**EXCELENTÍSSIMOS MINISTROS RELATORES EDSON FACHIN E ROSA WEBER DO SUPREMO TRIBUNAL FEDERAL**

**IDEC – INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR**, entidade civil sem fins lucrativos, legalmente constituída desde 1987, inscrito no CNPJ sob n°58.120.387/0001-08, com sede na Rua Desembargador Guimarães, 21, São Paulo/SP, CEP 05002-005, representado por sua Coordenadora Executiva Elici Maria Checchin Bueno e pelo pesquisador em telecomunicações Rafael Augusto Ferreira Zanatta, vem, respeitosamente, à presença de Vossas Excelências, apresentar as contribuições do Instituto para a "Audiência Pública Simultânea para Discutir Aspectos dos Arts. 10 e 12, III e IV, da Lei nº 12.965/2014 – Marco Civil da Internet (ADI 5.527, Rel. Min. Rosa Weber) – e a Suspensão do Aplicativo *WhatsApp* por Decisões Judiciais no Brasil (ADPF 403, Rel. Min. Edson Fachin)".

A presente petição sistematiza argumentos que serão apresentados oralmente na apresentação marcada para o dia 05 de junho de 2017 no Supremo Tribunal Federal.[1] O documento estrutura-se em seis partes. Na primeira, há uma breve síntese das ações que ensejam a Audiência Pública e a problemática técnica e jurídica por trás da convocatória. Na segunda, há uma explicação sobre o envolvimento do Idec nas discussões sobre bloqueio do WhatsApp no Brasil e interpretação do Marco Civil da Internet. Na terceira, há revisão da doutrina jurídica que trata dos artigos 10 e 12 da Lei 12.965/14, objeto de discussão de caráter constitucional. Na quarta parte, uma explicação sobre o modo de funcionamento da

[1] A petição foi elaborada pelo pesquisador Rafael Zanatta e contou com o auxílio dos assistentes de pesquisa Andressa Gomes (Faculdade de Direito da Universidade de São Paulo), Bárbara Simão (Faculdade de Direito da Universidade de São Paulo) e Victor Veloso (Instituto de Relações Internacionais da Universidade de São Paulo).

criptografia ponta-a-ponta e sua relação com os direitos assegurados no Marco Civil da Internet. Na quinta, defende-se a tese de inaplicabilidade das sanções previstas nos incisos do art. 12 da Lei 12.956/14 em casos de não cumprimento de ordens judiciais que exigem transmissão de comunicações privadas realizadas por meio de um provedor de aplicação de internet.

**1 – Breve síntese das ações que ensejam a Audiência Pública**

1.1. A presente Audiência Pública origina-se em duas ações constitucionais que possuem objetos jurídicos semelhantes e que, em um processo inovador no Supremo Tribunal Federal, foram reunidas para uma mesma discussão de caráter técnico e jurídico.

1.2. A convocatória originária para discussão do bloqueio do aplicativo WhatsApp por decisões judicias no Brasil ocorreu em 26 de outubro de 2016, pelo ministro relator Edson Fachin, no âmbito da Arguição de Descumprimento de Preceito Fundamental 403, ajuizada pelo Partido Popular Socialista (PPS). Nesta ADPF, o PPS indigna-se contra decisão do Juiz de Direito do Tribunal de Justiça do Estado de Sergipe, Marcel Maia Mantovão, que determinou a suspensão do aplicativo de comunicação WhatsApp em todo o Brasil. De acordo com relatório do ministro Fachin, os autores (i) sustentam que ato impugnado viola o preceito fundamental da liberdade de comunicação (art. 5º, IX, CF); (ii) defendem o cabimento da ADPF e preenchimento do critério da subsidiariedade; (iii) sustentam que a suspensão do WhatsApp com base em controverso fundamento viola o direito à comunicação; (iv) requerem concessão de medida liminar *ad referendum* para suspensão imediata da decisão que bloqueou o aplicativo por 72 horas; (v) requerem, no mérito, o reconhecimento de violação ao preceito fundamental da comunicação (art. 5º, IX), com a finalidade de não mais haver suspensão do aplicativo de mensagens WhatsApp por qualquer decisão judicial.

1.3. Após suspensão da decisão que determinou o bloqueio pelo Tribunal de Justiça do Estado de Sergipe, o Supremo ouviu a Procuradoria-Geral da República e intimou o Juízo prolator da decisão impugnada. Em sua resposta, afirmou que a Autoridade de Polícia Federal, em sede de representação cautelar criminal, requereu o bloqueio do WhatsApp em virtude de "reiterados descumprimentos de ordens emanadas do referido Juízo". A decisão de

bloqueio do WhatsApp baseou-se em parecer favorável do Ministério Público Estadual.

1.4. Em razão de nova decisão de bloqueio do WhatsApp, desta vez pela 2ª Vara Criminal da Comarca de Duque de Caxias (RJ), o Partido Popular Socialista pediu suspensão imediata da decisão ao Supremo Tribunal Federal. Em sede de medida liminar, o Ministro Ricardo Lewandowski determinou a suspensão da decisão proferida pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias e afirmou que "a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, de 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 e o bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa". Ato sequente, o ministro Edson Fachin solicitou informações ao Juízo, Ministério da Justiça, ao Departamento de Polícia Federal e à empresa Facebook Serviços Online do Brasil Ltda.

1.5. As divergências foram profundas nas respostas ao STF. Conforme relata o ministro Fachin, o juízo da 2ª Vara Criminal da Comarca de Duque de Caxias afirmou que (i) a determinação do bloqueio do aplicativo WhatsApp decorreu da "recalcitrância [da] empresa Facebook, proprietária do aplicativo, em descumprir a ordem judicial de quebra do sigilo e interceptação telemática de terminais envolvidos em procedimento investigatório sigiloso"; (ii) que a imposição de medida de suspensão do aplicativo sustenta-se na inexistência de ofensa ao direito de comunicação; e que (iii) não há ofensa ao direito de comunicação pois há disponibilidade de aplicativos equivalentes e outras formas de comunicação. O Facebook, por sua vez, sustentou que (i) coopera com autoridades brasileiras, respondendo aos requerimentos no limite de sua capacidade, (ii) que não exerce qualquer poder de acesso ou controle sobre o aplicativo WhatsApp, que está sob ingerência de pessoa jurídica independente; e que (iii) diferentes esferas do Judiciário vêm reconhecendo a ilegalidade da realização de bloqueio de valores decorrentes de multa por alegado descumprimento de ordem judicial. A Polícia Federal, por sua vez, afirmou que (i) não há ofensa a preceito fundamental; (ii) que há obrigatoriedade do cumprimento da lei brasileira pelo WhatsApp em virtude do serviço oferecido ao público brasileiro nos termos do art. 11, parágrafo 2º, da Lei 12.965/14; e

que (iii) as autoridades públicas podem compelir a empresa que explora atividade econômica no Brasil a "respeitar o ordenamento jurídico pátrio e colaborar com o monitoramento telemático de investigados". O Ministério da Justiça, por fim, informou o STF que (i) a decisão impugnada deveria ser corrigida com base no princípio da proporcionalidade; que (ii) ordenamento jurídico protege a livre manifestação do pensamento e da comunicação; e que (iii) o mesmo ordenamento garante ao Poder Público a prerrogativa de "fazer prevalecer a ordem, afastando e coibindo, dentro do plano da legalidade, eventuais desestímulos à paz social, na esteira do devido processo legal".

1.6. Conforme decidido pelo ministro Fachin, a ADPF 403 traz discussões sobre "(i) a possibilidade técnica ou não de interceptação de conversas realizadas por meio do aplicativo WhatsApp; (ii) a possibilidade ou não de suspensão temporária das atividades do aplicativo WhatsApp; (iii) a possibilidade ou não de colaboração do WhatsApp com as requisições judiciais baseadas no art. 5º, XII, CF, Lei 9.296/96 e na Lei 12.965/14". Na ocasião, em outubro de 2016, o ministro abriu a possibilidade de inscrição para participação na Audiência Pública desde que os participantes abordassem quatro questões técnicas:

> *1. Em que consiste a criptografia ponta a ponta 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?*
>
> *3. Seria possível desabilitar a criptografia ponta a ponta 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 esteja habilitada, seria possível espelhar as conversas travadas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?*

1.7. No mês seguinte, a convocatória feita pelo ministro Fachin foi expandida, tornando-se uma *convocatória conjunta* para discussão, em Audiência Pública, de questões envolvendo a ADPF 403 e a Ação Direta de Inconstitucionalidade 5.527, ajuizada pelo Partido da República em maio de 2016.

1.8. Na ADI 5.527, o Partido da República sustenta que o parágrafo 2º do artigo 10 do Marco Civil da Internet dá suporte à concessão de ordens judiciais para que aplicações de internet disponibilizem o conteúdo de comunicações privadas e que o artigo 12 prevê uma série de sanções aplicáveis ao descumprimento da ordem pela empresa responsável pelo serviço (variando da advertência até proibição do exercício da atividade). Ambos seriam inconstitucionais por violação de normas constitucionais. Primeiro, pois violariam o princípio constitucional da continuidade. Segundo, pois tais artigos entrariam em choque com o direito fundamental de liberdade de comunicação, previsto no art. 5º, IX, da Constituição. Terceiro, pois vigoraria no direito brasileiro o "princípio da responsabilidade pessoal do agente apenado", sendo que uma norma sancionadora não poderia penalizar agentes que não tem relação com o fato apenado. Quarto, pois a suspensão causaria prestação deficiente do serviço colocado à disposição dos consumidores, fazendo com que houvesse punição "das camadas mais frágeis da relação de consumo".

1.9. Diante da aproximação das discussões jurídicas da ADPF 403 e da ADI 5.527, os ministros relatores Edson Fachin e Rosa Weber decidiram que "tendo em vista a íntima e ínsita relação entre a discussão posta na ADPF 403 e o objeto da ADI 5.527, é recomendável que o escopo da Audiência Pública então convocada seja ampliado de modo a comportar as questões constitucionais postas em ambas as ações". Como afirmou o STF, a Audiência Pública tem por objetivo discutir "tanto a constitucionalidade de dispositivos do Marco Civil da Internet impugnados quanto a possibilidade de suspensão do aplicativo WhatsApp por decisões judiciais".

1.10. Cumpre-se destacar, no que toca aos pedidos formulados na ADI 5.527, que o Partido Republicano postulou "a adoção da técnica de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei n. 12.965/14, de forma a afastar a sua aplicação aos aplicativos de troca de mensagens virtual; ou, por último, que se dê interpretação

conforme a tais dispositivos, condicionando-se, em consequência, a aplicação das sanções de suspensão temporária e de proibição do exercício das atividades somente após as sanções previstas no art. 12, I e II, mostrarem-se frustradas" (fl. 40 da petição). Tal tese foi combatida pela Advocacia Geral da União, que alegou que "impossibilitar o Estado, em toda e qualquer situação, de determinar a suspensão ou a proibição do exercício das atividades mencionadas no artigo 11 da Lei n. 12.965/14 corresponderia a sobrepor os interesses econômicos dos provedores de conexão e de aplicações de internet aos direitos fundamentais dos usuários da rede". Para a AGU, as disposições questionadas "se compatibilizam com a Carta Republicana, não havendo afronta a nenhum dos preceitos fundamentais suscitados pelo requerente como parâmetros de controle" (fl. 19 da petição).

1.11. Eis, em síntese, a problemática em torno da Audiência Pública convocada pelo Supremo Tribunal Federal. Seguramente, pode-se afirmar que as questões em discussão não são meramente relacionadas à tecnologia da informação (funcionamento da criptografia ponta a ponta, possibilidade de desabilitação da criptografia para usuários específicos, possibilidade de "espelhamento" de conteúdo de conversa protegida por criptografia), mas envolvem discussões jurídicas sobre a possibilidade da suspensão do aplicativo WhatsApp por decisões judiciais e a constitucionalidade dos dispositivos do Marco Civil da Internet que tratam das comunicações privadas.

**2 – O envolvimento do Idec nas discussões sobre bloqueio do WhatsApp e aplicação do Marco Civil da Internet**

2.1. O Instituto Brasileiro de Defesa do Consumidor tem monitorado, com bastante preocupação, o desenvolvimento jurisprudencial sobre bloqueio de aplicações e atuado no debate público – entre juristas e especialistas – sobre os modos de utilização das sanções previstas no Marco Civil da Internet.

2.2. É importante relembrar que o Instituto participou ativamente do processo de construção normativa da Lei nº 12.965/14, contribuindo em consultas públicas que culminaram na formulação do Projeto de Lei nº 2126/11, apresentado ao Congresso Nacional para garantir o acesso à internet como "direito essencial ao exercício da cidadania" e, além de

outros direitos, "a inviolabilidade e o sigilo das comunicações pela internet". O Idec envolveu-se diretamente, também, no processo de negociação política para aprovação do Marco Civil da Internet na Câmara dos Deputados, evitando retrocessos e modificações ao texto do projeto de lei. Durante o período de 2012 a 2014, o Instituto desenvolveu diversas campanhas de informação sobre a importância do Marco Civil da Internet e a necessidade de definição de direitos básicos para uso da internet no país.[2] Diferentes estudos acadêmicos documentam a participação de entidades civis como o Idec na definição das normas jurídicas relacionadas à privacidade, neutralidade de rede e liberdade de expressão na versão final do Marco Civil da Internet, aprovada em abril de 2014.[3]

2.3. Como é sabido, a Lei 12.965/14 assegura que o uso da internet no Brasil tem como fundamento o *respeito à liberdade de expressão* (art. 2º), ao lado de fundamentos basilares como "os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais" (inciso II) e a "livre iniciativa, a livre concorrência e a defesa do consumidor" (inciso V). No artigo 3º da legislação, há um núcleo duro principiológico, constituído de oito princípios que *devem disciplinar* o uso da internet no Brasil. Tais princípios são (*i*) garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal, (*ii*) proteção da privacidade, (*iii*) proteção dos dados pessoais, (*iv)* preservação e garantia da neutralidade de rede, (*v*) preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com padrões internacionais e pelo estímulo ao uso de boas práticas, (*vi*) responsabilização dos agentes de acordo com suas atividades, (*vii*) preservação da natureza participativa da rede,

[2] Em campanha para votação do PL 2126/11 na Comissão Especial em agosto de 2012, o Idec informava: "O Marco Civil da Internet no Brasil é uma das mais importantes e avançadas propostas sobre o uso da Internet no mundo. É ele quem vai estabelecer os princípios, valores, direitos e responsabilidades sobre o uso da rede no nosso país. Por isso, é um projeto de lei essencial para garantir a democracia e a liberdade na Internet. (...) Se aprovado, o Marco Civil vai estabelecer os direitos e deveres no ambiente virtual: garantirá a liberdade de expressão e a proteção da privacidade; estabelecerá claramente os direitos dos usuários; definirá a responsabilidade dos provedores; e colocará a neutralidade de rede como um princípio básicos da Internet no país, trazendo mais igualdade e evitando a discriminação na navegação dos internautas". Ver: http://www.idec.org.br/email_mkt/marcocivil/alerta-06-08-12.html

[3] MARQUES, Rodrigo Moreno; PINHEIRO, Marta Macedo. Informação e poder na arena da Internet. *Informação & Sociedade*, v. 24, n. 1, 2014; CRUZ, Francisco Carvalho de Brito. *Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet*. 2015. Dissertação de Mestrado. Universidade de São Paulo; RADOMSKY, Guilherme; SOLAGNA, Fabricio. Marco Civil da Internet: abrindo a caixa-preta da agenda de uma política pública, *Liinc em Revista*, v. 12, n. 1, 2016.

(*viii*) liberdade dos modelos de negócios promovidos na internet.

2.4. Há ampla literatura jurídica sobre o assim chamado "caráter civil"[4] desta legislação – que reverteu uma tendência histórica de criminalização de condutas na internet e de domínio das legislações penais em questões envolvendo uso da internet no país –, estruturada para reafirmar direitos constitucionais como inviolabilidade da intimidade e da vida privada e a inviolabilidade e sigilo do fluxo de comunicações de cidadãos pela internet, *salvo por ordem judicial, na forma da lei* (art. 7º, II). Como será explicado no terceiro tópico, que trata da doutrina jurídica sobre proteção dos registros, dos dados pessoais e da comunicação privada, a arquitetura jurídica de sanção aos provedores de aplicação foi pensada para *combater violações à privacidade*.

2.5. A problemática do bloqueio do WhatsApp, que teve início em fevereiro de 2015 a partir de um caso originário da Central de Inquéritos de Teresina (Piauí), iniciou no país uma importante discussão os limites de atuação do Judiciário em casos de descumprimento de ordens de transmissão de informações e dados de usuários e provedores de aplicações. Segundo documentação fornecida pelo portal *Bloqueios.info*, do centro de pesquisa independente InternetLab,[5] o juiz de Teresina tentou bloquear o WhatsApp por "reiterados descumprimentos de ordens judiciais" e pela alegação de que o WhatsApp não teria escritório no país. A decisão foi direcionada às provedoras de conexão, que, no entanto, reagiram em desacordo com a interpretação do magistrado. Como relatado pelo InternetLab, as empresas GVT, Embratel e Claro alegaram que a determinação não poderia ser cumprida porque constituiria "ato destituído de razoabilidade, pois impõe o bloqueio do acesso de uma infinidade de usuários às funcionalidades do aludido aplicativo, apenas para atender a pretensões de um procedimento investigatório cujo fim pode ser alcançado por meio de inúmeras outras medidas"[6].

2.7. O argumento da razoabilidade foi acompanhado da discussão sobre a

[4] LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil, in: LEMOS, Ronaldo; SALOMÃO LEITE, George. *Marco Civil da Internet*. São Paulo: editora Atlas, 2014, p. 3-11. VIANA, Ulisses, Liberdade de expressão, comunicação e manifestação do pensamento como princípios fundamentais do Marco Civil, in: LEMOS, Ronaldo; SALOMÃO LEITE, George. *Marco Civil da Internet*. São Paulo: editora Atlas, 2014, p. 127-146.

[5] http://bloqueios.info/pt/casos/exemplo-de-post-em-casos/

[6] Idem.

*proporcionalidade da medida*, a qual se liga umbilicalmente.[7] O Desembargador do Tribunal de Justiça do Piauí, Raimundo Costa Alencar, argumentou que (i) em hipótese alguma se justificaria a interrupção do acesso a todo um serviço; que (ii) não se pode paralisar um aplicativo usado por milhões de pessoas em prol de uma investigação com um número limitado de suspeitos; e que (iii) organismos policiais possuem outros meios de investigação criminal.

2.8. Quando o segundo bloqueio do WhatsApp ocorreu, em dezembro de 2015, em razão de uma decisão de uma juíza de São Bernardo do Campo, o Instituto Brasileiro de Defesa do Consumidor publicou nota técnica que ganhou razoável repercussão midiática. Para o Idec, o fato de juiz ter acatado o pedido do Ministério Público de exigir a "suspensão temporária" dos atos que envolvem "operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações por aplicações de internet" (art. 11, Lei 12.965/14) resultou em grave problema de "proporcionalidade da decisão à luz dos direitos consumeristas".

2.9. Reproduzimos, *in verbis*, a construção do raciocínio jurídico do Idec na referida nota técnica:

> "(...) o bloqueio do aplicativo [WhatsApp] colocou em evidência a necessidade de uma interpretação dos artigos 10 a 12 do Marco Civil da Internet que seja favorável ao interesse coletivo e aos consumidores no país. Afinal, se o artigo 12 afirma que é preciso considerar o 'princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção', a decisão de bloqueio do WhatsApp em todo o país é proporcional? O Instituto Brasileiro de Defesa do Consumidor entende que não.
>
> É preciso lembrar que o direito brasileiro define que a disciplina do uso da Internet tem como fundamento a liberdade de expressão, o exercíio da cidadania em meios digitais e a defesa do consumidor (Art. 2º, Lei 12.965/14). Esses princípios precisam ser levados em conta no momento de aplicação das sanções previstas no artigo 12 do Marco Civil da Internet. O Código de Defesa do Consumidor é muito claro ao apontar que a Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores (Art. 4º, CDC) e que é dever do Estado garantir padrões adequados de

[7] Evidentemente, só faz sentido afirmar que uma decisão é *proporcional* se ela se mostra *razoável*.

> qualidade, durabilidade e desempenho de serviços, incluindo as aplicações de internet como o WhatsApp.
>
> O bloqueio do WhatsApp para mais de 90 milhões de usuários brasileiros gerou enormes transtornos para milhares de prestadores de serviços que dependem dessa aplicação de internet como instrumento básico de comunicação. A suspensão temporária de todas as funções do WhatsApp pode ter gerado potenciais danos coletivos aos consumidores brasileiros, em clara ofensa ao Artigo 6º, inciso VI, do Código de Defesa do Consumidor, que garante o direito à prevenção de tais danos. A Justiça de São Paulo poderia ter utilizado medidas menos danosas aos consumidores brasileiros, como a cobrança de multa para o grupo econômico do Facebook, que detém o WhatsApp e possui sede em São Paulo e contas bancárias no país"[8].

2.10. Importante destacar que a ponderação com o direito consumerista raramente foi realizada nas decisões judiciais de bloqueio do WhatsApp – e esse é um ponto de crítica importante do Idec. O Instituto entende que a aplicabilidade das sanções previstas no art. 12 do Marco Civil da Internet exige que o agente decisório tenha dois cuidados procedimentais. Primeiro, que aplique as sanções de modo *gradativo*, valendo-se de advertência, multa pecuniária e obrigações de fazer em caráter coercitivo, exaurindo as possibilidades de cooperação internacional quando há empresas internacionais sujeitas às sanções. Segundo, que a "gravidade da falta" seja avaliada com a "gravidade da sanção", observando, precisamente, (i) as consequências da sanção a terceiros e (ii) o potencial lesão de direitos decorrente da medida sancionatória.

2.11. No caso em tela, isso resultaria em uma série de perguntas a serem levadas em consideração pelo agente decisório e justificadas em sua decisão. Primeiramente: (i) qual é a "falta" cometida pelo provedor de aplicação?; (ii) se não há viabilidade técnica de entrega de conteúdo de comunicações privadas após ordem judicial, por que o provedor de aplicação deveria ser punido?; (iii) qual a distinção, em termos de gravidade, entre impossibilidade técnica de cumprimento de ordem de interceptação de dados e "obstrução de justiça" em caráter doloso?

2.12. Além da demonstração da gravidade do suposto fato lesivo, o passo mais

[8] Instituto Brasileiro de Defesa do Consumidor. Nota Técnica sobre o Bloqueio do WhatsApp. 17 de dezembro de 2015. Disponível em: http://www.idec.org.br/pdf/nota-tecnica-bloqueio-whatsapp.pdf

importante do agente decisório é contrapor a sanção almejada com a gravidade de sanção para terceiros. No caso da escolha pela suspensão temporária das atividades de coleta de dados pessoais e de comunicação privada – hipótese prevista no art. 12, inciso III – , deve-se avaliar: (i) de que modo essa suspensão afeta terceiros não relacionados diretamente com o processo?, (ii) existe potencial de lesão de direitos decorrentes desta medida, ou ela é aplicada justamente para proteger direitos?

2.13. Nas decisões que geraram o bloqueio do WhatsApp, esses testes de ponderação não foram aplicados, motivo pelo qual decisões de primeira instância foram reformadas em instância superior. As reformas ocorreram pelo fato de que tais decisões não consideraram o *potencial lesivo da sanção aplicada a um provedor de aplicação para terceiros*, como a limitação do direito dos consumidores de obterem a continuidade de um serviço prestado, garantido no Código de Defesa do Consumidor, e a limitação da liberdade de expressão garantida pela Constituição Federal. Tais decisões também não avaliaram o impacto que tais bloqueios tiveram nas relações comerciais entre pessoas físicas e jurídicas. Em um contexto de agravamento da crise econômica, de explosão dos Micro Empreendedores Individuais e dos milhares de pequenos serviços prestados com auxílio do WhatsApp (*e.g.* entrega de refeições por pequenos marmiteiros, pedidos de entrega de documentos, acertos logísticos de operações empresariais), não se avaliou corretamente de que modo ininterrupções forçadas do WhatsApp poderiam causar prejuízos a milhares de pessoas.

2.14. Nos casos subsequentes de bloqueio do WhatsApp em 2016, o Idec defendeu a desproporcionalidade das decisões e as lesões causadas a milhões de consumidores no Brasil. Essa lesão aos direitos dos consumidores, à liberdade de expressão e à livre iniciativa provocou uma espécie de "curto circuito" na interpretação jurídica do Marco Civil da Internet. Isso pois a legislação sobre uso da internet *não tem como pilar principiológico a intercepção de comunicações*, mas sim a garantia constitucional da liberdade de expressão, a proteção dos consumidores e a liberdade de empreendimento e do uso social da internet. Mais importante: não há, na doutrina jurídica, justificativa para suspensão das atividades de coleta de dados de provedores de aplicação que não cooperam com autoridades policiais na entrega de comunicações privadas após ordem judicial. As sanções foram pensadas para aqueles que violam regras de privacidade e as obrigações

positivas relacionadas à coleta e tratamento de dados pessoais.

**3 – A doutrina sobre "proteção aos registros, aos dados pessoais e às comunicações privadas" no Marco Civil da Internet: sanção por violação de obrigações de proteção do consumidor**

3.1. A Advocacia Geral da União, em petição disponível no processo da Ação Direta de Inconstitucionalidade 5.527, foi bastante feliz em reconhecer o posicionamento do Comitê Gestor da Internet (CGI.br) sobre a correta interpretação do art. 12, inciso III e IV da Lei n. 12.965/14. Para a AGU, o Marco Civil da Internet, no capítulo onde se situa o art. 12, possui normas que "tratam justamente de vedar a disponibilização indevida dos registros, dados e comunicações dos usuários, em homenagem às garantias de intimidade e privacidade dos usuários da internet" (fl. 15). Em consonância com o "espírito de elaboração" do MCI, a petição da AGU afirma que:

> "(...) o Comitê Gestor da Internet no Brasil – CGI.br, cujas recomendações serviram de inspiração para a elaboração do projeto que originou a lei questionada, esclareceu, por meio de nota referente à decisão judicial que suspendera o aplicativo WhatsApp no território nacional, que o artigo 12 da Lei 12.965/14 prevê um conjunto de sanções 'estritamente dirigidas aos atores que não cumpram as regras relativas à proteção de registros, aos dados pessoais e às comunicações privadas'. Ainda de acordo com o comitê referido, 'o art. 12 da Lei 12.965/14 autoriza tão somente a suspensão temporária das atividades que envolvam os atos elencados expressa e taxativamente no art. 11 do mesmo diploma legal: 'a operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet'. Nesse sentido, o teor do art. 12 do Marco Civil da Internet não se refere à aplicação extensiva da lei para que se determine a suspensão total e irrestrita das atividades de empresas prestadoras de serviços e aplicações Internet" (fl. 16).

3.2. A doutrina jurídica que se dedica à sistematização das normas presentes na Lei 12.965/14 é uníssona no que toca à consolidação do direito constitucional à privacidade – assegurado por diversas decisões do Supremo Tribunal Federal – no Marco Civil da Internet.

Há uma lógica por trás do encadeamento de normas nesta lei. O art. 7º, por exemplo, define os direitos básicos dos usuários de internet no país e dá especial atenção à proteção de dados pessoais, a inviolabilidade e sigilo "do fluxo de suas comunicações pela internet" (o modo como as comunicações são trafegadas por meio comutação de pacotes em protocolos TCP/IP) e o sigilo "de suas comunicações privadas armazenadas" (o modo como as comunicações são registradas em bancos de dados e servidores). Em aproximação às regras do Código de Defesa do Consumidor de clareza na informação e boa-fé, o Marco Civil da Internet estipula que um usuário de uma aplicação de internet – por exemplo, o WhatsApp – tem o direito de receber "informações claras e completas dos contratos de prestação de serviços com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações da internet" (art. 7º, VI). Tem, também, o direito de que o provedor de aplicações forneça a terceiros seus dados pessoais, "inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso ou nas hipóteses previstas em lei" (art. 7º, VII). O Marco Civil da Internet também garante que as informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais só podem ser utilizadas para finalidades que (i) justifiquem sua coleta, (ii) não sejam vedadas pela legislação, (iii) estejam especificadas nos contratos de prestação de serviços ou em termos de uso.

3.3. Em artigo doutrinário dedicado ao sigilo das comunicações eletrônicas diante do Marco Civil da Internet, o jurista João Azeredo, mestre pela Universidade de São Paulo, retoma as discussões constitucionais sobre sigilo das comunicações – especialmente no âmbito do Mandado de Segurança 21.729,[9] cujo acórdão foi publicado em 19/10/01; e no Recurso Extraordinário 418.416,[10] cujo acórdão foi publicado em 19/12/06 – e questiona o entendimento firmado de que o inciso XII do art. 5º da Constituição Federal protegeria "apenas a comunicação dos dados e que o sigilo sobre os dados propriamente não é absoluto". Segundo nota Azeredo, "apesar de ter sido limitado o escopo da proteção dada pelo inciso

[9] O MS 21.729 discutiu a legitimidade do Ministério Público para requerer informações sobre empréstimos feitos pelo Banco do Brasil, bem como a existência ou não de sigilo sobre essas informações.
[10] O RE 418.416 discutiu a admissibilidade de provas obtidas mediante análise pericial de dados gravados em microcomputador aprendido em sede de empresa diante de mandado de busca e apreensão regularmente expedido pelo juízo competente.

XII, os ministros do Supremo Tribunal Federal não enfrentaram, de forma direta, se o sigilo da comunicação de dados também se aplica ao objeto dessa comunicação antes e após a sua transferência, tendo se limitado a fazer a distinção entre o que denominaram 'dados em si mesmos' e 'comunicação de dados'"[11]. Para Azeredo, o STF não estabeleceu que a proteção da comunicação está limitada ao momento em que os dados estão em fluxo, pois esse ponto não foi enfrentado diretamente e, nos casos julgados pela Corte, não se estava diante de "comunicações privadas armazenadas, mas de dados atinentes à atividade de sociedades que estavam armazenados em computadores"[12]. De acordo com o jurista, o constituinte reconheceu a importância da proteção do sigilo das comunicações, estipulando de forma expressa os requisitos especiais para que ele seja afastado. Para Azeredo, "não nos parece ser possível defender que o inciso protege, tão somente, o efêmero momento em que os dados estão em fluxo, uma vez que a liberdade de omitir pensamento [liberdade de negação que garante ao indivíduo a discricionariedade de não emitir pensamento] é igualmente violada caso se tenha acesso às comunicações antes de saírem da esfera de controle de seu remetente ou após entregue ao seu destinatário"[13]. Assim, é preciso reconhecer uma falha conceitual e argumentativa no entendimento jurisprudencial de que o inciso XII, art. 5º, não se aplica às comunicações de dados que não estão em fluxo. Como argumenta Azeredo, "diante do bem jurídico que se visa a proteger, a quebra do sigilo dos dados, quando não estão em fluxo, é igualmente – ou até mais – invasiva"[14].

3.4. O Marco Civil da Internet demonstrou enorme preocupação do legislador ordinário em dar proteções mais concretas às inviolabilidades previstas nos incisos X e XII, do artigo 5º, da Constituição Federal. Conforme argumentado por Azeredo, o Marco Civil orienta-se pela preocupação com a privacidade e o regramento das hipóteses em que registros de acesso a aplicação da Internet podem ser obtidos por ordem judicial:

"(...) em que pese a garantia constitucional dessas esferas da vida do

[11] AZEREDO, João. Sigilo das comunicações eletrônicas diante do Marco Civil da Internet: in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia. *Direito & Internet III: Marco Civil da Internet*. Tomo II. São Paulo: Quartier Latin, 2014, p. 221.
[12] *Idem, ibidem*, p. 222.
[13] *Idem, ibidem*, p. 223.
[14] *Idem, ibidem*, p. 225.

> indivíduo, o Marco Civil da Internet, em alguma medida, supriu a ausência de estipulação legal de meios adequados para dar efetividade prática aos dispositivos constitucionais. Assim, o artigo 3º estabelece, como princípios, a proteção da privacidade (inciso II) e dos dados pessoais (inciso III), enquanto no artigo 7º, como já dito, em seus incisos II e III, estabeleceu como direitos do usuários de internet a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" (inciso II) e a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (inciso III). Além disso, a seção II, do capítulo III (artigos 10 a 12), estabelece as regras de proteção dos registros de acesso à internet e os registros de acesso a aplicação de internet, impondo a necessidade de obtenção de ordem judicial para que esses dados sejam revelados. Nesse sentido, o artigo 22 estabelece os requisitos do pedido para a obtenção desses dados, entre os quais estão a indicação dos indícios da existência de ilícito, bem como a delimitação do período determinado sobre os quais os registros estão sendo requeridos. Há, ainda, dispositivos que tratam de obrigações legais que devem ser observadas no processamento de dados pessoais, bem como outros que tratam da vedação de determinadas condutas por parte dos provedores de acesso e de aplicações de internet que poderiam implicar violação à vida privada e à intimidade.
> (...)
> Conforme previsto nos artigos 10 a 12 e 22, do Marco Civil da Internet, no que tange aos registros de conexão e acesso a aplicações de internet, o legislador não se limitou a impor a necessidade de ordem judicial para que o sigilo seja afastado, sendo necessário, também, indicar 'fundados indícios da ocorrência de ilícito' (inciso I, do artigo 22), 'justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória' (inciso II) e 'período ao qual se referem os registros' (inciso III). Além disso, a lei prevê regulamento que tratará de padrões de procedimentos de segurança que deverão ser adotados para proteger esses registros (parágrafo 4º do artigo 10º) e **sanções para o caso de descumprimento das obrigações** (artigo 12)".[15]

3.5. Importante notar que as sanções previstas no artigo 12 do Marco Civil da Internet são decorrentes de falhas em obrigações positivas assumidas por provedores de conexão e provedores de aplicações que coletam e processam dados pessoais e comunicações privadas. Como é evidente, os artigos 10 a 12 encontram na seção de *proteção dos direitos ao*

[15] AZEREDO, João. Sigilo das comunicações eletrônicas diante do Marco Civil da Internet: in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia. *Direito & Internet III: Marco Civil da Internet*. Tomo II. São Paulo: Quartier Latin, 2014, p. 228-229.

*usuário da internet.* Como argumentado pelo Laboratório de Pesquisa Direito Privado e Internet (LAPIN), em parceria com o Instituto Beta de Internet e Democracia, em petição protocolada na ADI 5.527, "as sanções previstas no art. 12, que remete à inobservância de condutas descritas nos arts. 10 e 11, somente *devem ser aplicadas como forma de punição da empresa que não promove o adequado gerenciamento, tratamento e manipulação dos dados do usuário*" (documento 27, f. 11). Essa compreensão é fundamental no julgamento da ADPF 403 e da ADI 5.527: a sistemática das sanções do artigo 12 foi construída para proteger o usuário quando uma empresa falha em manter suas obrigações legais de proteção da privacidade do usuário. Essa interpretação é corroborada por Cláudio de Lucena Neto em artigo publicado no Observatório do Marco Civil da Internet:

> "Em primeiro lugar, sendo a determinação de suspensão do serviço fundamentada nos termos do artigo 12, inciso III do MCI, é inevitável concluir que ela está errada. Vejo um exagero na representação ao CNJ, numa tentativa de transformar o incidente em ilícito administrativo, porque reconheço que há de fato uma divergência legítima, uma expectativa de poder geral de cautela, e sobretudo a intenção de buscar efetividade de uma decisão judicial, mas que o fundamento está absolutamente equivocado, isto sem dúvida está. A seção em que o dispositivo está inserido cuida exatamente do inverso, ou seja, da violação do sigilo de dados pessoais. As penalidades do Artigo 12, portanto, em hipótese alguma se aplicam em caso de negativa em fornecer dados. Ao contrário, só poderiam ser aplicadas em caso de fornecimento indevido destes dados. Há uma distorção do sentido da norma e um erro técnico indiscutível"[16].

3.6. O Instituto Brasileiro de Defesa do Consumidor entende que os mecanismos de sanção do artigo 12 são necessários para proteger a privacidade e os dados pessoais dos usuários de internet no Brasil, porém *devem ser aplicados de forma correta*. Um exemplo de correta aplicação dessas sanções, no entendimento do Idec, seria a punição ao WhatsApp por violações legais na implementação de seus termos de uso em agosto de 2016. Como argumentado pelo Idec no relatório *Consentimento Forçado?*[17], o WhatsApp falhou em

[16] http://omci.org.br/jurisprudencia/97/suspensao-do-bloqueio-do-whatsapp/
[17] IDEC. *Consentimento Forçado?: uma avaliação sobre os termos de uso do WhatsApp e o Marco Civil da Internet*. São Paulo: Idec, 2016. Disponível em: https://www.idec.org.br/pdf/relatorio-whatsapp-termos-de-uso.pdf

"garantir a escolha livre e informada sobre os processos de coleta, processamento e repasse para outras empresas de dados relacionados ao modo de uso do WhatsApp, registros de conexão e geolocalização". Houve violação ao artigo 7º, inciso XII, do Marco Civil da Internet, pois os usuários eram mal informados e não tinham o poder de escolha (via *opt-in*) sobre como desejavam compartilhar tais dados com o conjunto de empresas integrantes do grupo Facebook Inc. Como identificou o Idec durante o episódio dos novos termos de uso, nesse caso houve clara violação ao Marco Civil da Internet.[18] Neste caso, faria sentido a aplicação conjunta dos artigos 11 e 12 do Marco Civil da Internet. Trata-se de operação de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações" (art. 11), feito por um provedor de aplicação de internet, em desrespeito aos direitos à privacidade e proteção dos dados pessoais (art. 7º). Nesse caso, seria correta a aplicação do art. 12, uma vez respeitado o gradualismo sancionatório previsto no texto de lei:

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

[18] Argumentamos no relatório: "No caso do WhatsApp, a violação do Marco Civil parece ocorrer justamente neste ponto. O WhatsApp pretende fazer o repasse de dados pessoais a terceiros. Isso está expresso nos textos oficiais da empresa. Ela circulará os dados dos usuários do WhatsApp para empresas especializadas em publicidade comportamental e outros negócios. Independentemente das empresas fazerem parte de um mesmo conglomerado empresarial (*Facebook Inc.*), devemos interpretar esse repasse como *para terceiros* – pois as próprias finalidades do tratamento de dados serão outras (não mais relacionadas à 'melhoria da experiência de uso', mas outros usos comerciais no campo de 'análise da dados'). O consentimento, no entanto, não é livre. A única opção de escolha livre e informada é a do compartilhamento de informações da agenda telefônica para as empresas do grupo Facebook Inc. Esse tipo de dado, no entanto, é apenas a ponta do iceberg. O que realmente importa na mudança dos termos de uso do WhatsApp é o conjunto de informações relacionados a uma pessoa identificável – os dados relacionados ao modo de uso do aplicativo, os dados de geolocalização, o endereço IP, os modos de interação com outros usuários, os registros de conexão de aplicativo, entre outros. Para a coleta *desses dados* não há 'consentimento livre', mas sim 'consentimento forçado'. Ao mudar radicalmente seu modelo de negócios (saindo da lógica de comunicação 'pessoa para pessoa' para 'empresa para consumidor'), o WhatsApp deveria obter o consentimento livre, expresso e informado para a coleta de dados que não coletava antes. Além de ser uma quebra da expectativa legítima do consumidor com relação à privacidade, o modo como os termos de uso foram impostos falham ao passar no teste do art. 7º, inciso XII". IDEC. *Consentimento Forçado?: uma avaliação sobre os termos de uso do WhatsApp e o Marco Civil da Internet*. São Paulo: Idec, 2016, p. 18-19.

> 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".

3.7. Assim, não restam dúvidas de que o Marco Civil da Internet impôs um conjunto de obrigações às empresas – provedores de conexão e provedores de aplicações – relacionados à privacidade, proteção de dados pessoais e sigilo das comunicações privadas. É justamente a *falha em respeitar essas obrigações* que pode dar ensejo à aplicação das sanções previstas no art. 12, que remete expressamente as "infrações às normas previstas nos arts. 10 e 11". Deste modo, o Instituto Brasileiro de Defesa do Consumidor entende que o art. 12 possui uma importantíssima função na defesa de direitos dos usuários de internet no Brasil. Não deve prosperar o pedido formulado na ADI 5.527 de que há inconstitucionalidade desse dispositivo legal. O que o Supremo Tribunal Federal deve afirmar, em nosso entendimento, é que os mecanismos sancionatórios do art. 12 foram projetados para a proteção dos direitos dos usuários de internet e não podem ser utilizados para punição de um provedor de aplicação que possui impossibilidade técnica demonstrada para cumprimento de ordem judicial de interceptação e repasse de comunicações privadas feitas por meio do provedor de aplicação.

3.8. Discutiremos, a seguir, de que modo o funcionamento da criptografia ponta-a-ponta relaciona-se com os direitos assegurados no Marco Civil da Internet, especialmente a liberdade de expressão e a garantia da privacidade no uso da internet. Não discutiremos a possibilidade ou impossibilidade técnica de desabilitação da chave de criptografia de apenas alguns usuários, pois acreditamos que o ônus de demonstração técnica cabe à própria empresa WhatsApp e peritos com formação técnica especializada. O Idec entende que a aplicação de técnicas de "desabilitação" ou "quebra" criptografia para fins de intercepção de mensagens de determinados indivíduos sob investigação, por autoridades de investigação da Polícia e do Poder Judiciário, coloca em risco a segurança e privacidade de milhões de cidadãos de forma desproporcional, em clara violação ao art. 7º, II, da Lei 12.965/2014 (direito à inviolabilidade e sigilo do fluxo das comunicações pela internet) e ao direito constitucionalmente assegurado

de privacidade. Conforme argumentaremos, investigações criminais podem ser conduzidas a partir do conjunto de metadados coletados no WhatsApp, que revelam um rico conjunto de informações sobre os indivíduos quando analisados em conjunto.

## 4 – O funcionamento da criptografia ponta-a-ponta e sua relação com os direitos assegurados no Marco Civil da Internet

4.1. Em uma das decisões que demandou o bloqueio do WhatsApp no Brasil, a magistrada pediu à empresa a criação de uma "solução tecnológica" que permitiria que as autoridades tivessem acesso às mensagens em tempo real.[19] Esse tipo de proposta motivou o ministro Edson Fachin a formular algumas questões específicas sobre funcionamento da criptografia ponta-a-ponta, a possibilidade de "desabilitar a criptografia" para interceptação de usuários específicos mediante ordem judicial fundamentada e a possibilidade de soluções técnicas de "espelhamento" do WhatsApp utilizado em telefones celulares para computadores ou outros dispositivos. Entendemos que é preciso um mínimo de esclarecimento sobre o funcionamento da criptografia para que o debate possa avançar no julgamento da ADPF 403 e da ADI 5.527. Sem a pretensão de exaurir tecnicamente o tema, formularemos alguns conceitos básicos sobre criptografia assimétrica e criptografia ponta-a-ponta.

4.2. A criptografia é, em geral, um processo de cifragem de informação por meio de chaves numéricas[20] sem as quais não é possível analisar o conteúdo da informação cifrada. Na comunicação, a definição do conceito engloba as técnicas utilizadas por duas ou mais entidades (A e B) para transformar uma informação legível em ilegível para um agente externo atacante (C). Desta maneira, codifica-se a informação de modo que apenas o emissor

---

[19] "Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (como acontece com a interceptação de conversações telefônicas), antes de implementada a criptografia.". Ver o especial do InternetLab, publicado no jornal O Estado de São Paulo, sobre a (in)viabilidade técnica e política desta solução: http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/

[20] Em termos gerais, a chave é uma "sequência de símbolos que controla a operação de uma transformação criptográfica".

e o receptor possam decifrá-la. O elemento central que possibilita a comunicação cifrada entre as entidades A e B é a chave criptográfica. Como apontado na definição de Rafael Araújo, do Instituto de Matemática e Estatística (IME/USP), uma chave é o que "controla a operação de uma transformação criptográfica". A chave possui, então, o poder de criptografar e descriptografar a mensagem, tornando-a assim legível apenas para as entidades A e B e ilegível para a entidade C.

4.3. Também conhecida como criptografia de chave secreta, o conceito da criptografia simétrica reside na utilização de uma mesma chave criptográfica para encriptação e decriptação da mensagem, sendo essa compartilhada entre as partes que desejam emitir e receber as informações. O processo é esquematizado na figura seguinte:

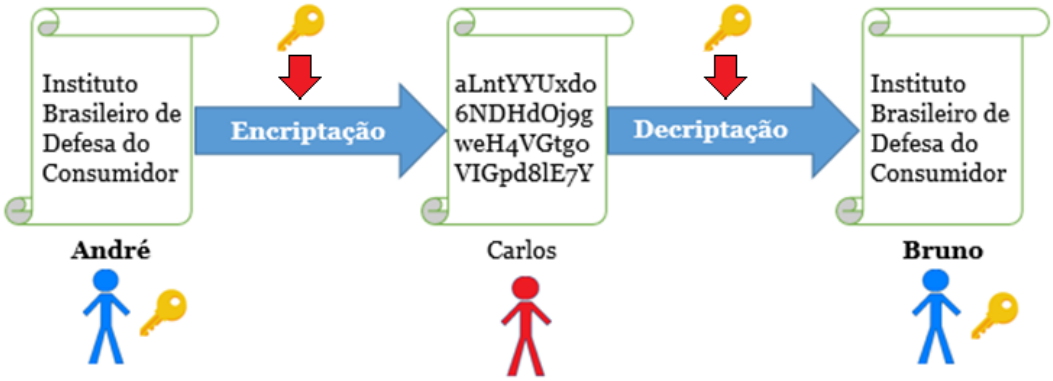



Figura 1: Encriptação Simétrica

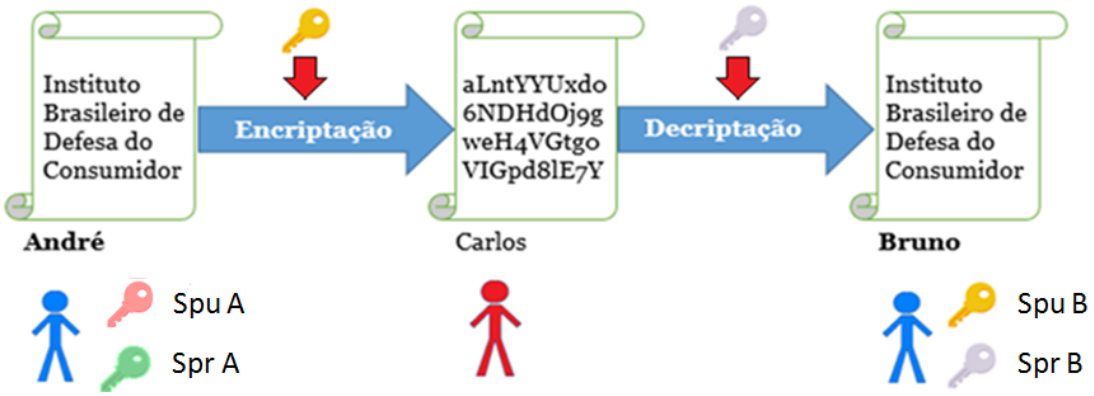
4.4. No esquema apresentado, André (A) utiliza sua chave para cifrar e enviar para Bruno (B) uma mensagem com o conteúdo "Instituto Brasileiro de Defesa do Consumidor". Carlos (C), o agente externo, ao tentar interceptar a mensagem, encontra o conteúdo ilegível, já que não possui a chave para decifrá-la. Bruno (B), ao receber a mensagem, a decifra utilizando a mesma chave que André (A) possui, sendo possível assim ler a mensagem que Bruno escreveu. De acordo com a cartilha de segurança do CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), a criptografia simétrica apresenta certos riscos a segurança. Visto que tanto a entidade emissora (A) quanto a receptora (B) deve possuir a mesma chave para efetividade da comunicação,

ambas necessitam de um canal de comunicação seguro para compartilhar a chave, tarefa que se torna complicada em um ecossistema como a Internet. Entretanto, ao garantir que a chave esteja apenas sob propriedade das pessoas pretendidas e que esteja compartilhada por um canal seguro, a confidencialidade da comunicação é garantida. Além disso, outra qualidade deste modelo de criptografia é sua velocidade, uma vez que ela necessita apenas de um processo de verificação para que a mensagem seja revelada. A confidencialidade deste tipo de criptografia reside muito mais no cuidado de seus usuários do que na tecnologia em si. Pela ótica dos princípios recomendados, a criptografia simétrica garante a confidencialidade e integridade da mensagem, uma vez que em seu trânsito do emissor ao destinatário ela se mantém escondida e ao ser decifrada se mantém da mesma forma que o usuário emissor enviou. Entretanto, pelo fato da chave ser única e, dessa forma, podendo ser utilizada por qualquer um que tenha em sua propriedade, os princípios da autenticação e irretratabilidade não são atendidos, já que *não existe garantia de quem seja o usuário emissor e permitindo que esse mesmo usuário possa negar a autoria de uma mensagem*. Dessa forma, as qualidades da criptografia simétrica são sua velocidade, simplicidade e eficácia. Já os defeitos são sua segurança e não possibilidade de autenticação, uma vez que qualquer agente externo que tiver acesso a chave pode se passar por uma pessoa autorizada.

4.5. A criptografia assimétrica foi criada com o intuito de resolver o problema de compartilhamento de chaves seguro que a criptografia simétrica possui. A grande questão era encontrar um método de compartilhamento de chaves onde as duas entidades não estivessem próximas fisicamente. O primeiro modelo de criptografia assimétrica foi idealizado no artigo *New Directions of Cryptography* (1976).[21] A principal diferença da criptografia simétrica a utilização de duas chaves por cada usuário: uma chave pública e uma chave privada. A chave pública, como próprio nome sugere, é acessível para qualquer agente externo, enquanto a chave privada é apenas acessível ao usuário que a possui. A chave pública e privada de ambos as entidades são utilizadas no processo de criptografia, no qual a privada da entidade A

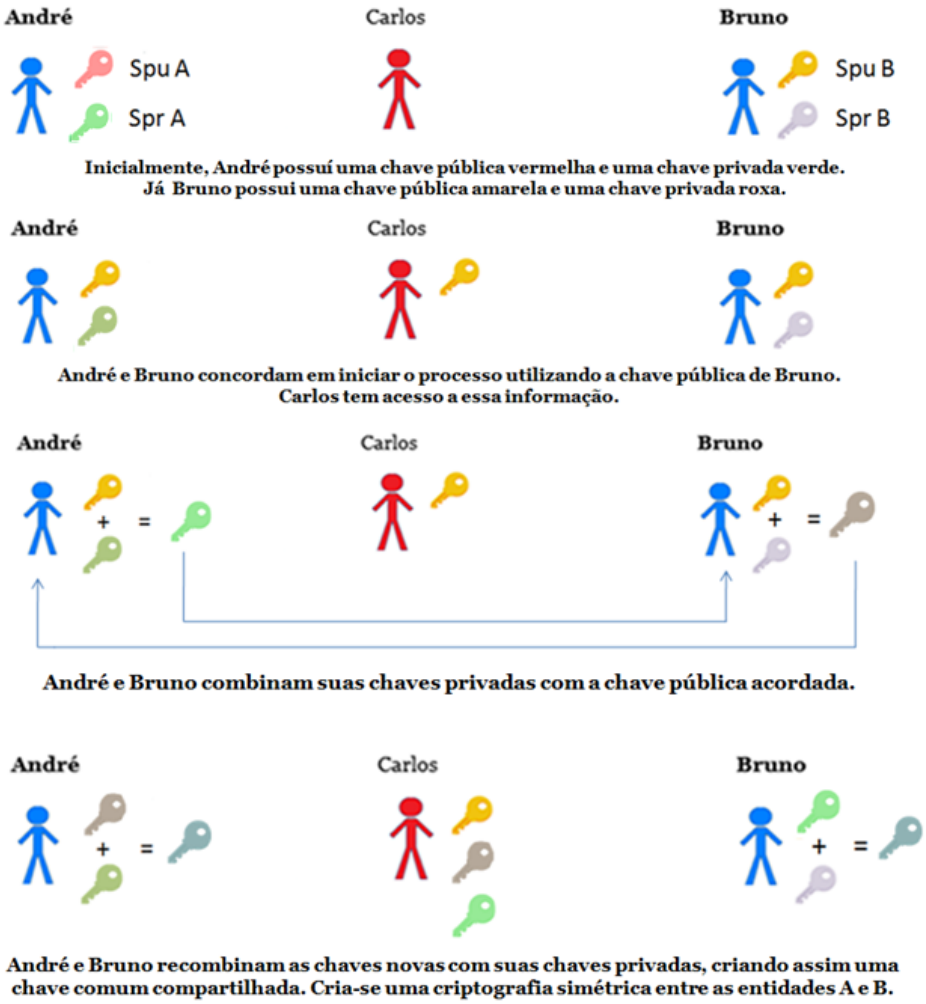
[21] DIFFIE, Whitfield; HELLMAN, Martin. New directions in cryptography. *IEEE transactions on Information Theory*, v. 22, n. 6, p. 644-654, 1976. Disponível em: http://math.boisestate.edu/~liljanab/MATH308/NewDirectionsCryptography.pdf ("the best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else").

apenas pode ser utilizada para descriptografar. No modelo mais simples, a mensagem que deseja ser enviada é criptografada com a chave pública de um usuário, que apenas poderá ser "descriptografada" utilizando-se de sua chave privada. Como exemplo, caso André (A) queira enviar uma mensagem para Bruno (B), André utiliza a chave pública de Bruno (Spu B) para criptografar sua mensagem e envia-la para Bruno, que ao recebe-la, descriptografa utilizando sua chave privada (Spr B). O mesmo processo se aplica caso Bruno queira enviar uma mensagem para André. O processo é ilustrado na figura seguinte:




4.6. Entretanto, esse modelo simples não atende o princípio da autenticidade e da irretratabilidade do emissor, visto que qualquer agente externo poderia criptografar uma mensagem se utilizando das chaves públicas das entidades legítimas. No mesmo artigo de Diffie e Hellman, os autores explicitam como resolver esse problema através de um modelo de troca de chaves. O processo se inicia quando a entidade A deseja enviar uma mensagem criptografada para a entidade B com o intuito de evitar que o agente externo C possa decifrá-la. Ambas concordam em utilizar uma mesma chave pública, de qualquer um dos dois agentes. Cada entidade combina sua chave secreta com esta chave pública escolhida, criando uma chave compartilhada e em seguida enviando-a para a outra entidade. Após esse compartilhamento, cada entidade combina esta chave compartilhada com sua chave secreta novamente, criando assim um chave compartilhada final, inacessível para qualquer agente externo. Este mecanismo é a solução para o compartilhamento seguro da chave criptográfica, além de garantir a autenticidade e irretratabilidade do emissor. Para decifrar uma mensagem no exemplo da criptografia simétrica, o agente externo precisa apenas descobrir a chave utilizada pelas entidades. Já na modalidade assimétrica, o agente externo possui apenas um dos fatores para decifrar a mensagem, a chave pública. Para descobrir a solução, o agente externo *precisaria possuir uma chaves privadas utilizadas pelas entidades*. O exemplo mais

utilizado para simplificar este raciocínio é imaginar as chaves como cores. Para início da ilustração, colocamos que André (A), possua uma chave pública de cor vermelha (Spu A) e uma chave privada de cor verde (Spr A). Já Bruno (B) possui uma chave pública de cor amarela (Spu B) e uma chave privada de cor roxo (Spr B). Ambos entram e em acordo para utilizar a chave pública de Bruno para iniciar o procedimento. André "mistura" sua chave privada, de cor verde, com a chave pública de Bruno, de cor amarela, criando assim um verde-claro. Bruno, por sua vez, "mistura" sua chave privada, de cor roxo, com sua própria chave pública, de cor amarela, criando assim a cor marrom. Ambos trocam suas "misturas" e as combinam novamente com suas chaves privadas, criando assim uma chave única de cor azul, que será utilizada de forma simétrica entre as duas entidades. O processo está ilustrado na figura abaixo:



4.7. Ao final do processo, cria-se uma criptografia simétrica, na qual a chave é compartilhada entre as entidades André e Bruno. Como observado na imagem, ainda que o agente externo Carlos tente interceptar as comunicações entre André e Bruno, ele não poderá ser capaz de determinar a chave que media a comunicação entre André e Bruno. Outra vantagem deste sistema, de acordo com a literatura especializada, é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens. Já a *criptografia ponta a ponta é um híbrido da modalidade de criptografia assimétrica e assimétrica*, utilizada comumente em aplicativos de mensagem como WhatsApp, Messenger, Signal,[22] Telegram[23] e Viber[24]. O intuito desse adereço é manter a privacidade das comunicações dos usuários, permitindo apenas que os mesmos possam ter acesso ao conteúdo das mensagens e impedindo os chamados ataques "man-in-the-middle" .

4.8. Especificamente, a criptografia do WhatsApp funciona como um "Centro Destribuidor de Chaves (CDC)", na terminologia de Stallings.[25] De acordo com o autor, o funcionamento do CDC se baseia em uma hierarquia de chaves. A comunicação entre os usuários finais é feita por uma chave de sessão efêmera, a qual é descartada ao final da conversa. A chave de sessão é transmitida de forma encriptada através de um modelo assimétrico de criptografia, composto pelo usuário e o servidor do aplicativo. De acordo com o documento técnico feito pela própria empresa, ao se instalar o aplicativo, é gerado um par de chaves público-privado para comunicação com o servidor do WhatsApp. Estas chaves serão utilizadas para confecção da *chave de sessão* e para identificação e autenticação dos usuários. Ao iniciar uma conversa, é gerada uma chave de sessão orientada pela Protocolo Signal. De forma simplificada, o Protocolo Signal funciona da seguinte forma: cada participante de uma conversa no WhatsApp possui uma chave de identidade (*long-term*

[22] Ver: http://www.techtudo.com.br/noticias/noticia/2015/11/signal-app-de-mensagens-super-seguro-chega-para-android.html
[23] Ver: https://core.telegram.org/api/end-to-end
[24] Ver: https://support.viber.com/customer/portal/articles/2017401-viber-security-faq
[25] STALLINGS, William. *Criptografia e segurança de redes: princípios e práticas*. Pearson Prentice Hall, 2008.

*identity key*) que é utilizada para criar uma chave efêmera. Esta chave efêmera é trocada entre membros utilizando o método de "troca de chaves de Diffie-Hellman" explicado anteriormente. O segredo compartilhado desta troca de chaves é utilizado para gerar três chaves para cada participante (uma chave do emissor, uma chave do receptor e o Código de Autenticação de Mensagem – CAM). O Código de Autenticação de Mensagem confirma a autenticidade e integridade da mensagem e é incluído em toda mensagem transmitida. Os CAMs são subsequentemente derivados da chave compartilhada garantindo que a mensagem tenha sido enviada pelo emissor. Esse processo, segundo a literatura especializada, "garante a integridade da mensagem intacta, ao passo que a autenticidade do emissor da mensagem que a originou possa ser posteriormente negada"[26].

4.9. Conforme informado pelo centro de pesquisa InternetLab, o cientista da computação Tobias Boelter sustenta que a criptografia forte ponta-a-ponta faz com que se torne impossível, para o WhatsApp, decifrar o conteúdo das mensagens enviadas pelo aplicativo.[27] Para Boelter, existiriam duas alternativas técnicas para implementar uma solução do tipo "man-in-the-middle", mas essas soluções passariam por fragilizar a segurança do sistema, destruir a confiança dos usuários no WhatsApp e colocar um grande número de pessoas em situação potencial de risco. De acordo com o especialista ouvido pelo InternetLab:

> "Há duas saídas que permitiriam que o WhatsApp encaminhasse o conteúdo de futuras mensagens para o Estado. Uma diferença fundamental entre a interceptação nesse caso e a interceptação "clássica" é que as pessoas que estão sendo investigadas vão conseguir descobrir se estão sendo vigiadas ou se já foram vigiadas antes, caso tenham conhecimento técnico suficiente. [Essas duas saídas, entretanto, exigiriam ou que a empresa se dispusesse a atuar como intermediário no repasse das mensagens para o Estado, burlando seu próprio sistema de criptografia, ou modifique o funcionamento técnico do aplicativo.]. A primeira saída é uma técnica conhecida como ataque do tipo "man-in-the-middle". Para a criptografia entre duas partes funcionar, elas devem trocar suas chaves públicas (*public keys*). O WhatsApp faz essa troca de chaves para você. Nesse processo, o aplicativo poderia decidir dar para as partes a chave privada e pessoal do WhatsApp em vez da que seria a correta. A partir daí, o WhatsApp conseguiria receber todas as

[26] RASTOGI, Nidhi; HENDLER, James. *WhatsApp Security and the Role of Metadata in Preserving Privacy*, 2016, p. 3. Disponível em: https://arxiv.org/ftp/arxiv/papers/1701/1701.06817.pdf

[27] Ver entrevista completa em: http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/

> mensagem que as duas partes enviassem uma para a outra, recriptografa-las com a chave correta e fingir que nada aconteceu. (...) A segunda saída é uma técnica que exigiria modificar o aplicativo para que ele mandasse (algumas) mensagens para o Estado além de enviá-las para o destinatário original. O WhatsApp poderia implementar esse "recurso" da mesma forma que fez com a criptografia de ponta-a-ponta: publicando uma versão nova do aplicativo nas loja de aplicativos (AppStore e outras). Isso seria a única alternativa técnica para o WhatsApp conseguir armazenar o conteúdo das mensagens. Mesmo assim, um usuário habilidoso ainda conseguiria descobrir se o seu aplicativo estiver encaminhando suas mensagens para o Estado. (...) A segunda saída [descrita acima], que envolve modificar o aplicativo em si, destruiria a confiança dos usuários no WhatsApp, pois eles estariam violando o compromisso de não serem capazes de ler as mensagens. Em suma, voltaríamos ao estágio no qual o WhatsApp não utilizava criptografia de ponta-a-ponta. Governos repressivos, empregados do WhatsApp com intenção maliciosa e hackers seriam capazes de invadir a infraestrutura do aplicativo e poder ler mensagens com conteúdo privado e sensível usando os mesmos mecanismos que o Estado usaria com uma ordem judicial legítima para investigar.[28]

4.10. O Instituto Brasileiro de Defesa do Consumidor entende que a *criptografia ponta-a-ponta é extremamente benéfica para o consumidor* e fortalece os direitos assegurados no Marco Civil da Internet.[29] Há, para além da privacidade assegurada constitucionalmente no Brasil, uma ampla conexão da criptografia com os direitos humanos. O Relator Especial da ONU, David Kaye, por meio do *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, defende que a privacidade do conteúdo de comunicações obtida por meio da criptografia funciona como um "portão de entrada" ao exercício da liberdade de expressão, estando os dois interligados.[30] É a privacidade que garante segurança aos indivíduos de que o conteúdo de suas comunicações está sendo recebido apenas pelos destinatários pretendidos, sem interferência ou alteração. Especialmente consideradas as informações possivelmente obtidas sobre a vida de um indivíduo a partir da análise apenas de seus metadados, "o anonimato tem um papel crítico em

[28] Entrevista disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/
[29] Ver nota técnica de abril de 2016: http://www.idec.org.br/pdf/criptografia_whatsapp.pdf
[30] Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*. 2015. pp. 7.

garantir a segurança de comunicações"[31]. Nesse sentido, é destacado também o papel crítico de empresas que armazenam dados, defendendo-se que haja um compromisso com criptografia e anonimato para a maior segurança de seus usuários. Diante disso, qualquer restrição a essa privacidade deve ser vista de maneira extremamente restritiva, conformando-se a testes estritos de necessidade e proporcionalidade para atingir um objetivo legítimo determinado.[32] O relatório destaca que a regulamentação da criptografia fere a liberdade de expressão em dois aspectos principais: (i) podem não ser restrições necessárias para a satisfação de um interesse legítimo específico ou (ii) afetam de maneira desproporcional os direitos à liberdade de expressão da população em geral.[33] Estes seriam os casos de restrições ao uso individual da criptografia ou de regras que exigissem licenças ou que estabelecessem padrões técnicos fracos para o uso de criptografia por empresas, como ocorre em casos em que a instalação de *back-doors* é exigida aos desenvolvedores de aplicativos.

## 5 – Conclusão: da inaplicabilidade do art. 12, III e IV da Lei 12.965/14 quando o provedor de aplicação utiliza técnicas de criptografia que impossibilitam o acesso ao conteúdo das comunicações privadas

5.1. Conforme argumentado até aqui, o Instituto Brasileiro de Defesa do Consumidor entende ser *inaplicável a suspensão temporária de atividades de coleta de dados* (ou a proibição dessas atividades), nos termos do artigo 12 do Marco Civil da Internet quando o provedor de aplicação utiliza técnicas de criptografia que impossibilitam o acesso ao conteúdo das comunicações privadas. Essa inaplicabilidade decorre de dois argumentos centrais. Primeiro, por uma questão de coerência lógica com a arquitetura jurídica formulada no Marco Civil da Internet, que prevê sanções no caso de descumprimento das obrigações

[31] Idem, *ibidem*, p. 11.
[32] Em análise no Observatório do Marco Civil, o jurista Guilherme Damasio Goulart faz análise semelhante: "O problema é muito maior e envolve a possibilidade dos Estados, de forma geral, colocarem limites ao uso da criptografia, o que implica em restrições à segurança da informação e também à liberdade de expressão (ambos direitos fundamentais). Não se perca de vista que a ONU, por meio do seu Human Rights Council, manifestou-se no sentido de que há um direito de se comunicar de forma anônima e com o uso da criptografia (cf. o Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression - A /HRC/29/32). O documento ainda afirma que qualquer limitação a esse princípio deve ser absolutamente estrita, observando os princípios da legalidade, necessidade, proporcionalidade e legitimidade". Disponível em: http://omci.org.br/jurisprudencia/97/suspensao-do-bloqueio-do-whatsapp/
[33] Idem, *ibidem*, p 13-14.

positivas de proteção de dados pessoais e dos direitos básicos assegurados no art. 7º da lei. Não faz sentido aplicar a punição para provedores de aplicação de internet que utilizam de meios técnicos para justamente *garantir a privacidade e o gozo dos direitos assegurados no Marco Civil da Internet*. Segundo, por uma questão de teste de proporcionalidade exigido pelo inciso II do art. 12, que prevê que a sanção almejada pelo agente decisório seja sopesada com a gravidade da infração (ou "falta", nos termos da lei). O Idec entende que esse teste de proporcionalidade envolve também um olhar cuidadoso para a *intensidade da sanção* em sentido amplo, para além da mera questão pecuniária (o valor de uma suposta multa), mas as consequências geradas pela suspensão das atividades de coleta de dados ou por um "bloqueio". Em nosso entendimento, uma eventual decisão de bloqueio do WhatsApp por descumprimento de ordem judicial em sede de investigação criminal não passa nesse teste de proporcionalidade por (i) limitar a continuidade de um serviço massivamente utilizado por consumidores, em violação às diretrizes do Código de Defesa do Consumidor, (ii) violar a liberdade de expressão de terceiros não relacionados com investigações criminais pontuais, em colisão com Constituição Federal e Marco Civil da Internet, e (iii) limitar a livre iniciativa e finalidade social da rede, considerando a dependência de milhões de empreendedores dos recursos oferecidos pelo WhatsApp, em violação da base principiológica do Marco Civil da Internet.

5.2. O Idec entende que a aplicação de técnicas de "desabilitação" ou "quebra" de criptografia para fins de intercepção de mensagens de determinados indivíduos sob investigação, por autoridades de investigação da Polícia e do Poder Judiciário, coloca em risco a segurança e privacidade de milhões de cidadãos de *forma desproporcional*, em clara violação ao art. 7º, II, da Lei 12.965/2014 (direito à inviolabilidade e sigilo do fluxo das comunicações pela internet) e ao direito constitucionalmente assegurado de privacidade. Investigações criminais podem ser conduzidas a partir do *conjunto de metadados* coletados no WhatsApp, que revelam um rico conjunto de informações sobre o indivíduos quando analisados no agregado.[34] Os termos de uso do WhatsApp, atualizados em agosto de 2016,

[34] Argumentação semelhante é produzida por Tobias Boelter, da Universidade de Califórnia: "em vez de insistir em backdoors na criptografia, as autoridades deveriam focar na sua capacidade de obter dados de outras fontes. Atualmente, produzimos mais dados do que nunca, sendo que aqueles pertencentes à criptografia de ponta-a-

deixam claro que o aplicativo faz a coleta de um conjunto de informações como número de telefone, duração das conexões, frequência de uso do aplicativo, localização do usuário, lista de contatos telefônicos, entre outros. Tais dados – que podem ser extremamente úteis em casos de investigação criminal, relevando informações tão ricas quanto o próprio conteúdo da comunicação textual – são armazenados pelos provedores de aplicações de Internet, conforme art. 15 da Lei 12.965/14. A disponibilização de *registro de acesso a aplicações de internet* é possível a partir de ordem judicial fundamentada, nos termos do art. 10º, §1º e §2º. Isso não se confunde com disponibilização de conteúdo de comunicação privada, que não possui previsão legal no Marco Civil da Internet.

5.3. Conforme manifestado pelo Idec em todas as ocasiões de bloqueio temporário do WhatsApp por descumprimento de decisão judicial envolvendo intercepção de comunicação de dados, não é juridicamente correto aplicar a sanção do art. 12, III (suspensão temporária das atividades que envolvam coleta de dados) quando o provedor de aplicação utiliza técnicas de criptografia que impossibilitam o acesso ao conteúdo das comunicações privadas. Os artigos 11 e 12 da Lei 12.965/14 foram criados para definir sanções a provedores de aplicações que *descumprem deveres de proteção de dados e tutela da privacidade*, em especial os direitos definidos no art. 7º do Marco Civil da Internet. Ou seja, caso um provedor de aplicação falhe em garantir clareza contratual, boa-fé nos termos de uso ou consentimento para coleta de dados, abre-se possibilidade de sanção civil, criminal e administrativa, valendo-se o agente decisório da sistema sancionatória escalonada de advertência, multa, suspensão temporária ou proibição das atividades que envolvam "operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações".

5.4. No que toca ao dilema institucional sobre como combater o crime organizado e como obter informações necessárias para processos de investigação, o Instituto Brasileiro de Defesa do Consumidor entende que há *outras formas* de se promover investigações criminais

---

ponta representam apenas uma pequena fração. A maior parte dos serviços requer que esse tipo de dado de comunicação não seja criptografado para que o serviço funcione, e nunca usarão uma criptografia forte. Mesmo quando se trata de comunicação, metadados sensíveis que indicam com quem, quando e por quanto tempo nos comunicamos são acessíveis às autoridades legais pelos métodos tradicionais". Ver: http://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/

para desmantelamento de quadrilhas envolvidas com narcotráfico e outros crimes que não envolvem o bloqueio de aplicações que não "colaboram com as autoridades" por impossibilidade técnica, distorcendo a correta aplicação dos artigos 10 a 12 do Marco Civil da Internet. Dentre as opções ventiladas por inúmeros especialistas, estão (i) a requisição de metadados sobre utilização de aparelhos celulares e registros de utilização de aplicações, mediante ordem judicial devidamente fundamentada; (ii) a obtenção de mandado de busca e apreensão de computadores e celulares, (iii) a realização de acordos de cooperação judiciária (Tratado de Assistência Jurídica Mútua)[35], e, até mesmo, a (iv) exploração de vulnerabilidades técnicas em um software comercial para tentativa de acesso ao telefone celular de um alvo (técnica chamada de *lawful hacking*[36] e amplamente discutida nos Estados Unidos da América no contexto "Apple vs. FBI").

5.5. Para o Idec, no julgamento da ADPF 403 e na ADI 5.527, os excelentíssimos ministros do Supremo Tribunal Federal precisam compreender que os dispositivos dos artigos 10 a 12 do Marco Civil da Internet servem para proteger a privacidade, a proteção de dados pessoais e o sigilo das comunicações privadas. Eles são necessários e seria potencialmente danoso declará-los inconstitucionais (isso deixaria consumidores em posição de vulnerabilidade, no caso de descumprimento das obrigações de tutela da privacidade por parte dos provedores de aplicações).

5.6. O Idec também espera que a Corte reconheça a necessidade de teste de proporcionalidade para aplicação das sanções previstas no artigo 12, III e IV, devendo, o

---

[35] Conforme argumentado por Ronaldo Lemos (UERJ) em entrevista para a BBC: "As ações de hoje mostram que as coisas no Brasil estão acontecendo num caminho errado. O Brasil tem acordos de cooperação judiciária com outros países, como o MLAT (Tratado de Assistência Jurídica Mútua, na sigla em inglês). Quando você pede dados de uma empresa que tem sede em outro país, você recorre a esse tratado. Os brasileiros ficariam muito surpresos se empresas brasileiras que operam no exterior fossem obrigadas a fornecer dados sem passar por um mecanismo de cooperação judiciária internacional. Mecanismos desse tipo têm sido usados pela operação Lava Jato, por exemplo, para obter dados de empresas em outros países. Este caminho não está sendo utilizado. Ao contrário, estamos vendo uma tentativa de compelir as empresas que operam aqui no Brasil a oferecer os dados ignorando a via diplomática. Acho que, nesse sentido, a decisão pode repercutir mal internacionalmente, especialmente num contexto em que a Apple, lá nos Estados Unidos, está justamente contestando um pedido judicial para quebrar o sigilo de seus telefones". Disponível em: http://www.bbc.com/portuguese/noticias/2016/03/160301_entrevista_ronaldo_lemos_facebook_jp

[36] BELLOVIN, Steven M. et al. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Nw. J. Tech. & Intell. Prop.,* v. 12, p. i, 2014. GROSS, Shannon. A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era. *Nw. J. Tech. & Intell. Prop.*, v. 15, p. 74-74, 2017.

agente decisório, considerar a intensidade da sanção e seu efeito para milhões de cidadãos que dependem da utilização de determinada aplicação. No caso do WhatsApp, é fato notório que o serviço de mensagens – utilizado por mais de 100 milhões de consumidores – tornou-se essencial para as comunicações dos brasileiros, para o empreendedorismo e para o próprio funcionamento das instituições públicas.

5.7. O Instituto reforça, por fim, que há uma profunda relação entre uso de técnicas de criptografia e os direitos humanos, como destacado pelo próprio relator especial para liberdade de expressão da Organização das Nações Unidas. É preciso lembrar que o Marco Civil da Internet possui três grandes pilares, além da liberdade de expressão protegida constitucionalmente no Brasil: a garantia dos direitos humanos (art. 2º, II), a defesa do consumidor (art. 2º, V) e a finalidade social da rede (art. 2º, VI). Seria uma violação dos princípios assegurados no art. 2º do Marco Civil da Internet avançar uma interpretação, pela Corte, de que há obrigação legal de "desabilitação da criptografia" pelo WhatsApp, enfraquecendo o sistema de segurança oferecido aos usuários da internet no país. Nesses termos, o Instituto Brasileiro de Defesa do Consumidor espera ter colaborado com o Supremo Tribunal Federal, parabenizando a Corte pela realização da presente Audiência Pública.

São Paulo, 22 de maio de 2017.

**ELICI BUENO**
**Coordenadora Executiva**

**RAFAEL A. F. ZANATTA**
**Pesquisador em Telecomunicações e Direitos Digitais**