

UNIVERSIDADE FEDERAL DO PARANÁ

ANA MARIA HIGUTI BECKER

**PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO NO CIBERESPAÇO:
LIMITES À INTERVENÇÃO JUDICIAL BRASILEIRA NO WHATSAPP**

CURITIBA

2016

ANA MARIA HIGUTI BECKER

**PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO NO CIBERESPAÇO:
LIMITES À INTERVENÇÃO JUDICIAL BRASILEIRA NO WHATSAPP**

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito, Setor de Ciências Jurídicas da Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Cesar Antonio Serbena.

CURITIBA

2016

*À família, ao meu amor e aos queridos amigos
que contribuíram para a realização deste
trabalho.*

AGRADECIMENTOS

Agradeço aos meus pais e ao meu irmão (Donatilio Becker, Doroti Aiko Higuti Becker e Carlos Augusto Higuti Becker) pela união nos momentos mais difíceis; pelo amor e carinho que temos uns pelos outros; pela compreensão de minhas ausências nos últimos anos devido à minha dedicação aos estudos e aos trabalhos; e pelo apoio dado a mim para que eu buscasse a realização de meus sonhos.

Ao meu querido namorado Josiel Q. de Oliveira, agradeço por toda a paciência durante os momentos mais estressantes da faculdade; pelos inúmeros livros separados em sebos e livrarias para me ajudar não só na graduação, mas também neste trabalho e no projeto de dissertação de mestrado; e pelo companheirismo demonstrado nos últimos dois anos, que contribui ao fortalecimento do amor que temos um pelo outro.

Ao meu professor orientador Dr. Cesar Antonio Serbena, agradeço por ter me dado a oportunidade de participar do projeto de Iniciação Científica e de ter aceito meu pedido de orientação neste trabalho, ajudando-me a descobrir e lapidar o interesse pelos temas pesquisados.

À professora Dra. Natalina Stamile, agradeço por aceitar meu pedido de co-orientação neste trabalho. Suas contribuições, aliadas às do professor orientador, foram essenciais para que este trabalho pudesse ser finalizado.

Aos meus colegas do gabinete da 25ª Vara Cível de Curitiba (Fabianno Raphael Gonçalves, Flávia Muniz Felix Piccoli, Júlia Carolina Collere Posseti, Marcelo Mazzali e Melanie Merlin de Andrade), agradeço pela oportunidade de estágio em um local tão incrível; pela parceria e pela união em busca da melhor prestação jurisdicional possível; e pelo incentivo dado a mim, impulsionando-me a ir cada vez mais longe em minha vida profissional.

Aos amigos (especialmente Gilson Rodrigues Cardoso da Silva, Guilherme Lages Guerra, Marcelo Brezolin Bortolotto e Matheus Aquino P. Krüger), agradeço pelo apoio durante esta árdua jornada na graduação.

RESUMO

Este trabalho tem por escopo o estudo de recentes decisões judiciais nacionais em primeiro grau de jurisdição, prolatadas de fevereiro de 2015 a julho de 2016, que ordenaram a suspensão do aplicativo *WhatsApp* em todo o território brasileiro por prazo determinado. Fez-se necessária a análise comparativa entre as decisões, a fim de encontrar pontos convergentes nas fundamentações dos diferentes Juízos e averiguar se houve respeito aos princípios da privacidade e da liberdade de comunicação no ciberespaço. Ainda, reputou-se imprescindível o estudo do Marco Civil da Internet, a fim de averiguar se serviria de suporte jurídico à concessão de ordens judiciais para que os aplicativos disponibilizassem conteúdo de comunicações privadas. Também foi feito um contraponto entre a legislação nacional de proteção de dados e a da União Europeia, a fim de extrair inspirações e comparações com o modelo nacional. Os objetivos perseguidos foram atingidos por meio de pesquisa jurisprudencial e bibliográfica, bem como através da extração de dados junto a diversos sítios eletrônicos da Web.

Palavras-chave: *WhatsApp*, Marco Civil da Internet, ciberespaço, suspensão.

ABSTRACT

This work has as scope the study of recent national judicial decisions in the first degree of jurisdiction, from February 2015 to July 2016, that ordered the suspension of the *WhatsApp* application throughout the Brazilian territory for a determined period. A comparative analysis of decisions was necessary in order to find convergent points in the grounds of the different judgments and to ascertain whether there was respect for the principles of privacy and freedom of communication in cyberspace. Also, it was considered essential to study the Civil Internet Framework, in order to find out whether it would serve as legal support for the granting of court orders for applications to make available private communications content. A counterpoint was also made between national data protection legislation and that of the European Union, in order to draw inspiration and comparisons with the national model. The objectives pursued were reached through a jurisprudential and bibliographical research, as well as through the extraction of data from various electronic websites.

Keywords: *WhatsApp*, Civil Internet Framework, cyberspace, suspension.

SUMÁRIO

1 INTRODUÇÃO	9
2 PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO NO CIBERESPAÇO.....	12
2.1 PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO COMO DIREITOS HUMANOS, FUNDAMENTAIS E DA PERSONALIDADE	12
2.1.1 Direitos humanos	12
2.1.2 Direitos fundamentais	14
2.1.3 Direitos da personalidade	15
2.2 CIBERESPAÇO E MUDANÇAS NA CONCEPÇÃO DE PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO	18
3 REGULAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL	25
3.1 REGULAÇÃO DA PROTEÇÃO DE DADOS: PARADIGMAS INTERNACIONAIS E O MARCO CIVIL DA INTERNET	25
3.2 PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA: CONTRAPONTO E INSPIRAÇÕES	35
4 JUDICIALIZAÇÃO DO DEBATE NO BRASIL: SUSPENSÕES NACIONAIS DO WHATSAPP	44
4.1 ESTUDO DAS DECISÕES JUDICIAIS QUE SUSPENDERAM O WHATSAPP EM PRIMEIRA INSTÂNCIA	44
4.1.1 Processo nº 0013872-87.2014.8.18.0140	45
4.1.2 Processo nº 0017520-08.2015.8.26.0564	49
4.1.3 Processo nº 20155500078	52
4.1.4 Processo nº 062-00164/2016	58
4.2 ENTENDIMENTO DO STF NA ADPF 403 MC/SE E NA ADI 5527	60
4.2.1 ADPF 403 MC/SE	61
4.2.2 ADI 5527.....	63
4.3 ANÁLISE CRÍTICA DOS DADOS OBTIDOS	65
5 CONCLUSÕES	74
REFERÊNCIAS	76

1 INTRODUÇÃO

A internet e, especialmente, aplicativos que permitem troca online instantânea de dados entre pessoas ocasionaram uma verdadeira transformação cultural que reclama do Direito e de seus operadores a apreciação mais detida desse fenômeno.

A crescente expansão do mundo virtual tem acarretado a superação de distâncias e fronteiras entre indivíduos, permitindo que a comunicação de um continente a outro ocorra, em tempo real, através de meros toques em um *smartphone*. Além disso, é um instrumento democrático de acesso à informação e difusão de dados de toda a natureza.

Por consequência, quanto mais disseminados os serviços de troca de mensagens pela internet, maior se torna a dependência dos indivíduos em relação a esses serviços¹.

No entanto, essas facilidades também podem ser utilizadas para fomentar a criminalidade. Segundo MARC GOODMAN, fundador do *Future Crimes Institute* e investigador de delitos cibernéticos, os criminosos atualizam continuamente suas técnicas para incorporar as mais recentes tecnologias em seus *modus operandi*. Eles “adotaram o mundo online muito antes que a polícia pudesse ao menos ter contemplado a ideia e, desde então, estão sempre um passo à frente das autoridades”².

Em que pese o suposto direito estatal de interceptar dados eletrônicos, sob o pretexto de garantir segurança aos cidadãos, o próprio Estado tem o dever de respeitar e proteger a privacidade e a liberdade de comunicação dos particulares no ciberespaço.

No Brasil, essa discussão ganhou relevância pois, entre fevereiro de 2015 e julho de 2016, alguns magistrados atuantes na primeira instância

¹ SHAPIRO, Carl; VARIAN, Hal R. *A Economia da Informação: como os princípios econômicos se aplicam à era da Internet*. Rio de Janeiro: Campus, 1999, p. 204-205.

² GOODMAN, Marc. *Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso*. São Paulo: HSM Editora, 2015, p. 7-8.

estadual do Judiciário proferiram decisões que suspenderam em todo o território brasileiro o *WhatsApp*, aplicativo tecnológico que viabiliza a troca de mensagens e dados entre seus usuários por meio da internet.

O debate tornou-se ainda mais complexo devido ao posicionamento do Supremo Tribunal Federal (STF) na Ação de Descumprimento de Preceito Fundamental (ADPF) 403 MC/SE.

Assim, no Capítulo 1 será feito um breve estudo dos princípios da privacidade e da liberdade de comunicação, a fim de verificar se possuem *status* de direitos humanos, fundamentais e de personalidade. Após, será analisado de que forma os avanços tecnológicos na web têm acarretado mudanças nos conceitos desses princípios.

No capítulo 2, proceder-se-á ao estudo da regulação de dados no Brasil feita pela Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet. Em seguida, haverá a apresentação da maneira como a União Europeia trata da proteção de dados e dos princípios estudados no Capítulo anterior, a fim de serem estabelecidas relações e inspirações ao modelo nacional.

No Capítulo 3, passar-se-á ao exame das decisões que determinaram a suspensão nacional do *WhatsApp*, a fim de que sejam encontrados fundamentos fáticos comuns entre elas. Também será averiguado se o Marco Civil da Internet foi utilizado como embasamento legal ao bloqueio do aplicativo. Após, haverá a abordagem da Ação de Descumprimento de Preceito Fundamental nº 403 e da Ação Direta de Inconstitucionalidade nº 5527, as quais tramitam no STF e versam sobre o tema tratado nas decisões de primeira instância. A partir dos dados colhidos, ocorrerá a análise crítica dos referidos atos judiciais, à luz dos princípios da privacidade e da liberdade de expressão no ciberespaço, da interpretação do Marco Civil da Internet adotada no Capítulo 2, bem como dos ensinamentos de J. J. CANOTILHO e outros a respeito da proporcionalidade.

Por fim, na conclusão, serão retomados os principais dados colhidos nos três Capítulos, apresentando-se sugestões para o incremento da proteção de dados, da privacidade e da liberdade de comunicação no ciberespaço nacional.

2 PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO NO CIBERESPAÇO

Neste Capítulo, será averiguado se os princípios da privacidade e da liberdade de comunicação podem ser considerados como direitos da personalidade, direitos fundamentais e direitos humanos.

Em seguida, passar-se-á ao exame do modo como o ciberespaço e o desenvolvimento de novas tecnologias como a criptografia transformaram a concepção clássica desses princípios.

2.1 PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO COMO DIREITOS HUMANOS, FUNDAMENTAIS E DA PERSONALIDADE

Segundo ANDERSON SCHREIBER, os termos “direitos humanos”, “direitos fundamentais” e “direitos da personalidade” destinam-se a contemplar atributos da pessoa humana merecedores de proteção jurídica, alterando-se apenas o plano em que essa personalidade se manifesta³.

Passa-se, então, à análise de cada um desses âmbitos de proteção dos direitos em análise neste trabalho.

2.1.1 Direitos humanos

Para SCHREIBER, a expressão “direitos humanos” é utilizada no plano internacional, independentemente do modo como cada Estado regula a matéria⁴.

³ SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011, p. 13.

⁴ *Idem*.

Nesse âmbito, então, pode-se citar a Declaração Universal dos Direitos Humanos (DUDH) como principal marco de proteção internacional da pessoa humana.

Elaborada por representantes de diferentes origens jurídicas e culturais de todas as regiões do mundo, a DUDH foi proclamada pela Assembleia Geral das Nações Unidas em Paris, em 10 de dezembro de 1948, através da Resolução 217 A (III) da Assembleia Geral, como uma norma comum a ser alcançada por todos os povos e nações. Ela estabeleceu, pela primeira vez, a proteção universal dos direitos humanos⁵.

Note-se que no artigo XII da DUDH restou consagrado o reconhecimento da privacidade como um direito humano. Assim, tornou-se expressa a proteção do sujeito em face de interferências ou ataques estatais à vida privada, em sua família, lar ou correspondência⁶.

Da mesma forma, o artigo III da Declaração alçou a liberdade em sentido amplo⁷ à condição de direito humano⁸.

Especificamente quanto à liberdade de comunicação, o artigo XIX de modo expresso garantiu o direito de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras⁹.

⁵ Informações disponíveis em < <http://www.dudh.org.br/declaracao/> >. Acesso em 10 de setembro de 2016.

⁶ “Artigo XII. Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”. Disponível em <<http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>>. Acesso em 10 de setembro de 2016.

⁷ Note-se que, embora este trabalho verse sobre a liberdade de comunicação, esta se refere a espécie do gênero “liberdade”, assim como a liberdade de expressão e de locomoção. Assim, tendo em vista que o princípio-gênero “liberdade” encontra guarida na DUDH, todas as suas ramificações também possuem o *status* de direito humano.

⁸ “Artigo III. Todo ser humano tem direito à vida, à liberdade e à segurança pessoal”. Disponível em <<http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>>. Acesso em 10 de setembro de 2016.

⁹ “Artigo XIX. Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras”. Disponível em <<http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>>. Acesso em 10 de setembro de 2016.

Desse modo, verifica-se que a privacidade e a liberdade de comunicação podem ser considerados direitos humanos.

2.1.2 Direitos fundamentais

O termo “direitos fundamentais” é normalmente utilizado para designar direitos positivados na Constituição de determinado Estado¹⁰. Por esse motivo, consoante SCHREIBER, é que esse termo designa a proteção humana no campo do direito público em face da atuação do poder estatal¹¹.

No mesmo sentido é a lição de CARLOS ALBERTO BITTAR, segundo o qual os direitos fundamentais são considerados objeto de relações de direito público para efeitos de proteção do indivíduo contra o Estado¹².

CLÁUDIO ARI MELLO vai além e ensina que os direitos fundamentais exercem funções negativas ou positivas, a serem respeitadas tanto pelo Estado quanto pelos particulares:

A tensão entre o princípio constitucional e o princípio democrático é em grande parte reflexo da tensão entre direitos fundamentais e democracia. A ideia de direitos fundamentais que se firmou no constitucionalismo moderno representa em geral o estabelecimento de limites negativos e positivos ao processo democrático. Os direitos fundamentais exercem uma função negativa ou restritiva quando proíbem a prática de determinadas condutas ao Estado e a particulares, e exercem uma função positiva ou diretiva quando impõem, principalmente ao Estado, a prática de outras condutas. O Estado é, portanto, o principal destinatário dos direitos fundamentais¹³.

¹⁰ FARIAS, Edilson Pereira de. *Colisão de direitos*. Porto Alegre: Sergio Antonio Fabris Editor, 2000, p. 72.

¹¹ SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011, p. 13.

¹² BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7. ed. Rio de Janeiro: Forense Universitária, 2008, p. 19.

¹³ MELLO, Cláudio Ari. *Democracia constitucional e direitos fundamentais*. Porto Alegre: Livraria do Advogado Editora, 2004, p. 143.

A Constituição Federal de 1988 optou por prestigiar e garantir maior estabilidade aos direitos fundamentais, concedendo-lhes *status* de cláusulas pétreas, conforme estabelecido no artigo 60, §4º, inciso IV da Carta Magna¹⁴.

Portanto, por reconhecer que os direitos fundamentais são indispensáveis à proteção da pessoa humana e à manutenção da democracia, o poder constituinte originário garantiu que eles jamais fossem abolidos por emenda constitucional, o que justifica, por consequência, que o intérprete assegure ampla proteção a esses direitos.

O artigo 5º da Constituição Federal está inserido no capítulo de direitos e deveres individuais e coletivos, motivo pelo qual também possui o referido *status* de cláusula pétrea.

Note-se que o inciso VIII do artigo 5º consagra a liberdade de comunicação como direito fundamental, independente de censura ou licença¹⁵.

Da mesma forma, o inciso IX do mesmo dispositivo garante a inviolabilidade da vida privada, assegurando o direito de indenização por dano moral ou material decorrente de sua violação¹⁶.

Pelo exposto, impõe-se o reconhecimento de que a privacidade e a liberdade de comunicação são, também, direitos fundamentais.

2.1.3 Direitos da personalidade

¹⁴ “Artigo 60, § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir: (...) IV - os direitos e garantias individuais”. *In* BRASIL. Constituição Federal. Brasília, Senado Federal, 1988.

¹⁵ “Art. 5º (...) IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”. *In* BRASIL. Constituição Federal. Brasília, Senado Federal, 1988.

¹⁶ Art. 5º (...) IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; X - 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. *In* BRASIL. Constituição Federal. Brasília, Senado Federal, 1988.

Para ANDERSON SCHREIBER, “direitos da personalidade” é o termo empregado em alusão a atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação com os particulares¹⁷.

CARLOS ALBERTO BITTAR acrescenta que se consideram como da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos do sujeito¹⁸.

Desse modo, o objeto dos direitos da personalidade são os bens constituídos por qualidades físicas ou morais da pessoa, individualizados pelo ordenamento jurídico. Tratam-se, segundo BITTAR, de direitos ínsitos da pessoa, em função de sua própria estruturação física, mental e moral¹⁹.

Esses direitos possuem peculiaridades como a intransmissibilidade e a irrenunciabilidade, que se revelam inclusive como limites à própria ação do titular²⁰.

No direito civil brasileiro, os direitos da personalidade são disciplinados na Parte Geral do Código Civil de 2002 (livro I – Das pessoas, Capítulo II).

Note-se que o direito à liberdade de comunicação, para BITTAR, consiste no poder que a pessoa tem de “direcionar suas energias, no mundo fático, em consonância com a própria vontade, no alcance dos objetivos visados”. Tal direito pode, no entanto, ser objeto de disposição, justamente para possibilitar a inserção da pessoa no contexto social, que exige o sacrifício da liberdade²¹.

¹⁷ SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011, p. 13.

¹⁸ Segundo o autor, “consideram-se se como da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos da pessoa, como a vida, a higidez física, a intimidade, a honra e outros tantos”. In BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7. ed. Rio de Janeiro: Forense Universitária, 2008, p. 1.

¹⁹ *Idem*, p. 5.

²⁰ *Idem*, p. 19.

²¹ *Idem*, p. 106.

Esse direito encontra-se expresso no artigo 20 do Código Civil, o qual garante a transmissão da palavra²².

Por sua vez, o direito à privacidade refere-se ao desejo do indivíduo de que certos aspectos de sua personalidade cheguem ao conhecimento de terceiros. Ou seja, segundo BITTAR, o referido direito elide qualquer atentado a “aspectos particulares ou íntimos da vida da pessoa, em sua consciência, ou em seu circuito próprio, compreendendo-se seu lar, a sua família e a sua correspondência”²³.

A proteção à privacidade está expressa no artigo 21 do Código Civil, segundo a qual a vida privada do indivíduo é inviolável²⁴.

Assim, a privacidade e a liberdade de comunicação também são considerados direitos da personalidade.

Saliente-se que a maior parte dos direitos da personalidade mencionada pelo Código Civil brasileiro encontram previsão expressa no artigo 5º do texto constitucional. Mesmo os implícitos são sempre referidos como consectários da dignidade humana, protegida no artigo 1º, inciso III, da Constituição Federal.

Assim, segundo SCHREIBER, os direitos da personalidade são, portanto, direitos fundamentais²⁵.

Diante do exposto, conclui-se que a privacidade e a liberdade de comunicação são direitos humanos, fundamentais e da personalidade.

²² Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. *In* BRASIL. Código Civil. Brasília, Senado Federal, 2002.

²³BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7. ed. Rio de Janeiro: Forense Universitária, 2008, p. 111.

²⁴ Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. *In* BRASIL. Código Civil. Brasília, Senado Federal, 2002.

²⁵ SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011, p. 13.

2.2 CIBERESPAÇO E MUDANÇAS NA CONCEPÇÃO DE PRIVACIDADE E LIBERDADE DE COMUNICAÇÃO

A internet vem ocasionando o encurtamento de distâncias e a facilidade, nunca antes vista, de acesso à informação.

Nesse sentido é a lição de LUÍS MAURO SÁ MARTINO, segundo o qual as transformações da tecnologia permitem um acesso cada vez maior às redes de computadores²⁶.

Assim, quanto mais o mundo virtual se expande, maior o número de indivíduos e grupos conectados, gerando e trocando informações, saberes e conhecimentos. Além disso, cria-se condições, na cibercultura²⁷, para que novos saberes sejam desenvolvidos – aplicativos, sites, programas etc.²⁸

Nesse contexto, o autor define o termo “ciberespaço” como a interconexão digital entre computadores e outras interfaces, como *smartphones* e *tablets*, ligados em rede e permitindo troca de dados²⁹.

MARTINO ressalta que uma das principais características do ciberespaço é sua arquitetura aberta, ou seja, sua capacidade de crescer indefinidamente. Desse modo, o ciberespaço é fluido: “dados são acrescentados e desaparecem; conexões são criadas e desfeitas em um fluxo constante”³⁰.

Por consequência, o ciberespaço está transformando a economia global. Segundo MANUEL CASTELLS, que intitulou essa nova fase econômica de “informacional” e “em rede”, as instituições e as empresas que interagem no

²⁶ MARTINO, Luís Mauro Sá. *Teoria das mídias digitais: linguagens, ambientes e redes*. 2 ed. Petrópolis: Vozes, 2015, p. 27.

²⁷ O termo “cibercultura” é definido por PIERRE LÉVY como “a reunião de relações sociais, das produções artísticas, intelectuais e éticas dos seres humanos que se articulam em redes interconectadas de computadores. É a cultura – entendida em um sentido bastante amplo como a produção humana, seja material, simbólica, intelectual – que acontece no ciberespaço”. In LÉVY, Pierre. *Cibercultura*. São Paulo: ed. 34, 1999, p. 26.

²⁸ MARTINO, Luís Mauro Sá. *Teoria das mídias digitais: linguagens, ambientes e redes*. 2 ed. Petrópolis: Vozes, 2015, p. 28.

²⁹ *Idem*, p. 29.

³⁰ *Idem*, p. 30.

mercado se veem deparadas com novos modelos de negócio, serviços e paradigmas organizacionais³¹.

Para DANILO DONEDA, essa mudança não é apenas quantitativa (aumento dos fluxos de informação), mas também qualitativa. Para o autor, o desenvolvimento da internet está mudando os eixos de equilíbrio na equação poder-informação-pessoa-controle³².

Obviamente, todas as mudanças que a internet vem proporcionando acarretam implicações no Direito.

Neste trabalho, a análise se limitará às mudanças ocorridas no âmbito dos princípios da privacidade e da liberdade de comunicação. Essas transformações vêm acompanhadas de intensos debates envolvendo, de um lado, a regulação estatal de dados e, de outro, a proteção desses direitos no ciberespaço.

Em um vértice do embate, agentes estatais invocam a proteção do interesse público como justificativa para o uso da *Interceptability*, termo utilizado por BERT-JAAP KOOPS para designar que:

As telecomunicações podem ser interceptadas tecnicamente nas redes ou serviços de telecomunicações que transportam as comunicações. Isso também inclui a capacidade dos provedores de telecomunicações para entregar dados do tráfego e do usuário, uma vez que estes podem ser necessários antes de que uma escuta possa ser encomendada. *Interceptability* significa, em suma, a habilidade de investigar telecomunicações³³.

³¹ CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999, p. 210.

³² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 15-16.

³³ Tradução livre do seguinte trecho: 'Interceptability' means that telecommunications can be intercepted technically on the telecommunications networks or services that transport the communications. It also includes the ability of telecommunications providers to deliver traffic data or user data, since these may be necessary before a wiretap can be ordered. Interceptability thus means, in short, the ability to investigate telecommunications. In KOOPS, Bert-Jarp; Bekkers, Rudi. *Interceptability of telecommunications: is US and Dutch Law prepared for the future?* Disponível em <<http://poseidon01.ssrn.com/delivery.php?ID=306070120093083024112086085112094095006031030087027036073099002024095030000116085026043019049012062042054090111096003087064005027080066016052014085126116011119088047020064113009125027080019003082091067112101015090064085008111120007093004101028017&EXT=pdf>>. Acesso em 05 de outubro de 2016.

Ou seja, defende-se nesse extremo o controle e a vigilância de dados eletrônicos pelo Estado a fim de que sejam utilizados como meio de prova em investigações e processos judiciais visando o combate à criminalidade. Destarte, nessa visão, a proteção do conteúdo de mensagens por meio de criptografia poderia ser considerada risco à sociedade, pois facilitaria a ocultação de ilícitos praticados por criminosos³⁴.

No outro extremo do debate, correntes mais libertárias propõem que o Estado deve eliminar suas expectativas regulatórias na web.

Um marco desse entendimento é a “Declaração de Independência do Ciberespaço”, uma carta escrita por JOHN PERRY BARLOW em 1996 como resposta à aprovação de uma lei estadunidense que regulamentaria a internet³⁵.

Nesse manifesto, BARLOW aduziu que a internet seria um fenômeno global independente do controle dos Estados e autorregulável conforme suas próprias necessidades:

Governos do Mundo Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não têm a independência que nos une.

(...)

Estamos formando nosso próprio Contrato Social. Essa maneira de governar surgirá de acordo com as condições do nosso mundo, não do seu. Nosso mundo é diferente.

O espaço cibernético consiste em ideias, transações e relacionamentos próprios, tabelados como uma onda parada na rede das nossas comunicações.

Nosso é um mundo que está ao mesmo tempo em todos os lugares e em nenhum lugar, mas não é onde pessoas vivem.

Estamos criando um mundo que todos poderão entrar sem privilégios ou preconceitos de acordo com a raça, poder econômico, força militar ou lugar de nascimento.

Estamos criando um mundo onde qualquer um em qualquer lugar poderá expressar suas opiniões, não importando quão singular, sem temer que seja coagido ao silêncio ou conformidade.

Seus conceitos legais sobre propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. Eles são baseados na matéria. Não há nenhuma matéria aqui³⁶.

³⁴ MARCACINI, Augusto Tavares Rosa. *Direito e Informática: uma abordagem jurídica sobre a criptografia*. São Paulo: Forense, 2002, p. 121.

³⁵ BARLOW, John Perry. *Declaração de independência do ciberespaço*. Disponível em <<http://www.dhnet.org.br/ciber/textos/barlow.htm>>. Acesso em 28 de setembro de 2016.

³⁶ *Idem*.

LAWRENCE LESSIG, professor estadunidense defensor da internet livre, explica o desafio do Estado de regular o comportamento de indivíduos no ciberespaço, fomentando um extenso debate:

Regulabilidade é a capacidade de um governo de regular o comportamento dentro do seu escopo. No contexto da internet, isso significa a habilidade do governo de regular o comportamento dos seus cidadãos na rede (...).

Para regular bem, você precisa saber (1) quem a pessoa é, (2) onde a pessoa está e (3) o que ela está fazendo. Dessa forma, quando a vida moveu-se para (a sua versão na) Internet, a “regulabilidade” da vida diminuiu. A arquitetura da rede tornou a vida nesse espaço menos regulável³⁷.

A partir dessas considerações, LESSIG defendeu que o ciberespaço demanda um olhar para além do escopo jurídico tradicional. Diferente do espaço real, regulado por Constituições e leis, o mundo virtual é ditado por códigos, que são o Direito do ciberespaço³⁸.

Outro marco da corrente libertária se deu com os chamados *cypherpunks*³⁹ como JULIAN ASSANGE, fundador da organização *Wikileaks*.

³⁷ Tradução livre do seguinte trecho: “Regulability is the capacity of a government to regulate behavior within its proper reach. In the context of the Internet, that means the ability of the government to regulate the behavior of (at least) its citizens while on the Net. (...) To regulate well, you need to know (1) who someone is, (2) where they are, and (3) what they’re doing. (...) Thus, as life moved on to (this version of) the Internet, the regulability of that life decreased. The architecture of the space— at least as it was—rendered life in this space less regulable”. In LESSIG, Lawrence. *Code - version 2.0*. 2006. Disponível em < <http://codev2.cc/download+remix/Lessig-Codev2.pdf>>. Acesso em 28 de setembro de 2016.

³⁸ Conforme LESSIG, “space demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer’s scope— beyond laws, or even norms. It requires a broader account of “regulation,” and most importantly, the recognition of a newly salient regulator. That regulator is the obscurity in this book’s title—Code. In real space, we recognize how laws regulate— through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different “code” regulates— how the software and hardware (i.e., the “code” of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace’s “law”. “Lex Informatica”, as Joel Reidenberg first put it, or better, “code is law”. In LESSIG, Lawrence. *Code - version 2.0*. Disponível em < <http://codev2.cc/download+remix/Lessig-Codev2.pdf>>. Acesso em 28 de setembro de 2016.

³⁹ O termo *cypherpunk* é um trocadilho com as palavras *cypher*, referente à criptografia, e *cyberpunk*, nome da subcultura *underground* aliada às tecnologias de informação e cibernética.

ASSANGE defende o uso massivo de criptografia⁴⁰ como meio de efetivação da privacidade e da liberdade de expressão dos usuários que interagem em rede⁴¹.

Ainda segundo ASSANGE, a liberdade de comunicação foi expandida em alguns aspectos, visto que atualmente muito mais pessoas podem interagir em curto período de tempo. Por outro lado, ela também foi bastante reduzida, porque não haveria mais privacidade – as comunicações no ciberespaço podem ser interceptadas, armazenadas e, como resultado, usadas contra os próprios usuários⁴².

Desse modo, para o *cypherpunk*, sistemas de interceptação legal não passam de um termo bonito para dizer “espionagem”⁴³.

Merece destaque, também, trecho do livro de ASSANGE em que há relato sobre um debate envolvendo a interceptação de dados pelo Estado *versus* a privacidade e a liberdade de comunicação no ciberespaço:

Fui à Tunísia depois da queda do regime de Ben Ali e conversamos sobre o Tor em uma aula de ciências da computação, que contou com um pessoal bastante técnico da universidade, e uma moça levantou a mão e perguntou: “e os bandidos?” E se pôs a citar os Quatro Cavaleiros do Infoapocalipse: lavagem de dinheiro, drogas, terrorismo e pornografia infantil. “E os bandidos?” Essas quatro ameaças são sempre enfatizadas e usadas para derrubar tecnologias de preservação da privacidade, porque ninguém questiona que são grupos que devem ser derrotados. Então eu perguntei para a turma: “Quem aqui já viu a página Ammar 404?”. Essa foi uma página de censura implantada pelo regime de Ben Ali antes e durante a revolução para bloquear o acesso. Todas as pessoas da sala, incluindo o professor do curso, levantaram a mão – exceto a moça que havia feito a pergunta. Eu olhei para ela e disse: “Olhe para todas as pessoas ao seu redor. Todos os seus colegas de turma. Você acha mesmo que fazia sentido oprimir toda esta sala para combater tais fantasmas?” E ela respondeu: “pensando bem, acho que também vou levantar a mão”⁴⁴.

⁴⁰ Segundo MARCACINI, a criptografia é a arte de escrever em código, de modo a permitir que somente quem conheça esse código possa ler a mensagem. Desse modo, convencionando um critério entre o emissor e o receptor, a criptografia torna possível o envio de mensagens codificadas, incompreensíveis para um terceiro que eventualmente venha a interceptá-las. In MARCACINI, Augusto Tavares Rosa. *Direito e Informática: uma abordagem jurídica sobre a criptografia*. São Paulo: Forense, 2002, p. 9.

⁴¹ ASSANGE, Julian. *Cypherpunks - Liberdade e o futuro da internet*. São Paulo: Boitempo, 2013, p. 143-149.

⁴² *Idem*, p. 106.

⁴³ *Idem*, p. 103.

⁴⁴ *Idem*, p. 89.

Diante do contexto aqui apresentado, torna-se valioso o alerta feito por DANILO DONEDA: nas relações jurídicas ligadas à tecnologia, o grau de indeterminação presente em toda tentativa de regulação feita pelo Direito é alto. Portanto, os juristas devem levar em consideração as novas variáveis introduzidas, de forma a refletir na modelagem de institutos adaptados a essa realidade⁴⁵.

Conclui-se, então, que a relação entre Direito e internet deu nova roupagem à privacidade e à liberdade de comunicação, intimamente ligada à proteção de dados na web. Segundo DONEDA,

Através da proteção de dados pessoais, as garantias que a princípio eram relacionadas com a privacidade passam a ser vistas através de ótica mais abrangente, pela qual outros interesses devem ser considerados, compreendendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais⁴⁶.

A partir disso, DONEDA defende que, se o dado identificar a pessoa à qual se refere, cria-se um vínculo específico entre eles. Assim, sendo a informação uma representação direta do próprio sujeito, deve o dado ser entendido como uma extensão de sua personalidade, merecendo proteção como tal⁴⁷.

Ademais, como bem apontado por MARCACINI, a “sociedade em rede” é profundamente dependente de criptografia. Seria impossível, a título de exemplo, falar-se na expansão das transações eletrônicas sem o uso de criptografia, pois só esta confere a segurança necessária a essas novas formas de comunicação e contratação no ciberespaço⁴⁸.

Desse modo, proibir a criptografia seria o mesmo, em termos de desproporção, que proibir o uso de automóveis ou motocicletas, diante da constatação de que os criminosos deles se utilizam para o crime ou para a fuga⁴⁹.

⁴⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 34.

⁴⁶ *Idem*, p. 204.

⁴⁷ *Idem*, p. 164.

⁴⁸ MARCACINI, Augusto Tavares Rosa. *Direito e Informática: uma abordagem jurídica sobre a criptografia*. São Paulo: Forense, 2002, p. 127.

⁴⁹ *Idem*, p. 128.

Ou seja, eventual banimento ou restrição do uso da criptografia não impediria que organizações criminosas obtivessem êxito em seus intentos. Acarretaria, ao revés, desproporcional desvantagem para a população em geral, impedindo-lhe de utilizar mecanismos para proteção de suas comunicações privadas e informações pessoais⁵⁰.

Ante o exposto, corrobora-se que a privacidade e a liberdade de comunicação adquiriram objetos mais complexos, sendo que seus conceitos não podem mais ser dissociados da proteção de dados eletrônicos e da criptografia.

São crescentes as tentativas de intervenção estatal no fluxo de dados online, o que pode representar violação aos princípios supramencionados.

Assim, passa-se à análise do modo como o Estado brasileiro, por meio de lei, vem se posicionando em meio a esse embate, tentando regular a proteção de dados.

⁵⁰ *Idem*, p. 130.

3 REGULAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL E NO DIREITO COMPARADO

O ciberespaço vem se tornando um instrumento cada vez mais democrático de acesso à informação e difusão de dados de toda a natureza.

Em atenção a isso, mostra-se imprescindível um breve levantamento da regulação da proteção de dados no Brasil.

Primeiramente, serão abordados documentos considerados como paradigmas da proteção da privacidade e da liberdade de expressão no ciberespaço, cujas premissas serviram de base à elaboração do Marco Civil da Internet.

Após, será feito um contraponto da regulação de dados no Brasil e as regras de privacidade na web adotadas pela União Europeia.

3.1 REGULAÇÃO DA PROTEÇÃO DE DADOS: PARADIGMAS INTERNACIONAIS E O MARCO CIVIL DA INTERNET

A Organização das Nações Unidas (ONU) divulgou um Relatório em 2012 sobre promoção e proteção do direito à liberdade de opinião, expressão e comunicação no ciberespaço. Nesse documento, a instituição considerou o referido acesso à informação na internet como um direito humano⁵¹.

A ONU recomendou, ainda, que nenhum Estado interrompesse o acesso à internet nem mesmo em situações de crises políticas, visto que o mundo virtual tem sido utilizado para a livre expressão da sociedade a favor ou contra determinados assuntos⁵².

⁵¹ Disponível em < <http://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech/>>. Acesso em 05 de outubro de 2016.

⁵² *Idem*.

Reforçando tal entendimento, o Conselho de Direitos Humanos da ONU publicou, em 27 de junho de 2016, Resolução sobre a promoção, a proteção e o gozo dos direitos humanos na internet.

Nesse documento, entendeu-se que medidas que intencionalmente impedem ou interferem no acesso ou na disseminação da informação online violam os direitos humanos⁵³.

Merece destaque o seguinte trecho do documento mencionado:

1. Os mesmos direitos que as pessoas possuem offline devem também ser protegidos online, em especial com relação à liberdade de expressão, que é aplicável independentemente de fronteiras e em quaisquer meios que alguém possa escolher, de acordo com os artigos 19 da Declaração Universal dos Direitos Humanos e do Pacto Internacional sobre Direitos Civis e Políticos; (...) 10. Condena inequivocamente medidas que intencionalmente impeçam ou interfiram no acesso ou disseminação da informação online por violação os direitos humanos internacionais e conclama os Estados a abdicarem e cessarem tais medidas⁵⁴.

Ainda em plano internacional, verifica-se que a Convenção Americana de Direitos Humanos de 1969 (Pacto de San José da Costa Rica), recepcionada pelo Brasil, reforça a proteção do direito de livre expressão e de comunicação:

Artigo 13.

3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões⁵⁵.

⁵³ Disponível em <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>>. Acesso em 05 de outubro de 2016.

⁵⁴ Tradução livre do documento original, que se encontra em língua inglesa: ““1. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights; (...) 10. Condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures”. Disponível em: <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>>, acesso em 05 de outubro de 2016.

⁵⁵ Convenção Americana Sobre Direitos Humanos, disponível em <https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>. Acesso em 03 de outubro de 2016.

A nível nacional, em consonância aos princípios constitucionais da privacidade e da liberdade de comunicação, o Comitê Gestor da Internet no Brasil (CGI) divulgou em 2009 uma Resolução com dez princípios para a governança e o uso da internet⁵⁶.

Dentre eles, dois merecem destaque.

O primeiro refere-se à liberdade, à privacidade e aos direitos humanos. Conforme o CGI, o uso da internet deve guiar-se pelos princípios acima mencionados, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática⁵⁷.

O outro é chamado de inimizabilidade da rede, segundo o qual o combate a ilícitos no ciberespaço deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos⁵⁸.

Nesse sentido, em harmonia às normativas nacionais e internacionais sobre o tema, foi editada a Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet.

Note-se que, segundo FRANCISCO CARVALHO DE BRITO CRUZ, a gênese do Marco Civil da Internet teve relação com a mobilização contrária a outro projeto de lei (PL) que visava à regulação da Internet no Brasil. Tratava-se do PL 84/1999, de autoria do deputado Luiz Piauhyllino (PSDB/PE)⁵⁹.

Esse projeto tinha como objetivo principal a instituição de regras criminais para o controle da internet, disciplinando direitos e liberdades dos

⁵⁶ Resolução CGI.br/RES/2009/003/P. Disponível em: <<http://www.cgi.br/resolucoes/documento/2009/003>>, acessado em 02 de outubro de 2016.

⁵⁷ Idem.

⁵⁸ Idem.

⁵⁹ CRUZ, Francisco Carvalho de Brito. *Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet*. 2015. 138 pp. Mestrado – Faculdade de Direito, Universidade de São Paulo. 2015. Disponível em <<http://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/pt-br.php>>. Acesso em 06 de outubro de 2016.

cidadãos. O PL foi, inclusive, apelidado de “AI-5 Digital”, conforme citado por RONALDO LEMOS⁶⁰.

Conforme as pesquisas de FRANCISCO CARVALHO DE BRITO CRUZ, o senador Eduardo Azeredo (PSDB/MG) foi designado como relator desse projeto de lei e incrementou ideias bastante polêmicas ao debate. Dentre elas, merece destaque o cadastramento obrigatório dos usuários que acessassem a internet ou qualquer rede de computadores, perante seu provedor ou junto a quem lhe tornasse disponível o acesso a dispositivo de comunicação ou sistema informatizado⁶¹.

Felizmente, o texto passou por profundas reformulações e foi aprovado em 07/11/2013, transformado na Lei nº 12.735/2012 – a qual alterou o Código Penal, o Código Penal Militar e a Lei nº 7.716/89 (Lei de crimes resultantes de preconceito de raça ou de cor) para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares⁶².

Assim, conforme a lição de BRUNO RICARDO BIONI e DIEGO CANABARRO, em vez de se apostar em uma dinâmica regulatória que freasse a participação social na rede por meio da lente punitiva do direito criminal, optou-se por assegurar direitos e garantias dos usuários para fomentar o seu uso por meio do Marco Civil da Internet⁶³.

⁶⁰ LEMOS, Ronaldo; et. al. *Comentários e sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL nº 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania*, novembro de 2010, disponível em <<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/7719>>. Acesso em 06 de outubro de 2016.

⁶¹ CRUZ, Francisco Carvalho de Brito. *Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet*. 2015. 138 pp. Mestrado – Faculdade de Direito, Universidade de São Paulo. 2015. Disponível em <<http://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/pt-br.php>>. Acesso em 06 de outubro de 2016.

⁶² *Idem*.

⁶³ BIONI, Bruno Ricardo; CANABARRO, Diego R. *A Internet no Congresso Nacional: um panorama dos números relacionados à regulação da rede no Brasil*. Disponível em <<http://observatoriodainternet.br/post/a-internet-no-congresso-nacional-um-panorama-dos-numeros-relacionados-a-regulacao-da-rede-no-brasil>>. Acesso em 09 de outubro de 2016.

Consoante PAULO RENÁ DA SILVA SANTARÉM, com o Marco Civil a abordagem de regulação da internet foi levada a outra perspectiva: a dos direitos dos usuários, e não das obrigações excessivas aos provedores⁶⁴.

Ainda segundo SANTARÉM, entre 2009 e 2011 a Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas(CTS-FGV), organizou uma plataforma virtual para construir de forma participativa com os cidadãos brasileiros o texto de um projeto de lei (PL) que regulasse a internet no Brasil⁶⁵.

Encerrada a fase de coleta de sugestões, o Poder Executivo enviou o Anteprojeto ao Congresso Nacional e os debates com a sociedade civil continuaram por meio do site *e-Democracia* até a aprovação do texto em ambas as Casas Legislativas⁶⁶.

Desse modo, como apontado por ANA CLAUDIA FARRANHA, o processo de debate e construção desse Projeto de Lei, assim como sua aprovação e regulamentação, expressaram a necessidade de que a privacidade e os dados dos usuários fossem adequadamente protegidos⁶⁷.

Esse percurso democrático de elaboração do Marco Civil se coaduna ao que dispõe a Exposição de Motivos nº 86 -MJ/MP/MCT/MC, segundo o qual o referido diploma legal foi elaborado com o objetivo primordial de proteger os direitos dos usuários da internet, de modo a conferir efetividade às garantias constitucionais de privacidade e liberdade de comunicação⁶⁸.

⁶⁴ SANTARÉM, Paulo Rená da Silva. *O direito achado na rede: a emergência do acesso à internet como direito fundamental no Brasil*. Dissertação de mestrado. Universidade de Brasília, 2010, p. 97. Disponível em <http://repositorio.unb.br/bitstream/10482/8828/1/2010_PauloRen%c3%a1daSilvaSantar%c3%a9m.pdf>. Acesso em 08 de outubro de 2016.

⁶⁵ *Idem*.

⁶⁶ Disponível em <<http://edemocracia.camara.gov.br/web/marco-civil-da-internet/andamento-do-projeto#.V3E6ZbgrJPY>>. Acesso em 08 de agosto de 2016.

⁶⁷ FARRANHA, Ana Claudia. *Estado, sociedade e interações digitais: expectativas democráticas*. *Revista de Pesquisa em Políticas Públicas*, n. 2, 2014.

⁶⁸ Exposição de Motivos referente ao projeto de lei que originou o Marco Civil da Internet. Disponível em <http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm>. Acesso em 08 de agosto de 2016.

Diversos artigos do Marco Civil corroboram o objetivo supracitado.

A Lei em análise adotou expressamente dispositivo que veda o bloqueio, a filtragem e o monitoramento de dados:

Art. 9º, § 3º. Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo⁶⁹.

Ainda, no artigo 10, há disposição sobre os deveres de guarda e de disponibilização dos registros de conexão e de acesso a aplicações de internet, de dados pessoais e do conteúdo de comunicações privadas⁷⁰.

Essa proteção, então, está em consonância com os direitos e garantias fundamentais dos cidadãos que protegem a intimidade, a privacidade e os dados pessoais que se encontram positivados nos incisos X e XII do artigo 5º da Constituição Federal de 1988⁷¹.

Saliente-se que o §1º do artigo 10 estabelece, dentre outras, a regra de que os provedores responsáveis pela guarda de registros eletrônicos somente

⁶⁹ BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷⁰ “Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição”. Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais

⁷¹ “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - 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; (...) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”. Disponível em BRASIL. Constituição Federal. Brasília, Senado Federal, 1988.

deverão disponibilizá-los, incluindo os demais dados para identificação do usuário, mediante ordem judicial, deixando claro que a regra é a proteção das informações⁷².

Já o §2º do mesmo artigo prevê que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial⁷³.

Ou seja, o texto da lei indica que a regra é a inviolabilidade da intimidade e da vida privada e o sigilo das comunicações, visto que fez menção aos incisos II e III, do art. 7º da mesma Lei, segundo os quais o sigilo do fluxo de comunicações pela internet e das comunicações privadas armazenadas são invioláveis, salvo por ordem judicial⁷⁴.

No mesmo sentido, o artigo 11, *caput*, do Marco Civil estabelece que:

Em qualquer operação de **coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional**, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (grifo nosso)⁷⁵.

Em sequência, o artigo 12 da Lei fixa as sanções pela violação de quaisquer deveres previstos no *caput* do artigo 11 – advertência, multa, suspensão temporária e/ou proibição de exercício das atividades acima destacadas⁷⁶.

⁷² “Art. 10. (...) § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º”. Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷³ “Artigo 10. (...) § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º”. Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷⁴ “Artigo 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial”. Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷⁵ Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷⁶ “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

Entretanto, a interpretação do artigo 12 do Marco Civil da Internet ainda é permeada por dissensos.

A título de exemplo, pode-se citar as divergências entre as notas técnicas emitidas pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) e pelo Ministério Público (Estaduais e Federal), ambas datadas de 2016.

O IDEC defendeu que a disciplina do uso da internet tem como fundamento a liberdade de expressão, o exercício da cidadania em meios digitais e a defesa do consumidor, princípios que precisariam ser levados em conta no momento de aplicação das sanções previstas no art. 12 do Marco Civil⁷⁷.

Por sua vez, o Ministério Público argumenta que as referidas sanções devem ser usadas sempre que necessário, após o esgotamento de outras medidas menos gravosas, para assegurar que empresas forneçam dados que trafeguem em aplicativos de mensagens online e, assim, colaborem com a obtenção de provas nas searas cível e criminal⁷⁸.

Em que pese os argumentos trazidos pelo Ministério Público, todo o contexto de elaboração do Marco Civil converge à interpretação de que as sanções constantes do artigo 12 só deverão ser aplicadas se o provedor não respeitar os deveres dispostos nos artigos 10 e 11 da Lei, ou seja, caso não haja a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas na guarda e na disponibilização dos registros de conexão e de acesso a aplicações de internet.

Em outras palavras, a aplicação das sanções do artigo 12 deverá ocorrer quando não houver a preservação dos dados pessoais e do conteúdo das comunicações privadas (artigo 10) ou, então, quando não houver respeito à

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. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País". Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁷⁷ Disponível em < <http://www.idec.org.br/pdf/nota-tecnica-bloqueio-whatsapp.pdf>>. Acesso em 05 de outubro de 2016.

⁷⁸ Disponível em < <http://www.mpf.mp.br/sp/sala-de-imprensa/docs/nota-tecnica-crimes-ciberneticos>>. Acesso em 05 de outubro de 2016.

legislação brasileira e aos direitos à privacidade, à proteção de dados e ao sigilo das comunicações privadas e dos registros em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet (artigo 11)⁷⁹.

Vale também apontar o Capítulo III da Lei, cujo título é “Da Requisição Judicial de Registros”. Essa Seção compreende os artigos 22 e 23 e dispõe, sobre o requerimento – a título de exceção – que poderá ser feito ao juiz para que este ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Veja-se:

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

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro⁸⁰.

O artigo 15 da Lei também merece destaque. Ele dispõe que o provedor de aplicações de internet deverá manter os registros de acesso, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento⁸¹.

Segundo LUKAS RUTHES GONÇALVES, isso significa, a título de exemplo, que aplicativos como o *WhatsApp* devem guardar, pelo período de seis meses, dados como as horas em que seus usuários utilizaram o aplicativo, seus

⁷⁹ LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 25.

⁸⁰ BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

⁸¹ “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”. Disponível em BRASIL. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

ID e com quem eles se comunicaram, mas não o conteúdo das comunicações em si⁸². Inclusive, dispõe o art. 17 da mesma lei que a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Note-se que parte do regulamento a que se refere o artigo 15 foi editado em 11 de maio de 2016 – trata-se do Decreto nº 8.771/2016, que trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações⁸³.

Além disso, tramita na Câmara dos Deputados o Projeto de Lei nº 5.276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural⁸⁴.

⁸² GONÇALVES, Lukas Ruthes. *WhatsApp. Criptografia ponta-a-ponta e o Marco Civil da Internet*. Disponível em <<http://intellinova.com.br/whatsapp-criptografia-marco-civil/>>. Acesso em 08 de outubro de 2016.

⁸³ BRASIL. Decreto nº 8.771, de 11 de Maio de 2016. Brasília, Senado Federal, 2016.

⁸⁴ Esse Projeto de Lei ainda encontra-se sujeito à apreciação do plenário, conforme as informações disponibilizadas pela Câmara dos Deputados em <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>>. Acesso em 09 de outubro de 2016.

3.2 PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA: CONTRAPONTO E INSPIRAÇÕES

Para enriquecer a discussão, foi escolhida a regulação de proteção de dados da União Europeia como contraponto ao tratamento dispensado pelo Brasil aos temas da proteção de dados, bem como da privacidade e da liberdade de comunicação no ciberespaço.

Essa escolha se deu porque a União Europeia apresenta avançadas discussões sobre o tema, dispondo inclusive de uma autoridade cuja função exclusiva é a garantia da proteção de dados.

Em 2004, foi criada a Autoridade Europeia para a Proteção de Dados (AEPD). Sua função primordial é garantir que todas as instituições e organismos da União Europeia (UE) respeitem o direito à privacidade dos cidadãos quando processam seus dados pessoais⁸⁵.

A AEPD é liderada pela Autoridade e pela Autoridade Adjunta, as quais são nomeadas para mandato de cinco anos pelo Parlamento Europeu. Atualmente, Giovanni Buttarelli e Wojciech Wiewiórowski foram, respectivamente, a Autoridade e a Autoridade Adjunta eleitas em 04 de dezembro de 2014⁸⁶.

Ainda, a AEPD recomenda que as instituições e os organismos da União Europeia não devem processar dados pessoais sobre origem racial ou étnica, opiniões políticas, posições religiosas, concepções filosóficas e filiação sindical⁸⁷.

Caso o cidadão entenda que houve violação a seu direito à privacidade por alguma instituição da União Europeia, poderá contatar os responsáveis

⁸⁵ Informações disponíveis em < http://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>. Acesso em 10 de novembro de 2016.

⁸⁶ Disponível em < <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Membersmission> >. Acesso em 11 de novembro de 2016.

⁸⁷ Informações disponíveis em < http://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>. Acesso em 11 de novembro de 2016.

locais pelo tratamento dos dados pessoais e, caso não se satisfaça com o resultado, o responsável da instituição UE onde foi cometida a suposta infração. Caso mesmo assim não haja resolução do conflito, pode ser apresentada queixa à AEPD, que investigará o caso e informará o requerente da decisão. Se não houver concordância com essa decisão, a questão poderá ser remetida ao Tribunal de Justiça da UE⁸⁸.

Então, essa instituição processa queixas, conduz inquéritos, trabalha com as autoridades nacionais dos países da União Europeia para garantir coerência na proteção de dados e monitora novas tecnologias suscetíveis de ter impacto em matéria de proteção de dados⁸⁹.

Além disso, aconselha, por meio de Pareceres, as instituições e os organismos da União Europeia sobre diversos aspectos do tratamento dos dados pessoais, das políticas e da legislação referente ao assunto.

Um dos Pareceres, o de nº 04/2015, intitulado “Rumo a uma nova ética digital”, merece destaque neste trabalho por sintetizar alguns dos entendimentos veiculados pela AEPD.

No referido documento, a instituição em estudo ressaltou que os princípios de proteção de dados definidos na Carta da União Europeia – tais como necessidade, proporcionalidade, justiça, minimização de dados, limitação da finalidade, consentimento e transparência – aplicam-se ao processamento de dados na sua totalidade, da coleta ao uso⁹⁰.

Ademais, defendeu que a privacidade e a proteção de dados são plataformas para um ambiente digital sustentável e dinâmico, não um obstáculo a ele. Assim, recomendou que o desenvolvimento desse sistema ocorra mediante interação entre desenvolvedores, empresas e reguladores no interesse

⁸⁸ *Idem.*

⁸⁹ *Idem.*

⁹⁰ Tradução livre do original, em língua inglesa: “The data protection principles defined in the EU Charter - necessity, proportionality, fairness, data minimisation, purpose limitation, consent and transparency - apply to data processing in its entirety, to collection as well as to use.”. Disponível em https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf. Acesso em 11 de novembro de 2016.

do indivíduo, de modo que o menor risco de vigilância dê aos indivíduos mais influência sobre as decisões que os afetam⁹¹.

Além disso, no Parecer nº 01/2016, o AEPD informou que, nos últimos anos, o Tribunal de Justiça Europeu afirmou os princípios de proteção de dados, incluindo a equidade, a exatidão e a relevância da informação, a supervisão independente e os direitos individuais dos sujeitos. Tais princípios são tão relevantes para os organismos públicos como para as empresas privadas, tornando-se ainda mais importantes considerando a sensibilidade dos dados necessários para a investigação criminal⁹².

Além da atuação do AEPD, merece destaque o Novo Regulamento Geral de Proteção de Dados (GDPR) – Regulamento 679/2016, o qual fora publicado em 04 de maio de 2016 no Jornal Oficial da União Europeia⁹³.

O GDPR prevê um período transitório de dois anos para sua total aplicação, permitindo que ocorra adaptação de governos, empresas e indivíduos às novas regras. Como o Regulamento é diretamente aplicável aos vinte e oito Estados-Membros da União Europeia, sem necessidade de transposição para

⁹¹ Segundo a AEPD, “Contrary to some claims, privacy and data protection are a platform for a sustainable and dynamic digital environment, not an obstacle. Independent data protection authorities like the EDPS have a key role in dispelling such myths and responding to individuals’ genuine concerns of loss of control over their personal information. The next generation of personal data is likely to be even less accessible to the individuals to whom it relates. Responsibility for shaping a sustainable digital single market is necessarily dispersed, but it is also interdependent, like an ecosystem, requiring effective interaction between developers, businesses and regulators in the interests of the individual. In this section we outline the contribution that these four essential players can bring”. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf >. Acesso em 11 de novembro de 2016.

⁹² Tradução livre do documento original em inglês: “The European Court of Justice in recent years has affirmed data protection principles including fairness, accuracy and relevance of information, independent oversight and individual rights of individuals. These principles are as relevant for public bodies as they are for private companies, regardless of any formal EU adequacy finding with respect to third countries data protection safeguards; indeed they become all the more important considering the sensitivity of the data required for criminal investigation”. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-02-12_EU-US_Umbrella_Agreement_EN.pdf >. Acesso em 11 de novembro de 2016.

⁹³ Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679> >. Acesso em 11 de novembro de 2016.

cada jurisdição, há garantias de harmonização legislativa da proteção de dados em todos esses Estados⁹⁴.

Esse Regulamento trouxe alterações que mudarão o modo como se recolhe e trata dados não só dentro da União Europeia, mas também fora dela. Isso porque as disposições do GDPR são aplicáveis às empresas, mesmo que não tenham estabelecimento na UE, desde que as suas atividades de tratamento de dados visem à oferta de bens e serviços aos titulares de dados pessoais, ou a monitorização dos seus comportamentos em território europeu⁹⁵.

Segundo o advogado RICARDO HENRIQUES, em artigo publicado em revista portuguesa:

Outras regras importantes serão revistas, tais como: as regras sobre consentimento; o direito de apagamento (também conhecido como “direito a ser esquecido”); o direito à portabilidade dos dados; entre outros. Mas a maior novidade e que terá mais impacto na vida das empresas, procurando assim motivar o seu cumprimento da lei, é a responsabilização das empresas que tratam dados pessoais ou a obrigação de prestação de contas. Aqui inclui-se, entre outras, a obrigação de manutenção de registos por responsáveis e subcontratantes; de cooperação com autoridades de supervisão; de avaliações de impacto (de medidas) sobre a protecção de dados; de consulta prévia com as autoridades de protecção de dados em casos de alto risco; de notificação de violação de dados às autoridades de protecção de dados no prazo de 72 horas após detecção de um incidente; e, por último, mas talvez a mais relevante, maiores penalizações em caso de incumprimento, podendo atingir até 20 milhões de euros, ou até 4% do volume de negócios anual total a nível mundial, o que for maior⁹⁶.

Com o objetivo de proteger a privacidade dos indivíduos, o art. 5º (1) (f) do Regulamento 679/2016⁹⁷ destaca a confidencialidade e a integridade como dois princípios essenciais para o tratamento de dados pessoais. A preocupação

⁹⁴ Disponível em < http://www.abreuadvogados.com/xms/files/pdf_off_line/Newsletter_APPITI_Novo_Regulamento.pdf>. Acesso em 11 de novembro de 2016.

⁹⁵ HENRIQUES, Ricardo. *Perspectivas para a protecção de dados pessoais*. Disponível em < <https://www.publico.pt/mundo/noticia/perspectivas-para-a-proteccao-de-dados-pessoais-1721553>>. Acesso em 11 de novembro de 2016.

⁹⁶ Idem.

⁹⁷ “Artigo 5º. 1. Os dados pessoais são: Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)". Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em 11 de novembro de 2016.

com este aspecto é tamanha que, no art. 25 (1)⁹⁸, o GDPR prevê que os dados devem ser protegidos desde sua concepção, ou seja, desde a definição dos meios de tratamento o responsável deverá prever formas adequadas de garantir a confidencialidade e integridade.

Ainda, o art. 23 (1) do GDPR 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 decorrem⁹⁹.

Em discurso proferido na Áustria em 2016 por GIOVANNI BUTARELLI, Autoridade do AEPD, ressaltou-se que com a aprovação do GDPR ocorrerá alteração da proteção de dados na Europa para a próxima geração¹⁰⁰.

⁹⁸ “Artigo 25º - Proteção de dados desde a concepção e por defeito. 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados”. Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em 11 de novembro de 2016.

⁹⁹ “Artigo 23º - Limitações. 1. O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.o a 22.o e no artigo 34.o, bem como no artigo 5.o, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.o a 22.o, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente: a) a segurança do Estado; b) a defesa; c) a segurança pública; d) a prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social; f) A defesa da independência judiciária e dos processos judiciais; g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas; h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g); i) A defesa do titular dos dados ou dos direitos e liberdades de outrem; j) A execução de ações cíveis”. Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em 11 de novembro de 2016.

¹⁰⁰ BUTARELLI, Giovanni. *Privacy in an age of hyperconnectivity*. Discurso de Giovanni Buttarelli no “*Privacy and Security Conference 2016*”, ocorrido em Neusiedler See, Áustria, em 2016. Disponível em < <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Public> >

BUTARELLI explicou que o GDPR incluirá uma referência direta ao "princípio da responsabilização" (*accountability principle*) no artigo 5º, 2, do Regulamento¹⁰¹ e exigirá, nos termos do artigo 24º¹⁰², a aplicação, pelos controladores, de medidas técnicas e organizativas adequadas para assegurar e demonstrar conformidade aos direitos individuais no tratamento de dados. Tais medidas foram pormenorizadamente descritas no Capítulo IV do GDPR, incluindo gestão de riscos de segurança informática, notificações de violação de dados, avaliações de impacto em matéria de protecção de dados, consultas prévias e agentes de protecção de dados¹⁰³.

Para BUTARELLI, o *accountability principle* ajuda a mover a protecção de dados da teoria à prática. Como controladores desses dados, os órgãos da UE tornam-se responsáveis quando são capazes de fazer as seguintes coisas fundamentais:

1. Em primeiro lugar, criar políticas internas transparentes de protecção de dados e de privacidade. Esses precisam ser aprovados e ativamente aprovados pelo mais alto nível de gestão da organização.
2. Em segundo lugar, implementar processos e instrumentos internos apropriados e eficazes para implementar estas políticas. Isso garante que os princípios e obrigações de protecção de dados são cumpridos

ations/Speeches/2016/16-09-30_accountability_speech_EN.pdf>. Acesso em 11 de novembro de 2016.

¹⁰¹ Artigo 5º, 2. "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»)". Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em 11 de novembro de 2016.

¹⁰² "Artigo 24. Responsabilidade do responsável pelo tratamento. 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades. 2. Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de protecção de dados pelo responsável pelo tratamento. 3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40º ou de procedimentos de certificação aprovados conforme referido no artigo 42º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento". Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em 11 de novembro de 2016.

¹⁰³ BUTARELLI, Giovanni. *Privacy in an age of hyperconnectivity*. Discurso de Giovanni Buttarelli no "Privacy and Security Conference 2016", ocorrido em Neusiedler See, Áustria, em 2016. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2016/16-09-30_accountability_speech_EN.pdf>. Acesso em 11 de novembro de 2016.

- e que os indivíduos estão adequadamente protegidos dos riscos decorrentes do tratamento dos seus dados pessoais.
3. Em terceiro lugar, informar e formar todas as pessoas na organização sobre como implementar essas políticas.
 4. Em quarto lugar, a responsabilidade recai no nível mais elevado de acompanhamento e avaliação da eficácia desta aplicação. Dessa monitoração e medição, a organização precisa ser capaz de demonstrar às partes interessadas externas e autoridades de supervisão a qualidade da implementação.
 5. Quinto e último ponto: A organização precisa implementar procedimentos para corrigir o mau cumprimento e as violações de dados¹⁰⁴.

Para concretizar ainda mais o *accountability principle*, GIOVANNI BUTARELLI anunciou em 2016 a construção de uma rede de jurisdições europeias para que as autoridades de defesa do consumidor, da concorrência e da proteção de dados conversem entre si sobre as suas preocupações comuns – uma iniciativa denominada *Digital Clearing House*¹⁰⁵.

Pelo exposto, a partir da análise realizada no item 2.1, verifica-se que é recente a regulamentação, no Brasil, da proteção de dados e da privacidade no ciberespaço.

¹⁰⁴ Tradução livre do original, que se encontra em língua inglesa: “1. Firstly, establish transparent internal data protection and privacy policies. These need to be proved and actively endorsed by the highest level of the organisation’s management. 2. Secondly, put in place appropriate and effective internal processes and tools to implement these policies. This ensures that data protection principles and obligations are complied with and that individuals are adequately protected from risks stemming from the processing of their personal data. 3. Thirdly, informing and training all people in the organisation on how to implement these policies. 4. Fourthly, responsibility lies at the highest level for monitoring and assessing the effectiveness of this implementation. Out of this monitoring and measuring, the organisation needs to be able to demonstrate to external stakeholders and supervisory authorities the quality of the implementation. 5. Fifth and last point: The organisation need to put in place procedures for redressing poor compliance and data breaches”. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2016/16-09-30_accountability_speech_EN.pdf >. Acesso em 12 de novembro de 2016.

¹⁰⁵ Tradução livre do seguinte trecho do discurso de BUTARELLI: “But personal data protection is no longer simply a matter of law - making and legal compliance. Modern and sustainable laws, effectively enforced, are one part of the Big Data Protection Ecosystem. That is why independent DPAs - like your local authority in Austria, led by Andrea Jelinek, and my own the EDPS - invest so much effort into cooperation and information sharing. In the digital era, there are multiple agencies responsible for ensuring the interests of the consumer are safeguarded. That is why we have proposed for the first time a cross - jurisdiction network for consumer, competition and data protection authorities to talk to each other about their common concerns - an initiative called the Digital Clearing House”. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2016/16-09-30_accountability_speech_EN.pdf >. Acesso em 12 de novembro de 2016.

Os temas ainda são e serão alvo de intensos debates, tendo em vista a incrível velocidade em que as inovações tecnológicas vão surgindo e desafiando os juristas a tentar acompanhá-las.

Após o breve estudo sobre a proteção de dados e da privacidade na União Europeia, pode-se inferir que a legislação estrangeira é bastante avançada em relação à brasileira, tendo em vista que o GDPR é um Regulamento fruto de consenso não só em um país, mas entre vinte e oito Estados, a ser aplicado em âmbito transnacional.

Ademais, merecem destaque alguns institutos importantes adotados pelo modelo europeu.

O primeiro deles é a Autoridade Europeia para a Proteção de Dados (AEPD) que, como visto, é um órgão específico que visa garantir o respeito à privacidade de cidadãos no ciberespaço e a proteção de seus dados pessoais em toda a União Europeia.

O outro refere-se ao *Digital Clearing House*, ou seja, a rede de jurisdições europeias criada para que as autoridades de defesa do consumidor, da concorrência e da proteção de dados conversem entre si sobre as suas preocupações comuns, contribuindo para decisões mais homogêneas e contextualizadas à relação entre Direito e Internet.

Ademais, é imprescindível apontar a importância dada pela União Europeia ao *accountability principle*, que dispõe sobre a responsabilização de controladores de dados a fim de que desenvolvam instrumentos transparentes para a proteção dos indivíduos no mundo virtual, proporcionando segurança aos cidadãos e evitando a violação de dados na web.

Esses institutos europeus não têm similares no Brasil, podendo servir de inspiração à experiência nacional em busca de maior efetividade na proteção de dados, bem como no respeito à privacidade e à liberdade de comunicação no ciberespaço.

Após a análise da forma como o Estado brasileiro regula a proteção de dados, passar-se-á ao modo como o Poder Judiciário nacional tem enfrentado o debate.

4 JUDICIALIZAÇÃO DO DEBATE NO BRASIL: SUSPENSÕES NACIONAIS DO *WHATSAPP*

Entre fevereiro de 2015 e julho de 2016, alguns magistrados atuantes na primeira instância estadual do Judiciário proferiram decisões que suspenderam em todo o território brasileiro o aplicativo de comunicação online chamado *WhatsApp*.

A seguir, será feita a pormenorizada pesquisa de cada uma dessas decisões, a fim de verificar qual o embasamento fático que levou à suspensão e se houve utilização do Marco Civil da Internet como fundamento legal para as ordens judiciais.

Após, estudar-se-ão dois processos que tramitam no Supremo Tribunal Federal (STF) – ADPF 403 MC/SE e ADI 5527, os quais versam respectivamente sobre o bloqueio do *WhatsApp* e sobre a eventual declaração de inconstitucionalidade do artigo 12, incisos III e IV, do Marco Civil da Internet.

Por fim, ocorrerá uma análise crítica das suspensões do referido aplicativo, à luz da interpretação majoritária que se defende a respeito da Lei nº 12.965/2014.

4.1 ESTUDO DAS DECISÕES JUDICIAIS QUE SUSPENDERAM O *WHATSAPP* EM PRIMEIRA INSTÂNCIA

No total, foram quatro as decisões que determinaram a suspensão do referido aplicativo: a primeira foi prolatada pelo magistrado atuante na Central de Inquérito da Comarca de Teresina/PI, no processo nº 0013872-87.2014.8.18.0140¹⁰⁶; a segunda, proferida pelo juízo da 1ª Vara Criminal de São Bernardo do Campo/SP, no procedimento de Interceptação Telefônica nº

¹⁰⁶ Disponível em <<http://s.conjur.com.br/dl/liminar-whatsapp-tj-pi.pdf>>. Acesso em 08 de agosto de 2016.

0017520-08.2015.8.26.0564¹⁰⁷; a terceira, no processo de nº 201555000783, proveniente do juízo da Vara Criminal da Comarca de Lagarto/SE¹⁰⁸; e a quarta, determinada pela 2ª Vara Criminal de Duque de Caxias/RJ, nos autos nº 062-00164/2016¹⁰⁹.

Passar-se-á, então, à análise de cada uma dessas decisões, a fim de investigar qual a fundamentação utilizada por cada Juízo para determinar o bloqueio do aplicativo. Também será abordado se houve reforma desses atos judiciais em segunda instância e qual o respectivo fundamento para tanto.

Após esse estudo, pretende-se o estabelecimento de pontos convergentes nas fundamentações dos diferentes Juízos.

4.1.1 Processo nº 0013872-87.2014.8.18.0140

Em 11 de fevereiro de 2015, o juiz de direito Luis Moura Correia, à época atuante na Central de Inquéritos da Comarca de Teresina/Piauí, determinou a suspensão do funcionamento do *WhatsApp* em todo o território brasileiro pelo período de 24 horas.

Após tentativas de consulta ao trâmite dos autos nº 0013872-87.2014.8.18.0140 junto ao sítio eletrônico do Tribunal de Justiça do Estado do Piauí (TJPI)¹¹⁰, verificou-se que o processo se encontrava em segredo de justiça. Desse modo, restou impossibilitada a visualização da mencionada decisão.

¹⁰⁷ Disponível em <<http://s.conjur.com.br/dl/tj-sp-suspende-bloqueio-whatsapp.pdf>>. Acesso em 08 de agosto de 2016.

¹⁰⁸ Disponível em <http://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf>. Acesso em 08 de agosto de 2016.

¹⁰⁹ Disponível em <<http://tecnologia.uol.com.br/noticias/redacao/2016/07/19/veja-o-texto-completo-da-decisao-que-mandar-bloquear-o-whatsapp.htm>>. Acesso em 08 de agosto de 2016.

¹¹⁰ Consulta processual de primeira instância disponível em <<http://www.tjpi.jus.br/themisconsulta/>>. Acesso em 23 de agosto de 2016.

Em que pese o referido segredo de justiça, o teor da ordem judicial pôde ser visto devido à circulação, no ciberespaço, de um mandado expedido pelo juízo no processo nº 0013872-87.2014.8.18.0140¹¹¹.

Nesse mandado, o magistrado determinou às empresas de telefonia (provedoras de acesso à internet) que suspendessem:

Temporariamente até o cumprimento da ordem judicial (...), em todo território nacional, em caráter de urgência no prazo de 24 horas após o recebimento, o acesso através dos serviços da empresa aos domínios whatsapp.net e whatsapp.com, bem como todos os seus subdomínios e todos os outros domínios que contenham whatsapp.net e whatsapp.com em seus nomes e ainda todos números de IP (Internet Protocol) vinculados aos domínios já acima citados¹¹².

Também houve determinação no sentido de que as referidas empresas deveriam:

Garantir a suspensão do tráfego de informações de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações entre usuários do serviço e servidores da aplicação de troca de mensagens multi-plataforma denominada Whatsapp, em que pelo menos um desses atos ocorra em território nacional¹¹³.

Além disso, o Núcleo de Inteligência da Secretaria de Segurança Pública do Estado do Piauí emitiu uma nota à imprensa logo após o vazamento da foto do mandado expedido pela Central de Inquéritos de Teresina. Nessa nota, o referido Núcleo ratificou a veracidade do mandado, bem como indicou a fundamentação utilizada pelo Juízo para embasar a suspensão do aplicativo em estudo:

A ordem judicial foi expedida em virtude de anterior descumprimento, por parte do provedor de aplicação de Internet WhatsApp, de outras determinações de caráter sigiloso do citado Juízo. Insta esclarecer, também, que os processos judiciais que originaram as referidas decisões tiveram início desde o ano de 2013, mas até a presente data os responsáveis pelo Whatsapp não acataram as ordens judiciais. O mandado judicial foi encaminhado aos provedores de infraestrutura (Backbones) e aos provedores de conexão (operadoras de telefonia móvel entre outras).

¹¹¹ Disponível em <<http://epoca.globo.com/colunas-e-blogs/felipe-patery/noticia/2015/02/juiz-do-piaui-manda-btirar-whatsapp-do-arb-no-pais-inteiro.html>>. Acesso em 23 de agosto de 2016.

¹¹² *Idem*.

¹¹³ *Idem*.

Por fim, cabe esclarecer que **todas as representações e decisões judiciais acima mencionadas foram tomadas com base na Lei que instituiu e disciplinou o Marco Civil da Internet** (grifo nosso)¹¹⁴.

Como destacado acima, nessa nota consta que a base legal da decisão judicial foi a “Lei que instituiu e disciplinou o Marco Civil da Internet”. Entretanto, conforme já analisado no presente trabalho, essa Lei apenas foi e está sendo regulamentada em 2016, por meio do Decreto nº 8.771/2016 e do Projeto de Lei nº 5.276/2016.

Ou seja, à época da prolação da decisão judicial, em fevereiro de 2015, não havia nenhuma Lei que disciplinasse o Marco Civil da Internet a não ser ele próprio. Portanto, neste trabalho, será considerada a referida legislação (nº 12.965/2014) como fundamento legal utilizado pelo magistrado para ordenar a suspensão nacional do WhatsApp.

Já o embasamento fático, conforme a mencionada nota de esclarecimento, refere-se ao descumprimento de determinações judiciais anteriores por parte do referido aplicativo.

Inconformadas, a Empresa Brasileira de Telecomunicações (Embratel), em conjunto com as empresas Global Village Telecom S/A (GVT) e Claro S/A, impetraram mandado de segurança em face do Juízo da Central de Inquéritos de Teresina.

O desembargador relator Raimundo Nonato da Costa Alencar prolatou decisão em 26 de fevereiro de 2015 na qual determinou a suspensão da eficácia da decisão emitida em primeiro grau. Posteriormente, a decisão monocrática foi mantida pelo TJPI, que derrubou o ato judicial de suspensão do *WhatsApp*.

Note-se que o relator, ao conceder a liminar, ressaltou que o bloqueio do aplicativo ocorreu devido à “recalcitrância (do *WhatsApp*) quanto ao

¹¹⁴ Nota de esclarecimento disponível em <http://www.pc.pi.gov.br/download/201502/PC27_2b21f112a7.pdf>. Acesso em 27 de agosto de 2016.

cumprimento de outra ordem judicial, cujo teor, por se encontrar o processo originário protegido por segredo de justiça, reveste-se de incertezas”¹¹⁵.

Merece destaque, também, o seguinte entendimento adotado pelo desembargador Alencar:

(...) Independente do teor da ordem descumprida, em hipótese alguma se justifica a interrupção de acesso a todo um serviço, cuja área de abrangência, sabe-se, transpõe as barreiras nacionais de qualquer nação e afeta, direta e surpreendentemente, a comunicação entre um sem número de pessoas (...).

A fim de melhor ilustrar a falta de proporcionalidade que emana do ato questionado, imagine-se um juiz que, insatisfeito com a contumácia de determinada empresa telefônica em prestar-lhe informações sigilosas, determine a suspensão, em todo território nacional, dessa modalidade de serviço de comunicação (...).

Apesar de, num primeiro momento, essa analogia parecer destoar um pouco da situação em apreço, (...) tem-se a mesma ideia, qual seja, a (tentativa de) paralisação de uma gigantesca e pesada estrutura, em prol de uma investigação criminal que, muito provavelmente, possui um número limitadíssimo de suspeitos.

Além disso, (...), os organismos policiais dispõem de diversos outros meios de investigação, não se mostrando plausível que toda uma investigação passe a depender de informações de natureza telemática¹¹⁶.

Pelo exposto, da análise dessas decisões é possível extrair as seguintes conclusões: (a) o Juízo da Central de Inquéritos de Teresina/PI adotou o suposto descumprimento de ordens judiciais pelo *WhatsApp* como fundamento fático para a suspensão nacional do aplicativo; (b) o embasamento legal foi o Marco Civil da Internet; (c) a decisão foi reformada em segundo grau, ao argumento de que foi desproporcional, ou seja, de que afetou milhões de pessoas alheias ao caso concreto.

¹¹⁵ Inteiro teor da decisão disponível em < <http://s.conjur.com.br/dl/liminar-whatsapp-tj-pi.pdf> >. Acesso em 26 de setembro de 2016.

¹¹⁶ Idem.

4.1.2 Processo nº 0017520-08.2015.8.26.0564

Em 12 de dezembro de 2015, a Juíza Sandra Regina Nostre Marques, atuante à época na 1ª Vara Criminal de São Bernardo do Campo/SP, determinou a provedoras de acesso à internet o bloqueio do *WhatsApp*, pelo período de 48 horas.

Após tentativa de acesso aos autos nº 0017520-08.2015.8.26.0564 no sítio eletrônico do Tribunal de Justiça do Estado de São Paulo (TJSP), verificou-se que o procedimento criminal nº 0017520-08.2015.8.26.0564 corre em segredo de justiça. Desse modo, restou impossibilitada a visualização da íntegra do mencionado ato judicial¹¹⁷.

Em que pese o referido segredo de justiça, o setor de imprensa do TJSP informou que a decisão teve como fundamento fático o descumprimento, pelo *WhatsApp*, de determinação judicial anterior, prolatada em 23 de julho de 2015. Em tal decisão, a empresa teria sido intimada a apresentar conteúdo privado de conversas trocadas via *WhatsApp* por um suspeito de cometer crimes de latrocínio, tráfico de drogas e associação ao Primeiro Comando da Capital (PCC). Ante a ausência de cumprimento da mencionada ordem, em 07 de agosto de 2015 a empresa foi novamente notificada, sendo fixada multa em caso de não cumprimento da ordem exarada pelo Juízo¹¹⁸.

Como, ainda assim, a empresa não atendeu à determinação judicial, o Ministério Público requereu o bloqueio dos serviços pelo prazo de 48 horas, com base no Marco Civil da internet, o que foi deferido pela magistrada¹¹⁹.

¹¹⁷ Disponível em <http://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=FO0003J750000&processo.foro=564&uidCaptcha=sajcaptcha_bf594d87c78945b395b7568abc05c6fc>. Acesso em 26 de setembro de 2016.

¹¹⁸ Disponível em <<http://www.tjsp.jus.br/institucional/canaiscomunicacao/noticias/Noticia.aspx?Id=29056>>. Acesso em 26 de setembro de 2016.

¹¹⁹ Idem.

Ademais, o teor de um ofício expedido a empresas telefônicas pôde ser visto por meio de arquivo que circula no ciberespaço¹²⁰.

Consoante tal ofício, a magistrada determinou que fossem:

Adotadas as medidas técnicas necessárias para que a empresa prestadora de serviço de acesso à internet, fixa ou móvel (provedor de acesso ou conexão), **suspenda pelo prazo de quarenta e oito horas**, a partir das 00h00 seguinte ao recebimento da presente ordem, **em todo o território nacional, o acesso através dos serviços da empresa aos domínios WhatsApp.net e WhatsApp.com e subdomínios existentes relativos a estes aplicativos, devendo bloquear o tráfego de qualquer conteúdo que contenha tais domínios e, ainda, todos os números de IP vinculados aos domínios e subdomínios, inclusive a limpeza de cache desses domínios e tudo o que mais for necessário para a suspensão do tráfego de informações, coleta, armazenamento, guarda e tratamento de registro de dados pessoais ou de comunicações entre os usuários da rede que trafeguem por meio de provedores de acesso ou provedores de conexão das empresas acima mencionadas e da empresa WhatsApp Inc.**, em que pelo menos um desses atos ocorra em território nacional, sob pena de desobediência e eventual incidência dos **artigos 2º, §1º ou artigo 21, ambos da Lei nº 12.850/2013**¹²¹ (grifo nosso).

Note-se que a fundamentação adotada pelo Juízo tem relação com o que dispõem os artigos 11, caput¹²², e 12, inciso III, do Marco Civil da Internet¹²³.

Ou seja, na decisão judicial proferida, a magistrada determinou a suspensão (sanção disposta no artigo 12, inciso III) do tráfego de informações, coleta, armazenamento, guarda e tratamento de registro de dados pessoais ou de comunicações entre os usuários da rede que trafeguem por meio de

¹²⁰ Disponível em < http://media.josevitor.blog.br/uploads/2015/12/doc_35326197.pdf>. Acesso em 26 de setembro de 2016.

¹²¹ Inteiro teor também disponível em < <http://www.oanalista.com.br/2015/12/17/entenda-o-motivo-real-do-bloqueio-do-whatsapp/>>. Acesso em 26 de setembro de 2016.

¹²² Art. 11. Em qualquer operação de **coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional**, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (grifo nosso). Disponível em BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF: Senado Federal, 2014.

¹²³ 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: III - **suspensão temporária das atividades que envolvam os atos previstos no art. 11**; (grifo nosso). Disponível em BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF: Senado Federal, 2014.

provedores de acesso ou provedores de conexão (determinação contida no artigo 11).

Desse modo, reforça-se a conjectura de que o fundamento legal utilizado na decisão também foi o Marco Civil da Internet.

Além do mencionado diploma legal, a juíza asseverou que, em caso de desobediência da decisão por parte dos provedores de acesso e conexão, seria aplicado o artigo 2º, §1º¹²⁴ ou o artigo 21¹²⁵, ambos da Lei nº 12.850/2013 (Lei de Organização Criminosa).

Irresignada, a empresa WHATSAPP INC. impetrou mandado de segurança em face do Juízo da 1ª Vara Criminal de São Bernardo do Campo/SP.

O desembargador relator Xavier de Souza, atuante no TJSP, prolatou decisão em 17 de dezembro de 2015 na qual cassou a decisão proferida em primeiro grau no tocante à suspensão temporária das atividades do aplicativo *WhatsApp*¹²⁶.

Saliente-se que o relator entendeu que a ordem proferida pelo Juízo da 1ª Vara Criminal de São Bernardo do Campo/SP foi desproporcional. Isso porque seria possível a majoração de multa anteriormente imposta ao WhatsApp a fim de que as determinações judiciais fossem eventualmente cumpridas – no caso, o fornecimento de informações privadas para auxiliar investigação criminal de um suspeito de cometimento de delitos:

Em face dos princípios constitucionais, não se mostra razoável que milhões de usuários sejam afetados em decorrência da inércia da

¹²⁴ Art. 2º. Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa: Pena - reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas. § 1º Nas mesmas penas incorre quem impede ou, de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa. Disponível em BRASIL. Lei nº 12.850/2013 - Lei de Organização Criminosa. Brasília, DF: Senado Federal, 2013.

¹²⁵ Art. 21. Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. Parágrafo único. Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei. Disponível em BRASIL. Lei nº 12.850/2013 - Lei de Organização Criminosa. Brasília, DF: Senado Federal, 2013.

¹²⁶ Inteiro teor da decisão disponível em < <http://s.conjur.com.br/dl/tj-sp-suspende-bloqueio-whatsapp.pdf>>. Acesso em 26 de setembro de 2016.

impetrante, mormente quando não esgotados outros meios disponíveis para a obtenção do resultado desejado.

Cita a magistrada que foi imposta multa coercitiva, sem sucesso, daí a adoção da medida extrema.

Mas é possível, sempre respeitada a convicção da autoridade apontada como coatora, a elevação do valor da multa a patamar suficiente para inibir eventual resistência da impetrante, solução que, aparentemente, não foi adotada na origem¹²⁷.

No julgamento do mandado de segurança pelo TJSP, a decisão liminar foi mantida a fim de cancelar em definitivo a determinação de suspensão temporária das atividades do *WhatsApp*¹²⁸.

Assim, da análise dessas decisões é possível extrair as seguintes conclusões: (a) o Juízo da 1ª Vara Criminal de São Bernardo do Campo/SP adotou o suposto descumprimento de ordens judiciais pelo *WhatsApp* como fundamento fático para a suspensão nacional do aplicativo; (b) o embasamento legal foi o Marco Civil da Internet e a Lei de Organização Criminosa – esta em caso de descumprimento da decisão pelos provedores de acesso à internet; (c) o ato judicial foi cassado em segundo grau, ao argumento de que foi desproporcional, ou seja, de que afetou milhões de usuários quando não esgotados outros meios disponíveis para a obtenção do resultado desejado.

4.1.3 Processo nº 20155500078

Em 02 de maio de 2016, o juiz de direito Marcel Maia Montalvão, atuante à época na Vara Criminal de Lagarto/SE, determinou a suspensão do *WhatsApp* em todo o Brasil pelo período de setenta e duas horas.

Essa ordem foi exarada no processo nº 20155500078, o qual era uma medida cautelar de interceptação e quebra de sigilo de dados telemáticos

¹²⁷ Idem.

¹²⁸ Conforme o andamento processual dos autos do Mandado de Segurança nº 2271462-77.2015.8.26.0000, disponível, com restrição de acesso devido a segredo de justiça, em <<https://esaj.tjsp.jus.br/cpo/sg/search.do?conversationId=&paginaConsulta=1&localPesquisa.cdLocal=4&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=2271462-77.2015&foroNumeroUnificado=0000&dePesquisaNuUnificado=2271462-77.2015.8.26.0000&dePesquisaNuAntigo=#>>>. Acesso em 26 de setembro de 2016.

requerida por autoridade policial na investigação de uma organização criminosa voltada para o comércio ilegal de tráfico interestadual de drogas.

Após consulta processual ao sítio eletrônico do Tribunal de Justiça do Estado do Sergipe (TJSE), verificou-se que o processo nº 20155500078 corre em segredo de justiça¹²⁹. Desse modo, foi inviabilizado, a princípio, o acesso ao teor da decisão prolatada.

Em que pese essa restrição de acesso, nos autos da Ação de Descumprimento de Preceito Fundamental (ADPF) 403 MC / SE, a qual será abordada em tópico próprio neste trabalho, foi acostada a íntegra da decisão proferida em primeiro grau¹³⁰.

Nessa decisão, o magistrado mencionou que as investigações policiais de uma organização criminosa interestadual restariam prejudicadas por conta do uso do *WhatsApp*, que seria uma “plataforma do crime” a ser utilizada pelos investigados sem que fossem incomodados pelo Estado¹³¹.

O juiz também aduziu ser latente um conflito entre as esferas pública e privada. Em sua visão, não poderia uma investigação criminal ter sua continuidade impedida por conta da irresponsabilidade de empresas, cuja recusa ao cumprimento de decisões judiciais teria apenas cunho comercial em detrimento da soberania nacional¹³².

¹²⁹ Consulta processual disponível em <<http://www.tjse.jus.br/portal/consultas/consulta-processual/numero-do-processo>>. Acesso em 26 de setembro de 2016.

¹³⁰ Peça processual inserida na movimentação 23 dos autos da ADPF 403 MC / SE, disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 28 de outubro de 2016.

¹³¹ Nas palavras utilizadas pelo juiz Marcel Montalvão, “as investigações policiais encontrar-se-iam interrompidas no tocante à possibilidade de serem desvendados fatos importantes para o fiel desbastamento daquela organização que se utilizaria do aplicativo ‘WhatsApp’, sabedores que são agora de que poderiam utilizar-se de sua ‘plataforma do crime’ sem serem incomodados, em território nacional brasileiro”. Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 28 de outubro de 2016.

¹³² Conforme o magistrado, “não se imagina que uma investigação criminal de tráfico interestadual de drogas, abrangente no território nacional em vários Estados, seja impedida de ter a sua continuidade por (ir)responsabilidade de uma bilionária empresa com fins meramente comerciais em detrimento da soberania nacional”. Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

Ademais, o juiz de direito afirmou que a empresa responsável pelo aplicativo *WhatsApp* estaria tentando transformar seus clientes em verdadeiros escudos humanos, que serviriam de proteção para seus interesses particulares¹³³”.

Nesse sentido, mostra-se imprescindível o destaque ao seguinte trecho da decisão:

O aplicativo conhecido como WhatsApp, bem como a própria Facebook não são sinônimos de internet. Internet, como sabido, vai muito, muito mais além. Estas Empresas servem-se, apenas e tão-somente desta para seus objetivos quaisquer que sejam. Por acaso o serviço oferecido pela Facebook e pela WhatsApp são considerados essenciais, pela legislação brasileira? É evidente que não. Nem aqui nem além-mar. A par do desconforto e do comodismo, nossos serviços essenciais deixariam de ser oferecidos com possível suspensão temporária ou definitiva de seus serviços? É evidente que não. Portanto, por que quedar-se inerte contribuindo para a perpetuação dos agentes criminosos? Seria razoável e proporcional desrespeitar-se o ordenamento jurídico deste País? É evidente que não.

O magistrado ainda discorreu sobre a criptografia, argumentando que o modelo *end-to-end* oferecido pelo *WhatsApp* para proteger a privacidade nas conversas trocadas no aplicativo seria opcional. Para ele, a impossibilidade de decifrar a referida criptografia já violaria a legislação nacional¹³⁴.

Desse modo, utilizando como supedâneo legal o Marco Civil da Internet, em especial seus artigos 10, *caput* e §1º; 11, *caput* e §2º; e 12, *caput* e inciso III, determinou a suspensão nacional do aplicativo por prazo determinado.

Além da decisão acima analisada, verificou-se que o TJSE emitiu nota de esclarecimento sintetizando que:

O magistrado atendeu a uma medida cautelar ingressada pela Polícia Federal, com parecer favorável do Ministério Público, em virtude do não atendimento, mesmo após o pedido de prisão do representante do Facebook no Brasil, da determinação judicial de quebra do sigilo das mensagens do aplicativo para fins de investigação criminal sobre crime organizado de tráfico de drogas, na cidade de Lagarto/SE.

¹³³ Idem.

¹³⁴ Conforme o magistrado, “a criptografia end-to-end (se existente) é opcional, diante das constatações de suas mensagens de sua própria autoria (item 23 desta decisão). Ainda que fosse impossível decifrá-la, bem como a menos recente, já violaria a legislação deste País. Ou, então, que se mude a lei para beneficiá-la...”. Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

O Juiz informou ainda, que a medida cautelar está baseada nos arts. 11, 12, 13 e 15, *caput*, parágrafo 4º, da Lei do Marco Civil da Internet¹³⁵.

Como se vê, o fundamento fático utilizado pelo magistrado para a determinação de suspensão foi o descumprimento, pelo *WhatsApp*, da ordem de quebra de sigilo de mensagens do aplicativo para auxílio em investigações sobre prática de crime organizado de tráfico de drogas.

Por sua vez, o fundamento legal foi o Marco Civil da Internet, mais especificamente seus artigos 11, 12, 13 e 15, *caput* e §4º.

Inconformada, a empresa WHATSAPP INC. impetrou mandado de segurança, autuado sob nº 201600110899, contra o ato prolatado pelo Juízo da Vara Criminal de Lagarto/SE. O referido processo foi ingressado durante o plantão noturno, sendo concluso ao desembargador plantonista Cezário Siqueira Neto. Após, o mandado de segurança foi distribuído mediante sorteio eletrônico ao desembargador Ricardo Múcio Santana de Abreu Lima, que foi o relator da mencionada ação.

Embora tal procedimento também se encontrasse em segredo de justiça, o TJSE trouxe mais informações a respeito do mencionado mandado de segurança em nova nota de esclarecimento¹³⁶.

Segundo a referida nota, o desembargador plantonista Cezário Siqueira Neto manteve, durante o plantão noturno, a decisão proferida em segundo grau. Merece destaque o seguinte trecho da decisão:

O direito à privacidade dos usuários do aplicativo encontra-se em conflito aparente com o direito à segurança pública e à livre atuação da Polícia Federal e do Poder Judiciário na apuração de delitos, em favor de toda a sociedade. Neste primeiro momento, percebo que a impetrante, em verdade, minimiza a importância da investigação criminal de componentes de organização criminosa que utilizam o aplicativo em questão, escamoteando a gravidade do delito supostamente praticado (tráfico interestadual de drogas), sob a pecha de garantir o direito à intimidade de seus usuários. Ora, o uso do aplicativo por quem quer que seja e para qualquer fim não pode ser tolerado sem ressalvas. Deve, sim, sofrer restrição quando atinge

¹³⁵ Nota de esclarecimento disponível em < <http://www.tjse.jus.br/agencia/decisoes/item/9187-juiz-criminal-de-lagarto-determina-suspensao-do-whatsapp-por-72-horas> >. Acesso em 26 de setembro de 2016.

¹³⁶ Nota de esclarecimento disponível em <<http://www.tjse.jus.br/agencia/decisoes/item/9189-desembargador-denega-liminar-em-ms-e-mantem-suspensao-do-whatsapp>>. Acesso em 26 de setembro de 2016.

outros direitos constitucionalmente garantidos, como no caso em comento¹³⁷.

Ainda segundo a nota emitida pelo TJSE, na decisão o desembargador plantonista ressaltou que outras medidas anteriores foram determinadas visando ao acesso à interceptação da comunicação pelo aplicativo, a exemplo da aplicação de multas diárias, posteriormente majoradas em desfavor da empresa WHATSAPP INC.; e a ordem de prisão do seu Vice-Presidente na América Latina, Sr. Diego Jorge Dzordan, a qual foi reformada em sede de liminar de habeas corpus. Porém, todas não teriam obtido o êxito pretendido pelo Juízo.

Após a distribuição por sorteio, entretanto, houve reconsideração da decisão pelo desembargador Ricardo Múcio Santana de Abreu Lima. A íntegra de tal ato judicial foi obtida mediante nova consulta aos autos da ADPF 403 MC / SE¹³⁸, tendo em vista a restrição de acesso aos autos nº 201600110899¹³⁹.

Em tal decisão, o relator aduziu que, em sede de primeiro grau, houve determinação ao *WhatsApp* para quebra do sigilo telefônico e telemático de trinta e seis usuários do aplicativo. Ainda, pormenorizou as medidas requeridas pelo Juízo de primeiro grau à empresa impetrante:

Naquele feito, o Magistrado da Comarca deferiu medida para que fosse oficiado à Impetrante para implementar a interceptação do aplicativo WHATSAPP e fornecer o **acesso irrestrito às conversas de texto, fotografias, vídeos, conversas de voz, agenda de contatos, bem como ao conteúdo dos grupos aos quais os envolvidos estavam adicionados, dos alvos/terminais que foram relacionados, bem como fornecesse, via e-mail, conversas de texto, fotografias, vídeos, conversas de voz e agenda de contatos, ficando estipulada uma multa de R\$ 50.000,00 diários, a qual poderia ser aumentada em até 10% do faturamento do grupo econômico**, que gerou o mandado de segurança nº 201600110899¹⁴⁰ (grifo nosso).

Adentrando ao mérito da questão, o desembargador mencionou que a suspensão do *WhatsApp* gerou caos social em todo o território nacional, tendo

¹³⁷ *Idem*.

¹³⁸ Peça processual inserida na movimentação 23 dos autos da ADPF 403 MC / SE, disponível em <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 28 de outubro de 2016.

¹³⁹ Íntegra da decisão disponível em <http://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf>. Acesso em 26 de setembro de 2016.

¹⁴⁰ *Idem*.

em vista a ocorrência de dificuldades no desenvolvimento de atividades laborativas, de lazer, em família etc.¹⁴¹

Além disso, argumentou que não há condições de se afirmar que as informações poderiam ser fornecidas pelo *WhatsApp* ou que estas podem ser descriptadas para servir à Justiça¹⁴².

Ainda, apontou a existência de conflito de princípios que permeia o uso da internet – sigilo x bem comum x acesso à informação. Alegou ser certo que:

A Justiça, ao decretar a interrupção dos serviços de *WhatsApp*, o está fazendo como punição para garantir o bem comum. Este mesmo bem comum deve ser resguardado com o desembaraço no uso da internet e das comunicações. No primeiro caso o bem comum é consequência, enquanto no segundo ele é imediato¹⁴³.

Então, a partir dos fundamentos acima assinalados, houve suspensão da decisão que determinou o bloqueio do aplicativo em estudo. Note-se que essa decisão foi mantida em julgamento definitivo ocorrido em 31 de agosto de 2016¹⁴⁴.

Pelo exposto, a análise dessas decisões permite concluir que: (a) o Juízo da Vara Criminal de Lagarto/SE adotou como fundamento fático o descumprimento de ordens judiciais pelo *WhatsApp* referentes a quebra de sigilo telefônico e telemático irrestrito dos investigados – ou seja, acesso completo da autoridade judiciária a conversas de texto, fotografias, vídeos, conversas de voz, agenda de contatos, bem como a conteúdo dos grupos aos quais os envolvidos estavam adicionados e dos alvos/terminais que foram relacionados pelos referidos investigados; (b) o embasamento legal foi o Marco Civil da Internet, em especial os artigos 11, 12, 13 e 15, caput e §4º; (c) o ato judicial foi cassado em segundo grau, o qual entendeu que a suspensão nacional do aplicativo gerou caos social no Brasil, resta ausente a comprovação de que seria possível ao *WhatsApp* fornecer todos os dados requeridos pelo Juízo de primeiro grau e que

¹⁴¹ *Idem.*

¹⁴² *Idem.*

¹⁴³ *Idem.*

¹⁴⁴ Conforme a consulta processual aos autos do Mandado de Segurança nº201600110899, disponível em <<http://www.tjse.jus.br/portal/consultas/consulta-processual/numero-do-processo>>. Acesso em 26 de setembro de 2016.

há um conflito de princípios que permeia a discussão acerca da suspensão do aplicativo; e (d) pela primeira vez, houve menção ao uso de criptografia nas mensagens trocadas via *WhatsApp*, o que, a princípio, inviabilizaria o fornecimento de qualquer conteúdo de mensagens privadas.

4.1.4 Processo nº 062-00164/2016

Em 01 de agosto de 2016, a juíza de direito Daniela Barbosa Assumpção de Souza, atuante à época na 2ª Vara Criminal de Duque de Caxias/RJ, determinou novo bloqueio nacional do *WhatsApp*, dessa vez pelo prazo de vinte e quatro horas.

Tal decisão foi prolatada nos autos de IP nº 062-00164/2016, que tramita em segredo de justiça, tendo sido possível o acesso ao referido documento graças à sua disponibilização nos autos da ADPF nº 403 MC / SE¹⁴⁵ e em página eletrônica no ciberespaço¹⁴⁶.

Da leitura do ato judicial, vê-se que o Juízo de Duque de Caxias determinou ao WHATSAPP INC. e ao FACEBOOK BRASIL, anteriormente, a desabilitação da chave de criptografia do *WhatsApp* a fim de que, mediante a interceptação do fluxo de dados, ocorresse desvio em tempo real das mensagens já recebidas pelo usuário antes de serem criptografadas¹⁴⁷.

Mesmo após três intimações, as empresas não cumpriram a mencionada decisão judicial, o que teria ensejado a adoção de medidas coercitivas pelo Juízo¹⁴⁸.

¹⁴⁵ Disponível na movimentação 35 dos autos da ADPF 403 MC / SE. Disponível em < <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

¹⁴⁶ Disponível em < <http://tecnologia.uol.com.br/noticias/redacao/2016/07/19/veja-o-texto-completo-da-decisao-que-mandar-bloquear-o-whatsapp.htm>>. Acesso em 08 de outubro de 2016.

¹⁴⁷ *Idem*.

¹⁴⁸ *Idem*.

Segundo a magistrada, a codificação criptografada não pode servir de “escudo protetivo para práticas criminosas que, com absurda frequência”, se desenvolvem através de conversas trocadas no aplicativo em análise¹⁴⁹.

Merece destaque, também, o seguinte trecho da decisão que determinou a suspensão de funcionamento do referido aplicativo:

A finalidade pública da persecução criminal sempre deverá prevalecer sobre o interesse privado da empresa em preservar a intimidade e privacidade de seus usuários, assim como também deverá prevalecer sobre os interesses desses últimos, sobretudo quando são investigados por praticarem crimes, uma vez que não há direito ou garantia constitucional em nosso ordenamento que se repute absoluta. Aqueles na sociedade que reclamam a simples ausência de um aplicativo, como se não nos fosse mais possível viver sem tal facilidade, como se outros similares não pudessem ser utilizados, como se outros meios de comunicação não existissem, deveriam lembrar que a maior vítima dos crimes ora investigados é a própria Sociedade, sendo certo que a todo o momento novas vítimas são feitas e novos crimes são cometidos sem que a Justiça possa impedir os fatos ou punir os responsáveis¹⁵⁰.

Note-se, também, que a magistrada utilizou como embasamento legal para concessão da suspensão do *WhatsApp* o Marco Civil da Internet, em especial os artigos 7º, inciso III e o artigo 10 do mencionado diploma legal¹⁵¹.

Tal decisão foi suspensa pelo Supremo Tribunal Federal em 19 de julho de 2016 na Arguição de Descumprimento de Preceito Fundamental (ADPF) 403 MC / SE, a qual será abordada com mais detalhes em tópico próprio deste trabalho.

Por ora, faz-se imprescindível destacar que o Ministro RICARDO LEWANDOWSKI, na referida decisão prolatada pelo STF, entendeu que a ordem proferida pelo Juízo de primeiro grau violou o Marco Civil da Internet e a

¹⁴⁹ *Idem.*

¹⁵⁰ *Idem.*

¹⁵¹ *Idem.*

liberdade de expressão¹⁵². Destacou, também, a importância do aplicativo até mesmo para intimação de despachos ou decisões judiciais¹⁵³.

Pelo exposto, a partir do estudo dessas decisões conclui-se que: (a) o Juízo da 2ª Vara Criminal de Duque de Caxias/RJ adotou como fundamento fático o descumprimento de ordens judiciais pelo *WhatsApp* referentes à desabilitação da chave de criptografia do aplicativo a fim de que, mediante a interceptação do fluxo de dados, ocorresse desvio em tempo real das mensagens já recebidas pelo usuário alvo de investigação policial antes de serem criptografadas; (b) o embasamento legal foi o Marco Civil da Internet, em especial os artigos 7º, inciso III e o artigo 10 do mencionado diploma legal; (c) o ato judicial foi suspenso pelo STF, ao argumento de ocorrência de violação ao Marco Civil da Internet e desrespeito ao princípio da liberdade de expressão.

4.2 ENTENDIMENTO DO STF NA ADPF 403 MC/SE E NA ADI 5527

4.2.1 ADPF 403 MC/SE

O debate acerca da suspensão do *WhatsApp* tornou-se ainda mais complexo devido ao posicionamento do Supremo Tribunal Federal (STF) na Ação de Descumprimento de Preceito Fundamental (ADPF) com pedido de medida cautelar nº 403 MC/SE.

A referida ação foi ajuizada pelo Partido Popular Socialista (PPS) em 03 de maio de 2016 contra a decisão judicial proferida nos autos nº 201655000183

¹⁵² Conforme o Ministro LEWANDOWSKI, “já se procurou dar contornos legais à matéria. **A Lei 12.965/2014 surgiu, exatamente, com o propósito de estabelecer “princípios, garantias, direitos e deveres para o uso da Internet no Brasil”** (grifo nosso). Íntegra da decisão disponível em < <http://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adpf403mc.pdf> >. Acesso em 08 de outubro de 2016.

¹⁵³ Informação disponível em < <http://www.conjur.com.br/2016-fev-27/klaus-koplin-urgente-intimacao-feita-whatsapp>>. Acesso em 08 de outubro de 2016.

pelo juiz de direito Marcel Maia Montalvão, atuante à época na Vara Criminal de Lagarto/SE¹⁵⁴.

Liminarmente, o requerente pleiteou a suspensão dos efeitos da decisão do Juízo da Vara Criminal de Lagarto. Em provimento final, pugnou pela declaração de violação ao princípio fundamental de liberdade de comunicação, previsto no artigo 5º, inciso IX, da Constituição Federal¹⁵⁵.

Após abertura de prazo para manifestação da Procuradoria-Geral da República e expedição de ofício ao Juízo Criminal de Lagarto/SE para obtenção da íntegra da decisão lá proferida, o demandante PPS noticiou novo bloqueio do *WhatsApp*. Dessa vez, tal suspensão ocorreu devido à decisão proferida nos autos nº 062-00164/2016 pela magistrada Daniela Barbosa Assumpção de Souza, atuante à época na 2ª Vara Criminal de Duque de Caxias/RJ¹⁵⁶. Então, requereu o demandante a imediata suspensão de tal ato judicial.

Assim, em 19 de julho de 2016 o ministro Presidente à época RICARDO LEWANDOWSKI, exercendo o poder geral de cautela, examinou o pedido liminar de suspensão da decisão exarada pelo Juízo de Duque de Caxias.

Asseverou o ministro que o direito de livre comunicação e expressão, insculpido no artigo 5º, inciso IX, da Constituição Federal, é cláusula pétrea¹⁵⁷.

Quanto à regulação do ciberespaço, entendeu que o Marco Civil da Internet (Lei nº 12.965/2014) dá contornos legais à matéria¹⁵⁸. Ressaltou o teor

¹⁵⁴ Conforme a petição inicial da ADPF 403 MC / SE, cuja íntegra está disponível em consulta processual em <
<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 05 de outubro de 2016.

¹⁵⁵ Idem.

¹⁵⁶ Conforme movimentação 34 da ADPF 403 MC / SE. Disponível em <
<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

¹⁵⁷ Artigo 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: inciso IX: é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”. Disponível em BRASIL. Constituição Federal. Brasília, DF: Senado Federal, 1988.

¹⁵⁸ Segundo o ministro, “a Lei 12.965/2014 surgiu exatamente com o propósito de estabelecer garantias, direitos e deveres para o uso da internet no Brasil”. Disponível na movimentação 44 dos autos da ADPF 403 MC / SE <

do artigo 3º, incisos I e V da referida Lei, os quais garantem, respectivamente, a liberdade de expressão e a preservação da estabilidade da rede¹⁵⁹.

Nesse sentido, consoante a decisão do ministro, o bloqueio nacional do *WhatsApp* violou tanto o Marco Civil da Internet quanto os princípios da privacidade e da liberdade de comunicação, sendo medida desproporcional ao motivo que lhe deu causa¹⁶⁰.

Destacou, ainda, a importância do referido aplicativo inclusive para a intimação de despachos ou decisões judiciais¹⁶¹.

Desse modo, o ministro determinou a suspensão da decisão prolatada pelo Juízo de Duque de Caxias.

Após a habilitação como *amici curiae* de Federação das Associações das Empresas de Tecnologia da Informação (ASSESPRO NACIONAL), Instituto Beta Para Democracia e Internet (IBIDEM) e Instituto de Tecnologia e Sociedade (ITS)¹⁶², o Ministro relator LUIZ EDSON FACHIN, em 27 de outubro de 2016, determinou a realização de audiência pública a fim de que sejam trazidas respostas às seguintes questões:

- 1 – Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o *WhatsApp*?
- 2 – Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo *WhatsApp* ainda que esteja ativada a criptografia ponta a ponta (end to end)?

<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

¹⁵⁹ “Art.3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; (...) V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas”. Disponível em BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF: Senado Federal, 2014.

¹⁶⁰ Consoante a íntegra da decisão, o ministro indicou que “a suspensão do serviço do aplicativo *WhatsApp*, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa”. Disponível na movimentação 44 dos autos da ADPF 403 MC / SE <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

¹⁶¹ Idem.

¹⁶² Conforme a movimentação 52, 103 e 112 dos autos da ADPF 403 MC / SE. Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 08 de outubro de 2016.

3 – Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?

4 – Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível “espelhar” as conversas travas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?¹⁶³

Desse modo, verifica-se que ainda não houve julgamento em definitivo sobre o caso acima analisado.

Mesmo assim, tendo como base a decisão monocrática proferida pelo ministro LEWANDOWSKI, pode-se inferir a tendência do STF em se pautar na proporcionalidade e na proteção de dados garantida pelo Marco Civil da Internet para a defesa de um posicionamento contrário à suspensão nacional do *WhatsApp*.

4.2.2 ADI 5527

Em 13 de maio de 2016, o Partido da República (PR) ajuizou uma Ação Direta de Inconstitucionalidade (ADI) com pedido de medida cautelar contra os artigos 10, §2º; e 12, incisos III e IV do Marco Civil da Internet. Subsidiariamente, pleiteou a interpretação conforme à Constituição aos dispositivos mencionados¹⁶⁴.

O demandante aduziu que as determinações judiciais de suspensão do aplicativo *WhatsApp* no Brasil são comparáveis às medidas de censura adotadas em países como a China, a Coreia do Norte e o Irã¹⁶⁵.

¹⁶³ Conforme a decisão de movimentação 145 dos autos da ADPF 403 MC / SE. Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 02 de novembro de 2016.

¹⁶⁴ Conforme movimentação 1 dos autos da ADI 5527, disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4983282>>. Acesso em 09 de outubro de 2016.

¹⁶⁵ Idem.

Também defendeu que a suspensão não penalizaria apenas a empresa, mas também toda a população usuária do serviço de comunicação online. Isso, segundo o demandante, violaria os princípios da individualização da pena, da proporcionalidade, da liberdade de expressão e de comunicação, da livre iniciativa e da continuidade¹⁶⁶.

A ministra relatora ROSA WEBER determinou a requisição de informações ao Presidente da República, ao Senado Federal e à Câmara dos Deputados, bem como posterior vista ao Advogado-Geral da União e ao Procurador-Geral da República¹⁶⁷.

Ainda, o Instituto Beta para Democracia e Internet – IBIDEM e o Instituto de Tecnologia e Sociedade do Rio (ITS RIO) pleitearam ingresso como amici curiae.

Como se vê, nesse processo ainda não há um posicionamento do STF em relação ao tema. Mas mostrou-se imprescindível a menção a tal processo, tendo em vista a possibilidade de eventual declaração de inconstitucionalidade de artigos do Marco Civil da Internet utilizados nas decisões que determinaram a suspensão do *WhatsApp*.

4.3 ANÁLISE CRÍTICA DOS DADOS OBTIDOS

¹⁶⁶ Conforme a petição inicial, “a suspensão de tais aplicativos, antes de ser uma punição à empresa responsável, torna-se, em verdade, uma medida que penaliza a própria população em geral, que confia no funcionamento de tais serviços de comunicação para a dinâmica de seus relacionamentos pessoais e profissionais. Argumenta-se que a atividade de comunicação pela internet rege-se pelo princípio da continuidade (art. 241 CF/88), de maneira que a sanção aplicada à empresa responsável pelo aplicativo de troca de mensagens não pode atingir usuários estranhos ao objeto da punição (art. 5º, XLV, CF/88), visto que tal medida inviabiliza arbitrariamente o direito de livre comunicação dos cidadãos (art. 5º, IX CF/88), além de ferir os princípios da livre iniciativa (art. 1º, IV, CF/88), da livre concorrência (art. 170, caput, CF/88) e da proporcionalidade”. Disponível em <
<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4983282>>. Acesso em 09 de outubro de 2016.

¹⁶⁷ Disponível em <
<http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4983282>>. Acesso em 09 de outubro de 2016.

Após pormenorizado exame das quatro decisões judiciais que determinaram o bloqueio nacional do *WhatsApp*, pode-se inferir que todas têm pontos comuns em suas fundamentações.

Verifica-se, em síntese, que todas as decisões usaram como fundamento fático o descumprimento de ordem judicial anterior em investigações policiais ou processos criminais. Ademais, utilizaram o Marco Civil da Internet como base legal para a determinação de bloqueio do aplicativo. Ainda, os dois últimos atos judiciais proferidos inovaram ao mencionar a criptografia utilizada pelo *WhatsApp* nas conversas entre usuários.

A partir desses pontos convergentes, reforça-se o entendimento já adotado neste trabalho no sentido de que o Marco Civil da Internet constitui um importante patamar regulatório de proteção dos direitos do usuário do ciberespaço.

Porém, a partir do exame das decisões judiciais supramencionadas, vê-se que essa Lei ainda requer uma cautelosa compreensão de suas premissas e a das formas de implementação das suas sanções.

Antes de se proceder à análise crítica dessas decisões, será feito um breve exame do conceito de proporcionalidade sugerido por CANOTILHO E LARENZ, bem como da metáfora da colisão de princípios formulada por ROBERT ALEXY a fim de enriquecer a posterior análise crítica do tema em estudo.

CANOTILHO ensinou que qualquer limitação a direitos, liberdades e garantias deve ser adequada (apropriada), necessária (exigível) e proporcional (com justa medida). Advertiu também que “o domínio lógico de aplicação do princípio da proporcionalidade estende-se aos conflitos de bens jurídicos de qualquer espécie”¹⁶⁸.

¹⁶⁸ CANOTILHO, J. J. Gomes. *Direito constitucional e teoria da constituição*. 4. ed. Coimbra: Almedina, 1993, p. 129.

Assim, o teórico indicou que há três subprincípios que, juntos, abrangem o conteúdo da proporcionalidade: adequação, necessidade e proporcionalidade em sentido estrito.

Quanto à adequação, explicou que se trata de um controle empírico da “relação de adequação medida-fim”¹⁶⁹. Assim, para verificar se a decisão a ser tomada é adequada, o jurista deve responder à seguinte pergunta: a medida proposta é capaz de atingir o fim com ela visado¹⁷⁰?

Quanto à necessidade, CANOTILHO argumentou que se trata do direito do cidadão à “menor desvantagem possível” – ou seja, o Estado deve empregar, dentro do possível, as medidas menos lesivas ou onerosas para os particulares¹⁷¹. Nesse caso, o jurista deve se perguntar: a medida proposta é a menos lesiva possível aos particulares¹⁷²?

Havendo adequação e necessidade da medida, esta então é sujeita ao crivo da proporcionalidade em sentido estrito, que tem por objetivo aferir a validade material da decisão. A proporcionalidade assume, então, o significado de “justa medida” – deve-se procurar saber se os resultados obtidos estão numa relação de “medida” ou de “desmedida” com a carga lesiva que acarretam¹⁷³. Assim, a seguinte pergunta deve ser respondida: o sacrifício imposto pela medida proposta é admissível à luz de parâmetros normativo-axiológicos¹⁷⁴?

¹⁶⁹ CANOTILHO, J. J. Gomes. *O problema da responsabilidade do Estado por atos ilícitos*. Coimbra: Almedina, 1974, p. 270.

¹⁷⁰ VICENTE, Laura Nunes. *O princípio da proporcionalidade: uma nova abordagem em tempos de pluralismo*. Disponível em <http://www.ij.fd.uc.pt/publicacoes/premios/pub_1_ms/numero1_pms.pdf>. Acesso em 10 de novembro de 2016.

¹⁷¹ CANOTILHO, J. J. Gomes. *O problema da responsabilidade do Estado por atos ilícitos*. Coimbra: Almedina, 1974, p. 270.

¹⁷² VICENTE, Laura Nunes. *O princípio da proporcionalidade: uma nova abordagem em tempos de pluralismo*. Disponível em <http://www.ij.fd.uc.pt/publicacoes/premios/pub_1_ms/numero1_pms.pdf>. Acesso em 10 de novembro de 2016.

¹⁷³ CANOTILHO, J. J. Gomes. *O problema da responsabilidade do Estado por atos ilícitos*, Coimbra: Almedina, 1974, p. 271.

¹⁷⁴ VICENTE, Laura Nunes. *O princípio da proporcionalidade: uma nova abordagem em tempos de pluralismo*. Disponível em <http://www.ij.fd.uc.pt/publicacoes/premios/pub_1_ms/numero1_pms.pdf>. Acesso em 10 de novembro de 2016.

KARL LARENZ acrescentou que o princípio da proporcionalidade se apresenta como uma exigência da medida indicada – adequação entre meio e fim e do meio mais idôneo do direito protegido diante de outro bem jurídico igualmente protegido¹⁷⁵.

Assim, o teórico defende que a ideia de ‘justa medida’ tem uma relação estreita com a de justiça, tanto no exercício dos direitos como no cumprimento de deveres e ônus, devendo o jurista buscar o equilíbrio de interesses reciprocamente contrapostos na linha do menor prejuízo possível¹⁷⁶.

Relacionando o princípio da proporcionalidade com o sistema constitucional brasileiro, PAULO BONAVIDES ensinou que:

A proporcionalidade pode não existir enquanto norma geral de direito escrito, mas existe como norma esparsa no texto constitucional. A noção mesma se infere de outros princípios que lhe são afins, entre os quais avulta, em primeiro lugar, o princípio da igualdade, sobretudo em se atentando para a passagem da igualdade-identidade à igualdade-proporcionalidade, tão característica da derradeira fase do Estado de Direito.

(...)

O princípio da proporcionalidade é, por conseguinte, direito positivo em nosso ordenamento constitucional. Embora não haja sido ainda formulado como ‘norma jurídica global’, flui do espírito que anima em toda a sua extensão e profundidade o § 2º do art. 5º, o qual abrange a parte não-escrita ou não expressa dos direitos e garantias da Constituição, a saber, aqueles direitos e garantias cujo fundamento decorre da natureza do regime, da essência impostergável do Estado de Direito e dos princípios que este consagra e que fazem inviolável a unidade da Constituição. Poder-se-á enfim dizer, a esta altura, que o princípio da proporcionalidade é hoje axioma do Direito Constitucional, corolário da constitucionalidade e cânone do Estado no quadro de juridicidade de cada sistema legítimo de autoridade. A ele não poderia ficar estranho, pois, o Direito Constitucional brasileiro. Sendo, como é, princípio que embarga o próprio alargamento dos limites do Estado ao legislar sobre matéria que abrange direta ou indiretamente o exercício da liberdade e dos direitos fundamentais, mister se faz proclamar a força cogente de sua normatividade¹⁷⁷.

Por sua vez, o professor alemão ROBERT ALEXY parte da premissa de que o Direito possui uma estrutura aberta e conectada à realidade. Ainda, nesse campo da abertura do Direito não se pode decidir com base no Direito

¹⁷⁵ LARENZ, Karl. *Metodologia na ciência do direito*. Tradução de José Lamego. 3.ed. Lisboa: Fundação Calouste Gulbenkian, 1989, p. 603.

¹⁷⁶ Idem, p. 603.

¹⁷⁷ BONAVIDES, Paulo. *Curso de direito constitucional*. 11 ed. São Paulo: Malheiros, 2001, p. 396-397.

estritamente positivo, mas somente com a ajuda de critérios não jurídicos ou extrajurídicos¹⁷⁸.

Além disso, partindo da teoria proposta por ALEXY, os princípios se distinguem das regras por serem mandados de otimização¹⁷⁹, ou seja, normas que podem ser cumpridas em graus diferentes e ordenam que algo seja realizado em máxima medida relativamente às possibilidades reais e jurídicas¹⁸⁰.

O âmbito das possibilidades jurídicas é determinado pelas outras normas (princípios e regras) que atuam em sentido contrário. Assim, a realização completa de um determinado princípio pode ser obstada pela realização de outro princípio.

Essa ideia é traduzida pela metáfora da colisão entre princípios criada por ALEXY, que deve ser resolvida por meio da ponderação para que se possa chegar a um resultado ótimo, que vai sempre depender das variáveis do caso concreto¹⁸¹.

Com base no arcabouço teórico acima sintetizado, infere-se que todas as decisões proferidas pelos Juízos de primeiro grau foram desproporcionais.

Respondendo às perguntas anteriormente formuladas a partir da teoria de CANOTILHO, vê-se que as decisões não foram adequadas, pois a determinação de suspensão do *WhatsApp* não foi capaz de atingir o fim por ela visado – a disponibilização do conteúdo das conversas privadas trocadas pelos investigados no referido aplicativo. Essas decisões também não foram necessárias, visto que as medidas tomadas pelo Poder Judiciário de primeira instância não usaram os meios menos lesivos aos particulares. Ou seja,

¹⁷⁸ ANDRADE, Melanie Merlin. **Administração pública e racionalidade material: pretensão à correção para além da legalidade.** Disponível em < <http://acervodigital.ufpr.br/bitstream/handle/1884/30567/R%20-%20D%20-%20MELANIE%20MERLIN%20DE%20ANDRADE.pdf?sequence=1>>. Acesso em 05 out. 2016.

¹⁷⁹ ALEXY, Robert. **Teoria dos direitos fundamentais.** Trad. Virgílio Afonso da Silva. 2 ed. São Paulo: Malheiros, 2011, p. 117.

¹⁸⁰ BUSTAMANTE, Thomas. **Princípios, regras e conflitos normativos: um modelo para a justificação das decisões contra legem a partir da teoria jurídica de Robert Alexy.** Disponível em < <http://direitoestadosociedade.jur.puc-rio.br/media/Artigo7%20Thomas.pdf> >. Acesso em 05 out. 2016.

¹⁸¹ SILVA, Virgílio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. Disponível em < http://constituicao.direito.usp.br/wp-content/uploads/2003-RLAEC01-Principios_e_regras.pdf >. Acesso em 05 out. 2016.

determinaram o bloqueio nacional de um aplicativo que é usado por milhões de pessoas, prejudicando-as por conta de alguns investigados na seara criminal. Ainda, não foram proporcionais em sentido estrito, pois os resultados obtidos com a suspensão do *WhatsApp* afetaram terceiros alheios à sanção.

Ademais, ao contrário do proposto por KARL LARENZ em sua teoria, as decisões judiciais em análise não respeitaram a adequação entre o direito protegido diante de outro bem jurídico igualmente protegido. Ou seja, impuseram a todos os usuários do aplicativo uma sanção que não lhes cabia, tolhendo sua liberdade de comunicação. De outro lado, determinaram o bloqueio do referido aplicativo como forma de sanção às tentativas frustradas de invasão autorizada judicialmente da privacidade de determinados usuários, alvos de investigações policiais.

Não bastasse isso, tomando por base as lições de ROBERT ALEXY, verifica-se que os magistrados não fizeram uso de métodos de ponderação entre princípios para o fornecimento de um resultado ótimo ao caso concreto.

Note-se que uma das decisões, proferida pelo Juízo de Lagarto/SE, beirou ao absurdo ao utilizar como argumento o suposto fato de que o *WhatsApp* seria uma “plataforma do crime” a ser utilizada pelos investigados sem que fossem incomodados pelo Estado, bem como que os usuários seriam usados como “escudo humano” para as empresas responsáveis pelo aplicativo garantirem seus interesses particulares¹⁸².

Assim, ao invés de se utilizar a ponderação entre o interesse público e a segurança, de um lado, e a privacidade e a liberdade de expressão, de outro, o que ocorreu foi tão somente a banalização de toda a discussão a fim de garantir a repressão estatal sobre a liberdade de comunicação e de expressão dos indivíduos.

DANILO DONEDA e JOANA VARON observaram que, ao contrário das três primeiras decisões, as quais determinaram a disponibilização dos IDs dos

¹⁸²

Disponível em <<http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500>>. Acesso em 28 de outubro de 2016.

usuários e o conteúdo das conversas, o último ato judicial, proferido pelo Juízo de Duque de Caxias/RJ, ordenou ao *WhatsApp* a desativação de sua criptografia, permitindo ao Estado o monitoramento em tempo real das conversas¹⁸³.

Permitir que tal ordem judicial continue válida abre perigosos precedentes ao controle estatal dos usuários na internet, na contramão de todo o arcabouço legal existente nacional e internacionalmente.

Cabe mencionar, ainda, que segundo esclarecimentos prestados por MATT STEINFELD, diretor de comunicação do *WhatsApp*, o referido aplicativo não armazena o conteúdo das mensagens¹⁸⁴.

Ainda, com a adoção do sistema de criptografia *end-to-end*, cada parte da conversa trocada entre usuários do aplicativo recebe uma chave e os dados (mensagens, fotos, vídeos) enviados entre elas são codificados e só podem ser acessados por quem detenha tal chave. Assim, ainda que guardassem as informações de seus usuários, os administradores do aplicativo alegam que não teriam como decodificar as mensagens, ainda que quisessem¹⁸⁵.

Também deve-se levar em conta que os artigos 10, 11 e 12 da referida Lei se inserem na seção de proteção dos direitos do usuário da internet, intitulada “Da proteção de registros, dados pessoais e comunicações privadas”.

Assim, conforme o entendimento do Instituto de Tecnologia e Sociedade do Rio – ITS Rio, preservar a “neutralidade” da rede, ou seja, protegê-la contra

¹⁸³ VARON, Joana; DONEDA, Danilo. *The battle of encryption in Brazil*. Disponível em <<https://www.privacyinternational.org/node/987>>. Acesso em 12 de novembro de 2016.

¹⁸⁴ SANTINO, Renato. **WhatsApp explica por que não entrega os dados que a polícia brasileira pede**. Disponível em <http://olhardigital.uol.com.br/fique_seguro/noticia/whatsapp-explica-por-que-nao-entrega-os-dados-que-a-policia-brasileira-pede/55829>. Acesso em 05 out.2016.

¹⁸⁵ GONÇALVES, Lukas Ruthes. **WhatsApp. Criptografia ponta-a-ponta e o Marco Civil da Internet**. Disponível em <<http://intellinova.com.br/whatsapp-criptografia-marco-civil/>>. Acesso em 05 out. 2016.

a interferência desnecessária do Estado e contra o abuso do poder econômico privado, foi uma das principais conquistas do Marco Civil da Internet¹⁸⁶.

Desse modo, admitir o bloqueio de aplicativos com base justamente no Marco Civil joga por terra esse princípio essencial da neutralidade da rede. Em outras palavras, o desvirtuamento da aplicação do artigo 12 ou sua supressão do ordenamento jurídico acarretaria a diminuição do padrão mínimo de proteção do usuário.

Como já exposto no Capítulo 2 deste trabalho, o descumprimento de ordens judiciais não pode acarretar automaticamente as sanções previstas no artigo 12 do Marco Civil. Isso porque elas visam, acima de tudo, o respeito dos provedores aos deveres elencados nos artigos 10 e 11.

Nesse sentido é o entendimento de BRUNO GARCIA REDONDO e RONALDO LEMOS:

Ocorre que o art. 12 estabelece sanções por práticas de atos gravíssimos, violadores das garantias e direitos fundamentais - dignidade, intimidade, vida privada, honra, imagem -, que podem repercutir não somente sobre aspectos pessoais individuais, como também sobre questões econômicas e de mercado (segredos profissionais, tratativas empresariais, etc.) e, até mesmo, sobre toda uma determinada coletividade (...). A não aplicação da sanção (art. 12) torna inócua a proteção conferida pelos arts. 10 e 11.¹⁸⁷

Dessa forma, o escopo do artigo 12 é exclusivamente o de proteger o direito à privacidade do indivíduo.

Então, as determinações de bloqueio do WhatsApp são incompatíveis com o Estado Democrático de Direito, consistindo em violações aos direitos humanos, conforme o supramencionado entendimento do Conselho de Direitos Humanos da Organização das Nações Unidas¹⁸⁸.

¹⁸⁶ “Lei não justifica bloqueio de apps, dizem especialistas” (Exame): Disponível em <<http://exame.abril.com.br/tecnologia/noticias/lei-nao-justifica-bloqueio-de-appsdizem-especialistas>>. Acesso em 08 de novembro de 2016.

¹⁸⁷ REDONDO, Bruno Garcia. *Infrações e sanções cíveis, penais e administrativas*. in LEMOS, Ronaldo; LEITE, George Salomão. *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 729.

¹⁸⁸ “10. Condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures”. Disponível em <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20>. Acesso em 08 de novembro de 2016.

O bloqueio do aplicativo viola, também, o princípio constitucional da livre iniciativa. Pelos princípios que orientam a ordem econômica constitucional, não deve haver intervenção desproporcional e desnecessária do Estado em atividades econômicas privadas. Ao ordenar o bloqueio nacional do WhatsApp, o Estado interfere diretamente no exercício de um imensurável número de atividades econômicas que funcionam em torno desse serviço online e dele dependem diretamente.

Se alguma empresa realizar a “operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet” prevista no artigo 11 em desconformidade com a legislação brasileira, somente a ela devem ser impostas de forma gradativa, específica, individualizada e proporcional às sanções do art. 12 do Marco Civil.

Saliente-se que em acórdão recente, o Superior Tribunal de Justiça sedimentou o posicionamento em torno da proteção e inviolabilidade do sigilo dos dados em si, e não apenas da comunicação de dados. Ao analisar a ilicitude da prova decorrente da apreensão de um telefone celular, cujo acesso aos dados e às mensagens instantâneas ocorreu sem prévia autorização judicial, a Corte afirmou serem também os dados sujeitos à proteção constitucional¹⁸⁹.

Tal entendimento demonstra profundo cuidado com o sigilo, a privacidade e a proteção de dados de terceiros não sujeitos à investigação criminal, enquanto que nas recentes decisões judiciais de suspensão dos serviços de comunicação instantânea sequer se atentou para essa possibilidade (grupos de mensagens compartilhadas, fotografias armazenadas em *cloud computing* etc.).

É certo que a garantia de inviolabilidade do sigilo de dados não é absoluta e a Constituição Federal veda o anonimato. Todavia, as decisões judiciais de interceptação para fins de investigação criminal devem ser proferidas em harmonia com a proteção dos direitos dos demais usuários, de modo a que

¹⁸⁹ STJ, RHC 51.531/RO, Rel. Min. Nefi Cordeiro, Sexta Turma, DJe 09.05.2016.

não sejam prejudicados. Quando veda o anonimato, a Constituição Federal o faz em associação à liberdade de manifestação do pensamento (art. 5.º, IV), o que não significa que em toda e qualquer interação no ciberespaço ele seja vedado¹⁹⁰.

Ademais, a atividade de comunicação pela internet rege-se pelo princípio da continuidade (artigo 241 da Constituição Federal), de maneira que a sanção aplicada à empresa responsável pelo aplicativo de troca de mensagens não pode atingir usuários estranhos ao objeto da punição (artigo 5º, inciso XLV, da CF), visto que tal medida inviabiliza arbitrariamente o direito de livre comunicação dos cidadãos (artigo 5º, inciso IX, da CF), além de ferir os princípios da livre iniciativa (artigo 1º, inciso IV, da CF), da livre concorrência (artigo 170, caput, da CF) e da proporcionalidade.

Pelo exposto, 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 investigações criminais e decisões judiciais, ao invés de constituir um sistema de proteção do sigilo de comunicação e dos dados da grande maioria dos usuários.

Então, as sanções previstas no artigo 12 do Marco Civil da Internet devem ser pautadas pelo princípio da proporcionalidade em sua cominação, tendo sempre em mira a adequação, necessidade, utilidade e proporcionalidade em sentido estrito do seu alcance.

¹⁹⁰ QASIR, Sophia. *Anonymity in Cyberspace: Judicial and Legislative Regulations*. Fordham Law Review, v. 81, p. 3651, 2012.

5 CONCLUSÕES

Este trabalho permite concluir que é latente a existência de um dilema de ordem jurídico-política envolvendo a proteção de dados: ao mesmo tempo em que há um suposto direito do Estado de interceptar dados eletrônicos, sob o pretexto de garantir segurança aos cidadãos, também tem o próprio ente estatal o dever de respeitar e proteger a privacidade e a liberdade de comunicação dos particulares na web.

Esse dilema traduz-se em um conflito de princípios: de um lado, a segurança e o interesse público; de outro, a privacidade e a liberdade de comunicação.

O debate torna-se ainda mais interessante devido à constatação de que a privacidade e a liberdade de comunicação adquiriram nova roupagem, sendo que seus conceitos não podem mais ser dissociados da proteção de dados eletrônicos e da criptografia.

Especificamente em relação ao *WhatsApp*, vê-se que a adoção do modelo criptográfico de ponta-a-ponta (*end-to-end*) tem por objetivo imprimir um padrão elevado de proteção de dados de seus usuários.

Esse padrão é uma notória aplicação do que prevê o Novo Regulamento Geral de Proteção de Dados da União Europeia (GDPR), no sentido de que os dispositivos, serviços e plataformas na internet devem garantir a proteção de dados e a privacidade por configuração e padrão de fabricação (*privacy by design* e *privacy by default*).

O GDPR também previu, no art. 23 (1), 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.

Assim como a normativa europeia, a atual legislação que regula a proteção de dados no Brasil, o Marco Civil da Internet, adota como perspectiva

o respeito aos direitos dos usuários, e não a imposição de obrigações excessivas aos provedores.

Desse modo, o Estado deve frear suas expectativas regulatórias na web. Isso porque as sanções constantes do artigo 12 do Marco Civil da Internet só deverão ser aplicadas se o provedor não respeitar os deveres dispostos nos artigos 10 e 11 da Lei, ou seja, caso não haja a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas na guarda e na disponibilização dos registros de conexão e de acesso a aplicações de internet.

Os julgamentos da ADPF 403 MC/SE e da ADI 5527 serão marcos decisórios importantes que nortearão o debate sobre o controle estatal de dados a um novo rumo.

Enquanto isso, a proporcionalidade é a principal peça-chave para o alcance do equilíbrio entre o direito à proteção dos dados pessoais e a segurança pública¹⁹¹.

¹⁹¹ SHAH, Reema. Law Enforcement and Data Privacy: A Forward-Looking Approach. *Yale Law Journal*, v. 125, 2015, p. 543.

REFERÊNCIAS

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2 ed. São Paulo: Malheiros, 2011.

ANDRADE, Melanie Merlin. *Administração pública e racionalidade material: pretensão à correção para além da legalidade*. Disponível em < <http://acervodigital.ufpr.br/bitstream/handle/1884/30567/R%20-%20D%20-%20MELANIE%20MERLIN%20DE%20ANDRADE.pdf?sequence=1>>. Acesso em 05 out. 2016.

ASSANGE, Julian. *Cyberpunks - Liberdade e o futuro da internet*. São Paulo: Boitempo, 2013.

BARLOW, John Perry. *Declaração de independência do ciberespaço*. Disponível em < <http://www.dhnet.org.br/ciber/textos/barlow.htm>>. Acesso em 28 de setembro de 2016.

BIONI, Bruno Ricardo; CANABARRO, Diego R. *A Internet no Congresso Nacional: um panorama dos números relacionados à regulação da rede no Brasil*. Disponível em < <http://observatoriodainternet.br/post/a-internet-no-congresso-nacional-um-panorama-dos-numeros-relacionados-a-regulacao-da-rede-no-brasil>>. Acesso em 09 de outubro de 2016.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7. ed. Rio de Janeiro: Forense Universitária, 2008.

BONAVIDES, Paulo. *Curso de direito constitucional*. 11 ed. São Paulo: Malheiros, 2001.

BRASIL. Decreto nº 8.771, de 11 de Maio de 2016. Brasília, Senado Federal, 2016.

_____. Código Civil. Brasília, Senado Federal, 2002.

_____. Constituição Federal. Brasília, Senado Federal, 1988.

_____. Lei nº 12.965/2014 - Marco Civil da Internet. Brasília, Senado Federal, 2014.

_____. Lei nº 12.850/2013 - Lei de Organização Criminosa. Brasília, DF: Senado Federal, 2013.

BUSTAMANTE, Thomas. *Princípios, regras e conflitos normativos: um modelo para a justificação das decisões contra legem a partir da teoria jurídica de Robert Alexy*. Disponível em < <http://direitoestadosociedade.jur.puc-rio.br/media/Artigo7%20Thomas.pdf> >. Acesso em 05 out. 2016.

BUTARELLI, Giovanni. *Privacy in an age of hyperconnectivity*. Discurso de Giovanni Buttarelli no “*Privacy and Security Conference 2016*”, ocorrido em Neusiedler See, Áustria, em 2016. Disponível em < https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2016/16-09-30_accountability_speech_EN.pdf>. Acesso em 11 de novembro de 2016.

CALDERÓN, César; LORENZO, Sebastián. *Open Government*. Algón, 2010.

CANOTILHO, J. J. Gomes. *Direito constitucional e teoria da constituição*. 4. ed. Coimbra: Almedina, 1993.

_____. *O problema da responsabilidade do Estado por atos ilícitos*. Coimbra: Almedina, 1974.

CASTELLS, Manuel. *A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de Janeiro: Jorge Zahar, 2003.

_____. *A sociedade em rede*. 6.ed. São Paulo: Paz e Terra, 2006.

CRUZ, Francisco Carvalho de Brito. *Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet*. 2015. 138 pp. Mestrado – Faculdade de Direito, Universidade de São Paulo. 2015. Disponível em < <http://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/pt-br.php>>. Acesso em 06 de outubro de 2016.

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

EISENBERG, José. *Internet, democracia e República*. *Dados*, v. 46, n. 3, p. 491-511, 2003.

FARACO, Alexandre Ditzel. *Democracia e regulação das redes eletrônicas de comunicação: rádio, televisão e internet*. Belo Horizonte: Fórum, 2009.

FARIAS, Edilsom Pereira de. *Colisão de direitos*. Porto Alegre: Sergio Antonio Fabris Editor, 2000.

FARRANHA, Ana Claudia. *Estado, sociedade e interações digitais: expectativas democráticas*. *Revista de Pesquisa em Políticas Públicas*, n. 2, 2014.

GONÇALVES, Lukas Ruthes. *WhatsApp. Criptografia ponta-a-ponta e o Marco Civil da Internet*. Disponível em <<http://intellinova.com.br/whatsapp-criptografia-marco-civil/>>. Acesso em 05 out. 2016.

GOODMAN, Marc. *Future crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso*. São Paulo: HSM Editora, 2015.

HENRIQUES, Ricardo. *Perspectivas para a protecção de dados pessoais*. Disponível em <<https://www.publico.pt/mundo/noticia/perspectivas-para-a-proteccao-de-dados-pessoais-1721553>>. Acesso em 11 de novembro de 2016.

LARENZ, Karl. *Metodologia na ciência do direito*. Tradução de José Lamego. 3.ed. Lisboa: Fundação Calouste Gulbenkian, 1989.

LEMOS, Ronaldo; et. al. *Comentários e sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL nº 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania*, novembro de 2010, disponível em <<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/7719>>. Acesso em 06 de outubro de 2016.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.

LESSIG, Lawrence. *Code - version 2.0*. 2006. Disponível em <<http://codev2.cc/download+remix/Lessig-Codev2.pdf>>. Acesso em 28 de setembro de 2016.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999.

LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. *A Proteção dos Dados Pessoais na Fase de Coleta: Aparentamentos sobre a Adjetivação do Consentimento Implementado pelo Artigo 7, Incisos VIII e IX do Marco Civil da Internet a partir da Human Computer Interaction e da Privacy By Default*. In *Direitos & Internet III –Marco Civil da Internet*. Tomo I. São Paulo: Quartier Latin, 2015.

KOOPS, Bert-Jarp; Bekkers, Rudi. *Interceptability of telecommunications: is US and Dutch Law prepared for the future?* Disponível em <<http://poseidon01.ssrn.com/delivery.php?ID=306070120093083024112086085112094095006031030087027036073099002024095030000116085026043019049012062042054090111096003087064005027080066016052014085126116>>

011119088047020064113009125027080019003082091067112101015090064085008111120007093004101028017&EXT=pdf>. Acesso em 05 out. 2016.

MARCACINI, Augusto Tavares Rosa. *Direito e Informática: uma abordagem jurídica sobre a criptografia*. São Paulo: Forense, 2002.

MARTINO, Luís Mauro Sá. *Teoria das mídias digitais: linguagens, ambientes e redes*. 2 ed. Petrópolis: Vozes, 2015.

MELLO, Cláudio Ari. *Democracia constitucional e direitos fundamentais*. Porto Alegre: Livraria do Advogado Editora, 2004.

MENEGUETTI, Tarcísio; CELANT, João Henrique Celant. *Liberdade e controle no ciberespaço: uma análise do Marco Civil da Internet e do governo eletrônico*. Disponível em <<http://www.publicadireito.com.br/artigos/?cod=1f9caf93105becc0>>. Acesso em 05 out. 2016.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet*. Curitiba: Juruá, 2006.

PINHO, José Antonio Gomes de. *Sociedade da informação, capitalismo e sociedade civil: reflexões sobre política, internet e democracia na realidade Brasileira*. Revista de Administração de Empresa, v.51, n.1, pp. 98-106, 2011.

PINTO, Álvaro Vieira. *O Conceito de Tecnologia*. Rio de Janeiro: Contraponto, 2005. 2v.

QASIR, Sophia. *Anonymity in Cyberspace: Judicial and Legislative Regulations*. Fordham Law Review, v. 81, 2012.

REDONDO, Bruno Garcia. *Infrações e sanções cíveis, penais e administrativas*. in LEMOS, Ronaldo; LEITE, George Salomão. *Marco Civil da Internet*. São Paulo: Atlas, 2014.

SANTARÉM, Paulo Rená da Silva. *O direito achado na rede: a emergência do acesso à internet como direito fundamental no Brasil*. Dissertação de mestrado. Universidade de Brasília, 2010, p. 97. Disponível em <http://repositorio.unb.br/bitstream/10482/8828/1/2010_PauloRen%c3%a1daSilvaSantar%c3%a9m.pdf>. Acesso em 08 de outubro de 2016.

SANTINO, Renato. *WhatsApp explica por que não entrega os dados que a polícia brasileira pede*. Disponível em <http://olhardigital.uol.com.br/fique_seguro/noticia/whatsapp-explica-por-que>

nao-entrega-os-dados-que-a-policia-brasileira-pede/55829>. Acesso em 05 out.2016.

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

SERBENA, César (coord.). *E-Justiça e Processo eletrônico - Anais do 1º Congresso de e-Justiça da UFPR*. Curitiba: Juruá, 2013.

SHAH, Reema. *Law Enforcement and Data Privacy: A Forward-Looking Approach*. *Yale Law Journal*, v. 125, 2015.

SHAPIRO, Carl; VARIAN, Hal R. *A Economia da Informação: como os princípios econômicos se aplicam à era da Internet*. Rio de Janeiro: Campus, 1999.

SIEGEL, Reva. *Constitutional Culture, Social Movement Conflict and Constitutional Change: The Case of the facto ERA*. *California Law Review*, nº 94, 2006.

SILVA, Virgílio Afonso da. *Princípios e regras: mitos e equívocos acerca de uma distinção*. Disponível em < http://constituicao.direito.usp.br/wp-content/uploads/2003-RLAEC01-Principios_e_regras.pdf >. Acesso em 18 de outubro de 2016.

SOLAGNA, Fabrício; SOUZA, Rebeca Hennemann V; LEAL, Ondina Fachel. *Quando o Ciberespaço faz as suas leis: o processo do Marco Civil da Internet no contexto de regulação e vigilância global*. *Revista Vivência*, Ed. Nº 45, 2015.

TAPIA, José Antonio Pérez. *Internautas e náufragos: a busca do sentido na cultura digital*. São Paulo: Loyola, 2006.

TEPEDINO, Gustavo. *Temas de Direito Civil*. 3. ed., rev. e atual. Rio de Janeiro: Renovar, 2004.

VARON, Joana; DONEDA, Danilo. *The battle of encryption in Brazil*. Disponível em < <https://www.privacyinternational.org/node/987> >. Acesso em 12 de novembro de 2016.

VICENTE, Laura Nunes. *O princípio da proporcionalidade: uma nova abordagem em tempos de pluralismo*. Disponível em <http://www.ij.fd.uc.pt/publicacoes/premios/pub_1_ms/numero1_pms.pdf>. Acesso em 10 de novembro de 2016.