UNIVERSIDADE FEDERAL DE CAMPINA GRANDE-UFCG
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS-CCJS
UNIDADE ACADÊMICA DE DIREITO-UAD

TÚLIO MARLON SARAIVA DE MEDEIROS

CRIPTOGRAFIA DE PONTA-A-PONTA E O MARCO CIVIL DA INTERNET

SOUSA-PB

2017

TÚLIO MARLON SARAIVA DE MEDEIROS

CRIPTOGRAFIA DE PONTA-A-PONTA E O MARCO CIVIL DA INTERNET

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande-UFCG, como exigência parcial para obtenção do título de bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Eduardo Pordeus Silva.

SOUSA-PB

2017

TÚLIO MARLON SARAIVA DE MEDEIROS

CRIPTOGRAFIA DE PONTA-A-PONTA E O MARCO CIVIL DA INTERNET

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande- UFCG, como exigência parcial para obtenção do título de bacharel em Ciências Jurídicas e Sociais.

.

Banca examinadora: Data da aprovação: 13/03/2017

_____

Eduardo Pordeus Silva – Doutor - UFCG

Professor Orientador

_____

Lourdemario Ramos de Araujo – Mestre – UFCG

Professor (a)

_____

Francisco César Martins de Oliveira – Mestre – UFCG

Professor (a)

Dedico este trabalho a todas as vítimas
de ataques na Internet que tiveram a
vida privada exposta e sofreram as
cruéis consequências por
simplesmente serem quem são.

AGRADECIMENTOS

Em primeiro lugar, agradeço aos meus pais, por todos os esforços realizados ao longo dos últimos cinco anos para que possibilitassem a minha graduação em Direito, o que não poderia acontecer sem o carinho, o apoio e a confiança deles.

Aos meus professores, em especial ao meu orientador, e todos os servidores do CCJS que contribuíram para a minha formação como profissional e ser humano, acrescentando ensinamentos que ultrapassam os limites acadêmicos.

Aos meus amigos, reais e virtuais, que permaneceram ao meu lado nos momentos mais importantes, experimentando comigo os sentimentos e as emoções desta jornada a qual chamamos de vida.

Agradeço à proteção espiritual que acredito sentir daqueles que partiram deste plano e que tenho fé que em algum lugar deste imenso universo retribuem aos meus mais sinceros agradecimentos.

Por fim, agradeço, com humildade, a todos aqueles que me subestimaram, dizendo a mim que eu não poderia, que não conseguiria ou que não deveria, os quais também me ajudaram, de certa forma, a me tornar quem sou hoje.

Muito obrigado.

If I ran away I'd never have the strength
to go very far
How would they hear
the beating of my heart?
Will it go cold the secret that I hide?
Will I grow old?
How would they hear?
When will they learn.?
How would they know?
Madonna

RESUMO

A partir do método dedutivo se propõe investigar quais são os possíveis conflitos entre a criptografia de ponta-a-ponta e a legislação sobre internet no Brasil. Especificadamente, busca-se demonstrar como, e sob quais argumentos, ocorrem os bloqueios ao uso do aplicativo WhatsApp a luz do Marco Civil da Internet. O trabalho se encontra organizado entre as seções que caracterizam a legislação brasileira sobre Internet; a criptografia ponta-a-ponta e o WhatsApp; e, ao fim, as investigações criminais e sua relação com os bloqueios do aplicativo. Distante de demonstrar nas conclusões as soluções para tal problemática, o presente estudo se propõe a uma reconstituição sucinta de seus antecedentes, a forma como especialistas, juristas ou não, enxergam a questão que envolve Judiciário e a aplicação no contexto brasileiro. Demonstrando, ao final, o fundo normativo, principiológico e técnico ao qual tal questão está inserida.

Palavras-chave: Criptografia; Direito Digital; Internet; Marco Civil; WhatsApp.

ABSTRACT

From the deductive method, it is proposed to investigate the possible conflicts between end-to-end encryption and Internet legislation in Brazil. Specifically, it seeks to demonstrate how, and under what arguments, blockages occur to the use of the WhatsApp application from the perspective of the Civil Registry of the Internet. The work is organized among the sections that characterize Brazilian legislation on the Internet; End-to-end encryption and WhatsApp; And, ultimately, criminal investigations and their relationship to the application's locks. Far from demonstrating in the conclusions the solutions to this problem, the present study proposes a brief reconstitution of its antecedents, the way specialists, jurists or not, see the question that involves Judiciary and the application in the Brazilian context. By demonstrating, at the end, the normative, theoretical and technical background to which this question is inserted.

Keywords: Civil Framework; Digital Law; Encryption; Internet; WhatsApp.

SUMÁRIO

INTRODUÇÃO

A conclusão de um curso de Bacharelado em Direito, em 2017, segunda década do século XXI, pode ser descrita como uma experiência fascinante. Ao produzir um trabalho de conclusão de curso e relacionar correntes epistemológicas da ciência jurídica com a realidade contemporânea, concomitante ao processo de criação deste trabalho, encontram-se as dificuldades e limites deste campo de estudos em prescrever condutas, conforme ensina Bobbio, em “A era dos Direitos”.

Busca-se, ao longo das próximas páginas, demonstrar o modo como o discurso jurisdicional do Estado brasileiro se adapta à revolução da informática: ao mesmo tempo em que esse procura guardar prerrogativas inerentes à privacidade individual, também objetiva construir instrumentos processuais que conduzam a criação de elementos probatórios factuais que possibilitem a aplicação de penas aos indivíduos que se aproveitam de determinadas funcionalidades disponibilizadas aos usuários de dispositivos móveis para a incorrência em ilícitos.

Identifica-se como oportunidade para “incorrer em ilícitos” a funcionalidade da criptografia ponta-a-ponta e a “impossibilidade” presumida de se acessar as informações intercambiadas entre usuários da aplicação WhatsApp, que utiliza de tal serviço, visando oferecer aos seus clientes maior segurança e inviolabilidade das informações trocadas por meio da aplicação.

A investigação aqui exposta objetiva, ao fim, identificar se a criptografia de ponta-a-ponta está de acordo com a legislação brasileira referente à Internet, destacado o Marco Civil, seus princípios e segurança. Bem como, especificamente, analisar se esta função de segurança potencializa delitos, ademais apontar se o bloqueio nacional do uso do aplicativo se configura como uma medida legal cabível ou proporcional às responsabilidades da empresa ao prestar serviços de comunicação em âmbito nacional.

Trata-se de uma tarefa árdua, ainda sim instigante. Neste processo criativo foram elencadas as mais diversas fontes informativas, a exemplo da doutrina jurídica, jurisprudência, relatórios técnicos do Congresso Nacional, Ministério Público, Polícia Federal, baseadas na legislação nacional e internacional vigente com respeito à temática.

Paralelamente, opiniões e análises de outros trabalhos acadêmicos que tangenciam o objetivo da pesquisa foram observadas e suas contribuições adicionadas.

Ademais, incluíram-se opiniões de especialistas em informática e criptografia, por meio de entrevistas fornecidas a reconhecidos meios de comunicação. Tais meios, também serviram de fio condutor à narrativa, pois forneceram elementos que ajudam a compreender de modo holístico como a questão da privacidade e dos bloqueios judiciais do aplicativo WhatsApp influenciaram a sociedade brasileira, bem como serve de guia ao explicitar o modo como tal questão gera interesse em âmbito nacional.

No primeiro capítulo, descreve-se a relação entre a massificação da internet móvel e seus desdobramentos jurídicos. Após uma discussão introdutória, voltada à reflexão histórica, lança-se luz sobre o Marco Civil da Internet e suas principais prerrogativas.

No segundo capítulo, a criptografia ponta-a-ponta é caracterizada a partir de uma perspectiva técnica sucinta, posteriormente sendo discutido o modo como a criptografia se relaciona à prática de crimes no ciberespaço.

No terceiro capítulo, o objeto desta investigação, o WhatsApp é apresentado como meio constituinte de provas e como empresa cujo descumprimento de determinação judicial leva a justiça brasileira a reagir, por meio do bloqueio, visando forçar a companhia a colaborar com os processos judiciais que ocorrem no país e encontram parte de seus fatos geradores, além de provas cabais, presentes na interação entre determinados usuários.

Ao fim, expõe-se as conclusões derivadas desta investigação. Deseja-se a todos uma agradável e instrutiva leitura.

1 O ADVENTO DA INTERNET E SUAS CONSEQUÊNCIAS NO UNIVERSO JURÍDICO

Desde os primórdios da civilização humana, na era dos antigos registros pictográficos[1], o homem tem utilizado e aperfeiçoado técnicas com a finalidade de transmitir e consignar informações de diversas naturezas. Após a modernidade e a popularização da escrita[2], ao conhecimento foi conferida maior relevância, capacitando os homens à busca de inovadores avanços científicos e métodos mais eficientes para a criação e o compartilhamento de ideias[3]. Tendo como escopo o auxílio nas atividades cotidianas ligadas à informação e ao seu gerenciamento, foi desenvolvida a comunicação informática, que mais tarde aboliu limites de tempo e espaço e possibilitou a transmissão instantânea de vários tipos de mensagens entre diferentes dispositivos informáticos[4]. A fim de que a troca imediata de conteúdo entre computadores ligados a uma rede fosse possível, fez-se necessária a conexão à Internet, além da implementação de uma linguagem comum de comunicação: o protocolo de Internet, ou simplesmente IP[5].

1.1 A Internet e seu advento no Brasil

A Internet teve origem nos Estados Unidos a partir dos anos 60, através de uma rede, inicialmente com finalidade militar. Pode ser apropriadamente definida através da conceituação do Procurador-Geral do Estado da Flórida, EUA, citada por Gustavo Testa Corrêa (2008) como “uma rede mundial, não regulamentada, de sistemas de computadores conectados por comunicações de fios de alta velocidade, e compartilhando um protocolo comum que lhes permite comunicar-se”.

A apropriação do conceito justifica-se em razão da globalização no século XXI, que confere ao meio de comunicação um alcance mundial e de alta velocidade. De acordo com a União Internacional de Telecomunicações, órgão vinculado à Organização das Nações Unidas, pelo menos 3,2 bilhões de pessoas acessam a

[1] Forma de expressão oriunda do período neolítico, continuada na antiguidade clássica e nas formas não-ocidentais por meio da arte rupestre.
[2] Em um processo conflitivo, a escrita se torna universal, a exemplo do encontro de Cajamarca durante a conquista da América.
[3] Como consequência do Renascimento europeu e do período Iluminista.
[4] Conforme salientou Leda Maria em sua dissertação apresentada em 2002. (p. 16)
[5] Protocolo de comunicação usado entre todas as máquinas em rede.

Internet[6], o que torna indubitável a predominância e a influência da rede na vida social global: quase metade da população mundial a utiliza. O meio, fruto do progresso tecnológico, expandiu de forma absurda o conhecimento humano, ultrapassando todas as barreiras físicas, de forma a capacitar o acesso prático aos mais diversos tipos de conteúdos.

A praticidade do tráfego de informações é sempre levada em conta na criação de aparelhos cada vez mais portáteis e com funcionalidades mais simplificadas. E o homem da sociedade de informação atual parece recepcionar muito bem essas inovações tecnológicas, uma vez que, anualmente, centenas de dispositivos são lançadas no mercado, atingindo êxito nas vendas e tornando inquestionável a influência dos dispositivos de informação em sua vida cotidiana.

Os meios de comunicação virtuais passaram a proporcionar muito mais do que o acesso à informação livre na área da educação; tornaram-se uma extensão da ação humana em uma nova esfera em estágio de crescimento desenfreado. As pessoas comercializam eletronicamente, interagem em fóruns virtuais e relacionam-se de múltiplas formas nas redes sociais que cada vez mais disputam a atenção de seus usuários. Profissionalmente, trata-se de uma necessidade real: o homem da atualidade precisa dominar o acesso à rede e saber utilizar determinados programas de computador.

A internet tem real importância no processo de mudança da vida humana, expandindo a interatividade entre homem e máquina[7]. É inquestionável a relevância da ferramenta no cenário do século presente, tanto que o Conselho de Direitos Humanos da ONU aprovou a resolução (A/HRC/C/L.20) regulamentando a proteção, promoção e gozo dos direitos humanos na Internet, bem como a coibição da interrupção ou liberação de informações online, além de inserir esses direitos no rol da lei internacional de Direitos Humanos[8].

A presença dos computadores na sociedade aperfeiçoou a capacidade de coletar e analisar dados pelas empresas e pelo Estado, além da disseminação veloz

---

[6] Conforme reportagem vinculada ao G1, disponível em: http://g1.globo.com/tecnologia/noticia/2015/05/mundo-tem-32-bilhoes-de-pessoas-conectadas-internet-diz-uit.html

[7] Conforme salienta Gustavo Testa Correa em seu livro “Aspectos Jurídicos da Internet” (p. 9)

[8] A resolução se encontra disponível na integra em http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20. A mesma fora motivada por outros relatórios de membros da comissão e discutida na Assembleia Geral em outras oportunidades, tais tratativas prévias se encontram nos relatórios e resoluções de número: A/HRC/17/27, A/HRC/23/40 and Corr.1, A/HRC/29/32, A/HRC/32/38, A/66/290 e A/HRC/31/64.

nas vias de telecomunicações, garantindo inúmeros benefícios, entretanto, trouxe, previsivelmente, um considerável lado negativo[9]. Devido às incontestáveis consequências no mundo jurídico, essa realidade não pôde fugir do campo de incidência do Direito, necessitando, então, de uma regulamentação satisfatória, ao contrário do que tem sido no final do século anterior, quando a ciência jurídica no país era bastante modesta em relação ao tema.

A compreensão, bem como o acompanhamento das inovações tem sido um desafio constante para o Direito, a fim de garantir a pacificação social, o desenvolvimento sustentável das novas relações e a manutenção do próprio Estado Democrático de Direito[10].

Elucido um breve histórico das inovações legislativas acerca da Internet, trazendo as primeiras preocupações dos operadores de Direito no cenário nacional com a rede, inicialmente no fomento à revolução da informática em sede brasileira e, posteriormente, com as primeiras regulamentações dos direitos e deveres das empresas e usuários, bem como as previsões necessárias a fim de garantir a reparação de lesões.

1.2 Legislação Brasileira e Inovações Jurídicas.

Datam-se do final da década de 70 as primeiras discussões sobre a criação de uma rede de transmissão de dados no Brasil, em virtude do inicial e modesto crescimento no número de equipamentos informáticos. Prevendo o crescimento da nova e promissora realidade à época, foi criada pelo Decreto 84.067, de 2 de outubro de 1979, a Secretaria Especial de Informática, como órgão do Conselho de Segurança Nacional, tendo como expressa finalidade a assessoria na formulação da Política Nacional de Informática que, após 5 anos, viria à tona através da Lei nº 7.232/84, conhecida como “Lei da Informática”, que também se dispunha a incentivar a criação de produtos nacionais de informática, tendo, portanto caráter predominantemente econômico, conforme preceitua seu art. 2º, o qual aponta como “[...] objetivo a capacitação nacional nas atividades de informática, em proveito do

[9] Conforme Gustavo Testa Correa (op.cit.)
[10] Ibidem.

desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira [...]"[11].

Cinco anos depois, com enfoque na comunidade acadêmica, o Ministério da Ciência e Tecnologia criou a Rede Nacional de Ensino e Pesquisa – RNP[12]. Mais tarde, em 1994, o acesso à Internet ainda era raro à população, disponível precisamente aos que fossem fornecedoras de informação, como agências de notícias, livrarias e editoras.

Em 1995 foi criado o Comitê Gestor da Internet no Brasil (CGI.br), com o objetivo de "assegurar qualidade e eficiência dos serviços ofertados, justa e livre competição entre provedores, e manutenção de padrões de conduta de usuários e provedores"[13]. O CGI reconhecia, também, a necessidade de coordenar e integrar todas as iniciativas de serviços Internet no país. A Portaria 148, de 31 de maio de 1995, veio com o objetivo de regular a Rede Pública de Telecomunicações para serviços de conexão à internet (Brasil, 1995b). Seria incumbido aos provedores privados de internet o envio desta aos usuários finais, mediante pagamento de uma taxa às empresas públicas de telecomunicações, que ficariam responsáveis apenas pela infraestrutura. Dessa forma, ocorreu significativa explosão da internet no país, havendo o aumento de um milhão de usuários finais. A partir daí o Ministério da Ciência e Tecnologia passou a objetivar a inclusão social de forma igualitária, criando, então, o Programa Sociedade da Informação (SocInfo).

Apesar do forte fomento ao crescimento da informática e de lograr êxito com a explosão do uso da Internet, o Brasil ainda carecia de regulamentação específica aos direitos e deveres dos usuários, ao passo que novos fatos jurídicos iam surgindo no cenário virtual brasileiro.

Atento ao crescimento da prática de crimes que se popularizavam no país, foi apresentado o Projeto de Lei 84/1999, conhecido como Lei Azeredo em virtude de ter sido Eduardo Azeredo o seu relator na Câmara dos Deputados e no Senado Federal, e objetivava dispor sobre os crimes cometidos na área da informática, além

---

[11] BRASIL. Lei nº 7.232, de 29 de outubro de 1984.

[12] Conforme a RNP sua função, quando criada é a de "disseminar o uso de redes no país. Em paralelo à implantação de sua primeira rede, em 1992, que alcançou 10 estados e o Distrito Federal, a RNP dedicou-se a tarefas diversas, tais como divulgar os serviços internet à comunidade acadêmica através de seminários, montagem de repositórios temáticos e treinamentos, estimulando a formação de uma consciência acerca de sua importância estratégica para o país e se tornando referência em aplicações de tecnologias internet. " Disponível em: https://www.rnp.br/institucional/nossa-historia.

[13] Criado por meio da Portaria Interministerial n° 147, de 31 de maio de 1995. Ministério das Comunicações, disponível em: http://www.cgi.br/portarias/numero/147.

de cominar penas e outras providências, caracterizando como crimes virtuais os ataques praticados por hackers e crackers, em especial a alteração de homepages e a utilização indevida de senhas[14]. O projeto apresentava a tipificação de 12 delitos contemporâneos à época. Objetivava, assim, estender o campo de incidência de algumas tipificações que já eram previstas no Código Penal, quando estas ocorressem em meios virtuais. Conforme o projeto:

> Acessar um sistema informatizado sem autorização.
> Obter, transferir ou fornecer dados ou informações sem autorização.
> Divulgar ou utilizar de maneira indevida informações e dados pessoais contidos em sistema informatizado.
> Destruir, inutilizar ou deteriorar coisas alheias ou dados eletrônicos de terceiros.
> Inserir ou difundir código malicioso em sistema informatizado.
> Inserir ou difundir código malicioso seguido de dano.
> Estelionato eletrônico.
> Atentar contra a segurança de serviço de utilidade pública.
> Interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado.
> Falsificar dados eletrônicos ou documentos públicos.
> Falsificar dados eletrônicos ou documentos particulares.
> Discriminar raça ou de cor por meio de rede de computadores.

Durante sua tramitação no Legislativo, o projeto fora aperfeiçoado, com a supressão de dezessete de seus artigos, a exemplo da “falsificação de cartões” e da “traição”. Ademais, fora criada uma estrutura policial que visaria o combate a tais condutas, conforme artigo 4º da Lei 12.375/2012, a qual se transformou: “Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. ” [15]

Como uma alternativa mais plausível à “Lei Azeredo”, o projeto de Lei 2.793/11 foi implantado a fim de tipificar os crimes cibernéticos mais graves. Maiores considerações serão feitas em seção própria para definição de delitos desta natureza, razão pela qual não há comentários mais profundos em relação ao tema neste momento.

---

[14] A integra da proposta está disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>

[15] O projeto revisado está disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>

Com a divulgação na rede de Internet de fotos íntimas da atriz brasileira Carolina Dieckmann, em maio de 2012[16], o que levou seu nome aos assuntos mais comentados na rede social *Twitter*"[17], fazendo com que a população brasileira adotasse a pauta da invasão de privacidade nas redes sociais, o projeto de Lei supracitado – que mais tarde levaria, popularmente, o nome da artista, recebeu maior atenção. A inovação legislativa restaurava vários artigos da "Lei Azeredo", todavia com uma linguagem mais precisa, menos ampla e com pena mais branda. Com um trâmite mais célere, logo foi aprovada pela presidente Dilma Rousseff e transformada na Lei 12.737/2012, alterando, igualmente, o Código Penal. A lei, que consta de 4 artigos, prevendo os crimes de Invasão de Dispositivo Informático; Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; e falsificação de documento particular[18] primou-se no direito à privacidade e consagrou um importante avanço na definição dos crimes cibernéticos, mas sem invadir o campo de discussão do projeto para o Marco Civil da Internet que já estava em trâmite na época.

1.3 O Marco Civil da Internet

Em razão do caráter democrático da Internet, o Projeto de Lei 2126/11, através de iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas – FGV – foi submetido ao público, no final de 2011, a fim de receber contribuições da população à elaboração e revisão do que formaria, anos depois, o Marco Civil da Internet. O processo foi inicialmente submetido à contribuição da sociedade civil entre os dias 29 de outubro e 17 de dezembro de 2009, através do portal eletrônico "Cultura Digital"[19], do Ministério da Justiça, dividindo-se em três tópicos principais versando sobre Direitos Individuais e Coletivos (privacidade, liberdade de expressão e direito de acesso), Responsabilização dos atores e Diretrizes Governamentais, estas relacionadas à abertura da rede, infraestrutura e capacitação social, apresentando, em cada subtópico, uma justificativa para sua normatização. Segundo

[16] Conforme noticiado pela revista Veja, disponível em: <http://veja.abril.com.br/entretenimento/vazam-fotos-que-seriam-da-atriz-carolina-dieckmann-nua/>
[17] Rede de micro blogs utilizada como referência sobre tendências de assunto em determinado lugar ou mesmo no mundo. Maiores informações, disponível em: <https://about.twitter.com/company>
[18] Sua integra está disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>
[19] O site segue disponível em: <http://culturadigital.br/marcocivil/>

o projeto, era necessário “reconhecer que a legislação brasileira enfrenta lacunas com relação à Internet [...] com prejuízo para direitos fundamentais dos indivíduos, para a inovação e para a segurança jurídica”[20], todavia, sem significar que os esforços seriam dirigidos a comprometer a liberdade saudável na Internet, conforme as premissas:

> A intenção do marco civil a ser proposto não é restringir o acesso ou uso da Internet. Tampouco se pretende normatizar localmente aquilo que depende de harmonização internacional para funcionar. O que se espera, com o marco civil a ser elaborado colaborativamente, é:
> (i) definir diretrizes claras para a ação governamental – tanto no que diz respeito à regulação quanto no que tange a formulação de políticas públicas para a Internet;
> (ii) reconhecer, proteger e regulamentar direitos fundamentais dos indivíduos, bem como estabelecer com clareza a delimitação da responsabilidade civil daqueles que atuam na rede como prestadores de serviço; e
> (iii) estabelecer balizas jurídicas que permitam ao judiciário atuar com precisão e de forma fundamentada para a resolução de conflitos envolvendo a utilização da rede. Alguns temas, como direitos autorais, comunicação de massa e questões criminais, estarão fora deste debate, por já contarem com discussões estruturadas.

Além disso, pode ser compreendido que, junto ao fato do Projeto de Lei buscar instituir direitos e deveres aos usuários e prestadores de serviço, mais uma vez reservava foco ao crescimento do acesso à Internet, através de políticas públicas para a mesma, sem invadir o campo de discussões dos projetos que se converteriam posteriormente nas Leis “Azeredo” e “Carolina Dieckmann”, bem como na pauta dos direitos autorais.

Nesta fase, ainda em 2009, e após intensos debates, o Comitê Gestor da Internet no Brasil – CGI – apresentou sua colaboração à criação do Marco Civil com a Resolução CGI.br/RES/2009/003/P, apresentando os seguintes princípios para a Internet no Brasil[21]:

> 1. Liberdade, privacidade e direitos humanos
> O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.
> 2. Governança democrática e colaborativa
> A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

[20] Conforme explicado na página vinculada ao projeto, disponível em: http://culturadigital.br/marcocivil/2009/10/29/boas-vindas/#more-92
[21] A íntegra da resolução se encontra disponível em: http://www.cgi.br/resolucoes/documento/2009/003

> 3. Universalidade
> O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.
> 4. Diversidade
> A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.
> 5. Inovação
> A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.
> 6. Neutralidade da rede
> Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.
> 7. Inimputabilidade da rede
> O combate a ilícitos na rede 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 humanos.
> 8. Funcionalidade, segurança e estabilidade
> A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.
> 9. Padronização e interoperabilidade
> A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.
> 10. Ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

É notável que a resolução foi respeitada pelo legislador, uma vez que os princípios se encontravam presentes de forma explícita e implícita na minuta do anteprojeto[22] disponibilizada no mesmo Portal em 8 de abril de 2010, após uma série de audiências públicas presenciais em muitos dos estados membros do país, para discussão por mais 45 dias, encerrando-se em 23 de maio do mesmo ano. O projeto, que após conclusão de sua fase secundária, ainda recebeu a contribuição de inúmeros órgãos, empresas e países, através do Itamaraty, foi enviado ao Congresso Nacional através da mensagem presidencial 326/2011[23].

O referido projeto seguiu em tramitação até 2014, durando quase três anos, todavia seu advento significou uma importante e inovadora conquista, ainda que tardia, para o Direito Brasileiro. Corrobora com isso o professor do Instituto de Tecnologia de Massachusetts e criador da rede mundial de computadores, Tim Berners-Lee, citado por Rosemary Segurado, et. al., em sua análise comparada sobre a regulamentação da Internet: “com a aprovação do texto do Marco Civil, o Brasil consolida a sua reputação como líder da democracia e ajuda a inaugurar uma

[22] Conforme apresentado pelo site, disponível em: <http://culturadigital.br/marcocivil/2010/04/07/minuta/>
[23] Disponível na íntegra em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=D272A93F3D42F351AE84E34549D702EC.node2?codteor=913021&filename=Tramitacao-PL+2126/2011>

nova era, na qual os direitos dos cidadãos do mundo serão protegidos por Constituições digitais" (Lima, Luiz 2014 apud Segurado, Rosemary, et. al., 2015). Entretanto, vale questionar a denominação "Constituições digitais" utilizada pelo professor, caso induza à ideia de que o Marco Civil é autônomo na normatização da Internet, independendo de sua conjugação com as normas da Carta Magna de 1988[24].

O Projeto de Lei se transformou na Lei 12.965/2014, envolvendo 33 artigos dispostos em 5 capítulos a versar sobre Disposições Preliminares, Direitos e Garantias dos Usuários, Provisão de Conexão e de Aplicações de Internet, Atuação do Poder Público e finalmente suas Disposições Finais[25]. Com a premissa de estabelecer princípios, garantias, direitos e deveres para o Uso da Internet no Brasil, a Lei tem como fundamentos em seu artigo 2º: a liberdade de expressão, reconhecendo o caráter mundial da Internet, os direitos humanos, o desenvolvimento da personalidade, garantida através da utilização da Internet ,principalmente nas redes sociais, bem como o exercício da cidadania nos meios digitais, reconhecida também pelo legislador mais à frente, no artigo 7º da mesma, a sua potencialização através da participação popular na Internet, o que ocorre de maneira bastante prática. Prevê, ainda, a pluralidade e a diversidade, a abertura e colaboração, as livres iniciativa e concorrência, assim como a defesa do consumidor, explicitando as relações comerciais praticadas na Internet, em conexão com o Código de Defesa do Consumidor e por último, mas não menos importante, a finalidade social da rede. Complementarmente, o artigo 3º do diploma legal apresenta, entre outros, a garantia da liberdade de expressão, comunicação e manifestação do pensamento, da privacidade e a proteção dos dados pessoais. Embora passíveis de proteção por advirem de princípios constitucionais, optou o legislador por explicitá-los no contexto da comunicação eletrônica.

Outras garantias que merecem igual atenção dizem respeito à neutralidade da rede, assim como a preservação de sua estabilidade, segurança e funcionalidade, preservação de sua natureza participativa, obedecidos padrões internacionais e práticas saudáveis, além da importante previsão de

[24] Discussão presente no tramite legislativo, disponível em: <http://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica.>

[25] Sua integra pode ser acessada em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

responsabilização dos agentes de acordo com suas atividades e a liberdade dos negócios promovidos na Internet, sem prejuízo de "outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte"[26].

Um dos mais relevantes aspectos da supracitada Lei diz respeito à neutralidade da rede, que ratifica o caráter democrático da Internet. No Marco Civil, "O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação"[27]. Dessa forma, a autonomia de quem a utiliza é resguardada, não havendo o favorecimento de determinada atividade em detrimento de outras. Segundo Eduardo Tomasevicius Filho (2015), "A ideia é que se possa acessar indistintamente uma página de internet, enviar um e-mail ou assistir a um filme ou conversar por videoconferência, sem prejuízo da velocidade de transmissão dos dados".

A importante garantia apresenta, porém, suas exceções, quando a descriminação é possível desde que decorre de requisitos técnicos indispensáveis e priorização de serviços de emergência[28]. Como exemplo, pode-se considerar "[...]cirurgias médicas que são feitas on-line, as quais jamais podem admitir atrasos no fluxo de dados, sob pena de frustração da operação médica"[29]. No conflito de direitos, o valor da vida é hierarquicamente superior. Todavia, o tema ainda carece de avanços se for levado em conta o cenário internacional, é que, aparentemente, conforme salienta o supracitado Eduardo Tomasevicius Filho (2015) " apenas se assegura que o tráfego desses dentro do Brasil será isonômico, mas não necessariamente se atribuirá o mesmo tratamento quando esses mesmos dados forem enviados para fora do Brasil ou solicitados do exterior" (sem página).

[26] Ibidem.
[27] Ibid, art. 9º.
[28] Ibidem.
[29] Conforme estudo técnico elaborado pelo Senado Federal, disponível em: http://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica pagina 9

1.3.1 Privacidade e Segurança

Um dos principais motivos para a aprovação de um complexo de normas acerca da Internet foi a questão da privacidade na rede virtual que, diante de uma vastidão de conteúdos e utilizadores num espaço livre e intangível pelo direito, acabou configurando uma ameaça para a dignidade dos indivíduos que buscam e trocam relevantes informações no meio. O direito fundamental, consagrado na Constituição Federal de 1988, artigo 5º, X e XII é imprescindível à constituição e manutenção de uma vida digna, seja na esfera física ou na realidade virtual.

A privacidade, aduzida na Declaração Universal dos Direitos Humanos (ONU, 1948)[30], em seu artigo 12, referindo-se à vida particular, família, lar e correspondência, resguardando, assim, a honra e a reputação dos indivíduos, pode ser compreendida como a parcela da vida social de um indivíduo a qual o conhecimento de seu conteúdo diz respeito somente a ele ou a quem tem o seu consentimento. Tem, portanto acessibilidade limitada, relacionando-se com os elementos: segredo, anonimato e solidão, conforme salienta Holanda (2005, p.50). A preservação da autonomia da vida privada de um indivíduo representa um importante fator para o seu bem estar psíquico, que por sua vez reflete na dignificação de sua existência, assim:

> O direito à vida privada é um agregado do qual também depende a manifestação livre e eficaz da personalidade, porque o bem-estar psíquico do indivíduo, consubstanciado no respeito à sua esfera íntima, constitui inegável alimento para o desenvolvimento sadio de suas virtudes. (JABUR, 2000, p. 254 apud HOLANDA, 2005, p. 61).

Tal manifestação livre no âmbito privado depende, porém, da certeza depositada pelo indivíduo na preservação de seu direito a ser tutelado pelo Estado, sob o risco de tolher sua liberdade nas relações particulares, uma vez que a expressão da vida humana não é a mesma no âmbito público, composta também de pessoas a quem não se confia, independentemente da razão para isso. De igual forma, na esfera virtual a privacidade representa um desafio para o Direito.

Não há que se pensar na utilização do meio, que possibilitou a transposição de tantas atitudes humanas, as quais se concretizam na transferência de informações, seja no campo profissional, na socialização cotidiana, no lazer, entre

[30] Carta de São Franscisco.

outros, sem a garantia da inviolabilidade, quando assim é necessário. Plausíveis de Danielle Spencer Holanda, quando considera que “[...] a Internet constitui mais um meio para manifestações humanas, a privacidade na rede mundial merece, por isso, proteção legal, uma vez que representa uma extensão da vida do indivíduo” (IBID p. 81).

Sendo assim, preocupou-se o legislador em delimitar a atuação dos usuários, bem como das empresas que oferecem Internet, respeitando a transparência das ações. O Marco Civil prezou pela inviolabilidade da vida privada e da intimidade, do sigilo do fluxo de comunicações pela Internet, bem como das comunicações privadas armazenadas[31], garantindo a mesma privacidade das comunicações tradicionais, além do não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet[32] no sentido de que as empresas de Internet que trabalham com os dados dos usuários para fins de publicidade, ao exemplo anúncios dirigidos que aparecem no seu perfil nas redes sociais, não podem repassar informações para terceiros sem o consentimento livre e expresso do usuário, devendo as políticas de uso serem claras e públicas .

Apesar da previsão quanto aos direitos que traduzem a privacidade, e prevendo a violação rotineira no meio virtual, prudente foi o legislador quando reservou a garantia por dano material ou moral decorrente da violação, ressalvando ainda, a exceção à inviolabilidade, quando por ordem judicial no termo da Lei, devendo atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, reconhecendo ao final do capítulo que “A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet”[33].

1.3.2 Liberdade de Expressão e Remoção de Conteúdo

No tocante à Liberdade de expressão, a inovação se deu através da necessidade também de ordem judicial para retirada de material do ar, com exceção dos casos de pornografia de vingança, garantindo aos usuários lesados o direito de reivindicar o reparo de violações de forma direta, devendo os provedores, ao acatar,

[31] Marco Civil, art. 7º, incisos I, II e III.
[32] Ibid, inciso VII.
[33] Ibid, art. 8º.

informarem “os motivos e informações relativos à não disponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo” .

Antes do advento da referida Lei, bastava à comunicação ao provedor, conforme julgados, devendo agir imediatamente sob pena de responder solidariamente com o autor direto do ano:

> [...] Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omitindo. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet [...] [34][35]

Aduz-se da supratranscrita jurisprudência, além da possibilidade de identificação do sujeito do delito, seja por protocolo na internet ou dados pessoais, que o critério cronológico para retirada, no caso em menos de 24 horas, deveria ser observado sob pena de responder solidariamente pelo dano. Com a mudança e posterior necessidade de ordem judicial, o prazo sofreu uma dilação indireta. Todavia, com fulcro no artigo 18 da mesma Lei, a regra é de que “O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”[36]. De acordo com o juiz Fábio Caldas de Araújo[37] em reflexão específica ao tema, a inovação é plausível, uma vez considerada a dificuldade de auferir a ofensa de um conteúdo, já que uma postagem virtual não revela um grau de relacionamento, tampouco seu contexto, ainda mais praticado por estranhos.

---

[34] AgRg no REsp 1309891/MG, Rel. Ministro SIDNEI BENETI, TERCEIRA TURMA, julgado em 26/06/2012, DJe 29/06/2012.
[35] REsp 1193764/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 14/12/2010, DJ 08/08/2011.
[36] Marco Civil, art. 18º
[37] Disponível em: <http://www.conjur.com.br/2014-jul-04/fabio-caldas-araujo-reflexoes-marco-civil-internet>

Conforme estudo legislativo elaborado pelo Senado Federal[38], faz-se necessária atualização da jurisprudência, uma vez que pode haver conflito em direito à liberdade de expressão e privacidade. Assim expõe:

> Há duas situações distintas tratadas no novo diploma legal. Primeiro: como regra geral, em prestígio à liberdade de expressão e em atenuação dos valores de proteção da privacidade, o art. 19 do Marco Civil da Internet somente responsabiliza civilmente os provedores de aplicações por conteúdos gerados por terceiros (como postagens, vídeos, etc.) se, após ordem judicial específica, esses provedores não retirarem o conteúdo ofensivo. Dessa forma, a jurisprudência do STJ terá de mudar, pois não bastará mero pedido extrajudicial da vítima para a retirada do conteúdo. Será necessária ordem judicial.
> [...]
> Segundo: em exceção, o art. 20 do Marco Civil da Internet valorizou a tutela da privacidade ao estabelecer que conteúdos envolvendo cenas de nudez ou de sexo deverão ser retirados do ar pelo provedor de aplicação após mero pedido extrajudicial da vítima. (2014, p. 19-20).

O diferenciado tratamento pode ser justificado pelo peso do direito material em pauta em relação com a rapidez da disseminação de um conteúdo sexual socialmente, uma vez que, materiais com características eróticas recebem grande atenção das pessoas, que as compartilham de forma igualmente veloz. Tal publicidade causa, inclusive, a morte de algumas vítimas que acabaram por ter sua intimidade virtualmente acessada e sua reputação pública soterrada razão do escárnio causado pela divulgação de material íntimo.

O tema é inerente à vida de uma sociedade que, erroneamente, cada vez mais se familiariza com a observação passiva da violação da vida alheia. Contribui para isto o fato de que, por vezes, a divulgação de determinado ato sexual, tido como proibido, é socialmente encarada como um aspecto punitivo para uma conduta interpretada como imoral.

[38] Disponível em: <http://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica.>

2 A CRIPTOGRAFIA PONTA-A-PONTA E A POTENCIALIZAÇÃO DE DELITOS

Há algo tão definidor do género humano quanto sua necessidade de produzir cultura, e assim se perpetuar no tempo? A habilidade da escrita é interpretada como um dos marcos definidores das sociedades humanas. Nascida, inicialmente de forma rudimentar, esta ferramenta se configurou, ao longo do tempo, como elemento chave para a conquista e formação de sistemas de poder que lançaram, em relação intrínseca com a modernidade, com as bases para o mundo em que vivemos, com suas relações de desigualdade e de poder que hoje percebemos como estabelecidas, ou mesmo definidoras de nosso tempo.

A ferramenta de comunicação permeada por relações de saber-poder, usando a definição Foucaultina em “As palavras e as coisas”[39], nos remete a outra necessidade latente, fazer-se inteligível ao interlocutor adequado. Quando colocada nestes termos, alinhando a grafia com a necessidade de esconder (kripto), temos um dos sistemas comunicativos quase tão antigos quanto a própria escrita, sua forma cifrada.

Das guerras às estratégias diplomáticas, tais quais narradas por Clausewitz[40]; a demanda de proteção da privacidade na era digital, das quais as denúncias de Snodwen[41] se destacam. Percebemos como as relações comunicativas são, em uma constante sócio-histórica, permeadas pela questão da privacidade individual e de interesses corporativos e estatais. Desenrola-se, na contemporaneidade, uma discussão não concluída neste trabalho, pois seus desdobramentos se estendem a temáticas maiores, a exemplo da intimidade e da livre expressão do pensamento, caras aos princípios de direitos humanos expressos no pacto de direitos civis e políticos, acordados pelos regimes internacionais e violados por atos administrativos nacionais, a exemplo do ato patriótico norte-americano[42].

As ferramentas pelas quais os indivíduos se protegem da ingerência sobre suas interações faz parte de seu conjunto de prerrogativas mais básicas. Mesmo assim, tais estratégias defensivas têm que de algum modo ser limitadas, pois podem

[39] Martins Fontes. São Paulo, 2000.
[40] PARET, Peter (2003) Clausewitz. p. 257-283. In: PARET, Peter (org.) Construtores da Estratégia Moderna: de Maquiavel à Era Nuclear. Rio de Janeiro: Bibliex. ed. [cap. 7]
[41] Publicada pelo Jornal The Guardian, o escândalo NSA files pode ser visitado por meio do portal, disponível em: <https://www.theguardian.com/us-news/the-nsa-files>
[42] USA Patriot Act. Lei promulgada após os atentados terroristas de 11 de setembro que expande a capacidade de vigilância das agências federais de inteligência norte-americanas.

se configurar como elemento promotor de injustiças. Um dilema político, ético e cívico se anuncia. Nas próximas seções tentarei caracterizar o modo como a criptografia se estabelece nos meios digitais para posteriormente discutir as formas como, juridicamente, a mesma é tratada em nosso contexto pátrio.

2.1 Contextualização e Conceituação Técnica

Como meio de asseverar a garantia da privacidade dos usuários no meio digital, no que tange especialmente aos seus já elucidados elementos “anonimato” e, principalmente, “segredo”, a criptografia de dados tem sido implantada nos mais diversos *softwares*[43] que oferecem ao consumidor a prestação de serviços em que a troca de informações é efetuada. Sucintamente, pode-se conceituar a criptografia como “[...]a aplicação de séries complexas de algoritmos sob determinados dados” (CORRÊA; GUSTAVO, 2008, p. 81), sendo aqueles nada mais do que a sequência matemática de raciocínios ou operações que oferecem a solução de certos problemas[44]. Basicamente, as informações são substituídas aleatoriamente por um agrupamento de números ou letras que não apresentam sentido desde que não se tenha acesso às chaves a fim de decodificar corretamente o conteúdo, passando a exibi-lo em sua forma inicial. Há uma variabilidade de métodos criptográficos, baseando-se todos no mesmo princípio, o qual foi utilizado de forma arcaica por muitos povos, tendo como um notável exemplo histórico a Cifra de César, em razão da desconfiança que o imperador romano nutria por seus mensageiros.

Primando-se acerca da aludida medida de segurança, o Decreto nº 3.587 de 5 de setembro de 2000, reconhecendo o avanço da tecnologia de informação, bem como de sua segurança e a consequente adaptação da sociedade brasileira, passou a estabelecer normas para a Infraestrutura de Chaves Públicas do Poder Executivo Federal, versando, sobretudo, pela utilização da criptografia como forma de viabilizar, entre outros: a oferta de sigilo; a validade; a autenticidade e integralidade

[43] “O conceito de *software* abarca todas as aplicações informáticas, como os processadores de texto, as folhas de cálculo e os editores de imagens (programas de apresentação gráfica). O *software* é desenvolvido através de diversas linguagens de programação, que permitem controlar o comportamento de uma máquina. Estas linguagens consistem num conjunto de símbolos e regras sintácticas e semânticas, que definem o significado dos seus elementos e expressões. Disponível em: http://conceito.de/software#ixzz4YwrvoAz7.

[44] Uma definição mais precisa sobre o termo algoritmo poderá ser acessada em: https://www.dicio.com.br/algoritmo/

de dados[45], dando-lhe caráter de "disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo"[46].

Extraindo-se do Decreto supramencionado a necessidade de métodos criptográficos para conferir às mensagens virtuais suas qualidades de sigilo e autenticidade, pode ser denotada a imprescindibilidade da ferramenta na concretização do direito de privacidade e da segurança na Internet, justificando sua importância também no campo patrimonial, através do comércio eletrônico. Assim expõe Esther Dyson:

> A criptografia é uma das poucas ferramentas poderosas da moderna tecnologia que é inteiramente defensiva: protege a informação e a privacidade e fornece amparos para um comércio eletrônico seguro, sigilo, integridade nas comunicações e a privacidade dos indivíduos, para não falar nas próprias comunicações da polícia. Sem ela, a Net nunca será o ambiente seguro e garantido, frequentemente, prometido pelos políticos e empresas de computadores. (DYSON, 1998, p. 374 apud CORREA, 2008, p. 82).

Para viabilizar essa segurança no ambiente virtual, não basta unicamente a implementação de um método criptográfico qualquer, uma vez que, a depender do seu nível de complexidade, o mesmo pode ser corruptível pela criminalidade, devendo, portanto, que a ferramenta esteja a par do avanço tecnológico, atingindo boa qualidade no mundo moderno. Segundo Barreto (2012, p. 54), falar de tecnologia informática é algo problemático se levada em conta a celeridade das transformações no seu âmbito, podendo-se correr o risco de imprimir data de validade a um estudo, bem como a um mecanismo.

Pautada na privacidade incorruptível, ou melhor exposto: no direito ao sigilo não passível de violação, a criptografia "*end to end*", conhecida no Brasil como "de ponta-a-ponta", tem como maior premissa a impossibilidade de ser decifrada, em virtude de sua constituição através de duas chaves públicas, disponíveis exclusivamente aos usuários, emissor e receptor. A complexa ferramenta apresenta-se como o mais seguro e atual meio de garantir a privacidade nos aplicativos sociais, sobretudo no WhatsApp, objeto do presente estudo, que detém, desde fevereiro de 2016, mais de 100 milhões de usuários no Brasil, ou seja, sua maioria absoluta, e a

[45] Detalhes da regulamentação e dos sentidos dos termos podem ser acessados em: https://www.planalto.gov.br/ccivil_03/decreto/d3587.htm. Destaca-se, para fins deste enunciado o Art.2º, § 2 da regulamentação.
[46] Ibid, glossário.

expressiva marca de 1 bilhão mundialmente, dando à criptografia de ponta a ponta maior publicidade.[47]

O WhatsApp menciona, em seu portal eletrônico, que a inclusão da já citada criptografia reside no fato da privacidade e da segurança estarem presente “em seu DNA”[48], garantindo ao consumidor de seus serviços que somente os agentes que estão se comunicando podem ler o que é enviado, ressaltando, também, que nem mesmo o próprio aplicativo teria acesso as informações permutadas.

Tecnicamente, isso é possível graças ao sistema de chaves assimétricas, que conforme entrevista do perito forense computacional Deivison Pinheiro Franco ao portal da Intel, seu processo de codificação e decodificação utiliza duas chaves diferentes: sendo uma pública, criada para a codificação, e disponibilizada publicamente ao remetente; e uma privada, criada para a sua posterior decodificação pelo destinatário, inexistindo a possibilidade de que isso aconteça sem ela.[49]

Conforme o portal do aplicativo, uma vez que esteja ativada para a proteção de mensagens, fotos, vídeos, mensagens de voz e ligações, não é possível desativar a criptografia de ponta-a-ponta. E segundo o perito, para fins de privacidade, ela é suficiente, mesmo havendo a possibilidade de torna-la ainda mais segura através de exigência de uso de assinatura ou certificado digital. Todavia, apesar da intangibilidade do conteúdo, a empresa detém as informações sobre quando e a partir de qual celular as mensagens foram enviadas, as quais podem, ainda de acordo com a entrevista concedida por Deivison, “estabelecer e comprovar conexões e comunicações entre pessoas”[50].

No aludido aplicativo de comunicação instantânea, cada uma das conversas dispõe de um código de segurança que visam a garantia do pleno funcionamento da mencionada criptografia, podendo ser encontrado através de seu respectivo menu, um código de segurança que, de acordo com o próprio WhatsApp, trata de uma

[47] Número de usuários conforme apresentado em matéria vinculada pelo jornal Folha de São Paulo, disponível em: http://www1.folha.uol.com.br/tec/2016/02/1736093-whatsapp-chega-a-1-bilhao-de-usuarios.shtml
[48] Conforme descrição fornecida pela própria empresa, através do link: https://www.whatsapp.com/faq/pt_br/general/28030015
[49] A entrevista completa está disponível no link: https://iq.intel.com.br/o-que-afinal-e-criptografia-e-por-que-ela-e-importante/
[50] Ibidem.

versão visível de uma chave especial compartilhada entre dois usuários, não significando, porém, uma chave de fato, a qual é sempre mantida em segredo[51].

2.2 A má utilização da Criptografia Ponta-a-Ponta

Constatada a eficiência técnica do método criptográfico de ponta-a-ponta disponível às mãos de mais da metade da população brasileira em 2017, faz-se mister considerar suas consequências benéficas à privacidade neste meio de comunicação inerente a sociedade. A crença do consumidor na segurança do WhatsApp, junto à praticidade deste, têm dado novos contornos para a comunicação pessoal ou profissional entre os indivíduos, que passaram a realizar, mediados pelo aplicativo, uma gama de atividades que antes demandavam maiores custos e prazos em outros meios de comunicação.

São notórios o sentimento de aproximação e o efeito de instantaneidade que o serviço proporciona à vida dos usuários, garantindo a estes melhor qualidade e maior expansividade, requerendo apenas a posse de um *smartphone*[52], acesso à Internet e vinculação daqueles a um número de celular que os individualiza. Dessa forma, uma infinidade de informações sobre inúmeras variações de temas são transmitidas diariamente para os destinatários conforme a opção dos remetentes, sendo muitas delas confidenciais e, portanto, carecendo do crivo de confiança deles. A segurança e a fruição dessa comunicação passam a depender exclusivamente da intenção de seus utilizadores, sendo necessário que haja discernimento acerca das consequências maléficas dessa nova realidade.

Apesar da melhora da vida social causada pelo WhatsApp e de seu método criptográfico, o homem pode corromper a finalidade do meio. Neste sentido, por meio de um artigo, Fabiani Borges expõe que aplicações virtuais “tem servido de escopo para a prática de delitos em si, assim como para a ocultação do cometimento dos mesmos, levando a crer que a criptografia tenha se tornado uma ameaça por si só”[53]. Todavia, reconhecendo que por trás das máquinas figura um indivíduo intencionado para o bem (ou para o mal), e apoiada no pensamento de Augusto Tavares Rosa Marcacini quanto ao proveito que se faz da tecnologia para

[51] Conforme informações disponibilizadas pelo aplicativo, disponíveis em: https://www.whatsapp.com/faq/pt_br/general/28030015

[52] Usado aqui como um sinônimo para dispositivos móveis.

[53] A íntegra do artigo está disponível em: http://fabianiborges.jusbrasil.com.br/artigos/363173950/criptografia-o-uso-malefico-de-uma-tecnologia-criada-para-a-protecao-da-privacidade-dos-usuarios

a fim de concretizar atividades lícitas ou ilícitas, conclui que atribuir à criptografia "[...]a vilania ou um caráter maléfico não parece ser correto, pela simples razão de que não é aquele mecanismo sozinho quem pratica ou perpetra qualquer ato, mas sim aquele que está por detrás do seu uso"[54].

Prevendo a utilização para a prática de delitos, o aplicativo em seus termos de serviço é claro na delimitação da vedação de algumas atividades que ensejariam a violação de direitos de diversas naturezas:

> Você não usará (ou ajudará outras pessoas a usar) nossos Serviços: (a) de forma a violar, apropriar-se indevidamente ou infringir direitos do WhatsApp, dos nossos usuários ou de terceiros, inclusive direitos de privacidade, de publicidade, de propriedade intelectual ou outros direitos de propriedade; (b) de forma ilícita, obscena, difamatória, ameaçadora, intimidadora, assediante, odiosa, ofensiva em termos raciais ou étnicos, ou instigue ou encoraje condutas que sejam ilícitas ou inadequadas, inclusive a incitação a crimes violentos; (c) envolvendo declarações falsas, incorretas ou enganosas; (d) para se passar por outrem; (e) para enviar comunicações ilícitas ou não permitidas, mensagens em massa, mensagens automáticas, ligações automáticas e afins; ou (f) de forma a envolver o uso não pessoal dos nossos Serviços, a menos que esteja autorizado por nós.[55]

Apesar da previsão contratual, tais termos parecem ser ignorados pelos usuários que tendem a delinquir, seja por passarem despercebidos no extenso ato de concordância dos mesmos, ou em razão da descrença nas consequências da delinquência.

Surge assim a situação hipotética de que a confiança na premissa de um serviço que atesta sua "não intervenção no gerenciamento de informações" influencia a prática de ações que não se materializariam virtualmente com a mesma frequência em sites ou redes sociais sob a vigilância do governo ou de outros usuários aptos a verificar seu conteúdo, podendo gerar denúncias e a posterior averiguação de conteúdo, conforme já tratado no capítulo prévio acerca do Marco Civil.

A preocupação com o sigilo foi fortalecida após a grande atenção global gerada em torno do embate de 6 semanas entre a FBI e a Apple nas investigações do massacre que vitimou 14 pessoas em San Bernardino, Califórnia[56], em especial

---

[54] Ibidem.
[55] Termos de serviço do WhatsApp, disponíveis em: <https://www.whatsapp.com/legal/#terms-of-service>
[56] Conforme amplamente noticiado pela mídia global, destaca-se matéria vinculada sobre a temática no portal da BBC, disponível em: <http://www.bbc.com/portuguese/noticias/2016/03/160330_fbi_apple_lab>

no que se refere à declinação da referida empresa do cumprimento de desenvolvimento de uma tecnologia que pudesse oferecer informações do dispositivo móvel do assassino relevantes ao processo, sob alegação da impossibilidade de o fazer sem causar um possível dano geral, uma vez que a chave mestra necessária para o feito poderia ser usada em qualquer dispositivo, fundamentada no direito de privacidade dos usuários, mostrando a supremacia deste em relação à investigação criminal, mesmo tendo o FBI logrado êxito através de uma solução alternativa.

Assim, importantes bens jurídicos são ameaçados cotidianamente no aplicativo que oferece privacidade ilibada análoga à da Apple, a partir de várias hipóteses, contemplando crimes que só podem ser realizados via Internet e crimes tipificados no Código Penal os quais também podem ser praticados tendo a rede de computadores como meio.

A disseminação de material íntimo, calunioso e ou difamatório, como textos, fotos, vídeos e áudios, é costumeiramente realizada com uma velocidade surpreendente, ampliando significativamente os efeitos da desonra objetiva ou subjetiva das vítimas, as transformando em virais[57] da Internet, podendo instigar consequências desastrosas, a exemplo do suicídio de duas jovens de 16 e 17 anos vítimas de pornografia de vingança.[58]

O aplicativo também se transforma num ambiente perfeito para a prática de alguns crimes de caráter hediondo como aqueles que envolvem a pedofilia, ao exemplo dos tipificados nos artigos 241, A e B, do Estatuto da Criança e do Adolescente, conforme seus caputs:

> Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> [...]
> Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.[59]

[57] Informações difundidas massivamente pela rede entre seus usuários.
[58] Conforme noticiado pela Revista Fórum, disponível em:<http://www.revistaforum.com.br/2013/11/21/revenge-porn-divulgacao-de-fotos-intimas-culmina-com-suicidio-de-duas-jovens/>
[59] Integra do Estatuto disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>

Apesar de ter o legislador sido prudente quanto à previsibilidade das condutas acima transcritas, quando utilizou “por qualquer meio”, na época de sua inclusão ao Estatuto da Criança e do Adolescente pela Lei 11.829/2008 afim de “aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet”[60], não foi capaz de prever, especificamente, a popularização massiva do WhatsApp e a complexidade de sua nova criptografia padrão que inviabiliza o controle e impulsiona o crime.

Neste sentido, posiciona-se o presidente da Associação Brasileira de Criminalística, Bruno Telles, em reportagem realizada por Geórgia Moraes para o Agência Câmara Notícias: “Você pode montar uma rede de pedofilia pelo WhatsApp, onde os dados são criptografados de ponta-a-ponta”[61]. Afirma, inclusive, a suspeita da Polícia Federal de que a maior rede de pedofilia esteja no aplicativo. Reforça a ideia o delegado do núcleo de Inteligência da Polícia Civil do Piauí, Alessandro Barreto, quando, baseado em inquéritos policiais, afirma para a BBC que “o aplicativo serve como facilitador no ambiente virtual para crimes cometidos em ambientes comuns"[62].

Outro expressivo delito penal de natureza grave favorecido pelo aplicativo em pauta diz respeito ao tráfico de drogas[63]. Em razão da abstração da territorialidade no campo virtual, é possível que a comunicação aconteça de forma sigilosa e segura, ao contrário do que outrora somente poderia ocorrer mediante ligações telefônicas ou negociações no campo real, sujeitando criminosos ao alcance da Polícia Federal.

Considerando a intangibilidade do conteúdo pelo Estado, o WhatsApp se assemelha, no tocante ao uso para atividades ilícitas, à *Dark Web*. Esta, segundo Franco e Magalhães (2015), pode ser compreendida como um espaço da Internet permeado pelo compartilhamento anônimo de todos os tipos de conteúdo, sendo impossível identificar o usuário por causa da criptografia. Para os autores, a principal

---

[60] A referida peça normativa está disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm#art2>

[61] A reportagem está disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/496093-PERITO-AFIRMA-QUE-DADOS-TROCADOS-NO-WHATSAPP-NAO-PODEM-SER-ACESSADOS.html>

[62] Conforme reportagem da BBC, disponível em: <http://www.bbc.com/portuguese/noticias/2015/02/150227_salasocial_bloqueio_whatsapp_rs>

[63] Um exemplo local está disponível em: <http://g1.globo.com/pb/paraiba/noticia/2016/11/presidiarios-comandavam-trafico-de-drogas-whatsapp-na-paraiba.html>

diferença entre a Internet e a *Dark Web*, é que nesta nada é rastreado, gerando privacidade e anonimato absolutos. Quanto ao conteúdo, os iniciais dizem respeito ao tráfico de drogas e as parafílias, como pedofilia e zoofilia. Tudo comercializável, revelam os autores[64]. É possível também encontrar sites com grupos onde o passatempo consiste no homicídio das mais bizarras formas, como o canibalismo, comércio de armas, contratação de assassinos de aluguel e até o turismo sexual oferecido pelos *cibe*rcriminosos.

Apesar da diferença quanto ao anonimato, uma vez que o cadastro no WhatsApp depende do número de celular do usuário, a rede negra também possui o seu lado positivo se for levada em consideração a intenção do usuário em consonância com a privacidade absoluta proporcionada e livre do uso comercial excessivo. Todavia, também não há forma de garantir a reparação por lesão de um direito nesse ambiente.

Seja no WhatsApp ou na *Dark Web*, conforme afirma Fabiani Borges a impossibilidade de rastrear ou acessar dados criptografados reacendem a discussão entre o direito ao sigilo e à privacidade contra a segurança pública ou nacional[65]. Para isso, utiliza-se da conceptualização de Marcelo Leonardi, em "Tutela e Privacidade na Internet" para realçar a dificuldade de controlar a sociedade e provir direitos uma vez que a privacidade é um disfarce perfeito para a prática e um escudo para a punibilidade. Entretanto, não parece argumento suficiente para banir o uso da criptografia, e para isso utiliza-se do princípio da presunção de inocência.

Considerando a realidade de uma pessoa real por trás da máquina e toda a sua virtualização, a autora traz ao debate o argumento até então inédito de que simplificar investigações criminais às telas de computadores e dispositivos não parece ser uma atitude razoável, uma vez que o Estado deve provir outros mecanismos necessários a coleta de indícios ou provas acerca de delitos[66].

É necessário também levar em consideração uma ponderação entre os prós e contras causados pela criptografia ponta a ponta, conjugada ao supramencionado princípio, de forma a perceber que a finalidade benéfica de proteção da privacidade sobressai em relação às atividades ilícitas cometidas.

---

[64] Ibid, p. 28
[65] Op. cit., sem página.
[66] Ibidem.

2.3. A Criptografia na evolução dos crimes cibernéticos

A tecnologia de informação e a Internet promoveram mudanças significativas em diversos aspectos da vida humana. Comparado ao tempo de sua inexistência, é fácil vislumbrar uma grande expressão de inovações que garantiram facilidades ao fluxo informacional. Os impressos foram substituídos por dados virtuais que ocupam pouco espaço e proporcionam muitas vantagens, como a possibilidade de acesso em qualquer hora e lugar. A produção, a manutenção e a digitalização simplificada de documentos particulares é uma realidade do século XXI: as novas gerações logo dispõem de endereços eletrônicos e dispositivos onde os registros da rotina e das ideias perpetuam-se para além da degradação biológica dos materiais que se destinavam a perecer, cabendo aos detentores o controle sobre o que passeia entre o público e o privado.

Não obstante a criptografia ser coagida ao mau uso para conferir status de anonimato a um *ciber*criminoso, pode se tornar o objeto principal de uma nova modalidade de crime a qual vem causando sérias preocupações no cenário mundial: o *crypto-ransomware*. Como todo *malware*[67], o novo delito se destina a causar ações danosas que podem comprometer um computador, entretanto os *ransomware* vão além de um crime de dano: causam o sequestro de informações particulares. A criptografia entra em cena criando uma nova modalidade para o código malicioso, podendo criptografar os dados sequestrados, sujeitando a vítima unicamente ao pagamento de um resgate, uma vez que é praticamente impossível a decodificação do conteúdo reconquistado, por outro meio.

Do ponto de vista legal, a inviolabilidade de dados positivada pelo inciso XII, do artigo 5º da Constituição Federal de 1988[68] não é o único direito lesionado através do ato, que visa retorno financeiro realizado também por uma espécie de moeda chamada *bitcoin*[69] que também utiliza criptografia. Apesar do crescimento

[67] Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.
[68] Inviolabilidade da Correspondência
[69] Conforme a página da Bitcoin trata-se de “uma rede que funciona de forma consensual onde foi possível criar uma nova forma de pagamento e também uma nova moeda completamente digital. É a primeira rede de pagamento descentralizada (ponto-a-ponto) onde os usuários é que gerenciam o sistema, sem necessidade de intermediador ou autoridade central. Da perspectiva do usuário, Bitcoin funciona como dinheiro para a Internet. Bitcoin também pode ser visto como o mais promissor sistema de contabilidade de entrada tripla existente”. Disponível em: <https://bitcoin.org/pt_BR/faq#o-que-e-bitcoin>

exponencial em 2015, como afirma a *Kaspersky Lab*[70], principalmente entre grandes empresas, a adequação típica pode ser perfeitamente vislumbrada logo no primeiro artigo adicionado pela Lei 12.737/ 2012 ao Código Penal:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (Art. 154-A)

É inquestionável a violação indevida, prevendo alternativamente a obtenção ou destruição de dados, além da finalidade de obtenção de vantagem ilícita. Contudo, mesmo tendo o legislador agido com visão vanguardista e genérica acerca de uma infinidade de possibilidades, não contava com a despreparação da máquina estatal para lidar com camadas de disfarces quase impossíveis de serem removidos: a criptografia moderna.

Neste sentido, posiciona-se Daniel Ackerman durante Congresso Nacional de Segurança Cibernética ao afirmar que "é necessário reconhecer que a tecnologia muda com uma velocidade muito rápida, o que prejudica a prevenção desse tipo de delito"[71]. Destarte a previsão de surgimento de métodos criminosos cada vez mais sofisticados no campo virtual, esclarece, ainda, o coordenador do Departamento de Propriedade Intelectual do Departamento de Justiça dos Estados Unidos que cada "vez mais cresce o número de possíveis sujeitos passivos desse e de mais outros tipos de crimes cibernéticos através da melhoria de dispositivos móveis, da capacidade de armazenamento e do seu consequente barateamento"[72].

Importante salientar a necessidade de prevenção desse tipo de ocorrência, o que é endossada pela disponibilização virtual de um manual de segurança criado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) – serviço prestado para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) – braço executivo do Comitê Gestor da Internet no Brasil (CGI.br)[73], uma das políticas públicas que,

---

[70] Conforme noticiado pelo portal TechTudo, disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/01/ransomware-brasileiro-usa-adobe-flash-player-para-sequestrar-dados.html>

[71] Conforme noticiado pelo portal da FIESP, disponível em: <http://www.fiesp.com.br/noticias/tecnologia-digital-se-transforma-rapidamente-e-dificulta-a-prevencao-de-crimes-ciberneticos/>

[72] Ibidem.

[73] A cartilha está disponível em: <http://cartilha.cert.br/>

conforme Ana Luiza Vieira Valadares Ribeiro, presidente da Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações, junto ao fortalecimento da Infraestrutura para lidar com crimes cibernéticos, apresentam-se como as soluções mais plausíveis para o desenvolvimento da vida virtual de forma segura, livre e privada que o Marco Civil visa garantir[74].

Assim, deve-se estar preparado para enfrentar um cenário futuro que deverá ser permeado por “atentados com motivações política e ideológica a informações, dados de usuários ou sistemas de computadores visando a resultados violentos”, conforme Eric Schmidt e Jared Cohen (2013, p. 161).

[74] Op. cit. Reportagem FIESP

3 INVESTIGAÇÕES CRIMINAIS E O BLOQUEIO DO WHATSAPP

Há de se reconhecer que dentre as inúmeras e distintas áreas existentes no Direito, a que trata dos bens jurídicos mais importantes, senão fundamentais, à sociedade se sobressai na satisfação popular, não exclusivamente em razão da inerência desses direitos a todos os indivíduos num Estado Democrático de Direito, mas, principalmente, pela expressividade e pelo sentimento de justiça provocados na população quando o Estado se dispõe a prestar a tutela jurisdicional e devolver ao agente infrator o dano que fora por ele causado à coletividade, através da fixação de uma pena de caráter retributivo e preventivo.

Para que tal retribuição seja justa, deve-se, como em todo processo de Direito, apurar responsavelmente os fatos com base na legalidade, seguindo um procedimento racionalizado, disponibilizando as prerrogativas necessárias à acusação e à defesa, até que finalmente seja possível se aproximar da verdade real almejada, solucionando o conflito e restaurando eficientemente a paz e a segurança social. Contudo, novos fatos jurídicos, como os delitos praticados na Internet, carecem de procedimentos simplificados a fim de se apurar indícios suficientes à comprovação de autoria de um indivíduo, bem como provas capazes de demonstrar a exatidão dos atos praticados na lesão de direitos de outrem e suas circunstâncias, possibilitando a devida responsabilização penal.

O inquérito policial, instrumento da investigação criminal incumbido à polícia judiciária a ser dirigido pelo delegado de polícia civil de acordo com o artigo 144, §4º da Constituição Federal, trata-se de um procedimento preparatório da ação penal que, conforme Nucci (2013, p. 155), objetiva a reunião preliminar de provas da autoria e da materialidade de uma infração penal formando a convicção do representante do Ministério Público, mas não somente isto, uma vez que também se destina à colheita de provas urgentes passíveis de desaparecimento posteriormente 88. De igual modo, tal incumbência à polícia judiciária e o objetivo do inquérito são previstos no artigo 4º do Código de Processo Penal, que ressalva também a competência territorial que deve ser limitada às circunscrições das autoridades policiais.

Seja no ambiente *off-line* ou no ambiente virtual, o procedimento aludido deve buscar o maior número de informações pertinentes à apreciação de determinado delito, não se limitando aos seus indícios. É indispensável que a

investigação reúna todos os instrumentos do crime e os objetos de prova a fim de demonstrar ao destinatário final da prova a realidade do ocorrido. Todavia, por causa do cometimento de crimes por meio da Internet, sobretudo em dispositivos de fácil desfeita e forte sigilo, a investigação pode encontrar óbices relevantes que dificultam, ou inviabilizam, o trabalho da polícia, necessitando da colaboração das empresas que prestam serviços na Internet, uma vez que o ambiente virtual apresenta as nítidas peculiaridades que serão tratadas a seguir.

3.1 Constituição de Provas no Ciberespaço

A investigação de crimes e a obtenção de provas no ciberespaço constituem uma tarefa complexa aos profissionais do Estado na apuração dos delitos que ali se materializam, principalmente quando ocorridos por meio de aplicativos de trocas de mensagens instantâneas como o WhatsApp, que utilizam de criptografia ponta a ponta para proteger fortemente o conteúdo telemático dos infratores.

Como já foi abordado no capítulo anterior, esse método criptográfico eficaz à preservação da privacidade de seus usuários apresenta um lado negativo do ponto de vista das investigações criminais: a dificuldade para a identificação de crimes praticados através do WhatsApp dos quais não se tem facilmente indícios específicos de autoria e materialidade, e a complexidade para a obtenção de provas relevantes para a solução de delitos no ambiente real, já que nem mesmo a empresa que oferece o serviço pode, segundo seus próprios termos, ter acesso a esse conteúdo privado.

3.1.1 Provas na Internet

Apesar da admissão da coleta de provas eletrônicas, desde que por meios legítimos conforme o que se apreende, a contrario sensu, do artigo 5º, LVI, da Constituição Federal, urge a necessidade de a mesma ter eficácia jurídica, o que dependerá essencialmente de sua credibilidade. Para isso, a genuinidade do documento não deverá ser afastada, o que representa um risco significativo de ocorrer através de alguma alteração voluntária ou involuntária. Com efeito, sintetizam Paganelli e Simões (2012):

> As informações digitais têm em sua essência a característica de serem reproduzidas livremente e também de poderem ser alteradas à conveniência daquele que a está manuseando. Todo e qualquer arquivo digital possui diversas "camadas" que podem ser alteradas de acordo com o conhecimento do usuário que o está manipulando, sem contar ainda, que o sistema computacional geralmente altera algumas informações apenas com a visualização.

Dessa forma, pode a prova eletrônica sofrer maior desconfiança quanto à sua autenticidade, dificultando ou impedindo a instauração imediata de um inquérito e uma possível instrução criminal, por causa da possibilidade de não se formar o convencimento necessário da respectiva autoridade. Importante destacar que a prova eletrônica tem natureza documental conforme o critério ampliativo do conceito de documento esclarecido por Nucci (2013, p. 512), que abrange bases que sejam suficientes ao registro de pensamentos ou outras manifestações da vontade, armazenadas no disco rígido de um computador.

Tratando-se de um delito realizado em algum site da Internet ou rede social, é de extrema importância que a vítima reúna informações suficientes, sejam de conversas ou fotos através de capturas de tela, salvando-as de forma segura, para dirigir-se a um cartório a fim de registrar os arquivos em ata notarial, que nas palavras de Ferreira (2010) é "o instrumento público pelo qual o tabelião, ou preposto autorizado, a pedido de pessoa interessada, constata fielmente os fatos, as coisas, pessoas ou situações para comprovar a sua existência, ou o seu estado." Conferida a fé pública aos documentos, deverá realizar o comparecimento a uma Delegacia de Polícia a fim de registrar um boletim de ocorrência que poderá dar início ao inquérito policial[75].

A partir daí, a problemática volta-se para a necessidade de interceptação de comunicação de dados ou de obtenção de registros, a depender do caso concreto, já que é possível que a autoridade responsável entenda que as informações apresentadas são suficientes para individualizar o autor de um delito inequivocamente constituído. A maioria dos *ciber*delitos demanda a quebra de sigilos de dados para que se possa auferir adequadamente a extensão do dano e outros detalhes imprescindíveis para a atribuição de culpa a todos os envolvidos, bem como as circunstâncias nas quais se realizaram a lesão de direitos, sendo os detentores do protocolo IP as testemunhas destes ilícitos.

[75] O autor disponibiliza um passo a passo para denúncia de crimes virtuais por meio do link: <http://direitosbrasil.com/denunciar-um-crime-virtual-passo-passo/>

A respeito dessa medida, o artigo 5º da Constituição Federal prescreve, em seu inciso XII, que:

> [...] 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. (meu grifo)

O permissivo legal submete às investigações aos termos da lei de Interceptação Telefônica, a Lei 9.296/96, o que parece apropriado conforme interpretação do artigo 69 da Lei Geral de Telecomunicações que define forma de comunicação como:

> [...] o modo específico de transmitir informação, decorrente de características particulares de transdução, de transmissão, de apresentação da informação ou de combinação destas, considerando-se formas de telecomunicação, entre outras, a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens.

Há de se considerar que, tecnicamente, tanto a comunicação de dados quanto a telefonia constituem meios de comunicação que transmitem informações. Convergentemente, a equiparação entre voz e dados é confirmada pela resolução 217/2016 do Conselho Nacional de Justiça.

Para a viabilização da interceptação, necessário se faz o preenchimento de alguns requisitos da sua respectiva Lei, sendo eles, conforme o artigo 2º, a exigência de indícios razoáveis da autoria ou da participação em infração penal, a inexistência de outro modo para demonstrar o apurado, o que aparentemente não há dificuldades de se constatar tratando-se de crime no ambiente virtual, portanto, materializado extraordinariamente na Internet e, por fim, admissão apenas para crimes punidos com reclusão, ou seja, em regime inicial fechado.

No que tange à obtenção de dados já produzidos, o Marco Civil da Internet prevê o registro necessário de algumas informações para a formação de conjunto probatório em processos que os demandem. Passarei a dar foco à previsão advinda da Lei de 2014 no que diz respeito à guarda dos registros e possibilidade de fornecimento mediante ordem judicial.

O referido dispositivo prescreve que:

> 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.

Verifica-se nos parágrafos mencionados que a disponibilização de conteúdos que gozam de privacidade só poderá ocorrer, assim como na interceptação, através de ordem judicial, o que parece suficiente para afastar a possibilidade de se percorrer livremente conteúdos íntimos a partir de meras alegações. Numa interpretação literal, o citado artigo confirma a inteligência do legislador ao incluir “bem como de dados pessoais e do conteúdo de comunicações privadas” no rol de registros que podem ser disponibilizados, já que no artigo 5º dá-se a “registros de conexão” e a “registros de aplicações de internet” referência tão somente às informações que versam sobre horários e datas de acesso, duração e endereço IP utilizado, não abarcando, num primeiro momento, o conteúdo privado o qual constitui muitas vezes a própria materialidade de um crime.

Logo, não restam dúvidas da importância da colaboração das empresas com à Justiça, que a deverão fazer nos termos da Lei, que em outrora, apresenta sanções cabíveis pelo descumprimento. Vale destacar o que diz o Ministério Público Brasileiro e o Conselho Nacional dos Procuradores Gerais em nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da Internet no sentido de que somente com a colaboração efetiva e a adequação das empresas provedoras de conexão e de aplicações às leis brasileiras que se poderão solucionar satisfatoriamente os ilícitos, sob pena de inviabilização do combate a esses crimes[76].

3.1.2 Provas no WhatsApp

Numa perspectiva generalizada, ou até mesmo pessimista, podemos concluir que onde ocorre interação humana, também podem ocorrer condutas ilícitas. Conforme exposto nas linhas anteriores, uma série de questões de ordem

[76] A íntegra da nota técnica está disponível em: <http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/>

ética e jurídica é levantada quando a violação de privacidade se mostra como meio necessário à coibição dos ilícitos, sobretudo, quando tal invasão é realizada em uma ferramenta que tem o pleno respeito a esse direito como imprescindível para o seu funcionamento. Entretanto, sabe-se que nenhum direito é absoluto, nem mesmo os fundamentais,[77] podendo haver sua relativização em prol da reparação de um dano.

Nesta seção ocorre a demonstração do como, em meio a intercomunicação dos agentes intermediados pelo aplicativo analisado, podem ser angariadas provas para a comprovação de ilícitos, proporcionando, ao final de tudo, a proteção jurídica dos usuários de boa fé e a punição dos malfeitores.

Sendo assim, serão discorridas as peculiaridades do aplicativo em pauta no tocante à formação de provas, tratando-se antes de sua submissão às normas que regulam a internet no Brasil, concluindo-se o tópico com a elucidação dos motivos que induzem ao pensamento de que a criptografia ponta a ponta, apesar de inicialmente convergir, diverge do que foi instituído pelo Marco Civil.

Assim como a maioria dos serviços desenvolvidos para utilização através dos smartphones, o WhatsApp é um aplicativo social que depende necessariamente do uso da Internet, podendo ser palco, inclusive privilegiado, para a prática de crimes, como já foi abordado. Em razão de ofertar serviço ao público brasileiro, ainda que não se trate de uma empresa brasileira, deve ser regulado pelo ordenamento pátrio.

Através do artigo 5º, inciso VII, do Marco Civil, que considera aplicações de internet todo “o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”, pode-se vislumbrar o pleno enquadramento do aplicativo ao que foi aludido. Vale considerar a definição de Frederico Meinberg Ceroy em estudo sobre o conceito dos provedores à luz do Marco Civil:

> Provedor de Aplicação de Internet (PAI) é um termo que descreve qualquer empresa, organização ou pessoa natural que, de forma profissional ou amadora, forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos.

A partir desta definição que abarca as funcionalidades oferecidas ao público, independentemente de retorno econômico, como troca de mensagens de

[77] Conforme salienta João Trindade em Teoria Geral dos Direitos Fundamentais, disponível em: <http://www.stf.jus.br/repositorio/cms/portaltvjustica/portaltvjusticanoticia/anexo/joao_trindadade__teoria_geral_dos_direitos_fundamentais.pdf}>

texto e de áudio, transferência de arquivos multimídia e chamadas por vídeo e/ou voz, faz-se mister apontar o critério que confirma a submissão às normas brasileiras: a oferta de serviço ao público do país.

O artigo 11 é claro quanto ao tema:

> 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.

Mesmo que se considere o fato de que o WhatsApp se trata de uma empresa norte-americana, ainda que não possua sede no Brasil e tenha a pretensão de que seus termos e controvérsias jurídicas sejam regidas exclusivamente pelas leis americanas do estado da Califórnia, conforme seus termos de serviço[78], a previsão do legislador brasileiro afasta qualquer possibilidade de escusa, eis que:

> O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Através de uma interpretação sistemática do referido parágrafo e do caput referido, é inequívoca a submissão do WhatsApp à jurisdição local, uma vez que, conforme o Senado, é possível concluir que o respeito à legislação brasileira deve ocorrer no que se refere aos dados pessoais, aos registros de conexão e de acessos a aplicações e a comunicações dos internautas[79], suficientes ao menos a dirimir conflitos que se materializam total ou parcialmente no ciberespaço.

Visando a necessidade de utilização para reparar danos, o Marco Civil impõe, em seu artigo 15, § 1, igualmente de forma clara, que tais registros devem ocorrer pelo prazo de 6 meses ou mais, independendo da existência de finalidade econômica nos aplicativos, já que o supracitado parágrafo engloba outras aplicações a despeito do presente no caput que aduz a esses fins, devendo, porém, apontar fatos específicos em períodos determinados, mediante ordem judicial, podendo ainda dilatar o prazo mencionado.

---

[78] Op. cit.

[79] Disponível em: <http://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica>

Quanto à disponibilização material do WhatsApp às autoridades, o que pode ser obtida por meio da consulta ao aplicativo através do acesso físico ao smartphone de um agente criminoso, não se vislumbra maiores dificuldades no que diz respeito à coleta de provas, desde que o mesmo não realize a exclusão de seus dados. Contudo, cabe a análise de eventual ilicitude do ato, que pode ser realizada em consonância com o Informativo de Jurisprudência 582 do Superior Tribunal de Justiça[80]. Destaca-se menção à prova ilícita, considerando o ensinamento de "Nucci" (2013, p. 101) acerca do assunto, que engloba tanto as provas ilegalmente colhidas quanto as ilegitimamente produzidas, gozando ambas de inadmissibilidade. A fim de sanar eventual celeuma, a 6º turma do STJ entendeu como ilegal o acesso a mensagens e dados do aplicativo WhatsApp sem prévia autorização judicial, no caso concreto onde o telefone celular de um indivíduo em prisão em flagrante foi apreendido e consequentemente investigado. De acordo com o Juiz de Direito Leonardo Grecco, fica entendido a partir do julgado que as mensagens do aplicativo podem ser plenamente utilizadas como meios idôneos de prova, desde autorizadas judicialmente, acrescentando pertinentemente que:

> O Supremo Tribunal Federal já resvalou a questão quando analisou a Queixa-Crime proposta pelo Senador Romero Jucá contra o também Senador Telmário Mota, nos autos da Ação Originária – AO 2002/DF, aceitando até mesmo *imagem da tela* (prints) *do aparelho móvel,* a representar mensagens trocadas pelo WhatsApp, como prova dos fatos discutidos na demanda. [...] Entender que as mensagens de WhatsApp não podem ser usadas como prova no processo, de qualquer forma, é condená-lo ao retrocesso. Enfim, apenas o cuidado de se devassar a intimidade tão somente diante de autorização judicial é que se pretende, de modo a legitimar esse tipo de prova.[81]

Acerca da legitimação das provas no WhatsApp, independentemente da colaboração do aplicativo, passa-se a pensar em alternativas voltadas para a instalação de vírus, obtenção de backups ou infiltração de agentes em grupos, analisadas em pesquisa de Wagner Francesco, que conclui igualmente sobre a necessidade de autorização judicial quanto às duas primeiras, sob pena de configurar crime de invasão de dispositivo de informática conforme a Lei Carolina

[80] Conforme noticiado em: <http://www.conjur.com.br/2016-jun-02/acesso-mensagens-whatsapp-autorizacao-justica-ilegal>

[81] A íntegra da opinião do jurista pode ser acessada em: <http://estadodedireito.com.br/as-mensagens-de-whatsapp-como-meio-de-prova/>

Dieckmann, bem como quanto à última, havendo obrigatoriamente a respectiva instauração de inquérito[82].

Depreende-se, portanto, que a relativização da privacidade não é de nenhuma forma realizada indiscriminadamente, encontrando em quaisquer hipóteses a devida e plausível fundamentação por intermédio do crivo judicial de um profissional por excelência.

Aparentemente, a regulação da Internet que confere direitos, deveres e garantias possui potencial para assegurar o funcionamento da rede com a preservação da segurança necessária, conferindo às diversas ramificações do meio a liberdade de funcionamento em observância das medidas imprescindíveis para a eventual intervenção estatal à necessidade do usuário lesado, que dispõe de técnicas pessoais para formalizar uma denúncia ao que lhe chega ao conhecimento. Todavia, quando os aplicativos de Internet passam a declinar do que é ordenado pela Justiça, tornando o Estado incapaz de satisfazer as demandas de seus usuários lesados, nasce um problema que se agrava à medida que as consequências se acentuam.

Imaginar a impossibilidade da interceptação de dados e de acesso a registros capazes de elucidar crimes de múltiplos potenciais ofensivos, em sua maioria de grande reprovação social, faz pensar na Internet como um território sem lei a qual a sociedade está submetida e não pode mais de desfazer.

O tópico a seguir tratará do foco principal do presente trabalho: a criptografia do WhatsApp como óbice para as investigações criminais em face da alegada impossibilidade técnica.

3.2 Determinação judicial x Impossibilidade técnica

Através da internet ao alcance das mãos, seja por conexão *Wi-Fi,* ou mediante telefonia móvel, que permite o instantâneo acesso a inúmeras redes sociais consagradas pelo uso reiterado no Brasil, um palco ilimitado é ofertado para a disseminação de notícias diárias por meio de postagens e compartilhamentos nas linhas do tempo dos usuários. Assim, logo se torna público e notório o conhecimento

[82] Disponível em: <https://wagnerfrancesco.jusbrasil.com.br/artigos/364856315/grampo-no-whatsapp-uma-prova-ilegal>

acerca de assuntos que importam genericamente a uma grande massa virtual, independentemente da seleção de conteúdo mediante algoritmos.

Desde 2015, o público brasileiro tem sido pego de surpresa com a "viralização" de notícias acerca da possibilidade real e súbita de suspensão do WhatsApp, todas pautadas em decisões judiciais, o que coloca em imediato risco a continuidade da comunicação de todos os seus usuários.

Vidrada nas consequências diretas da medida, sobretudo nessa emergente cessação do imprescindível tráfego de informações para a manutenção de determinadas atividades, a sociedade acaba muitas vezes por preterir o conhecimento das razões que ensejaram a interrupção dos serviços, passando a tecer comentários precipitados e descompromissados com a verificação da aplicação idônea da justiça.

Data-se de 11 de fevereiro de 2015 a primeira intervenção da Justiça Brasileira no sentido de aplicar a prevista sanção de suspensão dos serviços do Provedor de Aplicações de Internet WhatsApp, realizada por meio de mandado judicial do Juiz da Central de Inquéritos da Comarca de Teresina – Piauí. Convém explicitar que o processo gozava de segredo de justiça por envolver crimes contra crianças e adolescentes, e conforme nota do Núcleo de Inteligência da Secretaria de Segurança Pública do referido estado federativo, sua respectiva ordem foi motivada pelo descumprimento de outras determinações referentes a processos judiciais autuados em 2013[83].

Sem lograr êxito, instaurou-se o que pode ser compreendido nesta pesquisa como o marco da insubmissão do WhatsApp à Lei Brasileira, a partir das inúmeras decisões anteriores descumpridas que não surtiram os efeitos jurídicos almejados, tendo a condenação ao pagamento de multas sequer provocado uma resposta do aplicativo americano.

Dez meses depois, em 17 de dezembro de 2015, a primeira suspensão do aplicativo foi realizada no plano fático por força da decisão da 1º Vara Criminal de São Bernardo do Campo – SP, igualmente motivada por não cumprimento de decisão judicial referente à colaboração com investigação criminal. Todavia, os serviços logo foram restabelecidos por liminar concedida pelo Tribunal de Justiça

[83] Conforme amplamente noticiado, a exemplo da notícia, disponível em: <http://www.ebc.com.br/noticias/2015/02/justica-do-piaui-determina-suspensao-do-aplicativo-whatsapp-no-brasil

correspondente. A medida resultou também na manifestação pública – e virtual – do dono da rede social *Facebook* Mark Zuckerberg, proprietário também do WhatApp[84].

Em 1º de Março de 2016, Diego Dzodan, o vice-presidente do Facebook na América Latina, foi preso preventivamente pela Polícia Federal em razão, mais uma vez, de descumprimento de ordens judiciais à colaboração com a justiça brasileira, referentes a crime organizado e tráfico de drogas, igualmente sob trâmite em segredo de justiça, em Sergipe. A intervenção granjeou a manifestação extrajudicial do aplicativo acerca do ocorrido, que exteriorizou seu desapontamento com a justiça brasileira quanto ao que considerou medida extrema, alegando não ser capaz de fornecer informações que não as possui, alertando, ainda, para a implementação de uma criptografia ainda mais forte[85].

Prevendo a recorrência da medida de suspensão, afirmou em entrevista a advogada especialista em Direito Digital Rubia Ferrão, quanto ao suporte dado pelo Marco Civil, que as empresas de serviços ofertados ao público brasileiro teriam de se adaptar às regras brasileiras. Nesta mesma entrevista, realizada por Felipe Pontes, posicionou-se o promotor Frederico Ceroy, presidente do Instituto Brasileiro de Direito Digital, no sentido de que o WhatsApp se recusa voluntariamente a entregar os dados requisitados e que a contribuição geraria altos custos à empresa[86]. Logo o ato foi reiterado, no início de maio, pela Justiça do Sergipe, e em 19 de julho de 2016, desta vez por determinação judicial da juíza Daniella Barbosa Assumpção de Souza, da 2ª Vara Criminal de Duque de Caxias - RJ.

Conforme aduzido do breve histórico apresentado nos parágrafos anteriores, o aplicativo em análise ausentou-se de viabilizar sua colaboração para com a justiça brasileira através de um posicionamento inicialmente soberbo, de forma a ignorar plenamente as primeiras investidas dos juízes, e posteriormente, de maneira superficial, resumindo-se tão somente na alegação de impossibilidade de fornecer um conteúdo o qual não detém, sem sequer demonstrar a exatidão desse fato, gerando no Brasil uma repercussão que muito se assemelha com o caos experimentado internacionalmente em relação ao tema.

---

[84] Disponível em: <http://tecnologia.ig.com.br/2015-12-17/zuckerberg-lamenta-suspensao-do-whatsapp-e-um-dia-triste-para-o-pais.html>

[85] Noticiado pelo jornal El País, disponível em: <http://brasil.elpais.com/brasil/2016/03/01/tecnologia/1456843819_998702.html>

[86] Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2016-03/medidas-como-prisao-de-vice-do-facebook-devem-se-repetir-dizem-especialistas>

Por via de mandado de segurança em face da decisão do Juiz de Lagarto/SE que determinou o bloqueio do WhatsApp por 72 horas, a empresa pleiteou o restabelecimento de seus serviços com a reunião de argumentos que versam, entre outros, sobre impossibilidade jurídica e técnica de se determinar a interceptação do conteúdo.

Quanto à impossibilidade jurídica, suscitada sobretudo nas alegações de discricionariedade ampla e restrita do juiz, fazendo menção também a eventual quebra de sigilo indiscriminada, mostra-se improcedente, uma vez que, como abordado no tópico anterior, o Marco Civil autoriza expressamente em seu artigo 10 a disponibilização de registros e conteúdos para fins de salvaguardar direitos em violação, o que foi ordenado pelo magistrado com devido fundamento no Estado Democrático de Direito, obedecendo ao critério de especificidade necessário. Pontua a questão, em abordagem a conflitos de direitos, o desembargador Cezário Siqueira Neto em relatório referente à concessão de liminar no *writ*[87], negando desproporcionalidade ou prejuízo à privacidade, bem como ausência de fundamento legal ou caráter antijurídico, realçando, ainda, a supremacia do interesse público na preservação de direitos que compõem a essência da vida em sociedade, como a própria vida, a liberdade e a segurança pública.

Acerca da impossibilidade técnica alegada, importante destacar que sua comprovação jamais foi efetivada, valendo-se os magistrados do conhecimento técnico fornecido pela Polícia Federal conjugado com a racionalidade das ciências humanas a fim de deliberar sobre o assunto. Dessa forma, questiona-se a plausibilidade da criptografia, compreendida neste como método para codificação de mensagens que visa a segurança, como justificativa para o não fornecimento de dados necessários a uma investigação criminal, nem mesmo em tempo real, através de interceptação telemática. Com efeito, tem-se do Informativo Técnico da Polícia Federal nº 31/2016 a seguinte conclusão:

> Como a implementação da criptografia fim-afim foi incremental e considerando a implementação de clientes de terceiros encontrados na internet, há fortes indícios que a criptografia fim-a-fim seja opcional e teoricamente poderia ser desabilitada mediante parâmetros configuráveis nos equipamentos servidores da empresa...Recursos Adicionais, com o WhatsApp Web e o serviço de notificações teoricamente podem ser utilizados para permitir a duplicação das mensagens e posterior interceptação mediante ordem judicial.

[87] Equivalente, neste contexto, a Mandado de Segurança.

Apesar dos fortes indícios de viabilidade técnica apontados por quem detém conhecimento suficiente a respeito de informática e tecnologia, e partindo do pressuposto lógico de que nenhuma criptografia é inquebrável, não se pode fazer comprovação de fato algum sem que seja realizada uma íntegra análise do objeto. Assim argumenta o Ministério da Justiça, que instiga a seguinte reflexão: se é certa e exata a impossibilidade técnica alegada, por que o WhatsApp não faz prova exata do tema? Por que se recusa a colocar frente a frente os responsáveis por essa área com o corpo técnico da Polícia Federal?

Tal posicionamento induz a ideia de que a empresa se vale do enigma que o caso configura, como forma de perpetuar-se de maneira inerte perante a Justiça e imune no mercado, em atenção quase que exclusiva ao retorno econômico e a reputação de suas atividades, o que poderia sofrer déficit com a eventual migração de usuários para uma plataforma equivalente caso a confiança depositada for fragmentada, o que também acaba ocorrendo quando o aplicativo sofre suspensão temporária.

Assim, permite-se indiretamente a atribuição genérica de um caráter malicioso para a Criptografia, o que ocorre quando se considera muito mais a sua utilização para a delinquência, como óbice à atividade da polícia e para a escusa da Lei do que o seu papel precípuo de preservar os elementos de intimidade e segredo. Neste sentido, expõe o Ministério da Justiça, que defende a necessidade das empresas se adaptarem ao ordenamento pátrio:

> Não só a utilização de recursos tecnológicos como a criptografia atua como barreira ao acesso a informações que possibilitem o exercício do poder de polícia estatal, em especial na investigação de ilícitos penais, mas também a desatualização legislativa.

Apesar de tais escusas quanto à obtenção de dados nos termos do Marco Civil da Internet, importante se faz elucidar que a repercussão da mídia deturpa a veridicidade do que é objetivado para garantir a solução dos ilícitos que se formam rotineiramente e que se aproveitam do descaso que a situação configura para subsistir em detrimento do uso de outros meios de comunicação com precedentes favoráveis ao controle do Estado.

Visando contornar a situação, e considerando relativamente a contestação do WhatsApp quanto à impossibilidade de fornecimento de dados dos quais não tem

acesso, a justiça tem optado pela debilitação da criptografia com foco na possibilidade de fomentar a interceptação telemática, entretanto também não tem logrado êxito. Acontece que a empresa se apoia na força do método criptográfico de ponta a ponta, fortificando seu argumento na necessidade de oferecer segurança "plena" – e inquebrável - aos seus usuários e permanecer confiável, contudo não se atenta ao fato de que sua postura não viabiliza as garantias para a segurança jurídica em face das recorrentes violações protagonizadas pelos de má-fé. Vale destacar as palavras da magistrada Daniela Barbosa Assumpção de Souza em sua decisão de bloqueio dos serviços:

> Nem se deve entender que a quebra do sigilo e interceptação telemática do aplicativo traria insegurança aos usuários, uma vez que a decisão judicial é sempre fundamentada, específica e abarca usuários que estejam praticando crimes dentro do território nacional. Ora, se assim não fosse, inviável seria a quebra do sigilo de correspondência, ligações telefônicas ou correios eletrônicos (Gmail, Yahoo, Hotmail etc.), sempre possível em decorrência de ordem judicial, sendo certo que tais serviços – ou suas empresas – jamais deixaram de ser confiáveis em virtude da possibilidade legal de quebra.

Embora se paute a empresa de Mark Zuckerberg principalmente na atenção à segurança da sociedade, quando preza pelo pleno funcionamento de uma criptografia ilibada, o que merece reconhecimento numa ótica específica, não se pode afirmar que a mesma preocupação é destinada para aqueles que são vítimas da justiça ainda mais tardia em decorrência de seus entraves, nem que a qualidade das comunicações virtuais e a satisfação social estão ligadas somente ao fornecimento de privacidade, uma vez que o Brasil apresenta índices de criminalidade progressivos. Interessa transcrever mais uma vez a magistrada do Rio de Janeiro, em consideração acerca da questão:

> O prejuízo maior, assim, quando o Facebook do Brasil descumpre uma ordem judicial, é da sociedade, ante a impunidade gerada pela negativa em fornecer informações que serão fundamentais para a consecução das investigações e, posteriormente, para robustecer o processo criminal de provas que sejam úteis à formação da convicção das partes e do juiz. 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 responsáveis[88].

Prevalecido a impossibilidade técnica a despeito da punibilidade inalcançada nas citadas investigações criminais, que tratam de crimes de grave potencial ofensivo como tráfico de drogas e pedofilia, ambos em segredo de justiça, faz-se necessária uma análise da matéria sob o prisma dos especialistas na área, os quais espera-se que apresentem propriedades suficientes a dirimir dúvidas e estabelecer parâmetros básicos à solução do conflito que desde 2015 mantém a celeuma.

Convém voltar-se para a contribuição da pesquisadora na área de criptografia no *Center For Internet and Society da Stanford Law School* (EUA), Riana Pfefferkorn, em entrevista realizada em 2016. Para ela, ainda que não seja viável o acesso ao conteúdo das mensagens criptografadas de ponta a ponta, é possível a descoberta de informações acerca "de quem está mandando mensagem para quem, quando e com que frequência"[89], o que remete às informações de registros previstas no Marco Civil. A partir desses dados, as autoridades podem realizar diligências a fim de suplementar a investigação, através de mandados de busca e apreensão, o que pode culminar na obtenção do conteúdo a partir do acesso direto ao aparelho. A pesquisadora aduz, também, a possibilidade de interceptação telefônica, entretanto logo a considera inapta, em razão da previsibilidade quanto à não realização de telefonemas por parte de quem está envolvido em atividades criminosas e evita a vigilância. No tocante à proibição da criptografia em análise, acrescenta pertinentemente que as tentativas do Estado são: "inúteis", vislumbrando o acesso clandestino a outros aplicativos equiparados; e "equivocadas", apontando o caráter essencial da criptografia em sua finalidade precípua, de forma a proteger transações, serviços bancários, entre outros.

Uma interessante questão levantada por Pfefferkorn diz respeito à possibilidade de má utilização pelos criminosos até mesmo da própria ferramenta que poderia ser desenvolvida para o acesso aos conteúdos discriminadamente pelo Estado:

---

[88] Decisão na integra disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/07/Decis%C3%A3o_WhatsApp1.pdf

[89] Disponível em matéria do jornal O Estado de São Paulo, disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/

> Se a criptografia é quebrada para a aplicação da lei, esse mesmo *backdoor* poderá ser usado por bandidos também. Se o Brasil exige um *backdoor* na criptografia, então todo mundo usando a criptografia está em risco. Isso poderia incluir empresas brasileiras, que precisam se proteger contra a espionagem econômica; os bancos brasileiros que poderiam ser invadidos; e até mesmo o Estado brasileiro, que precisa manter os segredos de Estado seguros em relação a Estados inimigos. Forte criptografia é uma "defesa contra vilões", mesmo que os vilões possam usá-la para esconder suas atividades.[90]

Diante dessa alternativa que a pesquisadora classifica como "sopesamento negativo", em razão da inviabilidade técnica, a atenção pode-se voltar, eficientemente, aos metadados (registros de aplicações). Assim, "munidos" de informações sobre quem deve ser investigado, a Polícia Federal poderia estabelecer como foco os dispositivos móveis, podendo explorar vulnerabilidades para ter acesso ao conteúdo, inclusive através da instalação compulsória de um programa de monitoramento.

Já conforme Tobias Boelter, doutorando na *University of California*, Berkeley, Departamento de Engenharia Elétrica e Ciência da Computação, com foco em Segurança e Criptografia, em entrevista para a mesma matéria, ainda que não seja possível o acesso ao conteúdo por causa da criptografia ponta a ponta, há duas possibilidades técnicas para a interceptação: através de um ataque conhecido como *"man-in-the-middle*", onde o aplicativo forneceria sua própria chave privada e pessoal ao invés das que são normalmente públicas; ou por meio de uma modificação do aplicativo, com atualização de sua versão nas lojas, permitindo a função "secreta" de enviar algumas informações também para o Estado. Entretanto, segundo o Doutorando, ambas as "gambiarras" poderiam ser descobertas pelos usuários mais habilidosos.

Quanto à primeira hipótese de interceptação, não parece concebível que a empresa se comprometeria a tal intermediação, burlando o seu próprio funcionamento, uma vez que se verifica o desdém com o qual o WhatsApp lida com as ordens do poder judiciário brasileiro nos precedentes referentes ao tema. De igual modo, as tentativas de imposição para a criação de um recurso específico apto a possibilitar eventual interceptação, o que se assemelha à segunda hipótese, não atingiram êxito. Acerca dos registros de aplicações, o óbice da criptografia ponta a ponta estende seus efeitos até mesmo a eles, inviabilizando a única alternativa que

[90] Disponível em: <http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/>.

se mostra plausível e que não demanda a decifração ou o grampo telemático: a disponibilização de metadados.

Assim pode ser apreendido, conforme nota técnica do Ministério Público Federal[91]:

> O uso do modelo criptográfico nas comunicações ponto a ponto é tema da mais alta complexidade que envolve, de um lado, a política de segurança adotada quanto aos conteúdos das mensagens e a privacidade dos usuários e, de outro, a maior dificuldade na obtenção de provas nas searas cível e criminal. Contudo, habitualmente as empresas utilizam este argumento para também se esquivar da obrigação de fornecer registros de comunicação, dados armazenados e os metadados, que não são criptografados.

Tal complexidade precisa ser compreendida em sua plenitude, desatando as mãos do Poder Judiciário para que sejam possíveis o trato jurídico adequado ao tema e a articulação técnica das autoridades de investigação com eficiência, em conformidade com as diretrizes da Lei que regula o uso da Internet no Brasil.

O Supremo Tribunal Federal, ao considerar sua insciência em relação ao tema do ponto de vista técnico enquanto juristas, decidiu em 27 de outubro de 2016, a partir da Arguição de Descumprimento de Preceito Fundamental 403, pela convocação de uma audiência pública para discutir o bloqueio do aplicativo, reconhecendo o ministro relator Edson Fachin que questões ligadas à possibilidade técnica de interceptação, suspensão e colaboração com as requisições judiciais extrapolam os limites estritamente jurídicos e exigem conhecimento transdisciplinar[92].

Por força da decisão, o futuro esclarecimento considerará o respaldo técnico já introduzido ao presente trabalho advindo da Polícia Federal e do Ministério Público Federal, bem como dos órgãos governamentais relacionados ao uso e desenvolvimento da Internet no Brasil, além do setor empresarial e de especialistas com notável saber técnico acerca do tema.

Imprescindível transcrever as questões preambulares definidas na convocação da audiência[93] a serem satisfeitas por artifício da qualificação técnica dos órgãos, especialistas ou entidades:

---

[91] Inteiro teor disponível em: <http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/>
[92] Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf>
[93] Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf>

> 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*)?
> 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.

É nítido que a Suprema Corte aceita, pelo menos a princípio, a impossibilidade de decodificação das mensagens criptografadas de ponta a ponta, bem como a inocorrência de armazenamentos delas, pelo fato de destinar-se exclusivamente à solução de imprecisões acerca da interceptação em tempo real, seja com o método criptográfico ativado ou desativado. Do contrário, objetivaria conjuntamente esclarecimentos sobre alternativas razoáveis para o conhecimento do conteúdo a ser registrado, assim como preceitua o artigo 15 do Marco Civil.

Apresenta-se o STF, portanto, com cautela em relação ao objeto em debate, vislumbrando a utilidade dos serviços ofertados para mais de 100 milhões de pessoas no país, inclusive para fins de intimações judiciais permitidas pela regulamentação nº 10 do Tribunal Regional Federal da 3ª Região que considera, entre outros, a celeridade, a integralização e a eficiência da plataforma[94].

Assim, o cenário apresenta-se em 2017 configurado à ponderação adequada dos problemas suscitados, o que poderá ensejar novas suspensões ou até mesmo a proibição de exercício das atividades do WhatsApp prevista no artigo 12, IV do Marco Civil, bem como a efetiva atribuição de ilegalidade, em face de seus atos contrários ao que a Lei determina.

Por fim, vale salientar que a legislação brasileira não regula suficientemente a aludida criptografia, motivo pelo qual estão em trâmite nas casas legislativas projetos que visam disposições consistentes referentes ao tema.

---

[94] Disponível em: <http://web.trf3.jus.br/diario/Consulta/VisualizarDocumento?CodigoTipoPublicacao=1&CodigoOrgao=1&CodigoDocumento=0&IdMateria=492004&NumeroProcesso=0>

3.3 O Bloqueio do WhatsApp

Conforme abordado brevemente no tópico antecedente, a Justiça Brasileira tem aplicado sanções diversas ao provedor de aplicações de internet WhatsApp, todas fundamentadas na Lei 12.965/2014, como forma de impulsionar o cumprimento de diligências substanciais à solução de litígios graves. As sanções referentes à suspensão dos serviços do aplicativo virtual promoveram maior comoção social pelo fato de terem atingido, genericamente, todos os seus usuários no país. Seus efeitos, porém, foram cessados por força de decisões liminares posteriores, considerando sobretudo a desproporcionalidade da medida.

O presente tópico pretende demonstrar a fundamentação legal dos bloqueios judiciais, direcionando-se à sua finalidade e às suas consequências, a fim de responder se o texto legal do Marco Civil da Internet autoriza sua aplicação conforme os casos que se reiteram no Brasil, bem como instigar a apropriada reflexão sob a luz dos direitos fundamentais pertinentes.

Apesar do segredo de justiça conferido aos casos específicos que motivaram a interrupção do WhatsApp, é indubitável que as ordens de suspensão foram fundamentadas na supracitada Lei, que conforme já demonstrado, aplica-se adequadamente ao aplicativo em razão da natureza de seus serviços ofertados.

Quanto à previsibilidade das sanções expostas, o artigo 12 apresenta o seguinte rol de medidas:

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

É fato que a justiça brasileira atendeu a ordem implícita das sanções acima, quando se primou pela advertência reiterada e a multa majorada, somente suspendendo “temporariamente” as atividades posteriormente à ineficácia das

medidas mais leves. Desse modo, respeitou-se a hierarquia com vista na gravidade das sanções, atingindo em um primeiro momento somente a empresa, como deve ser segundo o advogado Marcelo Frullani Lopes[95].

O cerne da questão reside no fato do artigo que prevê as comentadas sanções fazer menção às atividades que envolvam os atos do artigo 11º, o qual:

> 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.

Assim, instala-se o conflito a partir da hermenêutica do dispositivo. Literal e sistematicamente, pode ser depreendido que a suspensão ou o bloqueio podem ter aplicação somente no que tange às operações de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet", sugerindo o equívoco de interpretação dos magistrados, conforme declaração do pesquisador e co-gestor do Centro de Tecnologia e Sociedade (CTS) da FGV Direito Rio, Luiz Moncau para entrevista realizada por Rosanne D'Agostino ao G1[96].

Por outro lado, a extensão dos efeitos ao livre tráfego de informações pode ser realizado se compreendido que as supra elencadas operações, a exemplo de coleta, no sentido de "recolhimento", configuram espécie ou pressupostos indispensáveis para a troca de informações, cabendo a necessidade de um entendimento substancial e definitivo.

Sob o prisma dos direitos fundamentais violados, como a liberdade de expressão e de comunicação, que gozam de proteção também pelo Marco Civil, percebe-se que a medida apresenta exorbitante desproporcionalidade quando seus efeitos são aplicados em detrimento de 100 milhões de usuários.

Importante evidenciar a pertinente justificativa do Ministro Ricardo Lewandowski em decisão liminar da Suprema Corte[97] que suspendeu o bloqueio do WhatsApp:

---

[95] Disponível em: <http://justificando.cartacapital.com.br/2016/05/02/suspensao-do-whatsapp-nao-e-permitida-pelo-marco-civil-da-internet/>

[96] Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/05/por-que-juiz-pode-bloquear-whatsapp-no-brasil-veja-perguntas-e-respostas.html>

[97] Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf>

> Ora, 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.

O entendimento do ministro se coaduna assertivamente com o disposto nos artigos 2º e 3º do Marco Civil, que representam os fundamentos e princípios que disciplinam toda a matéria cibernética no Brasil.

Quanto à finalidade de obrigar a sujeição ao poder judiciário, destacada pelos magistrados protagonistas das suspensões, é correto destacar que não foi verificada, uma vez que as investigações não prosperaram e o prejuízo foi da sociedade como um todo. Destaca-se, ainda, com atenção ao caput do já citado artigo 12, que as sanções cíveis, criminais e administrativas podem significar uma alternativa de mais valia aos magistrados, conforme compreendido pelo Doutor em Direito Ericson Meister Scorsim que sugere a adequação típica da conduta do WhatsApp ao crime de desobediência previsto no artigo 330 do Código Penal Brasileiro[98].

Por fim, cabe fazer alusão ao posicionamento legal do WhatsApp através de petição ao STF protocolada em 1º de fevereiro de 2017 por meio de seu advogado Davi de Paiva Costa Tangerino. Na ocasião, a defesa do aplicativo pauta-se na proteção constitucional da liberdade de expressão e comunicação, no princípio da proporcionalidade das medidas, bem como a proteção da livre iniciativa e concorrência, esta que seria afetada em razão das sanções que privilegiam indiretamente a migração para outras plataformas; além da interpretação em favor da proibição de tais sanções pelo Marco Civil e discricionariedade irregular do juiz para aplica-las[99].

A empresa visa os efeitos da declaração de inconstitucionalidade e ilegalidade dos bloqueios, de forma a evitar novos prejuízos em seus serviços. Assim, o Supremo Tribunal Federal como defensor da Constituição priva-se do juízo definitivo até que se possa amadurecer suficientemente a questão, reunindo todo o arcabouço técnico e jurídico indispensável para a aplicação mais justa da lei.

---

[98] Disponível em: <https://ericsonscorsim.jusbrasil.com.br/artigos/269940617/bloqueio-judicial-do-whatsapp-no-brasil>

[99] Disponível em: <http://s.conjur.com.br/dl/whatsapp-alega-stf-bloqueios-ferem.pdf>

4 CONSIDERAÇÕES FINAIS

Esta investigação fora pautada pelo método dedutivo visando identificar se a criptografia de ponta-a-ponta empregada pelo aplicativo WhatsApp está de acordo com os princípios do marco civil da internet.

A favor da criptografia pode-se destacar a sua funcionalidade enquanto meio para garantir o sigilo das conversas intermediadas pelo WhatsApp. Sendo assim, a criptografia, per si, é um elemento que gera confiança ao usuário quanto à inviolabilidade de suas conversas; por conseguinte, é um elemento basilar à realização do princípio da privacidade dos usuários do aplicativo.

Do ponto de vista jurídico, o que se anuncia como contrário à criptografia será de ordem colateral, vinculado às condutas dos usuários dela, não sendo o método criptográfico de ponta-a-ponta, por si mesmo, instrumento gerador de uma atividade ilícita.

Deste modo, as responsabilidades sobre a prática de crimes cibernéticos no provedor de aplicações WhatsApp não decorrem necessariamente do fato do mesmo propiciar aos seus usuários a inviolabilidade de suas correspondências.

Mesmo assim, tais práticas, quando constituem conduta ilícita, devem ser investigadas e os modos processuais para apurar determinada situação de conflito devem ser facilitados pelo fornecedor do serviço como condição de seu próprio status como empresa e seu devido funcionamento no país.

Enquanto o WhatsApp continuar incorrendo na prática de não fornecer às autoridades judiciais elementos probatórios demandados aos processos, a aplicação estará faltando com sua finalidade social, fundamento para atuação de qualquer companhia no Brasil.

O que se percebe hoje, com a queda de braço entre justiça e a aplicação, é o interesse econômico e de merchandising da marca WhatsApp em se manter como empresa cuja política de segurança dos dados intermediados por ela são, e sempre serão, invioláveis.

Tal situação gera uma conjuntura peculiar, enquanto bancos, companhias telefônicas, empreiteiras e empresas dos mais diversos setores têm os dados de seus clientes passíveis de acesso diante de uma ordem judicial. O WhatsApp se coloca como não colaborador à realização da justiça, atuando, assim, como elemento ocasionador de insegurança jurídica.

Em tal situação, magistrados distribuídos por todo o Brasil colocam a conduta da empresa em questão. Estaria o aplicativo incorrendo em uma conduta ilegal?

Neste trabalho fora demonstrado que existe sim a possibilidade da lei regular as interações criptografadas, bem como há a possibilidade do aplicativo utilizar de ferramentas para o gerenciamento de seus dados de modo a dar suporte à justiça em sua realização de direitos individuais ou até mesmo coletivos.

Como forma de conclusão, este trabalho pressupõe que o bloqueio da aplicação em todo o Brasil é um ato desproporcional, devido ao grande volume de informações intercambiadas diariamente por meio do WhatsApp.

Garantias à liberdade de informação, comunicação e privacidade estão elencadas tanto no marco civil, quanto nos termos de uso do aplicativo e na Constituição Federal. A questão que urge, contemporaneamente, versa a respeito de como o judiciário brasileiro e o WhatsApp irão "ajustar condutas" para que outros direitos e princípios constitucionais não venham a ser depreciados por terceiros, em casos concretos, de acordo com o modo como hoje a situação se anuncia.

O Estado brasileiro tem progredido em matéria de direitos na, e para o uso, da internet; o marco civil da internet é, apesar da redundância, um verdadeiro marco neste sentido.

Contudo, as políticas públicas de cunho transversal, voltadas para a qualificação do acesso e formas de interação entre os usuários são tão necessárias quanto este instrumento normativo.

Dadas as consultas públicas iniciadas pelo STF em relação à temática do “judiciário versus WhatsApp”, prognosticam melhoras e uma normalização das relações em médio prazo, sendo precipitado falar sobre as mesmas em um momento tão preliminar das tratativas.

Vislumbra-se neste trabalho a possibilidade de realização de direitos individuais e coletivos, como a privacidade e seus elementos, a liberdade de expressão e a segurança jurídica, em uma relação de estranhamento e enfrentamento. Percebe-se a possibilidade de evolução paulatina para uma estrutura possível de coexistência pacifica em um futuro menos conflitivo e mais colaborativo, onde a educação virtual seja uma constante. Pois, ao fim, tanto o judiciário quanto o WhatsApp se interessam por uma saída positiva e/ou propositiva deste conflito.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Fabio Caldas de. **Reflexões sobre o Marco Civil da Internet**. Consultor Jurídico, 2014. Disponível em:< www.conjur.com.br/2014-jul-04/fabio-caldas-araujo-reflexoes-marco-civil-internet.>. Acesso em: 13 de janeiro de 2017.

ARAYA, ERM., and VIDOTTI, SABG. **Criação, proteção e uso legal de informação em ambientes da World Wide Web [online]**. São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2010. 144 p. ISBN 978-85-7983-115-7. Disponível em: SciELO Books http://books.scielo.org.

BRASIL. **Constituição da República Federativa Do Brasil de 1988.**
_____. Decreto no 3.587, de 5 de setembro de 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Lei nº 7.232 de 29 de outubro de 1984**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L7232.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Lei nº 8.069, de 13 de julho de 1990**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L8069.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Lei nº 9.296, de 24 de julho de 1996**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Lei nº 11.829, de 25 de novembro de 2008**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm> Acesso em: 17 de fevereiro de 2017.

_____**. Lei nº 12.735, de 30 de novembro de 2012**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em: 17 de fevereiro de 2017.

_____**. Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 17 de fevereiro de 2017.

_____. **Ministério das Comunicações**. Portaria Interministerial n° 147, de 31 de maio de 1995. Disponível em: < http://www.cgi.br/portarias/numero/147> Acesso em: 17 de fevereiro de 2017.

_____. **Ministério das Comunicações**. Comitê Gestor da Internet no Brasil. Resolução CGI.br/RES/2009/003/P. São Paulo, 2009. Disponível em: <http://www.cgi.br/portarias/numero/147>. Acesso em: 17 de fevereiro de 2017.

_____. **Superior Tribunal de Justiça** - REsp 1193764/SP, Rel. Ministra NANCY ANDRIGHI, Data do Julgamento: 14/12/2010 T3 - TERCEIRA TURMA, Data da Publicação: DJ 08/08/2011. Disponível em: < https://stj.jusbrasil.com.br/jurisprudencia/25125629/agravo-regimental-no-recurso-especial-agrg-no-resp-748474-rs-2005-0075503-8-stj/inteiro-teor-25125630> .Acesso em: 17 de fevereiro de 2017.

_____. **Superior Tribunal de Justiça** - AgRg no REsp: 1309891 MG 2012/0035031-2, Relator: Ministro SIDNEI BENETI, Data de Julgamento: 26/06/2012, T3 - TERCEIRA TURMA, Data de Publicação: DJe 29/06/2012. Disponível em: < https://stj.jusbrasil.com.br/jurisprudencia/25125629/agravo-regimental-no-recurso-especial-agrg-no-resp-748474-rs-2005-0075503-8-stj/inteiro-teor-25125630> .Acesso em: 17 de fevereiro de 2017.

_____. **Supremo Tribunal Federal**. Medida Cautelar na Argüição de Descumprimento de Preceito Fundamental 403 Sergipe – ADPF 407/SE. Brasília, 19 de julho de 2016. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf> Acesso em: 17 de fevereiro de 2017.

_____. **Supremo Tribunal Federal**. Argüição de Descumprimento de Preceito Fundamental 403 Sergipe – ADPF 407/SE. Brasília, 27 de outubro de 2016. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf> Acesso em: 17 de fevereiro de 2017.

_____. **Tribunal Regional Federal da 3ª região**. Resolução nº 10. Diário Eletrônico Da Justiça Federal Da 3ª Região. Edição nº 226/0 - São Paulo, sexta-feira, 09 de dezembro de 2016. Disponível em: <http://web.trf3.jus.br/diario/Consulta/VisualizarDocumento?CodigoTipoPublicacao=1&CodigoOrgao=1&CodigoDocumento=0&IdMateria=492004&NumeroProcesso=0> Acesso em: 17 de fevereiro de 2017.

_____. **Ministério Público Federal**. Conselho Nacional do Procuradores-Gerais. Nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da internet. Disponível em: <http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/> Acesso em: 17 de fevereiro de 2017.

BARRETO, Ricardo de Macedo Menna. **Redes sociais na Internet e direito**: a proteção do consumidor no comércio eletrônico. Curitiba: Juruá, 2012.

CÂMARA NOTÍCIAS. **Perito afirma que dados trocados no WhatsApp não podem ser acessados**. Brasília: Câmara dos Deputados, Data da Publicação: 15/09/2015.

CARVALHO, Leda Maria Maia Rodrigues de. **A insegurança do mundo digital**: Um olhar crítico acerca da pedofilia na Internet. Recife: UFPE, 2002.

CAVALCANTE FILHO, JOÃO TRINDADE. **Teoria Geral dos Direitos Fundamentais**. Acesso em 17 de fevereiro de 2017. Disponível em: <http://www.stf.jus.br/repositorio/cms/portaltvjustica/portaltvjusticanoticia/anexo/joao_trindadade__teoria_geral_dos_direitos_fundamentais.pdf> Acesso em: 17 de fevereiro de 2017.

CORREA, Gustavo Testa. **Aspectos jurídicos da Internet**. 4ª edição. São Paulo: Saraiva, 2008.

COHEN, Jared. SCHMIDT, Eric. **A nova era digital**: como será o futuro das pessoas, das nações e dos negócios. UNESP: São Paulo, 2013.

FRANCO, Deivison Pinheiro. MAGALHÃES, Suyanne Ramos. **A Dark Web** – Navegando No Lado Obscuro Da Internet. Amazônia em Foco, Castanhal, v. 4, n.6, p. 18-33, jan./jul, 2015.

HOLANDA, Danielle Spencer. **Direito à privacidade**: uma análise sob a ótica da nova sociedade da informação. Recife: UFPE, 2005.

LEAL, Katia Minatto. **Direito na Rede**: um breve estudo sobre os direitos na Internet. Porto Alegre: UFRGS, 2004.

LIMA, Glaydson de Farias. **Manual de Direito Digital**: Fundamentos, Legislação e Jurisprudência. Curitiba: Appris, 2016.

____, Glaydson de Farias. **Os Dilemas Da Criptografia De Mensagens Na Internet**. São Paulo: IBMEC/BOVESPA, 2016.

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal**. 10ª edição. São Paulo, Revista dos Tribunais, 2013.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet:** subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014 (Texto para Discussão nº 148). Disponível em: <www.senado.leg.br/estudos>. Acesso em 29 de abril de 2014.

OLIVEIRA, Rafael Santos de. Et. al. **Judicialização De Conflitos No Ciberespaço**: Desafios À Liberdade De Expressão Na Blogosfera. Revista de Direitos Fundamentais e Democracia: Curitiba, v. 13, n. 13, p. 160-178, janeiro/junho de 2013.

ONU. **Declaração Universal dos Direitos Humanos**. São Francisco, 10 de dezembro de 1948.

SANCHES, Rosana. Et. al. **Direito e Internet**. Caderno Jurídico - julho/02 - Ano 2 - n. º 4. São Paulo: ESPM, 2002.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. **Regulamentação da internet**: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. Hist. cienc. saúde-Manguinhos, Rio de Janeiro , v. 22, supl. p. 1551-1571, Dec. 2015 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-59702015001001551&lng=en&nrm=iso>. Acesso em: 17 de fevereiro de 2017.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet**: uma lei sem conteúdo normativo. Estud. av., São Paulo , v. 30, n. 86, p. 269-285, Apr. 2016. Disponível em:<http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso>. Acesso em: 17 de fevereiro de 2017.