas apenas nas situações em que há uma organização/tratamento desproporcional desta coleção de dados que tenham objetivos além daqueles previamente delimitados.

Quanto a proporcionalidade, considerou-se que o período de conservação de 6 meses atenderia o critério, pois, não haveriam formas menos drásticas que habilitaram uma detecção tão ampla e semelhante.

Admite-se que todo o tráfego de dados dos cidadãos seria armazenado, sem relação direta com uma conduta culpável atribuída a eles ou a uma situação de risco, tendo em vista que não se restringiria quais formas de telecomunicações estariam excluídas da obrigação legal. Consequentemente, gerar-se-ia um armazenamento das mais diversas interações diárias, que são cada vez mais indispensáveis para participação da vida social no mudo moderno de sociedades em rede.

Como resultado, a Corte reconheceu que a princípio uma retenção nesses moldes é capaz de criar a sensação ameaçadora de que se está sendo vigiado a todo momento, o que pode prejudicar o livre exercício de direitos fundamentais, como a liberdade religiosa em uma sociedade não laica.

Todavia, o Tribunal Constitucional Alemão rebateu essa alegação afirmando que o dever legal de guarda dos logs não é realizado pelo Estado, mas pelos provedores de

serviço, de forma que esses dados se distribuam em diversas empresas. A priori, os agentes estatais não teriam acesso a esses dados, pois a recuperação em relação a uma evento específico dependeria do requerimento estar vinculado a critérios legalmente definidos, como forma de maior proteção.

Mostra-se insatisfatório este fundamento, pois não é possível inferir que apenas com essas simples guarda pelos provedores seja assegurada a proteção aos cidadãos de uma intromissão indesejada e ilegal a seus dados pessoais.

Como medida prévia para que a guarda de logs seja imposta é indispensável que seja possível e garantido que se dê conhecimento do uso desses dados e que se mantenha limitado às previsões legais, de forma que se leve em conta o peso da extensiva coleção de dados e restrinja a recuperação e seu real uso apenas dos dados que sejam absolutamente necessários[20].

O ponto central da análise da Corte se deu a partir da compreensão que o armazenamento de trafego de dados requer uma garantia legal de uma elevado padrão de segurança de dados, em razão do potencial valor informativo proporcionado pela reunião de tais metadados. Apenas se uma disposição legal suficientemente bem definida houver sido elaborada seria possível que a guarda de logs atendesse aos critérios da proporcionalidade em sentido estrito.

Deve-se ter em mente que os provedores serviços privados atuam a partir da lógica dos seus interesses, especificamente do lucro e da redução de custos, tendo incentivos negativos para garantir a segurança dos dados, quais sejam, notificação de descumprimento da obrigação de fazer, multa e outras penalidades. Em contraponto, há vários atores que possuem grande interesse nessas informações e agem ilegalmente para ter acesso a esses dados e roubá-los.

Como exemplo é possível citar o recente caso noticiado de roubo de dados do Yahoo, em que pelo menos 500 milhões de usuários tiveram suas contas violadas[21]. Soube-se que a empresa considerava de pouco valor a garantia da segurança, considerando tais falhas como parte inerente e ordinária do cotidiano, e que tais custos posteriores seriam absorvíveis[22].

---

[20]ALEMANHA. Tribunal Constitucional Federal Alemão.,BvR 256/08 - §214 ,Julgadoem 02/03/2010

[21]https://www.theguardian.com/technology/2016/sep/22/yahoo-hack-data-state-sponsored

[22] http://www.nytimes.com/2016/09/29/technology/daily-report-latest-hack-shows-yahoos-weak-security-history.html

Meses antes já se suspeitava do ocorrido, tendo em vista que foram postas à venda no mercado negro da Deep Web[23] cerca de 200 milhões de informações sobre contas do Yahoo, por um grupo de hackers. Antes mesmo do ocorrido, foi sob este prisma que a Corte Constitucional Alemã afirmou que "tais exigências de segurança de dados se aplicam tanto para a armazenagem quanto para a transmissão; similarmente, essas efetivas salvaguardas são imprescindíveis para assegurar que os dados sejam devidamente deletados"[24].

Levando em conta o que foi exposto pelos experts na área, a Corte entendeu que entre as práticas a serem adotadas dever-se-ia incluir, a título de exemplo, o armazenamento dos dados em computadores separados não conectados a internet, criptografia assimétrica, um protocolo de acesso seguro, como o princípio dos quatro olhos (segregação das várias funções, verificações cruzadas, dupla assinatura), entre outras medidas. No entanto, a lei básica de retenção de dados não previu medidas técnicas especificas de segurança, deixando-as para serem definidas a partir do que o setor privado entende como necessário.

Por todo o exposto, a Corte concluiu que os novos dispositivos legais da Lei de Telecomunicações não atenderam aos requisitos para que não houvesse uma violação ao direito fundamental de proteção do sigilos das telecomunicações, disposto no art.10.1 da Constituição Alemã, sendo assim considerados desproporcionais.

A inconstitucionalidade se deu primordialmente pela ausência da garantia de um alto padrão de segurança, constitucionalmente necessário, pois apenas foi assegurado de forma genérica que medidas técnicas e organizacionais deveriam ser tomadas, individualmente por cada provedor, para o acesso desses dados pelas autoridades competentes.

Essa escolha legislativa se mostrou problemática, partindo do pressuposto que a maior garantia de proteção acarreta mais gastos para os provedores de serviço, que atuam em condições de concorrência e pressão para diminuir os custos aos usuários finais.

A simples obrigação de que os provedores devessem nomear um indivíduo como autoridade de segurança que fosse criada uma política de segurança não seriam suficientes para atender os critérios de proporcionalidade.

Inicialmente, para que se preenchesse os requisitos seriam necessários, além disso, um sistema de sanções bem definidos que atribuíssem igual valor às violações de segurança e ao próprio dever de guarda. No entanto, a variedade de multas administrativas,

---

[23] http://www.dailymail.co.uk/sciencetech/article-3720699/Is-email-address-password-sale-Hacker-claims-200m-Yahoo-accounts-listed-dark-web-market.html

[24] ALEMANHA. Tribunal Constitucional Federal Alemão.,BvR 256/08 - §222 ,Julgado em 02/03/2010

para aqueles que não cumprissem a obrigação, eram muito maiores no caso das violações do dever de guarda.

Outro aspecto relevante foi que o uso desses metadados para a persecução criminal, de acordo com os padrões estabelecidos, também não seriam compatíveis com o princípio da proporcionalidade, considerando que diferentemente da utilização apenas em crimes graves, especificada pela Diretiva Europeia, não foram listados quais se enquadrariam nestes critérios e, consequentemente, eram aceitas em qualquer tipo de crime.

Com o aumento da importância das telecomunicações e da internet no dia a dia, o uso desses dados perde seu caráter excepcional, e podem ser de grande utilidades para a realização das tarefas persecutórias. No entanto, considerando os direitos fundamentais em questão e os padrões de proporcionalidade, a Corte afirmou que nem toda medida que é útil também é permissível, mesmo que no caso individual seja necessária para a investigação criminal.[25]

Em uma perspectiva de transparência do uso e autodeterminação informativa, que não foram atendidas, seria necessário explicitar que a recuperação desses dados sem o conhecimento da pessoa é exceção e requer uma decisão judicial fundamentada. A regra é, tão logo seja requisitado, o indivíduo tem o direito de ser notificado.

O único fator que atende aos critérios constitucionais da norma é obrigação de uma ordem judicial para recuperação dos dados, somado ao fato que as autoridades não tem acesso direto, mas obriga que os provedores intermedeiem o processo com filtragem e posterior entrega dos logs.

Quanto ao argumento trazido pelos provedores que fornecem a anonimização aos seus usuários, não há qualquer violação constitucional a violação ao livre exercício de profissão, tendo em vista que tais serviços continuam operacionáveis e o objetivo de manter suas identidades protegidas contra hackers e terceiros se mantém inalterada. Essa anonimização só seria desvelada pelas autoridades estatais de acordo com as excepcionais previsões de requerimento legalmente definidas.

Por todos os fundamentos expostos, em 2 de Março de 2010, o Tribunal Constitucional Alemão considerou inconstitucional os dispositivos de retenção de dados da Lei de Telecomunicações da forma em que se encontrada, razão pela qual foram declaradas nulas desde o momento de sua promulgação em 1 de Janeiro de 2008, com a consequente

[25]ALEMANHA. Tribunal Constitucional Federal Alemão.,BvR 256/08 - §222 ,Julgadoem 02/03/2010

eliminação desses metadados pelas empresas provedoras de serviços de telecomunicações privados.

## 2.3)A importância da proporcionalidade como fundamento do acórdão C-293/12 do Tribunal de Justiça da União Europeia

Quatro anos após a Corte Alemã ter se pronunciado pela inconstitucionalidade da norma que seguia a Diretiva 26/2004/EC, o Tribunal de Justiça Europeu firmou seu posicionamento acerca da validade da norma de harmonização dentro do bloco, ao ser questionado pela Suprema Corte da Irlanda e pela Corte Constitucional Austríaca, acerca da possível violação de direitos fundamentais estabelecidos na Carta Europeia de Direitos Humanos e de que modo as limitações a esses direitos são válidas.

Inicialmente, a Organização Não Governamental *Digital Rights Ireland*, que promove a proteção dos direitos cívicos e dos direitos do homem no âmbito das tecnologias de comunicação, interpôs recurso perante a Suprema Corte Irlandesa requerendo a anulação da legislação interna que habilitava as autoridades do país de obrigar a guarda de dados aos provedores e pôs em cheque a validade da Diretiva 2006/24, à luz da Carta dos Direitos Fundamentais e/ou da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

Através do instituto do Reenvio Prejudicial, que permite a uma jurisdição interrogar o Tribunal de Justiçada União Europeia sobre a interpretação ou a validade do direito europeu, logo permite garantir a segurança jurídica através de uma aplicação uniforme do direito dentro do bloco, o Supremo Corte Irlandesa e a Corte Constitucional Austríaca concretamente indagaram:

> (ii) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.o da Carta e no artigo 8.o da [CEDH] ?
>
> (iii) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.o da Carta?

O Advogado Geral do Tribunal de Justiça da União Europeia, em sua análise do caso,não centrou-se na questão da harmonização, mas se a instituição da obrigação de conservação desses registros de dados qualificar-se-ia como demasiada ingerência no gozo dos direito fundamentais, à luz dos artigos 7º e 8º da Carta, respectivamente, o direito ao respeito pela vida privada e o direito à proteção dos dados pessoais.

A partir de uma leitura holística da Carta, o artigo 52, nº 1 exige que qualquer restrição ao exercício de direitos fundamentais seja prevista em lei e que se verifique a observância do princípio da proporcionalidade. Assim, o Advogado Geral afirmou que:

> Nesta perspectiva, a prossecução pelas instituições da União do objetivo pretendido pela Diretiva 2006/24, ou seja, assegurar a disponibilidade dos dados conservados para efeitos de repressão de infrações criminais graves, só pode ser admitida sob a condição de se conciliar, designadamente, com o direito ao respeito pela vida privada[26].

O Advogado concluiu que a finalidade de guarda daqueles dados seria legítimas e atenderiam os objetivos perseguidos. Todavia, mostrou-se dificultoso provar que aquela medida seria a menos invasiva à privacidade para atingir sua finalidade.

Assim, o parecer emitido concluiu que a Diretiva 2006/24/EC seria incompatível e não atenderia os critérios de proporcionalidade porque entre outros motivos procurou apenas implementar uma obrigação aos fornecedores de serviços de comunicações eletrônicas e de internet sem tomar o devido cuidado em igual proporção com as garantias que deveriam regular o acesso aos dados conservados e sua exploração.

Tomando como ponto de partida as conclusões do Advogado Geral, a Corte se debruçou sobre a existência de uma violação aos direitos fundamentais consagrados nos artigos 7º e 8º da Carta de Direitos Fundamentais da União Europeia.

Em princípio, é necessário salientar que a Corte já firmou jurisprudência[27] no sentido de que para demonstrar a existência de uma ingerência no direito ao respeito da vida privada, pouco importa que as informações tenham ou não caráter sensível, ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência.

Percebe-se que tal estrutura legal da União Europeia considerou que o tipo de dados revelado pelos metadados como menos importantes do que os dados de conteúdo. No entanto, como afirma Elitsa Stoeva[28], aqueles também podem revelar uma grande quantidade

---

[26]Conclusões do Advogado-Geral Pedro Cruz Villalón apresentadas em 12 de dezembro de 2013 nos processos apensados C-293/12 e C-594/12http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d51de752300d774c8ab97fb5743d6e0306.e34KaxiLc3eQc40LaxqMbN4Pa3uNe0?text=&docid=145562&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=290518

[27]EUROPA. Tribunal de Justiça da União Europeia. Acórdão nos apensos C-293/12 e C-594/12 § 33. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d51de752300d774c8ab97fb5743d6e0306.e34KaxiLc3eQc40LaxqMbN4Pa3uNe0?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=290518. Acessado em 23/09/2016

[28] STOEVA, ELITSA. The Data Retention Directive and the right to privacy. Academy of European Law.Published online: 23 January 2015 pág. 579

de informações, ainda que não se saiba o conteúdo exato das comunicações, e não deveriam ser subestimados em seu poder de violação da privacidade.

Em consonância com Stoeva, a Corte entendeu que:

> Estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados.[29]

A preocupação de uma vigilância panóptica[30] por parte da sociedade somou-se ao fato de que uma interferência deste tipo além de abrangente demais,pois,em prol da garantia de segurança pública, todos os provedores estavam obrigados a conservar o tráfego de dados sem diferenciação, limitação ou exceção, também permitiu que os dados retidos poderiam ser utilizados posteriormente sem que os usuários fossem informados.

A maior deficiência da Diretiva de Retenção de dados foi sua ausência de previsibilidade e objetividade em diversos aspectos.

Não foram estabelecidos critérios claros para garantir que o acesso e uso dos dados pelas autoridades competentes seria concedidos somente para persecução de crimes graves, atendendo ao princípio basilar da finalidade, de modo a evitar a ocorrência de abusos.Como afirma a Corte, tais garantias são imprescindíveis e ainda mais importante quando os dados pessoais estão sujeitos a tratamentos automáticos e há o risco de acesso ilícito aos mesmo.

Outro ponto problemático e de vagueza explicitado foi a duração de conservação dos dados pelo período de 6 meses a 2 anos de retenção, pois não se baseou em regras precisas para limitar ao que fosse estritamente necessário.

Feiler (2010, p. 10)[31] afirma que em razão da ausência de estudos empíricos que provem que a extensão de dados retidos durante um certo período seja necessário para investigar, detectar ou perseguir crimes graves, não é possível determinar se um período de dois anos ou maior é realmente necessário, em uma perspectiva de proporcionalidade stricto sensu, o que pode configurar uma concreta violação ao direito à privacidade.

---

[29]EUROPA. Tribunal de Justiça da União Europeia. Acórdão nos apensos C-293/12 e C-594/12 §27

[30]BLANCHETTE, Jean-François.Johnson, Deborah G. Data retention and the panoptic society:The social benefits of forgetfulness. Disponívelemhttp://polaris.gseis.ucla.edu/blanchette/papers/is.pdf

[31]Feiler, L., The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, European Journal of Law and Technology, Vol. 1, Issue 3, 2010.

Adiciona-se a este fato que a Diretiva requereu que estes dados fossem mantidos dentro do território da União Europeia, o que poderia inviabilizar a garantia do requerido controle por uma autoridade independente. Loideain [32] considera que a partir dessa compreensão a Corte estabeleceu um direito a soberania dos dados como elemento-chave para que o direito a proteção de dados seja garantido sob o prisma do art. 8 da Carta.

Por fim, falha também ao não garantir a aplicação pelos referidos fornecedores de um nível elevado de proteção e de segurança através de medidas técnicas e organizacionais, e em certa medida autorizar que se leve em conta considerações econômicas na determinação do nível de segurança que aplicariam, no que se refere aos custos de execução das medidas de segurança, pondo em xeque a plena integridade e confidencialidade dos dados em questão.

Em julgamento emblemático, pela primeira vez, o Tribunal de Justiça anulou completamente um instrumento legal a União Europeia, com efeitos *ex tunc,* em razão de sua incompatibilidade com a Carta Europeia de Direitos Fundamentais e não atendimento aos critérios de proporcionalidade.

Tendo em vista que pode-se inferir do acórdão que nem toda medida de retenção de dados é incompatível com os direitos fundamentais protegidos,o julgamento, de forma não usual, forneceu uma mapa claro para que os legisladores do Parlamento Europeu se orientem sobre quais medidas devem ser implementadas para que a guarda de logs de dados sejam realizada, através de uma novo instrumento legal, sem que isso caracterize uma violação à privacidade e à proteção de dados pessoais.

Tomando como ponto de partida ambas as decisões europeias e os fundamentos que delinearam sob quais termos a guarda de logs não fere direito a proteção de dados pessoais e o direito à privacidade, pretende-se analisar concretamente no capítulo seguinte se a recente legislação sancionada no Brasil, qual seja, a lei 12.965/14 (Marco Civil da Internet) e o decreto que a regulamentou, obtiveram sucesso em garantir a segurança dos dados dos cidadão, não somente em um nível individual, mas precipuamente na perspectiva de uma garantia de segurança para a sociedade como um todo.

[32]LOIDEAIN, Nora Ni.EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era Media and Communication, 2015, Volume 3, Issue 2, Pág. 58

# 3) Marco Civil da Internet

## 3.1) O contexto de formulação até a promulgação da Lei 12.965/14

De acordo com dados da Pesquisa Nacional Por Amostra de Domicílios (PNAD), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), desde 2014 mais da metade da população brasileira tem acesso à internet em suas residências[33].

Isso se deu não só pelo incentivo governamental da diminuição dos custos dos computadores e seus componentes,com isenção de impostos como IPI,mas está diretamente ligada à popularização dos smartphones, tablets[34] e pacotes de banda larga móvel acessíveis, que também contribuíram para que em um período de 10 anos o percentual de internautas no território nacional saltasse de 20,9% para 54% da população brasileira.

O paradigma da sociedade da informação, em que se experienciou esta vertiginosa expansão, tornou imprescindível a melhor regulamentação das questões jurídicas que inevitavelmente viriam a surgir no plano digital.

Dentre os diversos projetos que tramitavam no Congresso Nacional, surgiu em 2009, a partir da Secretaria de Assuntos Legislativos do Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro, a iniciativa para a criação do Marco Civil da Internet.

Fabro Steibel[35] (2014, p. 18) narra que ambos se propuseram a fomentar o debate por meio da internet, ao criar de forma pioneira um plataforma para consulta pública integralmente online, dividida em duas fases, que resultou na contribuição de mais de 250 pessoas dos mais diferentes setores(idem, p. 21). Criou-se assim colaborativamente o projeto de lei 2126/11, que veio a ser analisado pelo Congresso e levou em consideração as propostas apresentadas pelos agentes inseridos.

O projeto de lei do Marco Civil da Internet, chamado de "Constituição" da Internet Brasileira,tratou de forma sintética de temas como o princípio da neutralidade de

---

[33] Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE. Disponível em:<http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html>. Acesso em: 12 out. 2016.

[34] Celulares superam computadores no acesso à internet. Disponível em: <http://www.brasil.gov.br/infraestrutura/2016/04/pela-primeira-vez-celulares-superaram-computadores-no-acesso-a-internet-no-pais >. Acesso em: 12 out. 2016.

[35] STREIBEL, Fabro. O Portal de Consulta Pública do Marco Civil da Internet. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 Pág.18

rede, responsabilidade civil dos provedores, direito a privacidade dos usuários e a guarda de registros pelos provedores de acesso e de aplicação.

No entanto, Ronaldo Lemos afirma que o projeto permaneceu parado até 2013, momento em que foi revelado por Edward Snowden, ex-consultor da National Security Agency (NSA),que instituições do governo brasileiro e a então presidente Dilma Rousseff haviam sidos espionados e tiveram suas privacidades violadas[36].

Após severas críticas a clara ausência de proteção aos usuários e de segurança nacional, o Senado Federal vislumbrou no Marco Civil da Internet a solução para os anseios da sociedade e rapidamente aprovou à lei 12.965/14em abril de 2014.

Isso se deu porque naquele mesmo mês o Brasil sediaria a conferência NETMundial - Encontro Multissetorial Global Sobre o Futuro da Governança da Internet - esua sanção pela Presidente da República na abertura do evento de grande relevância internacional[37], além de simbólico, mostraria que o país alinhava-se a defesa dos direitos fundamentais, como a proteção à privacidade e à liberdade de expressão, em um modelo de seara digital pluralista e democrática.

Como o relator do projeto[38], o Deputado Federal Alessandro Molon, pontua o Marco Civil ancorou-se em uma perspectiva oposta a de projetos mais adiantados à época como o da Lei de Crimes Virtuais, do senador Eduardo Azeredo, tendo em vista que não visava simplesmente criminalizar condutas antes mesmo de garantir direitos e deveres aos usuários e aos provedores.

## 3.2) O direito à proteção dos dados pessoais e a limitação de retenção de dados

Entres os pontos chaves do Marco Civil da Internet destaca-se a ênfase na proteção da privacidade, disposto no art. 7º, inciso I, e que permeia todo o texto legal, ao assegurara inviolabilidade da intimidade e da vida privada, e o direito a indenização pelo dano material ou moral decorrente de sua violação.

---

[36].LEMOS, RONALDO. Marco Civil da Internet, uma construção da sociedade In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. 3

[37] DILMA sanciona o Marco Civil da internet na abertura da NETMundial. Disponível em:<http://g1.globo.com/tecnologia/noticia/2014/04/netmundial-inicia-com-obrigado-snowden-e-defesa-da-internet-livre.html >. Acesso em: 13 out. 2016.

[38]MOLON, ALESSANDRO. Marco Civil da Internet, uma construção da sociedade. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. XXVIII

Para Lênio Streck[39] é despicienda a formulação desse direito ao usuário e princípio do uso da internet no Brasil, considerando a subordinação à Constituição Federal, que já prevê direito fundamental idêntico no art. 5º, inciso X, assim enunciado *"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"*.

A reafirmação do direito na seara virtual se justificaria unicamente para contrapor a ideia ingênua do liberalismo cibernético de que a internet é um ambiente livre e imparcial, fora do alcance das jurisdições de todos os Estados, e que não o considera como ambiente de disputa política e soberania estatal, como pode ser visto na Declaração de Independência do Ciberespaco escrita em 1996 por John Perry Barlow:

> Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer.
> Vocês não nos conhecem, muito menos conhecem nosso mundo. O espaço cibernético não se limita a suas fronteiras. Não pensem que vocês podem construi-lo, como se fosse um projeto de construção pública. Vocês não podem. Isso é um ato da natureza e cresce por si próprio por meio de nossas ações coletivas[40].

Com a transição das interpretações do conceito do direito a privacidade,inicialmente como "o direito de ser deixado a só" para aquele que o conceitua modernamente ligado também à proteção dos dados pessoais[41], criou-se em certa medida um consenso internacional sobre os princípios que deveriam reger o tratamento de dados pessoais em um cenário de governança democrática da internet.

Danilo Doneda[42] sinteticamente sistematiza esse núcleo encontrado na maioria dos ordenamentos jurídicos que se debruçaram sobre o problema em alguns princípios basilares.

O princípio da finalidade[43] caracteriza-se pelo dever do tratamento de dados pessoais atender à finalidade informada ao interessado antes,durante e depois de sua coleta, de

---

[39] STRECK, LUIZ LÊNIO. Apontamentos hermenêuticos sobre o Marco Civil Regulatório da internet. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. 340

[40] BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 13 out. 2016.

[41] SCHREIBER, Anderson. Direitos da personalidade - São Paulo: Atlas, 2011. p. 129-130

[42] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª. ed. Rio de Janeiro: Renovar, 2006. p. 215

[43] DONEDA, Danilo op. cit.,p. 216

maneira que se evite, por exemplo, o compartilhamento de dados sem o consentimento e/ou conhecimento a terceiros, evitando que ocorra abusos.

O Marco Civil da Internet satisfatoriamente dispõe no art. 7º, incisos VII e VIII, que será assegurado o não fornecimento a terceiros de dados pessoais, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei, e o direito à informações claras e completas sobre o tratamento e a proteção dos dados pessoais, que somente serão utilizados para as finalidades que justifiquem sua coleta, não sejam vedadas pela legislação ou que estejam nos contratos de prestação de serviços ou nos termos de uso das aplicações da internet.

A título exemplificativo da relevância de tal princípio, a empresa de telecomunicações OI, detentora do provedor de acesso a internet Velox, foi multada em R$ 3,5 milhões de reais,em 2014, por violar a privacidade de dados dos seus usuários e adotar práticas comerciais desleais que infringiram o Código de Defesa do Consumidor[44].

O Departamento de Proteção e Defesa do Consumidor, a partir das informações recebidas e posterior investigação, concluiu que a Oi realizara parceria com a empresa britânica Phorm para desenvolver um software chamado "NAVEGADOR" capaz de mapear o tráfego de dados do consumidor na internet tecendo um perfil de navegação comercializável para anunciantes, agências de publicidade, ofertando publicidade e conteúdo personalizados[45].

Ainda que não tenha sido aplicada diretamente a Lei 12.965/14 no caso,esta foi mencionada na nota técnica[46] como um complemento ao entendimento de que o internauta tem garantido o direito à inviolabilidade da vida privada, aqui incluídos os dados, comunicações e quaisquer outras informações de caráter pessoal na rede.

A decisão é um marco histórico para a jurisprudência brasileira e vai ao encontro do esposado posteriormente no art. 14 do diploma legal, que estabelece que aos provedores de conexão, seja de maneira onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

---

[44] BRASIL. Departamento de Proteção e Defesa do Consumidor. Processo Administrativo nº 08012.003471/2010-22Disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=43&data=23/07/2014 . Acesso em 13/10/2016

[45] OI é multada em R$ 3,5 milhões por invasão de privacidade feita por Velox. Disponível em:<http://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505>. Acesso em: 13 out. 2016.

[46] RENÁ, Paulo.**Fundamentos da multa aplicada à OI por monitorar a navegação de internautas**. Disponível em:<http://ibidem.org.br/fundamentos-da-multa-aplicada-a-oi-por-monitorar-navegacao-de-internautas/>. Acesso em: 13 out. 2016.

Essa garantia da proteção de dados e da privacidade correlaciona-se não só com o princípio da finalidade, mas também com a preservação da neutralidade de rede, visto que se os provedores de conexão não fossem proibidos de guardar os registros de acesso às aplicações, seriam capazes a partir das informações coletadas saber quais seriam as aplicações mais acessadas por seus usuários.

A partir disto, Cláudio Conalgo sugere que com a ausência desse dever negativo seria totalmente plausível que fossem firmados acordos de acessos preferenciais diretamente com os provedores de aplicação, interferindo excessivamente no meio ambiente digital[47].

O princípio da exatidão[48] ou qualidade dos dados preceitua que os dados devem ser fiéis à realidade, de modo que a coleta e o tratamento sejam feitos com cuidado e correção, com atualizações periódicas. Já o princípio da transparência[49] exige que a existência de um banco de dados seja de conhecimento público para que se viabilize a accountability dos bancos de dados.

É notório que antes mesmo da revolução tecnológica das últimas duas décadas, a Constituição de 1988, em seu art. 5º, inciso LXXII, previu o instituto do habeas data, muito em face da recente história política brasileira, na qual dados pessoais eram armazenados nos arquivos sigilosos do regime ditatorial militar.[50] O instituto, em correlação com os princípios supracitados,visa assegurar o conhecimento de informações relativas ao próprio cidadão, constantes no registro ou banco de dados e, se necessário, retifique essas informações.

Em consonância com a qualidade de dados é possível citar também o Código de Defesa do Consumidor ao preceituar:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

Por fim, segundo o princípio da segurança física e lógica, os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação ou acesso não autorizado.

---

[47]COLNAGO, CLAUDIO OLIVEIRA SANTOS, Provedores de conexão e guarda de registros de acesso a aplicações da internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.767

[48]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª. ed. Rio de Janeiro: Renovar, 2006. p. 215

[49]DONEDA, Danilo. **op. cit.,** p. 216

[50]DONEDA, Danilo. **op. cit.**, p. 217

Isso pode ocorrer por meio de adoção de medidas técnicas protetivas como a manutenção desses dados em ambiente controlado e seguro, que sigam procedimentos específicos prevenindo e resguardando de qualquer tentativa de violação de hackers.

Entre as diversas críticas que a Lei 12.965/14 foi alvo, pretende-se abordar a problemática quanto ao armazenamento cautelar da guarda de logs de conexão e aplicação, não se questionando por si só a constitucionalidade dos art. 13 e 15 do Marco Civil da Internet, mas no que se refere as medidas de segurança regulamentadas pelo Decreto 8.771/16, para que o direito à privacidade e à proteção dos dados pessoais não sejam violados.

Os dispositivos do Marco Civil da Internet que tratam da guarda preventiva de logs são os seguintes:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.
>
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

A guarda desses metadados não é novidade no cenário brasileiro, apesar de anteriormente não ser uma obrigação legal. O que se tinha, como Marco Antônio Assunção Cabello[51] demonstra,eram recomendações do Comitê Gestor da Internet de boas práticas para os administradores de redes de internet, entre elas, a que os logs de conexões deveriam ser mantidos disponíveis por pelo menos 3 anos.

O STJ, em precedente anterior à promulgação do Marco Civil da Internet, no Recurso Especial nº 1.417.641[52] já havia expressado entendimento no sentido de que as informações necessárias para identificação dos usuários deveriam ser armazenadas também pelos provedores de conteúdo por um prazo mínimo:

> CIVIL E CONSUMIDOR. INTERNET. PROVEDOR DE CONTEÚDO. USUÁRIOS.IDENTIFICAÇÃO. DEVER. GUARDA DOS DADOS. OBRIGAÇÃO. PRAZO.DISPOSITIVOS LEGAIS ANALISADOS: ARTS. 4º, III, DO CDC; 206, §3º, V, 248, 422 e 1.194 DO CC/02; E 14 E 461, § 1º DO CPC.
> 1. Ação ajuizada em 30.07.2009. Recurso especial concluso ao gabinete da Relatora em 04.11.2013.
> 2. Recurso especial que discute os limites da responsabilidade dos provedores de hospedagem de blogs pela manutenção de dados de seus usuários.
> 3. **Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada**. Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo. Precedentes.

---

[51]COLNAGO, CLAUDIO OLIVEIRA SANTOS, Provedores de conexão e guarda de registros de acesso a aplicações da internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.767

[52] Brasíl. STJ. REsp 1417641/RJ, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 25/02/2014, DJe 10/03/2014)https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1300948&num_registro=201303417872&data=20140310&formato=PDF

> 4. Uma vez ciente do ajuizamento da ação e da pretensão nela contida - de obtenção dos dados de um determinado usuário - estando a questão sub judice, o mínimo de bom senso e prudência sugerem a iniciativa do provedor de conteúdo no sentido de evitar que essas informações se percam. Essa providência é condizente com a boa-fé que se espera não apenas dos fornecedores e contratantes em geral, mas também da parte de um processo judicial, nos termos dos arts.
> 4º, III, do CDC, 422 do CC/02 e 14 do CPC.
> **5. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço.**
> 6. Recurso especial a que se nega provimento.

Com a vigência da lei, houve uma redução e diferenciação do prazo com base no tipo de provedor abordado. Atualmente, os provedores de acesso a internet e os provedores de aplicação têm de manter, sob sigilo, em ambiente controlado e de segurança, respectivamente, pelo prazo de 1 ano os registros de conexão e de 6 meses dos registros de acesso a aplicações de internet, nos termos do regulamento a ser editado.

Todavia, quem seriam os provedores de aplicação? Pela definição de aplicação de internet do marco regulatório, entende-se por qualquer pessoa jurídica ou física que provê um conjunto de funcionalidades acessíveis por meio de um terminal conectado à internet.

Conforme aduz Frederico Meinberg Ceroy[53], o provedor de correio eletrônico, o provedor de hospedagem e o provedor de conteúdo estariam incluídos no conceito de provedor de aplicação do marco regulatório.

É necessário ressaltar que a norma explicita que nem todos os provedores de aplicações tem o dever de guarda, mas apenas aqueles estabelecidos na forma de pessoa jurídica e com fins econômicos, isto é, aqueles que não se encaixassem poderiam alegar judicialmente a inexigibilidade de guarda preventiva de logs.

Excetuados os casos, em que mesmo não enquadrados no dever legal, há ordem judicial obrigando-os a realizar a guarda, por tempo certo dos logs relativos a fatos particulares em período determinado.

Isso desconsidera que a prática de crime no meio eletrônico ocorre em todo tipo de provedor de aplicação, organizado ou não legalmente, tanto em um site de compra e vendas fraudulento ou em um site de download de *torrents* de filmes grátis quanto para acesso de redes sociais, blogs, emails, bancos online, etc.

---

[53] CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil da Internet**. Disponível em:<http://www.migalhas.com.br/dePeso/16,MI211753,51045-os+conceitos+de+provedores+no+Marco+Civil+da+Internet>. Acesso em:20 out. 2016.

O art. 5º define tecnicamente que os registros de conexão abarcam o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pela interface ou dispositivo de recebimento do pacotes de dados. Enquanto que os registros de acesso a aplicações de internet incluem o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Poder-se-ia argumentar que o Protocolo de Internet (IP) não pode violar a privacidade em razão da limitação estrutural do modelo atual mais utilizado, o protocolo de navegação IPv4, que já atingiu seu esgotamento, e logo não configuraria dado pessoal.

Ora, sabe-se que o número de IP atribuído pelo provedor de acesso ao dispositivo utilizado pelo usuário é alterado constantemente a cada conexão para atender as demandas de acesso exigidas ao sistema, fazendo indiretamente com que em razão dessa limitação o usuário seja menos rastreável e navegue com certa anonimidade.

No entanto, é incorreta esta percepção de que o protocolo de internet não é um dado pessoal, pois, ainda que o registro do provedor de aplicação não consiga sozinho identificar o usuário, há a razoável possibilidade de fazê-lo através do tratamento de dados, especificamente, relacionando-o com outras informações como o registro de conexão dos provedores de acesso, que informa quem estaria utilizando o IP naquele momento especificado, mesmo quando se cuida de IPs dinâmicos.

Reema Saah[54] (2015, p. 543) considera que os recentes desenvolvimentos, como a *deep packet inspection* (inspeção do pacote de dados), fizeram com que evitar ser detectado por sua condutas seja bem mais tecnologicamente desafiador e, consequentemente, pouco provável que um fluxo de dados permaneça tão obscuro que os provedores de acesso a internet ou outros não possam estimar sua origem.

Em recente julgado internacional, de 19 de outubro de 2016, o Tribunal de Justiça da União Europeia considerou que tanto os IPs estáticos quanto os dinâmicos são dados pessoais, pois pelo ângulo objetivo há a potencialidade de identificação considerando que os meios legais permitem o cruzamento dessa informações para se chegar com precisão ao

[54] SHAH, Reema. Law Enforcement and Data Privacy: A Foward-Looking Approach. The Yale Law Journal 125(2): p. 543-558 · Novembro 2015 Disponível em: https://www.researchgate.net/publication/287221402_Law_Enforcement_and_Data_Privacy_A_Forward-Looking_Approach

menos qual dispositivo detinha o IP no momento determinado, e, assim, estariam sob a proteção da Diretiva 95/46/EC.[55]

A jurisprudência consolidada no Superior Tribunal de Justiça, prévia ao marco regulatório é no sentido de que o IP seria meio suficiente para a identificação de um indivíduo na rede:

> AGRAVO REGIMENTAL NO RECURSO ESPECIAL. DIREITO ELETRÔNICO E RESPONSABILIDADE CIVIL. DANOS MORAIS. PROVEDOR DE BUSCA NA INTERNET SEM CONTROLE PRÉVIO DE CONTEÚDO. ORKUT. MENSAGEM OFENSIVA.NOTIFICAÇÃO PRÉVIA. INÉRCIA DO PROVEDOR DE BUSCA. RESPONSABILIDADE SUBJETIVA CARACTERIZADA. AGRAVO DESPROVIDO.
> 1. Este Tribunal Superior, por seus precedentes, já se manifestou no sentido de que: I) o dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site por usuário não constitui risco inerente à atividade desenvolvida pelo provedor da internet, porquanto não se lhe é exigido que proceda a controle prévio de conteúdo disponibilizado por usuários, pelo que não se lhe aplica a responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC/2002; II) a fiscalização prévia dos conteúdos postados não é atividade intrínseca ao serviço prestado pelo provedor no Orkut.
> 2. A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato.
> **3. O fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio satisfatório de identificação de usuários.**
> 4. Na hipótese, a decisão recorrida dispõe expressamente que o provedor de busca foi notificado extrajudicialmente quanto à criação de perfil falso difamatório do suposto titular, não tendo tomado as providências cabíveis, optando por manter-se inerte, motivo pelo qual responsabilizou-se solidariamente pelos danos morais infligidos à promovente, configurando a responsabilidade subjetiva do réu.
> 5. Agravo regimental não provido.[56]

Entretanto, a despeito da legislação vigente, o Tribunal de Justiça do Estado de São Paulo se contrapôs a essa jurisprudência, no acórdão de agravo de instrumento nº 2206954-25.2015.8.26.0000, ao manter uma decisão que obrigava o provedor de aplicação Google a fornecer inclusive os números das Portas Lógicas de origem dos IPs, apesar de a

[55] RITZER, Cristoph. **CJEU Judgement: Dynamic IP Addresses Constitute Personal Data**. Disponível em:<http://www.dataprotectionreport.com/2016/10/cjeu-judgement-dynamic-ip-addresses-constitute-personal-data/>. Acesso em: 24 out. 2016.

[56] BRASIL. STJ. Quarta Turma. AgRg no REsp 1402104/RJ. Relator: ARAUJO, Raul. Julgado em 27/05/2014. Disponível em :https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1324580&num_registro=201201547156&data=20140618&formato=PDF Acesso em 04/11/2016

definição de registro de aplicação no Marco Civil da Internet não incluir tais metadados como obrigatória na guarda de logs, sob o fundamento de que o rol do art. 5 seria meramente exemplificativo.

Francisco Brito Cruz[57]afirma que não há obrigação da guarda desses metatados e que tal precedente não considera a possibilidade de que se resulte na criação de uma obrigação de fazer excessiva e sem baliza legal.

Cruz evidencia que a decisão contribui para interpretações judiciais extensivas de que qualquer dado que possa permitir a identificação de um usuário de Internet pode ser fruto de um pedido, mesmo que não haja o deve legal de armazenamento do provedor de aplicação ou conexão, sob pena das possíveis sanções do art. 12.

Assim,põe-se em questão os riscos de abusos a que tais direitos estão sujeitos, pois, como Bruna Garcia e Mário Furlano Neto[58] pontuam, as informações que podem ser extraídas de tais registros envolvem questões que tangenciam a privacidade e a intimidade, abrangidas pelo rol de direitos fundamentais dispostos no art. 5º, inciso X, da Constituição de 1988, tendo em vista a capacidade de armazenar tudo e quando que um indivíduo acessa ou posta na rede, ficando na posse dos provedores.

O tratamento desses metadados gerou uma mudança significativa do que se entende por privacidade, tendo em vista que como José Luis Bolzan de Morais e Elias Jacob de Menezes Neto aduzem:

> "No século XXI, tudo é passível de ser transformado em dados analisáveis, inclusive os próprios dados. Como resultado, o acesso ao fluxo de dados e qualquer tipo de informação armazenada é muito mais do que um problema de privacidade. Passa a ser um problema de violação da igualdade."[59]

Por outro lado, a obrigatoriedade de guarda não é despropositada, considerando que a partir desses logs de conexão e aplicação é possível identificar autores de atos ilícitos e aumentar a probabilidade de que sejam punidos por tais condutas. O importante é que o registro dos metadados seja realizado de forma não abusiva, respeitado um prazo de guarda

[57] CRUZ, Francisco Brito. Análise do Agravo de Instrumento 2206954-25.2015.8.26.0000/TJ-SP. Disponívelhttp://www.omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/

[58] NETO, MARIO FURLANO. GARCIA. BRUNA PINOTTI Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.776

[59] BOLZAN, José Luis. NETO. Elias Jacob Menezes. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma do surveillance. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.418

razoável, e que o uso desses dados atenda a procedimentos de acesso e segurança dos dados que respeitem a privacidade dos cidadãos, em atenção, especialmente, aos princípios da finalidade e da necessidade.

Cite-se o recente julgado de 20 de outubro de 2016, no processo nº 1109039-47.2016.8.26.0100,em que a 23ª Vara Cível do Tribunal de São Paulo deu procedência ao pedido da ABTA - Associação Brasileira de Televisão Por Assinatura, para que diversos provedores de acesso a internet fornecessem os registros de conexão e dados cadastrais de usuários:

> Neste juízo de cognição sumária, nos termos dos artigos 298 e 300, do CPC, resta somente aferir se presentes os requisitos necessários à concessão da providência urgente, quais sejam, a probabilidade do direito e o perigo de dano irreparável ou o risco ao resultado útil do processo. Pretende a autora o fornecimento das informações indispensáveis à identificação dos usuários de linhas telefônicas, com acesso à internet, que integram uma rede de websites destinados à comercialização ilícita de transmissão de canais de TV por assinatura, evidenciando-se a prática criminosa. A medida pretendida não implica violação à garantia constitucional de sigilo das comunicações de dados, diante da ofensa a direito. A par da garantia da livre manifestação do pensamento, a Constituição Federal também veda o anonimato. Como consabido, nos dias atuais o cognominado Marco Civil da Internet, a Lei nº 12.965, de 23.04.2014, em seu artigo 15, disciplina expressamente a guarda de registros de acesso a aplicações da internet enquanto obrigação legal que pesa sobre tais prestadores de serviços. Ademais, não se pretende a quebra de sigilo de dados e comunicações tutelados pela Lei nº 9.296/96, mas sim e tão somente o acesso a dados cadastrais de agentes potencialmente responsáveis pela prática de ilícitos, cuja elucidação se persegue.
> Assim, defiro a tutela de urgência e determino que as empresas CLARO S/A, OI S/A, TELEFONICA S/A, TIM CELULAR S/A e COPEL TELECOMUNICAÇÕES S.A., forneçam, em cinco dias, as informações sobre dados cadastrais, registros de IP de origem, com datas e horários, e demais registros eletrônicos dos usuários dos endereços de IPs indicados na inicial, incluindo-se os números telefônicos de origem das conexões, sob pena de aplicação de multa diária no valor de R$ 5.000,00 (cinco mil reais), sem que haja comunicação a seus criadores, sob pena de frustrar-se a eficácia da decisão judicial. Servirá a presente decisão como ofício, incumbindo à autora instrui-lo com os endereços de IPs indicados na inicial.

Um dos mais importantes direitos fundamentais é o direito à liberdade de expressão, delineado no art. 5º, inciso IV, da Constituição Federal, mas entre suas limitações há a vedação ao anonimato.

Na seara do mundo virtual, em que a possibilidade de transitar anonimamente pela rede e a sensação de que o manto de impunidade sobre quaisquer manifestações são muito maiores, tendo em vista a facilidade encontrada para utilizar-se de perfis falsos ou de mecanismos que escondam a identificação de origem do dispositivo, tal vedação é repercutida pela admissão de certa interferência legislativa, de modo a identificar indivíduos ou

organizações que virão a ser responsabilizados civil ou penalmente, sob pena de inviabilizar o combate a crimes mais gravosos e comuns nesse âmbito como a pornografia infantil.

Considerando o princípio de proporcionalidade adotado nas decisões europeias e alemã, em que a guarda preventiva desses dados deve levar apropriadamente em conta o peso que tal retenção constitui sobre o exercício dos direitos fundamentais, entende-se que a restrição a esses direitos é justificável desde que sirva a propósitos legítimos de interesse público.

No entanto, isto atende apenas a proporcionalidade em sentido amplo, e, para firmar um posicionamento se há violação de tais direitos, é essencial que os meios sejam aptos de realizar os objetivos perseguidos, o que comprovadamente os são, mas também que não ultrapassem aquilo que estritamente necessário para alcançar o pretendido, dependendo assim de uma análise em conjunto do que veio a ser regulado pelo Decreto 8.771/16.

## 3.3)Decreto 8.771/16: solução ou mais questionamentos?

Na véspera da votação para o afastamento da presidente Dilma Rousseff abertura do processo de impeachment no Senado Federal foi publicada uma edição extra do Diário Oficial da União que promulgou o Decreto 8.771/16[60], trazendo novos aspectos à Lei 12.965/2014.

Diferentemente do que se pode inferir pelo momento em que foi promulgado,a regulamentação foi alvo de um período prévio de consulta pública em plataforma online[61] semelhante à da primeira fase do Marco Civil da Internet, na qual cidadãos puderam sugerir ideias ao texto até o dia 29 de fevereiro de 2016.

Entre os pontos centrais, o decreto que regulamentou o Marco Civil da Internet definiu as hipóteses em que poderia ocorrer a discriminação de pacotes de dados da internet e de degradação do tráfego, sem que se viole o tratamento isonômico baseado na neutralidade de rede. Além disso, teve como objetivo indicar procedimentos para a guarda e proteção de dados por provedores de conexão e de aplicações e parâmetros para fiscalização e apuração das infrações cometidas.

---

[60] Conheça detalhes do decreto que regulamenta o Marco Civil da Internet. Disponível em:<http://www.ebc.com.br/tecnologia/2016/05/conheca-detalhes-do-decreto-que-regulamenta-marco-civil-da-internet>. Acesso em: 24 out. 2016.

[61]Marco Civil da Internet 2ª Fase: o que é? Disponível em http://pensando.mj.gov.br/marcocivil/ Acessado em 24/10/2016

Em um contexto de que a autodeterminação informacional passa a ser cada vez mais anacrônica frente à ubiqüidade da tecnologia e seu efeito primordial de desequilíbrio de poderes entre o indivíduo e os organismos que processam tais dados, questiona-se o real poder de controle individual sobre o fluxo dos dados[62].

Por isso, não deve-se perder de vista que a regulamentação perpassa tanto pela dimensão substancial quanto da dimensão procedimental do direito a privacidade[63], isto é, pelo emprego das informações obtidas e pela adoção de medidas de segurança da informação que consideram as empresas e também aqueles que requerem judicialmente o acesso a esses registros.

As diretrizes para os provedores foram dispostas na seção "Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas":

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
>
> I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
>
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
>
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
>
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.
>
> § 1ºCabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.

Apesar do detalhamento das medidas técnicas, como a criptografia e autenticação dupla para acesso aos registros, chama atenção na leitura do artigo a nomenclatura escolhida, qual seja, diretrizes a serem observadas, o que põe em dúvida qual seria o grau de obrigatoriedade dessas medidas de segurança, tendo em vista que ao intérprete assemelham-se mais a recomendações do que propriamente à obrigações.

[62]MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito do consumidor. 1ª Edição. São Paulo:Saraiva, 2014, p. 78

[63]SCHREIBER, Anderson. Direitos da personalidade - São Paulo: Atlas, 2011. p. 132-133

O nível de comprometimento com a implementação, que inevitavelmente tem repercussões técnicas e econômicas para os provedores e afetam indiretamente aos usuários, acaba dependendo da fiscalização a ser exercida e da apuração das infrações pelos diferentes órgãos.

Afinal, no art. 13 §1º, o legislador compreende que essas medidas são exemplificativas e passíveis de alteração, pois não desconsidera a dificuldade de controlar um ambiente em constante evolução e liquidez como o que a internet propicia, dando relevo às recomendações procedimentais e estudos do Comitê Gestor de Internet para que se mantenha um padrão mínimo de segurança.

Ainda assim, em atitude acertada, a legislação dispõe que a guarda desses logs deverá ser mantida, sob sigilo, em ambiente controlado e de segurança, e foi deixado de lado pelos legisladores a obrigação de que os provedores mantivessem guardados os dados em servidores localizados no território brasileiro.

Diferentemente do que em um primeiro momento pode-se supor, esta medida de territorialidade não faz com que os dados estejam mais seguros. Ao tornar obrigatória a guarda desses dados em um único local todos, torna-se mais fácil a possibilidade de que os servidores sejam alvos de hackers, em contraposição ao sistema de *cloud computing* (computação em nuvem), além do que pode resultar em uma efetiva balcanização da Internet, isto é, a sua fragmentação para o aumento de barreiras e controles locais sobre a rede[64].

O que se percebe também é que não houve por parte do legislador o devido cuidado na fase posterior à obtenção dos dados, pois após o acesso aos registros não há um procedimento de proteção claro e uma forma correta para que eles sejam utilizados, razão pela qualo decreto falha ao não responder questões essenciais. Eis algumas delas.

Exemplificativamente, por qual período de tempo esses dados podem ficar na posse das autoridades requerentes? Quem são as autoridades administrativas competentes? Onde os dados devem ser guardados? Os dados cadastrais são taxativos? Após sua utilização, há exclusão desses dados? E no caso de violação pelo próprio Poder Público, qual é o procedimento específico para apuração das infrações e das sanções cabíveis? Há notificação ao usuário de que seus dados foram requeridos ou isto é a exceção?

[64] SHAH, Reema.Law Enforcement and Data Privacy: A Foward-Looking Approach.The Yale Law Journal 125(2): p. 543-558 · Novembro 2015 Disponível em: https://www.researchgate.net/publication/287221402_Law_Enforcement_and_Data_Privacy_A_Forward-Looking_Approach

Tais questões que poderiam ter sido melhor regulamentadas no decreto não o foram.

Inicialmente, o enfoque dado para a exclusão dos registros permeia apenas os provedores de conexão e aplicação, desconsiderando a necessidade de que as autoridades estatais também a excluam quando atingida a finalidade almejada[65].

Outro ponto que chama a atenção é o requerimento cautelar por autoridade administrativa competente ou pelo Ministério Público de guarda de logs por prazo superior àquele estabelecido e também da possibilidade de acesso aos dados cadastrais, pois o escopo genérico abrangido por autoridade administrativa é por demasiado amplo, o que dá margem para interpretações extensivas que não se coadunam com a preservação da privacidade dos usuários.

Antes mesmo da aprovação da lei já tinha havido proposta de Emenda nº 20 do PLC 21/2014 no Senado Federal para que se evitasse o imbróglio:

> JUSTIFICAÇÃO
> Nosso objetivo, por meio desta emenda, é reproduzir garantias e proteções constitucionais constantes ao cidadão no uso da internet. A substituição da expressão "autoridade administrativa" pelo elenco taxativo das autoridades públicas que efetivamente têm, conforme preconiza a Constituição Federal, competência para mitigar, em determinados e expressos casos, a proteção à inviolabilidade de comunicação do cidadão é medida que se impõe. Da forma como está disposto no texto aprovado pela Câmara dos Deputados, está-se conferindo uma cláusula aberta, que dependerá de leituras sistêmicas complexas, mas que poderá permitir interpretações distantes da vontade legislativa. A se conceituar "autoridade administrativa", pode-se descer a discussões indesejadas na aplicação da norma.

Com a sua não implementação, o deputado Aloysio Nunes Ferreira propôs o PLS 180/2014[66],com o intuito de estabelecer a finalidade e restringir o rol de autoridades públicas que podem ter acesso a dados privados do cidadão na internet apenas aos delegados de polícia ou ao Ministério Público, ao alterar a redação dos art. 13 e 15 da Lei 12.965/2014.

Ademais, o decreto se manteve silente quanto aos requisitos mínimos de solicitação precaucional, como fundados indícios da ocorrência do ilícito, competência legal da autoridade, justificativa da utilidade dos registros solicitados para fins de investigação, etc., o que é fundamental para se verificar o atendimento ao princípio da necessidade, preconizado

---

[65] Brasil. Lei 12.965/14. Art. 13
§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, 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; ou
II - se encerrado o prazo determinado por obrigação legal.

[66] http://www25.senado.leg.br/web/atividade/materias/-/materia/117646

tanto pelo direito à proteção de dados pessoais, quanto pelo princípio da proporcionalidade. Afinal, a inexistência desses requisitos legais pode incentivar o uso completamente abusivo e excessivo desses dados.

Ainda que se tenha na lei o prazo de 60 dias para que as autoridades peçam judicialmente o acesso a esses registros, não há clareza quanto ao limite de extensão máxima de retenção para que garantir que seja mantido pelo prazo estritamente necessário e que não configure uma interferência, além de não esclarecer os termos finais e iniciais da contagem de prazo para guarda de registros, por um imperativo de segurança jurídica, como propuseram diversas entidades do setor[67].

O artigo 21 enuncia de forma genérica que a apuração de sanções previstas no Marco Civil atenderá aos procedimentos internos de cada um dos órgãos fiscalizatórios, e que a apuração ocorrerá de ofício ou mediante requerimento de qualquer interessado, mas não estabelece nenhuma diretriz mínima sobre a apuração das sanções dentro de cada órgão e se apresenta mais nebulosa quando não há delimitação legal específica de quem são as autoridades competentes**.**

Diferentemente do que ocorreu quanto às sanções aos provedores, que em certa medida foram delimitadas:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, **conforme o caso**, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Sabe-se que há uma infinidade de possibilidades quanto a condutas passíveis de ilicitude e que a tentativa de regulação pelo estabelecimento de um tipo *numerus clausus* iria de encontro com a dinamicidade das relações na internet.No entanto, considerando aspectos de segurança jurídica e previsibilidade, teria sido adequado delimitar critérios mínimos aplicáveis a cada sanção, para aqueles que estão obrigados legalmente à guarda desses

[67]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. 965/14p. 31. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/08/Relat%C3%B3rio-ILABReporta-MCI.pdf

registros e do tratamento de dados, o que se esperava encontrar no Decreto 8.771/16 e não sucedeu.

Assim, os provedores, sem prejuízo das sanções em outras searas,poderão ser responsabilizados por condutas similares ou até mesmo idênticas com sanções variadas de acordo com o entendimento do Juiz acerca do caso.

Mostra-se problemática também a omissão quanto ao dever dos provedores de notificar o usuário, o maior interessado,sobre o acesso a esses registros ou a violação de dados, o que inviabiliza o conhecimento dos usuários e consequentemente limita a busca pela reparação civil.

Em abril de 2016 foi publicada a pesquisa "Quem Protege Seus Dados?" [68], realizado em uma parceria entre o InternetLab e a Eletronic Frontier Foundation, que buscou promover a transparência e adoção de boas práticas em relação à privacidade e proteção de dados pelas empresas provedoras de acesso à Internet no Brasil.

Os resultados apontam que metade dos maiores provedores de conexão do Brasil não informam seus usuários sobre as condições de entrega de dados a agentes do Estado, de forma a garantir que só irão fornecer os registros de conexão por meio de ordem judicial.

Quanto à postura que essas empresas adotam em relação à privacidade de seus usuários no Judiciário, houve uma grande contraste entre banda larga móvel e banda larga fixa.

Na banda larga móvel, todas empresas se mostraram mais resistentes e contestaram judicialmente pedidos abusivos de acesso a dados de usuários alegando que extrapolavam as prerrogativas legais da autoridade autora do pedido ou eram desproporcionais, enquanto que ao tratar de banda larga fixa metade das empresas não contestava os pedidos e aqueles que o faziam, ainda assim não havia semelhante compromisso de proteção.

O art. 16 do decreto dispõe que "*as informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais".*

No entanto, uma medida simples como a do quesito publicação de relatório de transparência sobre pedidos de dados não foi atendida por nenhuma das empresas pesquisadas.

[68] Relatório Quem Defende Seus Dados?. Disponível em: <http://quemdefendeseusdados.org.br/pt/ >. Acesso em: 24 out. 2016.

Por fim, o último quesito da pesquisa foi saber se as empresas notificam os usuários sobre pedido de acesso a seus dados, quando o sigilo não é imposto por lei ou no primeiro momento em que o sigilo é levantado e a notificação é permitida,mas nenhum dos provedores de acesso à internet cumpriu o requisito para informar o interessado.

Como não há uma obrigação legal para que isso aconteça, tanto no decreto quanto no próprio Marco Civil da Internet,na maioria das vezes tais violações passam despercebidas pelos usuários e contribui para que não se desenvolva uma cultura de proteção à privacidade como as que se encontram consolidadas em diversos países.

Nas palavras de Stefano Rodotá:

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações.[69]

A notificação é condição para o efetivo exercício do direito à autodeterminação informativa, e está em consonância com o princípio da ampla defesa, pois viabiliza não só que as empresas, que como se sabe nem todas estão totalmente interessadas em prolongar disputas judiciais onerosas, mas também que os cidadãos contestem pedidos ilegais, sem que haja uma dependência do provedor, para que ao fim protejam a privacidade.

Por esses motivos o decreto não atendeu a dimensão procedimental do direito a privacidade, ao não estabelecer exigências técnicas e procedimentais claras para assegurar que banco de dados esteja protegido contra ingerências não autorizadas pelos interessados ou legalmente, pondo em risco à proteção desses dados pessoais e, por conseguinte, da dimensão substancial do direito à privacidade.

Para além do explanado surgem contradições entre o que a legislação exige e o que o Judiciário vem obrigando dos provedores, considerando que está expresso nas diretrizes do decreto que se utilize de soluções de gestão dos registros através de técnicas que garantam a inviolabilidade dos dados, como a encriptação.

Lessig afirma que a criptografia talvez seja uma das melhores ferramentas tecnológicas de acomodação necessária para balancear a perda de controle dos indivíduos, na medida em que os aparatos de coleta de dados e tratamento avançaram na extensão em que a

[69]RODOTÁ, Stefano. A Vida na sociedade da vigilância: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. São Paulo. Renovar. 2008. p. 37

privacidade decaiu, justamente porque a quantidade de informações guardadas sobre um indivíduo considerado no espaço público se alterou drasticamente[70].

Todavia, em apenas dois anos após a sanção da lei, surgiram decisões que obrigaram provedores de conexão a suspender temporariamente provedores de aplicação, em todo o território nacional, por não fornecerem as conversas de investigados em processo criminal, mesmo que fosse alegado que sigam a lógica do *privacy by design* com adoção da criptografia de ponta-a-ponta.

A interpretação equivocada quanto às sanções do marco regulatório e a pretensão punitivista leva a decisões desproporcionais que promoveram, *a contrario sensu*, o oposto da finalidade de uma investigação em curso, ao impedir a apuração dos fatos ilícitos supostamente ocorridos.

No mandado de segurança, com pedido liminar, impetrado contra a decisão de juiz do Tribunal de Justiça do Piauí, entre as sanções voltadas a punir o provedor de aplicação, salta aos olhos a notificação determinando que os provedores de conexão suspendam conjuntamente com a atividade do próprio aplicativo, a própria guarda dos registros de conexão.

Toda essa incompreensão levou ao ajuizamento da Ação de Descumprimento de Preceito Fundamental nº 403/DF, pelo Partido Popular Socialista, e da Ação Direta de Inconstitucionalidade 5.527/DF, pelo Partido da República.

Em breve síntese, os Partidos objetivam respectivamente impedir e declarar inconstitucional a determinação judicial de suspensão de provedores de aplicação, como sanção pelo descumprimento da ordem de disponibilização de registros de aplicações e conteúdo de comunicações privadas, tal qual vem sendo aplicada por magistrados brasileiros, e a declaração de violação ao preceito fundamental da liberdade de comunicação.

O Instituto Beta para a Democracia e Internet-IBIDEM e Laboratório de Pesquisa Direito Privado e Internet – LAPIN da Universidade de Brasília ingressaram como *amicus curiae* na ADPF nº 403e fazem apontamentos interessantes quanto à importância da proporcionalidade:

> "A regulação do ciberespaço e as particularidades desta arena pública de interação social parecem ser algo de difícil compreensão para algumas autoridades estatais , as quais enxergam a arquitetura da rede apenas como um meio de obstaculizar

[70] LESSIG, Lawrence. Reading de Constitution in Cyberspace. p. 11 Disponível em http://emoglen.law.columbia.edu/LIS/archive/const-theory/lessig-reading.pdf

> investigações criminais e decisões judicias, ao invés de constituir um sistema de proteção do sigilo de comunicação e dos dados da grande maioria dos usuários.
> [..]
> Neste sentido, ganha relevo o princípio da proporcionalidade que atuará de maneira a estabelecer o equilíbrio entre as medidas restritas e o direito à proteção de dados pessoais. E com amparo nesta premissa o art. 23 (1) do Regulamento 679/2016 afirma que as atividades de prevenção, investigação, repressão e sanção criminal podem limitar o direito à proteção de dados pessoais desde que minimamente respeitem a essência dos direitos e liberdades fundamentais que dele decorrem. Percebe-se, portanto, que a proporcionalidade é a peça-chave para o alcance do equilíbrio entre o direito à proteção dos dados pessoais e a segurança pública"[71]

Ainda que tenham sido ajuizadas antes da edição do decreto 8.771/16, a regulamentação manteve-se flexível e opaca, e combinada com uma casuística decisional descontextualizada, contribuindo para não sanar os principais problemas apresentados e deixando as empresas e os cidadãos sob o constante risco de abusos de seus direitos fundamentais, diante da ausência de previsibilidade quanto a que postura será tomada em relação à proteção dos dados pessoais pelo Judiciário.

[71]BRASIL. STF. APDF Nº 403. Pedido de ingresso amicuscuriae. ADPFInstituto Beta para a Democracia e Laboratório de Pesquisa Direito Privado e Internet da Unb, pág 19 Disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=570497013#48%20-%20Pedido%20de%20ingresso%20como%20amicus%20curiae%20(39941/2016)%20-%20Pedido%20de%20ingresso%20como%20amicus%20curiae

## 3) Medidas para a construção de uma cultura de proteção de dados no ordenamento jurídico brasileiro

O Marco Civil da Internet e o decreto que o regulamentou indubitavelmente tiveram o mérito de enfrentar temas tão complexos a um só tempo, mas falharam por alguns motivos expostos anteriormente. Pretende-se neste capítulo realizar apontamentos com objetivo de tentar solucionar algumas desses embaraços.

No que se refere especificamente à questão proposta na presente monografia, é preciso salientar que, diferentemente do que alguns setores entendem, a guarda preventiva de logs não é inconstitucional por si só e, não violaria desde logo o direito à privacidade e à proteção dos dados pessoais.

A violação desses direitos fundamentais perpassa um aspecto mais primordial, qual seja, a essencialidade de uma legislação que seja robustamente acompanhada de garantias.

No que se refere à guarda de logs é necessário que se estabeleçam procedimentos administrativos claros para apuração de infrações, termo inicial e final da contagem do prazo de retenção, em quais circunstâncias esses dados poderão ser acessados, sob o risco de que aconteça algo semelhante com o que se verificou a partir de dados do Conselho Nacional de Justiça, um verdadeira banalização judicial e expansão das interceptações telefônicas[72].

Esta percepção de que os direitos e garantias fundamentais dos cidadãos estavam em cheque, o que enfraqueceria o próprio Estado Democrático de Direito, fez com que o STF atestasse a existência de repercussão geral no Recurso Extraordinário 625.263 quanto a discussão sobre a possibilidade de se renovar sucessivamente a autorização de interceptação telefônica para fins de investigação criminal, sem limite definido de prazo, diferentemente do disposto no artigo 5º da Lei 9.296/96, que permite a prorrogação uma só vez por igual período[73].

Essa banalização é vislumbrada no que se refere a guarda de dados quanto à requisição de dado cadastral por autoridade administrativa, que exige apenas o fundamento legal de competência expressa e motivação para o acesso desses dados[74], não sendo necessária ordem judicial, como no caso dos registros de conexão e aplicação.

---

[72]http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Intercepta%C3%A7%C3%B5es-para-o-site.pdf

[73]http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=242810

[74]BRASIL. Decreto 8.771/16. Art. 11.

Diante da facilidade de acesso a esses dados, as autoridades vêm requerendo informações que vão além daquilo delimitado na categoria, em visível tentativa de ampliação de informações acessíveis, apesar de a regulamentação ter expressamente considerado apenas a filiação,o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário[75], conforme se observa no julgado abaixo:

> Trata-se de Mandado de Segurança, com pedido de liminar, impetrado por TWITTER BRASIL REDE DE INFORMAÇÃO LTDA em face do DELEGADO DE POLÍCIA FEDERAL, objetivando a obtenção de provimento jurisdicional que determine a anulação da requisição emanada da autoridade coatora que exigiu o fornecimento do "máximo de dados possíveis, como o IP de acesso da máquina do responsável, datas de acesso, qualificação completa dos responsáveis e dados cadastrais do usuário @EnkiEa666". Requer, ainda, que seja determinado à autoridade coatora que se abstenha de instaurar inquérito policial ou adotar qualquer medida contrária à impetrante, seus representantes legais, responsáveis ou empregados, em decorrência da negativa de fornecimento de tais dados sem ordem judicial. 7o".
> Depreende-se que a lei permite às autoridadesadministrativas, com competência para tanto, requisitar informações aos provedores de internet referentes aos seus usuários, desde que tais informações se limitem a dados cadastrais, como qualificação pessoal, filiação e endereço. Entendo, pois, que informações relacionadas aos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, dependem de autorização judicial, como expressamente previsto no referido 1, do art. 10, da Lei n. 12.965/14[76].

No caso em questão, após a negativa de fornecimento, a representante legal da empresa foi intimada a comparecer à Superintendência Regional da Polícia Federal em São Paulo para prestar esclarecimentos no interesse da Justiça, na tentativa de que as informações fossem fornecidas sem a ordem judicial.

A incessante busca dos agentes estatais por maiores informações, aliada a uma insegurança em relação a que tipo efetivamente de proteção dos dados pessoais há no ordenamento jurídico pátrio, depende da postura dos provedores de conexão e de aplicação de se manterem firmes em proteger os usuários e os seus serviços, judicializando as demandas quando os requerimentos forem questionáveis..

Considerando o critério da proporcionalidade, não foi levado em conta a quantidade de metadados que virá a ser gerada a partir da consolidação do paradigma computacional da Internet das Coisas.

---

[75] § 2º São considerados dados cadastrais:
I - a filiação;
II - o endereço; e
III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

[76] BRASIL. TRF-3. Mandado de Segurança 0001972-91.2015.4.03.6100. Disponibilização no D.Eletrônico de sentença em 28/04/2015

Esta é caracterizada por seu papel transformador da rede, na qual objetos do cotidiano passam a ser combinados com a conectividade da Internet, relacionando-se entre si, trazendo uma imensurável capacidade analítica de dados pessoais e sensíveis, que promete transformar a forma como nos relacionamos em todos os aspectos da vida em sociedade[77].

Dispositivos tais como computadores, celulares e tablets, já não são mais os únicos conectáveis à internet. E, diante do potencial de rentabilidade dessa nova tecnologia, uma das maiores empresas de pesquisa e consulta de tecnologia da informação, Gartner Inc., estima que o crescimento até 2020 no mundo será da ordem de 20,8 bilhões de aparelhos com essa interface, anteriormente não conectáveis, o que representa três vezes mais dispositivos do que se têm conectados atualmente[78].

Em um contexto em que os objetos cada vez mais tendem a tornarem-se dispositivos conectáveis ou automatizados, estariam os provedores obrigados a armazenar também os logs de conexão e de aplicação?

Imaginemos o cenário de uma casa completamente automatizada em que a televisão, a geladeira, a iluminação, o climatizador do ambiente, a garagem e o sistema de segurança estejam conectadas a internet, interajam entre si e adaptem-se às preferências do proprietário do imóvel. Ou então o exemplo de uma grande empresa varejista, que utilize de máquinas automatizadas para controlar melhor sua produtividade e reduzir os custos, aumentando assim o lucro.

Ora, é questionável, para os fins que justificam a guarda de logs, investigação e apuração de ilícitos, a proporcionalidade legal da coleta dos metadados desses dispositivos com o objetivo de dar efetividade ao direito à segurança frente à larga contribuição para a tão temida sensação do cidadão estar sendo vigiado a todo momento pelo risco de violação do acesso desses dados.

O Instituto de Tecnologia e Sociedade do Rio atentou para este fato e propôs que a regulação do Marco Civil poderia ter estabelecido uma exceção expressa quanto à guarda de registros relativos à Internet das Coisas[79], justamente porque o volume deste tipo de registro é gigantesco, o que gera custos elevados e desproporcionais aos provedores, além das implicações inerentes ao maior volume de dados para a privacidade dos cidadãos, e afirma

[77]ESKENS, Sarah Johanna. Profiling the European consumer in the internet of things: how will the general data protection regulation apply to his form of pesonal data processing and how should it?
[78]http://www.gartner.com/newsroom/id/3165317
[79]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. ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA

que a maior parte desses dados seria exorbitante e prescindíveis para atividades de exequibilidade legal.

Pode-se argumentar que é um exercício de futurologia tentar lidar com tais questões no cenário brasileiro, afinal, ainda não se sabe com que velocidade estas tecnologias serão implementadas e terão real aplicabilidade. No entanto, certamente o Judiciário e o Legislativo precisarão enfrentar esses novos dilemas que irão surgir em um período não tão distante da realidade atual.

Em um panorama mais basilar e perceptível, um das maiores preocupações de especialistas quando se trata de proteção de dados pessoais no ordenamento jurídico brasileiro é a defasagem legislativa e a regulação esparsa em comparação a outros países, o que acaba gerando insegurança jurídica aos cidadãos e às empresas estrangeiras que desejam investir no país.

A despeito disso, é perceptível que o papel do Marco Civil não foi detalhar sobremaneira a discussão sobre privacidade e proteção de dados, até porque se esboçava inicialmente uma legislação de caráter fundamentalmente principiológico

Ainda assim, apesar de controverso e exposto a inúmeras críticas, somente a partir da vigência do decreto 8.771/16 se definiu legalmente dados pessoais como qualquer "*dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa"*.

A Organização Privacy International divulgou recentemente uma relatório global chamado de "Estado de vigilância", para testar as políticas de vigilância de e práticas nos países pesquisados e, assim, traçar um padrão eficiente frente aos desafios inerentes ao direito a privacidade e que estão cada vez mais em voga.

De acordo com o relatório, 9 dos 16 países pesquisados não possuem uma lei de proteção de proteção de dados compreensiva, ainda que os mesmos tenham se voltado para o incentivo de inovações, sejam startups ou cidades inteligentes, entre esses o Brasil estaria incluído[80].

Até o presente momento não há no território brasileiro lei vigente específica acerca do tratamento de dados pessoais, que não pode mais ser analisado através do prisma meramente instrumental, pois é umas das condições essenciais e intrínsecas para que se assegure a proteção dos dados e o livre desenvolvimento da personalidade no meio virtual.

[80]https://privacyinternational.org/node/986

Curiosamente, muito mais pela conjuntura histórica do que pela demanda da sociedade, o Brasil é um dos poucos países que possui uma Lei de Acesso a Informação anterior a uma Lei de Proteção de Dados.

O atual estágio em que se encontra a sociedade caminha para que cada vez mais empresas utilizem do processamento de grande volume de dados coletados para retirar inteligência disto e tomar decisões que irão influenciar diretamente seus modelos de negócios, por exemplo, possíveis novos empregados em processos seletivos, concessão de financiamento após o credit scoring, big data e sua estreita relação com as eleições.

Para além das situações mencionadas, a ausência de uma regulação comprometida gera casos como o que Ministério Público Federal de São Paulo recentemente encontrou[81]: descobriu-se que o INSS havia fornecido dados pessoais sigilosos de milhares de beneficiários da previdência para que uma empresa de crédito consignado enviasse correspondências aos aposentados e pensionistas com propostas para a concessão de empréstimos.

O MPF/SP ajuizou ação civil pública pedindo além do pagamento de indenizações por danos morais individuais e coletivos, que a autarquia federal fosse obrigada a implementar medidas que garantissem o sigilo de dados pessoais sob seus cuidados e deem publicidade a episódios de violação.

Encontra-se em discussão o Projeto de Lei 5.276/2016, que objetiva recolocar o Brasil no patamar necessário para que se dê maior proteção aos dados pessoais do usuário e segurança jurídica para empresas e provedores, ao oferecer limites claros de atuação.

Percebendo a relevância do tema, com a irrefreável tendência mundial de utilização dessas informações, ainda que tenha sido retirado do regime de urgência, a Câmara criou uma comissão para analisar o projeto de lei 5.276/16, em 26 de outubro de 2016, em que se apresentará um plano de trabalho buscando ouvir todos os setores interessados[82].

Sob o enfoque técnico, o projeto esquematiza conceitos e princípios de proteção de dados pessoais, delimitando de maneira concisa seu escopo de aplicação e os critérios interpretativos necessários, e esclarece pontos antes obscuros, tais quais: requisitos do início ao término do tratamento de dados pessoais (arts. 7º a 16); os direitos do titular (art. 17 a 22);

---

81 http://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/mpf-sp-processa-inss-e-financeira-que-usou-dados-sigilosos-para-oferecer-credito-consignado

82 http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/518461-INSTALADA-COMISSAO-PARA-ANALISAR-REGRAS-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html

o debate não é centrado no setores privado, pois vê a necessidade de regular especificamente o tratamento dos dados pessoais do cidadão pelo Poder Público (arts. 23 à 32); responsabilidade civil da cadeia de agentes inserida no tratamento (art. 42); a regulação da transferência internacional dos dados pessoais (art. 33 a 35); mecanismos de incentivo à segurança e boas práticas para o setor regulado (art. 45 a 51); e, as infrações administrativas e respectivas sanções.

Fundamental é o artigo 6º que estabelece os princípios da proteção de dados pessoais, além dos já mencionados princípios da finalidade, adequação transparência, necessidade, qualidade dos dados,estão expressamente também os princípios do livre acesso, da segurança, da prevenção e da não discriminação.

É louvável a proposição de se criar uma autoridade específica à matéria, simbolizado pelo Conselho Nacional de Proteção de Dados Pessoais, que será composto por representantes de órgãos de todas as esferas. Somado ao órgão fiscalizatório competente, ambos terão o papel fundamental para tornar plenamente efetiva a regulação da lei geral de dados e formular e implementar políticas públicas relacionadas à proteção de dados pessoais.

É digno de nota que, de acordo com artigo 61, §1º, inciso II, da Constituição Federal, somente projetos de lei de autoria do executivo como o em questão podem criar cargos, funções ou empregos públicos que são necessários para a implementação do órgão fiscalizador, o que torna ainda mais singular tal iniciativa legislativa.

Ter um ambiente claro sobre tratamento de dados, vazamentos, modelos de transferência, procedimentos de apuração de infrações e como atuará uma futura autoridade de proteção de dados interessa muito a todos os setores, por isso mais de 40 organizações da sociedade civil, brasileiras e internacionais, já manifestaram abertamente apoio ao projeto de lei:

> Trata-se, portanto, de uma proposta legislativa capaz de suprir eficazmente grave lacuna no ordenamento jurídico brasileiro, a ponto de trazer segurança jurídica para o cidadão, para a atividade empresarial e para a administração pública no tratamento dos dados pessoais, o que só reforça o regime de tramitação em urgência constitucional atribuído à matéria[83].

Ressalte-se que não há um modelo único correto de proteção de dados pessoais e que diferentes países adotam diferentes métodos para proteger seus cidadão, mas relegar a discussão de proteção de dados pessoais, apesar de a ocorrência de violações não ser perceptível no dia a dia,em uma perspectiva macro, tem diversas consequências e riscos.

[83]http://intervozes.org.br/wp-content/uploads/2016/06/Carta-Aberta.-PL-Dados-Pessoais.02.06.2016.pdf

# 5) CONCLUSÃO

Voltemos a pergunta inicial proposta no presente trabalho: considerando a análise feita pela jurisprudência europeia sobre a retenção de logs, o Marco Civil da Internet e o Decreto 8.771/16, ao preverem a guarda preventiva de dados por tempo determinado, atenderam aos padrões de segurança técnicos e procedimentos claros para a proteção em última medida da privacidade para o desenvolvimento da personalidade dos usuários da rede?

O que se vislumbrou, após a análise comparada, é que tanto o Marco Civil quanto o Decreto não adotaram procedimentos e critérios técnicos de segurança, mantendo, assim, em constante ameaça a garantia de que o acesso a esses metadados atendam a finalidade legal preceituada e de que o direito a proteção dos dados pessoais e à privacidade não sejam violados seja pelo setor público ou privado.

A imprescindibilidade de discussão de um modelo de proteção de dados pessoais ocorre não somente em nível nacional, mas também mundial, pois, após 20 anos de vigência da Diretiva 95/46/EC, o Parlamento Europeu aprovou em 2016 novas regras de proteção de dados pessoais, atualizadas em função do progresso tecnológico ocorrido, principalmente em relação ao refinamento da coleta e tratamento de dados, com o objetivo de retomar o controle perdido pelos cidadãos quanto às suas informações que circulam na rede.

Um dos pontos mais relevantes e que está diretamente correlacionado com as decisões analisadas de guarda de logs preventiva é o estabelecimento de um sistema mais apurado de accountability e de níveis das medidas de segurança, proporcionais ao risco envolvido na atividade de processamento de dados pessoais.[84]

Ainda que alguns Cortes Constitucionais tenham declarado inconstitucionais leis que determinavam a retenção de dados em seus países e sinalizaram pela impossibilidade de se introduzir novas legislações, Hans-Jörg Albrecht[85] afirma que a Alemanha já se movimenta e discute uma nova lei quanto ao tema compromissada com uma máxima proteção de dados e mínima retenção de dados, na tentativa de reconciliar com o princípio da proporcionalidade e fundamento da declaração de inconstitucionalidade da Corte Constitucional Alemão.

---

[84]Hert,.Paul de.Papakonstantinou, Vagelis The new General Data ProtectionRegulation: Still a sound system for the protection of individuals http://www-sciencedirect-com.ez54.periodicos.capes.gov.br/science/article/pii/S0267364916300346

[85]ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA. Direito à privacidade e a guarda obrigatória de dados para investigações: entrevista com Prof. Dr. Dr. h.c. Hans-Jörg Albrecht. 2016 Disponível em http://www.internetlab.org.br/wp-content/uploads/2016/06/Entrevista_ProfHans_final.pdf

Conclui-se, portanto, que devem ser implementadas medidas técnicas e procedimentais claras e concisas para proteção não só da guarda de registros de conexão e aplicação, tema central abordado neste trabalho, mas também de todo uma ampla gama de dados gerados para que os novos rumos da proteção de dados no Brasil se relacionem ao livre desenvolvimento da personalidade do indivíduo e também da livre iniciativa, fornecendo um ambiente com igualdade de oportunidades para que cada um persiga os seus objetivos de vida em uma comunidade democrática.

# Referências


ALEMANHA,Tribunal Constitucional Federal Alemão. BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08, disponível em http://www.bverfg.de/e/rs20100302_1bvr025608en.html

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA. Direito à privacidade e a guarda obrigatória de dados para investigações: entrevista com Prof. Dr. Dr. h.c. Hans-Jörg Albrecht. 2016 Disponível em http://www.internetlab.org.br/wp-content/uploads/2016/06/Entrevista_ProfHans_final.pdf

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA 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.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 13 out. 2016.

BLANCHETTE, Jean-François.Johnson, Deborah G. Data retention and the panoptic society: The social benefits of forgetfulness Disponívelemhttp://polaris.gseis.ucla.edu/blanchette/papers/is.pdf

BRASIL. Departamento de Proteção e Defesa do Consumidor. Processo Administrativo nº 08012.003471/2010-22 Disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=43&data=23/07/2014 . Acesso em 13/10/2016

BRASIL. STJ. Quarta Turma. AgRg no REsp 1402104/RJ. Relator: ARAUJO, Raul. Julgado em 27/05/2014.

BRASIL. STJ. REsp 1417641/RJ, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 25/02/2014, DJe 10/03/2014

BOLZAN, José Luis. NETO. Elias Jacob Menezes. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma do surveillance. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.418

CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil da Internet**. Disponível em:<http://www.migalhas.com.br/dePeso/16,MI211753,51045-os+conceitos+de+provedores+no+Marco+Civil+da+Internet>. Acesso em:20 out. 2016.

COLNAGO, CLAUDIO OLIVEIRA SANTOS, Provedores de conexão e guarda de registros de acesso a aplicações da internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014

CRUZ, Francisco Brito. Análise do Agravo de Instrumento 2206954-25.2015.8.26.0000/TJ-SP. Disponívelhttp://www.omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª. ed. Rio de Janeiro: Renovar, 2006.

EUROPA. Tribunal de Justiça da União Europeia. Acórdão nos apensos C-293/12 e C-594/12 Disponível em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d51de752300d774c8ab97fb5743d6e0306.e34KaxiLc3eQc40LaxqMbN4Pa3uNe0?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=290518. Acessado em 23/09/2016

ESKENS, Sarah Johanna. Profiling the european consumer in the internet of things: how will the general data protecion regulation apply to his form of pesonal data processing and how should it?
[1]http://www.gartner.com/newsroom/id/3165317

Feiler, L., The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, European Journal of Law and Technology, Vol. 1, Issue 3, 2010.Disponível em: http://ejlt.org/article/view/29/75

Handbook on European Data Protection Law, pág 19Disponívelemhttp://www.echr.coe.int/documents/handbook_data_protection_eng.pdf
INTERNETLAB. Direito à Privacidade e a Guarda Obrigatória de Dados para Investigações: entrevista prof. Dr. Dr. h.c. Hans-Jörg Albrecht Disponível em http://www.internetlab.org.br/wp-content/uploads/2016/06/Entrevista_ProfHans_final.pdf

Hert.Paulde.Papakonstantinou, Vagelis The new General Data Protection Regulation: Still a sound system for the protection of individuals http://www-sciencedirect-com.ez54.periodicos.capes.gov.br/science/article/pii/S0267364916300346

JANSEN, Bernard J. , Search log analysis: What it is, what's been done, how to do it. Library &Information Science Research 28 (2006) pág. 408. Disponível em: http://www.sciencedirect.com/science/article/pii/S0740818806000673

KAISER, Anna-Bettina.*German Federal Constitutional Court:* German Data Retention Provisions Unconstitutional In Their Present Form; Decision of 2 March 2010, NJW 2010, p. 833. European Constitutional Law Review, Outubro 2010. Vol. 6, Iss. 3Disponível em https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S1574019610300083

LEMOS, RONALDO. Marco Civil da Internet, uma construção da sociedade In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. 3

LESSIG, Lawrence. Reading de Constitution in Cyberspace. p. 11 Disponível em http://emoglen.law.columbia.edu/LIS/archive/const-theory/lessig-reading.pdf

Loideain, Nora Ni.EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. Media and Communication, 2015, Volume 3, Issue 2Disponívelem: http://www.cogitatiopress.com/ojs/index.php/mediaandcommunication/article/view/297

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito do consumidor. 1ª Edição. São Paulo:Saraiva, 2014

MOLON, ALESSANDRO. Marco Civil da Internet, uma construção da sociedade. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. XXVIII

NETO, MARIO FURLANO. GARCIA. BRUNA PINOTTI Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p.776

POLI, SARA, The Legal Basis of Internal Market Measures With a Security Dimension. Comment on Case C-301/06 of 10/02/2009, EuropeanConstitutional Law Review, 2010, Vol. 6, No. 1, pp. 137-157Disponívelem: http://cadmus.eui.eu/handle/1814/40038

RENÁ, Paulo.**Fundamentos da multa aplicada à OI por monitorar a navegação de internautas**. Disponível em:<http://ibidem.org.br/fundamentos-da-multa-aplicada-a-oi-por-monitorar-navegacao-de-internautas/>. Acesso em: 13 out. 2016.

RODOTÁ, Stefano. A Vida na sociedade da vigilância: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. São Paulo. Renovar. 2008. p. 37

Relatório Quem Defende Seus Dados?. Disponível em: <http://quemdefendeseusdados.org.br/pt/ >. Acesso em: 24 out. 2016.

SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou Retrocesso? A Responsabilidade Civil por Dano derivado do Conteúdo Gerado por Terceiro. Disponível em http://www.andersonschreiber.com.br/downloads/artigo-marco-civil-internet.pdf

SCHREIBER, Anderson. Direitos da personalidade - São Paulo: Atlas, 2011

SHAH, Reema. Law Enforcement and Data Privacy: A Foward-Looking Approach. The Yale Law Journal 125(2): p. 543-558 · Novembro 2015 Disponível em: https://www.researchgate.net/publication/287221402_Law_Enforcement_and_Data_Privacy_A_Forward-Looking_Approach

STOEVA, ELITSA. The Data Retention Directive and the right to privacy. Academy of European Law. Publicado em 23/01/2015 pág. 579 http://link.springer.com/article/10.1007/s12027-015-0370-7

STRECK, LUIZ LÊNIO. Apontamentos hermenêuticos sobre o Marco Civil Regulatório da internet. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 p. 340

STREIBEL, Fabro. O Portal de Consulta Pública do Marco Civil da Internet. In: George Salomão Leite, Ronaldo Lemos (coordenadores) – **Marco Civil da Internet.** São Paulo: Atlas, 2014 Pág.18

TZANOU, Maria, Is Data Protection the same as privacy? An Analysis of Telecommunications Data Measures, Journal of Internet Law, September 2013, Setembro, 2013, Vol.17 (3).

UNIÃO EUROPEIA. Carta de Direitos Fundamentais da União Europeia. Disponível em http://www.europarl.europa.eu/charter/pdf/text_pt.pdf