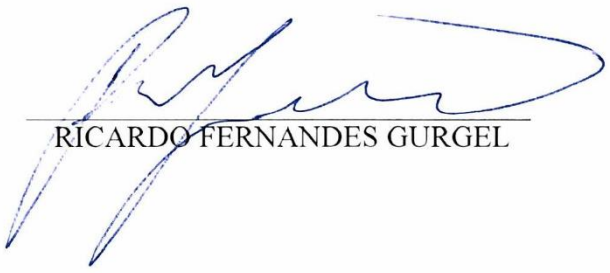
RICARDO FERNANDES GURGEL

A FALTA DE CONTROLE NOS SERVIÇOS DE MENSAGERIA E O POSSÍVEL IMPACTO NA SEGURANÇA E SOBERANIA NACIONAL

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Orientador: Carlos Maurício de Borges Mello – Maj EB R1

Brasília
2022



RICARDO FERNANDES GURGEL

RICARDO FERNANDES GURGEL

A FALTA DE CONTROLE NOS SERVIÇOS DE MENSAGERIA E O POSSÍVEL IMPACTO NA SEGURANÇA E SOBERANIA NACIONAL

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 21 de OUTUBRO de 2022

CARLOS MAURÍCIO DE BORGES MELLO – Maj R1 EB (ESD)
Orientador

IVAN CARLOS SOARES DE OLIVEIRA - Cel R1 EB (ESD)
Membro 1

MARCO AURÉLIO CARVALHO LEANDRO – CF RM1 (ESD)
Membro 2

A falta de controle nos serviços de mensageria e o possível impacto na segurança e soberania nacional

Ricardo Fernandes Gurgel[1]

RESUMO

A comunicação por aplicativos de mensageria tem se tornado cada dia mais frequente. Diante da facilidade e difundida proteção à privacidade desse tipo de comunicação, criminosos preferem utilizar essa funcionalidade para evitar monitoramento. O objetivo do trabalho é analisar o impacto que a falta de controle na utilização dos serviços de mensageria, caracterizada pela impossibilidade de interceptação das mensagens e a recalcitrância das plataformas em se enquadrarem na legislação vigente, pode causar à segurança pátria e eventual reflexo na soberania nacional. Foi estudado o funcionamento dos dois principais aplicativos de mensageria em uso, *WhatsApp e Telegram*; analisada a legislação nacional que ampara a interceptação das mensagens e fornecimento de dados por parte dos aplicativos; bem como os casos de destaque, analisados pelo judiciário, que enfrentaram o tema; além de formas alternativas de investigação ante as barreiras apresentadas e o eventual impacto na segurança e defesa nacionais**.** Realizou-se uma revisão bibliográfica da legislação, documentos, doutrina e jurisprudência, com o objetivo de fazer um contraponto entre os casos já conhecidos e as possibilidades de interferência na Segurança e Defesa. Por fim, concluiu-se que o uso descontrolado dos serviços de mensageria tem levado criminosos a fazer uso dessas plataformas para se comunicarem, encontrando um verdadeiro terreno fértil para planejar suas práticas delituosas e não serem alcançados pela Justiça, garantindo a execução de suas ações criminosas e impunidade de seus atos, fragilizando a segurança nacional, além de afrontar a soberania.
Palavras-chave: interceptação; *WhatsApp*; *Telegram*; segurança nacional.

The lack of control over messaging services and the possible impact on national security and sovereignty

ABSTRACT

Communication by messaging apps has become more and more frequent. Given the ease and widespread privacy protection of this type of communication, criminals prefer to use this functionality to avoid monitoring. The objective of this work is to analyze the impact that the lack of control in the use of messaging services, characterized by the impossibility of intercepting messages and the recalcitrance of platforms to comply with current legislation, can cause homeland security and possible reflection on national sovereignty. The functioning of the two main messaging applications in use, WhatsApp and Telegram, was studied; analyzed the national legislation that supports the interception of messages and the provision of data by the applications; as well as the outstanding cases, analyzed by the judiciary, that faced the issue; in addition to alternative forms of investigation in light of the barriers presented and the possible impact on national security and defense. A bibliographic review of the legislation, documents, doctrine and jurisprudence was carried out, with the objective of making a counterpoint between the already known cases and the possibilities of interference in Security and Defense. Finally, it was concluded that the uncontrolled use of messaging services has led criminals to make use of these platforms to communicate, finding a true fertile ground to plan

---

[1] Delegado de Polícia da Polícia Civil do Distrito Federal. Especialista em Direito Penal e Processual Penal. Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Defesa (ESD), 2022.

their criminal practices and not be reached by Justice, ensuring the execution of their criminal actions. and impunity for their acts, weakening national security, in addition to affronting sovereignty.
***Keywords**: interception; Whatsapp; Telegram; national security.*

1 INTRODUÇÃO

A comunicação e transmissão de informações sempre foram uma necessidade humana e desde a pré-história, os acontecimentos são registrados pelos homens através de pinturas em pedras. Ainda na idade antiga, com o surgimento da escrita, os relatos foram feitos por meio de cartas se utilizando de serviços de entrega, fazendo uso de mensageiros até chegar aos serviços de correios.

No século XVIII, mantendo a necessidade de comunicação, com a criação do telégrafo, as mensagens puderam ser encaminhadas com mais rapidez, independente das distâncias entre os interlocutores. Mas a evolução não parou por aí, ocorrendo o surgimento do rádio e do telefone.

Por fim, o advento dos computadores, da internet e a evolução dos aparelhos celulares, impulsionou a comunicação a um patamar de evolução antes inimaginável. Por meio dos *smartphones* é possível acessar qualquer conteúdo da internet, mandar mensagens instantâneas, fazer chamadas de vídeo, compartilhar conteúdos, acessar redes sociais e, é claro, fazer chamadas, fazendo uso de serviços de mensageria como o *WhatsApp* e *Telegram*.

Os aplicativos de troca de mensagens passaram a ser mais utilizados que o serviço de telefonia tradicional, não só pela praticidade, mas também por uma questão de cultura que vem dos hábitos das novas gerações (MEIOS, 2022).

É inegável que a comunicação é necessária para todo tipo de ação a ser realizada em conjunto, seja lícita ou ilícita, sendo certo que esses aplicativos de mensagens são facilitadores na comunicação entre indivíduos no dia a dia.

Criminosos se aproveitam dessa facilidade e se utilizam da ferramenta para auxiliá-los na prática dos crimes, visto que esses aplicativos se utilizam da criptografia de ponta a ponta de forma a proteger seus usuários de invasão de terceiros.

O que à primeira vista parece ser uma coisa boa, é utilizado pelas empresas responsáveis por esses aplicativos para negar a interceptação do fluxo das comunicações telefônicas quando há indícios razoáveis da autoria ou participação em infração penal, determinada por ordem judicial com base no regramento jurídico vigente.

Assim, a eventual interceptação de telefonia móvel tradicional, por si só, não traz todos os elementos de informação necessários para o desenrolar de uma investigação, visto que os investigados são extremamente cautelosos em suas comunicações telefônicas ordinárias, sendo recorrente os momentos em que os interlocutores se furtam a mencionar informações que os

comprometam criminalmente. Assim, decidem alterar o contato para uma plataforma mais segura para eles como é, por exemplo, o *WhatsApp* e *Telegram.*

A questão está tão difundida que uma reportagem recente do Fantástico apontou que o aplicativo *Telegram* abriga a prática de uma série de crimes, como: negociações de drogas, venda de armas sem registro, pornografia infantil, estelionato, venda de notas de dinheiro falsas (EXCLUSIVO, 2022).

Atualmente as investigações encontram uma grande dificuldade com a impossibilidade de interceptação do fluxo das conversas travadas via aplicativos de mensageria. A investigação de grupos criminosos é extremamente complexa e exige uma gama de recursos extraordinários de investigação.

Ao fazer uso de uma plataforma mais segura para eles, os criminosos se encontram em um verdadeiro terreno fértil para planejar suas práticas delituosas e não serem alcançados pela Justiça, garantindo a execução de suas ações criminosas e impunidade de seus atos.

Importante frisar que não é só fluxo das comunicações que não é possível interceptar, há uma recalcitrância, também, por parte das empresas, em encaminhar dados cadastrais básicos dos usuários desses aplicativos.

Não só criminosos comuns se utilizam desses subterfúgios, grupos terroristas em ações pelo mundo, também, têm procurado utilizar de meios alternativos de comunicação para preparar suas ações, seja por intermédio de esteganografia, chat de jogos on-line, telefones por satélite, *Dead drops*[2], dentre outros, visando comunicar livremente e se livrar de interceptações e vigilâncias.

> (...) Em um parque de Moscou, em 2006, a agência de inteligência MI6 da Grã-Bretanha foi pega em flagrante com uma "pedra de espionagem" - uma pedra falsa, contendo um transmissor sem fio onde informantes podiam deixar informações que poderiam ser recuperadas por outra pessoa, em uma versão moderna de *dead drops*. Hoje, com os avanços da informática, uma forma de *dead drop* digital é escrever uma mensagem por e-mail e não apertar enviar, e a mensagem será armazenada na pasta de rascunhos. O destinatário, que recebeu o login e a senha para aquela determinada conta de e-mail, pode ver a mensagem e se necessário responder(...) (GARDNER, 2013, n.p.).
>
> (...)Como todo mundo já deve ter visto nos noticiários, a França – e o mundo – sofreu um dos piores ataques terroristas dos últimos anos, com mais de 150 mortos em uma operação casada de vários ataques ocorrendo ao mesmo tempo em Paris, enquanto França e Alemanha jogavam uma partida de futebol. Toda a ação foi reivindicada pelo ISIS e segundo os terroristas, muito mais está por vir (GRUPO, 2015, n.p.).
>
> Então, a França e os países que são contra essas ações terroristas, precisam ir além em suas pesquisas para identificar como essas pessoas brutais estão se comunicando e

[2] Antigo método usado por espiões durante a Guerra Fria para deixar pacotes com informações, ou fotografias, em lugares como moitas ou atrás de latas de lixo. Estes eram, então, recuperados por alguém que estivesse passando por perto, provavelmente assobiando e vestindo um chapéu específico.

> pasmem, o Playstation 4 é uma das ferramentas para os mal feitores combinarem suas ações e ataques, segundo o ministro do Interior da Bélgica, Jan Jambom. O Ministro declarou que a ferramenta de chat do Playstation 4, sejam por voz ou texto, é uma das formas mais usadas de comunicação entre os terroristas (...) (GRUPO, 2015, n.p.).
>
> (...) Troca de mensagens criptografadas por *WhatsApp* e *Telegram*. Hashtags espalhadas pelo Twitter. Selfies no Instagram. Vídeos no YouTube. Troca da moeda virtual bitcoin. Parecem inocentes ações de quem é antenado em tecnologia, mas são a forma como usa a internet o grupo jihadista Estado Islâmico, que, na opinião de especialistas, faz uso sem precedentes dos meios digitais, a ponto de os Estados Unidos chamarem o movimento de "terrorismo viral (SIMÕES, 2015, n.p.)
>
> Não estamos mais caçando terroristas vivendo em cavernas que apenas se comunicam via mensageiros. Estamos encarando inimigos cujas mensagens e chamados de ataque são postados e promovidos em tempo real", diz Michael McCaul, deputado republicano que chefia o comitê de segurança nacional dos EUA (...) (SIMÕES, 2015, n.p.).
>
> A atuação digital do EI não se resume a propaganda. "O grupo terrorista está usando essas tecnologias e sites hospedados nos EUA para recrutar, encorajar pessoas a executar ataques terroristas em todo o mundo e para levantar dinheiro", afirma ao G1 Michael Smith II, cofundador da Kronos Advisory, consultoria norte-americana em assuntos de defesa (...) (SIMÕES, 2015, n.p.).
>
> (...)O FSB[3] disse que um homem-bomba que se explodiu no metrô de São Petersburgo no dia 3 de abril usou o *Telegram* para planejar o ataque com seus cúmplices. O ataque matou ao menos 15 pessoas. Para a agência, o serviço é o aplicativo mais usado por terroristas na Rússia (...) (RÚSSIA, 2017, n.p.).

Uma das bandeiras desses aplicativos é proteger a liberdade e privacidade dos usuários, pregando valores de anonimato, privacidade e liberdade. A título de exemplo, mais de dois bilhões de pessoas, em mais de 180 países, usam o *WhatsApp* para manter o contato com amigos e familiares, a qualquer hora ou lugar. A própria empresa ao indicar sua missão, afirma:

> O WhatsApp surgiu como uma alternativa ao sistema de SMS e agora possibilita o envio e recebimento de diversos arquivos de mídia: textos, fotos, vídeos, documentos e localização, além de chamadas de voz. Alguns de seus momentos mais importantes são compartilhados no WhatsApp. Por essa razão, implementamos a criptografia de ponta a ponta no nosso aplicativo. Por trás de cada decisão está o nosso desejo de possibilitar que as pessoas se comuniquem sem barreiras, em qualquer lugar do mundo (WHATSAPP, 2022, n.p.).

O *Telegram* segue a mesma linha e conforme artigo publicado no Jota está presente em 53% dos celulares do Brasil (BOTTINO, ARCHEGAS; PADRÃO, 2022).

Esse trabalho visa analisar o impacto que a falta de controle na utilização dos serviços de mensageria, caracterizada pela impossibilidade de interceptação dos fluxos das conversas e a recalcitrância ao enquadramento na legislação vigente pode causar a segurança pátria e o reflexo na soberania nacional.

Para tanto, foi estudado o funcionamento dos dois principais aplicativos de mensageria em uso, analisada a legislação nacional que ampara a interceptação das mensagens e

[3] O serviço de segurança russo, agência que sucedeu a KGB da era soviética.

fornecimento de dados por parte dos aplicativos, bem como os casos de destaque, analisados pelo judiciário, que enfrentaram o tema, além das formas alternativas de investigação ante as barreiras apresentadas e o eventual impacto na segurança e defesa nacional**.**

A metodologia aplicada a este trabalho baseou-se na revisão bibliográfica da legislação, documentos, doutrina e jurisprudência, com o objetivo de fazer um contraponto entre os casos já conhecidos e as possibilidades de interferência na Segurança e Defesa, visando refutar ou corroborar a tese apresentada de que a impossibilidade de rastreamento de mensagens fragiliza a segurança nacional e afeta a soberania.

2 O FUNCIONAMENTO DOS APLICATIVOS DE MENSAGERIA, *WHATSAPP* E *TELEGRAM*

Os aplicativos de mensageria surgiram como uma alternativa ao sistema de Mensagens Curtas (*Short Message Service - SMS*) possibilitando o envio e recebimento de diversos arquivos, como: textos, fotos, vídeos, documentos e localização; além de permitir a realização de chamadas de voz.

Esses aplicativos fazem uso da tecnologia de criptografia de ponta a ponta que, em síntese, garante que as mensagens trocadas entre os interlocutores caso venham a ser interceptadas não possam ser lidas.

Nas palavras de Mariana Coutinho a criptografia de ponta a ponta (*end-to-end encryption* ou E2EE) é um recurso de segurança que protege os dados durante uma troca de mensagens, de forma que o conteúdo só possa ser acessado pelos dois extremos da comunicação: o remetente e o destinatário. A ferramenta é uma implementação da criptografia assimétrica e garante que as informações não sejam interceptadas. Ninguém mais além dos envolvidos na conversa deve ter acesso ao conteúdo transmitido por meio da criptografia de ponta a ponta, nem mesmo as empresas dos *apps* (COUTINHO, 2019).

A mesma especialista explica o que vem a ser criptografia.

> Criptografia é o nome dado aos mecanismos que transformam informações que eram transparentes em algo que não possa ser compreendido por um agente externo. Uma chave de criptografia é usada com o algoritmo para embaralhar as mensagens, de modo que seja impossível para um intermediário que tenha acesso a elas compreender o conteúdo. Portanto, as informações são codificadas. Para tornar o texto compreensível novamente, é necessário ter acesso à chave correta. Dessa forma, apenas a pessoa que detém a chave pode ver os dados originais. A chave é uma sequência muito longa de números gerada pelo software, seja um app de mensagens ou um serviço de *e-comm* (COUTINHO, 2022, n.p.).

Excerto do Voto do Ministro Edson Fachin, na ADPF 403, citado na ementa do RMS 60531 / RO traz explicação sobre a criptografia ponta a ponta e a impossibilidade de se realizar a interceptação.

> (...) o Professor Anderson Nascimento explicou em linhas gerais em que consiste a criptografia, afirmando que seu objetivo é a garantia da integridade, autenticidade e confidencialidade. Segundo ele, o *WhatsApp* utiliza a criptografia de chave pública ou assimétrica, onde cada usuário possui duas chaves, uma para cifrar e outra para decifrar. O objetivo de tais sistemas é criar um túnel criptográfico entre os usuários, sendo que as mensagens enviadas e recebidas passam por um servidor que tem a função de estabelecer protocolos de sinalização, descobrir os endereços IPs das partes, auxiliar na troca de chaves, dentre outros. O Professor esclareceu que não é possível a interceptação de mensagens criptografadas do *WhatsApp* devido à adoção de criptografia forte pelo aplicativo. Explica que esse tipo de criptografia utiliza o Protocolo *Signal* que, no entendimento da comunidade científica, não possui vulnerabilidade, ou seja, é um protocolo seguro, não podendo ser quebrado. Em relação às alternativas para a interceptação, discorreu o seguinte. Sobre a possibilidade de espelhamento das conversas travadas no aplicativo para outro smartphone ou computador em face de um usuário específico, indicou que seria preciso, para tal intento, que fosse criado um ponto central de falha, o qual, por sua vez, poderia ser utilizado por parte não autorizadas. Quanto à desabilitação da criptografia ponta a ponta de um ou mais usuários específicos, seria preciso modificar o protocolo criptográfico. Destacou, ainda, a existência de outros aplicativos de mensagens que não possuem representação no Brasil e que poderiam ser utilizados pelos usuários, inclusive com a possibilidade de facilmente criptografar as mensagens e, posteriormente, colar tal mensagem no *WhatsApp*, para enviá-la a outro usuário, de modo que, mesmo que houvesse a interceptação da mensagem pelo *WhatsApp*, seria impossível desencriptá-la. Quanto aos demais instrumentos que podem auxiliar as investigações, aponta a importância da utilização dos metadados e da geolocalização, ressaltando a riqueza de dados a serem explorados pelas autoridades públicas (BRASIL, 2019).

O *WhatsApp* ao implementar a criptografia de ponta a ponta, no dia 05/04/2016, alegou proteção das comunicações pessoais, afirmando que todas as ligações, as mensagens, fotos, vídeos, arquivos e mensagens de voz que forem enviadas pelos usuários estarão protegidas com a criptografia. Afirmando que quando se envia uma mensagem, a única pessoa que poderá ler será o contato ou o grupo para o qual a mensagem foi enviada, destacando que ninguém poderá ver o conteúdo daquela mensagem, mais ou menos como se fosse uma conversa face a face. Acrescentando que a criptografia é uma das ferramentas mais importantes que os governos, empresas e pessoas em geral possuem para promover segurança e estabilidade, entendendo que qualquer esforço feito com o objetivo de enfraquecer a função da criptografia coloca as informações das pessoas à exposição e possível abuso de cibercrimonosos, hackers ou Estados-pária (CRIPTOGRAFIA, 2016).

3 A INTERCEPTAÇÃO DAS MENSAGENS E FORNECIMENTO DE DADOS POR PARTE DOS APLICATIVOS DE MENSAGERIA

3.1 AMPARO LEGAL

A interceptação telemática, para fins de investigação criminal ou instrução processual penal, é autorizada pelo art. 5º, XII, CF/88[4] (BRASIL, 2022a), tendo referido inciso constitucional sido regulamentado pela Lei n.º 9.296/1996 (Lei de Interceptação de Comunicações Telefônicas) que prevê no parágrafo único do artigo primeiro que referido diploma legal se aplica à interceptação do fluxo de comunicações em sistemas de informática e telemática[5] (BRASIL, 1996).

Os requisitos da interceptação telemática, que pode ser determinada pelo juiz de ofício, ou mediante representação da autoridade policial ou diante de representação do órgão do Ministério Público, são os mesmos para a autorização judicial da interceptação telefônica, quais sejam: presença de indícios razoáveis da autoria ou participação em infração penal punido com pena de reclusão e a inexistência de outros meios de obtenção dos elementos de prova disponíveis (BRASIL, 1996).

Já com relação aos metadados que são marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas, pode se dizer resumos de informações sobre a forma ou conteúdo de uma fonte (dados sobre dados) (MENDES, 2022), o acesso tem fundamento no Marco Civil da Internet, Lei 12.965/14, que em seu art. 22 expõe os requisitos legais para execução da medida, quais sejam: fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e período ao qual se referem os registros (BRASIL, 2014).

No mesmo diploma legal, o art. 10 prevê que o provedor de acesso, mediante ordem judicial, será obrigado a disponibilizar informações que possam contribuir para a identificação do usuário ou terminal. No art. 11, há determinação de ser respeitada, em qualquer operação, a legislação brasileira, bem como os direitos à privacidade, à proteção dos dados pessoais, o sigilo das comunicações privadas e dos registros. E no art. 15 há determinação para os provedores de aplicações de internet manterem os registros de acesso pelo prazo de seis meses.

---

[4] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[5] Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

O Marco Civil da Internet, também, apresenta no seu art. 12 sanções que podem ser aplicadas de forma isolada ou cumulativa, sem prejuízo das demais sanções cíveis, criminais ou administrativa, em caso de infringência das normas previstas nos seus artigos 10 e 11, sendo-as: advertência, multa de até 10% do faturamento do grupo econômico, suspensão temporária das atividades e proibição de exercício das atividades que envolvam os atos previstos no art. 11.

3.2 JURISPRUDÊNCIA

3.2.1 Relacionada ao *WhatsApp*

O aplicativo já teve seu serviço interrompido algumas vezes no território nacional. Apesar de ter ocorrido em processos sigilosos, do pouco que foi divulgado se extrai que os bloqueios ocorreram pelo fato da empresa responsável não colaborar com investigações criminais.

No início de 2015, o Juiz de Direito da Central de Inquérito da Comarca de Teresina, atendendo representação do Núcleo de Inteligência da Policial Civil daquele Estado, após ouvir o Ministério Público, determinou a suspensão das atividades no Brasil em razão de reiterados descumprimentos de ordens judiciais em diversos procedimentos que apuravam crimes da mais elevada gravidade e conforme afirmado pelo d. magistrado, ante a postura arrogante da empresa que sob alegação de não ter escritório no Brasil, se mantém inerte às solicitações da Justiça, tornando-se verdadeira "terra de ninguém" atentando contra a Soberania nacional (ARAÚJO, ROMERO, 2015).

O bloqueio não chegou a ser efetivado, tendo sido suspensa a eficácia da ordem pelo Tribunal de Justiça do Piauí, no mesmo dia, em decisão monocrática exarado nos autos do Mandado de Segurança nº 2015.0001.001592-4 (PIAUÍ, 2015).

O Desembargador Relator fundamentou na falta de proporcionalidade do ato e a grave lesão aos usuários do aplicativo.

> (...) em hipótese alguma se justifica a interrupção de acesso a todo um serviço, cuja área de abrangência, sabe-se, transpõe as barreiras nacionais de qualquer nação e afeta, direta e surpreendentemente, a comunicação entre um sem número de pessoas, envolvendo não somente os usuários nacionais, mas também aqueles que, fora de nossas fronteiras, tentem contatar parentes, amigos e afins residentes no Brasil (...) (SÃO PAULO, 2015).

No fim de 2015, um segundo bloqueio, pelo prazo de quarenta e oito horas, foi determinado pela 1ª Vara Criminal de São Bernardo do Campo/SP, que ocorreu no âmbito de investigação de tráfico de drogas, após a empresa se negar a realizar a interceptação telemática de alguns investigados conforme determinado sob a alegação de impossibilidade de

atendimento da ordem judicial e recalcitrância no cumprimento mesmo diante de sanção pecuniária.

A ordem foi suspensa poucas horas depois pela 11ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo sob o argumento que a medida violava o princípio da proporcionalidade e existência de outros meios disponíveis para obtenção do resultado, afirmando que em face dos princípios constitucionais, não se mostra razoável que milhões de usuários sejam afetados em decorrência da inércia das empresas, mormente quando não esgotados outros meios disponíveis para a obtenção do resultado desejado (SÃO PAULO, 2015).

Após a implementação da criptografia de ponta a ponta, o *WhatsApp* sofreu, pelo menos, mais duas interrupções no seu serviço. A Vara Criminal da Comarca de Lagarto/SE determinou a suspensão do aplicativo por setenta e duas horas, tendo o bloqueio sido suspenso pelo Tribunal de Justiça de Sergipe nos autos do Mandado de Segurança 201600110899 sob o entendimento que a interrupção gerou um caos em todo o Brasil e por não ser possível afirmar que as informações poderiam ser fornecidas pelo aplicativo ou serem desencriptadas (SERGIPE, 2016).

O outro caso foi determinado pela 2ª Vara Criminal de Duque de Caxias/RJ, tendo o bloqueio sido suspenso pelo Supremo Tribunal Federal sob o argumento que a paralisação do serviço além de ser desproporcional, violava a liberdade de expressão, destacando que a importância desse tipo de comunicação até mesmo para intimação de despachos ou decisões judiciais (BRASIL, 2016d).

Diante dos bloqueios e da imensa repercussão social que os casos ganharam, o Supremo Tribunal Federal foi acionado, tendo sido ajuizadas a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403 (BRASIL, 2020) e a Ação Direta de Inconstitucionalidade (ADI) nº 5527 (BRASIL, 2022b), ambas questionando, em síntese, a validade jurídica das ordens de bloqueio do *WhatsApp*.

A ADPF 403 alega que as ordens judiciais que determinam o bloqueio/suspensão dos serviços de mensageria violam o princípio fundamental da liberdade de comunicação (art. 5º, IX, da CF), além do princípio da proporcionalidade ao resultar na inacessibilidade da plataforma por toda a sociedade brasileira (PEREIRA; RODRIGUES; VIEIRA, 2021).

Já a ADI 5527 busca declarar a inconstitucionalidade dos incisos III e IV do art. 12 da Lei nº 12.965/2014 (Marco Civil da Internet) que são utilizados para fundamentar as ordens judiciais de bloqueio/suspensão dos serviços de Mensageria, além disso, busca limitar os efeitos do art. 10, §2º, para que o dispositivo seja aplicável apenas a casos de persecução penal e não

para descumprimento de ordens judiciais na esfera cível (PEREIRA; RODRIGUES; VIEIRA, 2021).

O julgamento de ambas as ações se encontra suspenso ante o pedido de vista do Ministro Alexandre de Moraes, sendo que o Ministro Edson Fachin (Relato da ADPF 403) votou no sentido de ser procedente o pedido formulado para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta a ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet, sendo acompanhado do voto da Ministra Rosa Weber (BRASIL, 2020).

Paralelamente, instado a se manifestar sobre as multas impostas as empresas por descumprimentos das decisões judiciais, o Superior Tribunal de Justiça em harmonia com os votos já proferidos pelos Ministros do STF nas ações citadas acima, entendeu que não obstante possa significar prejuízos para investigações criminais, feita a ponderação de valores, os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia, devendo ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível (BRASIL, 2019).

Desta forma, o STJ concluiu pela impossibilidade de aplicação de multa contra os aplicativos de mensageria pelo fato de as empresas não conseguirem interceptar as mensagens que são protegidas por criptografia de ponta a ponta.

3.2.2 Relacionada ao *Telegram*

No início deste ano, mais precisamente no mês de março, o Supremo Tribunal Federal (STF), em decisão monocrática exarada pelo excelentíssimo Ministro Alexandre de Moraes, utilizando como base legal o Marco Civil da Internet, determinou[6] a suspensão completa e integral do funcionamento do aplicativo atendendo representação da Polícia Federal, fundamentando a decisão em reiterados descumprimentos de ordem judicial por parte da empresa e poder geral de cautela, nos autos da Petição n.º 9.935/DF (BRASIL, 2022c).

Analisando detidamente a decisão, Alexandre de Moraes indica as alegações apontadas pela Polícia Federal, quais sejam:

---

[6] No âmbito da investigação contra o blogueiro Allan dos Santos, do canal Terça Livre

a) o descumprimento por parte do *Telegram*, mesmo após ser comunicado nas vias indicadas em seu sitio de internet de ordem emanada da Suprema Corte Nacional;
b) o fato de o aplicativo *Telegram* ser notoriamente conhecido por sua postura de não cooperar com autoridades judiciais e policiais de diversos países, inclusive colocando essa atitude não colaborativa como uma vantagem em relação a outros aplicativos de comunicação, o que o torna um terreno livre para proliferação de diversos conteúdos, inclusive com repercussão na área criminal;
c) o *Telegram* está entre os aplicativos de mensageria mais usados por abusadores sexuais de crianças, sendo que a plataforma está sendo utilizada com a finalidade de adquirir imagens de abuso infantil visando a difusão do conteúdo;
d) o *Telegram* não fornece qualquer dado (nem cadastral, nem pessoal, nem cibernético) para os órgãos de persecução penal em relação a criminosos;

Ao fundamentar sua decisão Alexandre de Moraes fez dura afirmação indicando o desprezo à Justiça e a falta total de cooperação da plataforma com órgãos judiciais.

> (...) O desprezo à Justiça e a falta total de cooperação da plataforma *Telegram* com os órgãos judiciais é fato que desrespeita a soberania de diversos países, não sendo circunstância que se verifica exclusivamente no Brasil e vem permitindo que essa plataforma venha sendo reiteradamente utilizada para a prática de inúmeras infrações penais(...) (BRASIL, 2022b).

Poucos dias após, a decisão de bloqueio, Alexandre de Moraes revogou a suspensão determinada, fundamentando que o *Telegram* atendeu integralmente determinações, como, dentre outras, indicar à Justiça um representante oficial no Brasil e implementação de medidas para combater a desinformação.

Destaca-se que essa decisão, diferentemente dos bloqueios a plataforma WhatsApp, foi a primeira a ser fundamentada com base no Marco Civil da Internet, Lei 12.965/14, uma vez que foi baseada no art. 12 que prevê a possibilidade de bloquear provedores de aplicação (BRASIL, 2014).

Referida decisão foi muito repercutida, havendo severas críticas, destacadamente com relação a proporcionalidade da medida, a eficácia e a fundamentação jurídica que foi embasada. Artigo publicado no site Jota, a época da decisão, concatena bem as críticas (BOTTINO, ARCHEGAS; PADRÃO, 2022).

No referido documento, primeiramente discorrem sobre a exequibilidade da medida, alertando da complexidade de cumprimento das ordens de bloqueios envolvendo provedores de aplicação, seja pela delimitação geográfica, seja pela possibilidade de se esquivar do bloqueio.

Sendo que, com relação a delimitação geográfica foi lembrado que em uma das vezes que o *WhatsApp* foi bloqueado no Brasil em 2015, acabou ficando fora do ar também em partes da Argentina e Chile. Já com relação a esquivar do bloqueio, usuários podem utilizar uma Rede Privada Virtual (VPN - *Virtual Private Network*)[7] para continuar acessando o serviço (O QUE, 2022).

Com relação a proporcionalidade da medida, as críticas ecoam outras já proferidas na época das ações de suspensão em desfavor do *WhatsApp* no sentido de em que pese os provedores de aplicações de internet[8] operarem no território nacional e serem obrigados a respeitar a legislação brasileira, não pode esquecer do impacto negativo da interrupção dos serviços em termos sociais e econômicos, visto que os aplicativos são utilizados por um sem-número de pessoas em atividades lícitas.

Polemizaram, também, a fundamentação jurídica da decisão que foi ancorada no art. 12 do Marco Civil da Internet que estabelece sanções quando houver descumprimento dos deveres contidos nos artigos 10 e 11 do mesmo diploma legal que versa sobre a preservação da intimidade, da vida privada, honra e imagem das partes envolvidas na guarda e na disponibilização dos registros de conexão e de acesso a aplicações de internet.

Além do que a interpretação literal do art. 12, segundo o artigo, permite apenas o bloqueio das atividades de tratamento pessoais e não o do serviço em si. Assim, não existiria autorização para interferências na infraestrutura da rede, tendo o Supremo Tribunal Federal revertido decisão de bloqueio do *WhatsApp* com fundamento similar, conforme demostrado alhures no caso que foi determinado pela 2ª Vara Criminal de Duque de Caxias/RJ.

Lado outro, especialistas indicaram diferenças em relação aos bloqueios anteriores e entendem haver fundamento, conforme dito pelo advogado, especializado em direito digital, Rafael Pellon.

"O bloqueio não foi por ter conteúdo 'x' ou 'y' sendo disseminado, não entra na regulação da liberdade de expressão. Está discutindo a negligência, que é o que está no MCI. Em termos jurídicos, funciona, tem fundamento, mas tem uma onda de impacto" (AMARAL, 2022, n.p.).

---

[7] Uma VPN oculta seu endereço IP deixando que a rede redirecione você por meio de um servidor remoto especialmente configurado executado por um host VPN. Isso significa que se você navegar online com uma VPN, o servidor VPN se tornará a fonte de seus dados. Isso significa que seu Provedor de Serviços de Internet (ISP) e terceiros não podem ver quais sites você visita ou quais dados você envia e recebe online. Os servidores VPN atuam essencialmente como suas proxies na Internet. Como os dados de localização demográfica vêm de um servidor em outro país, sua localização real não pode ser determinada.

[8] Conforme art. 5º, VII da Lei 12.965/14, aplicações de internet são o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet (BRASIL, 2014).

Na mesma linha, o ministro Luís Roberto Barroso (2022, n.p.) ao comandar o Tribunal Superior Eleitoral fez afirmações duras:

"Nenhum ator relevante no processo eleitoral pode atuar no país sem que esteja sujeito à legislação e a determinações da Justiça brasileira. Isso vale para qualquer plataforma".

"O Brasil não é casa da sogra para ter aplicativos que façam apologia ao nazismo, ao terrorismo, que vendam armas ou que sejam sede de ataques à democracia que a nossa geração lutou tanto para construir"

"Como já se fez em outras partes do mundo, eu penso que uma plataforma, qualquer que seja, que não queira se submeter às leis brasileiras deva ser simplesmente suspensa. Na minha casa, entra quem eu quero e quem cumpre as minhas regras."

4 FORMAS ALTERNATIVAS DE INVESTIGAÇÃO

Diante da impossibilidade da interceptação do fluxo da comunicação, outras medidas são defendidas para instrumentalizar a investigação, como descobrir o emissor/receptor da mensagem enviada através dos aplicativos, a frequência de comunicação, além da localização do suspeito através do prestador de serviços de telefônica móvel, bem como acesso a nuvens em caso de *backup* como *iCloud*[9] (INTRODUÇÃO, 2022), como defendido por Riana Fefferkorn (2016), pesquisadora na área de criptografia no *Center for Internet and Society da Stanford Law School* (EUA).

A mesma especialista defende a criptografia robusta visando a proteção de direitos fundamentais e transações comerciais, além de afirmar que não se trata de uma ameaça a segurança.

> (...) uma criptografia robusta é tão importante para a economia, para proteger transações, tais como serviços bancários, para proteger nossos dados de hackers ou ladrões, para proteger os direitos fundamentais como a privacidade e a liberdade de expressão etc. (...) Criptografia forte promove uma forte segurança, ou seja, isso não ameaça a segurança. O debate sobre a criptografia versus aplicação da lei é um debate "segurança versus segurança", não um debate "privacidade versus segurança". 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(...) (PFEFFERKORN, 2016, n.p.).

[9] é o serviço da Apple que armazena com segurança suas fotos, arquivos, notas, senhas e outros dados na nuvem e os mantém atualizados em todos os seus dispositivos automaticamente.

Tobias Boelter (2016) , doutorando na *University of California*, Berkeley, Departamento de Engenharia Elétrica e Ciência da Computação, com foco em Segurança e Criptografia, à época do bloqueio do *WhatsApp,* seguiu a mesma linha de Riana, defendendo que ao invés de "insistir em *backdoors* na criptografia, as autoridades deveriam focar na sua capacidade de obter dados de outras fontes", pois os dados pertencentes a criptografia de ponta a ponta representam uma pequena fração de todo dado que é produzido, além do que tão logo os casos nos quais os Estado utilizasse essa técnica se tornassem públicos, os investigados e potenciais investigados mudariam para outro serviço mais seguro de comunicação.

A respeito de soluções tecnológicas que permitiriam, em tese, a interceptação das mensagens trocadas pelos aplicativos de mensageria, Boelter (2016) elenca algumas com ponderações.

a) Utilização da técnica conhecida como ataque do tipo "*man-in-the-middle*" que consistiria, no caso, em o aplicativo trocar as chaves públicas, dando para os interlocutores uma chave privada do próprio aplicativo ao invés da chave correta, recebendo assim todas as mensagens que as duas partes enviassem uma para a outra, recriptografá-las com a chave correta e fingir que nada aconteceu. Ponderações: diferentemente da interceptação clássica, as pessoas investigadas, caso tenham algum conhecimento técnico, vão conseguir descobrir se estão sendo vigiadas ou se já foram vigiadas. Nesse caso não há introdução de novas fraquezas aos sistemas, apenas as inerentes a criptográfica ponta a ponta;
b) modificar o aplicativo para que ele encaminhasse a mensagem para o Estado além de enviá-las para o destinatário original. Ponderações: usuário habilidoso conseguiria descobrir se o seu aplicativo estiver encaminhando mensagem para o Estado. Quebra da confiança dos usuários. Governos repressivos e hackers seriam capazes de invadir a infraestrutura do aplicativo e ter acesso as mensagens, usando o mesmo mecanismo que o Estado usaria com uma ordem judicial;
c) procurar vulnerabilidades do sistema operacional do telefone a ser investigado, explorá-las e ter acesso às mensagens armazenadas no aparelho e instalar um programa oculto de monitoramento para espiar comunicações futuras. Ponderações: O Estado deveria divulgar, por questão moral, as vulnerabilidades conhecidas aos fornecedores do aparelho que deveriam corrigir para manter a segurança de todos os usuários.

Na prática policial para ter acesso as conversas travadas pelos aplicativos de mensageria, tem se usado da busca e apreensão dos aparelhos celulares com fundamento no art. 240 do Código de Processo Penal (BRASIL, 1941).

Destaca-se que o Superior Tribunal de Justiça entendeu ser ilícita a prova colhida mediante acesso aos dados armazenados no aparelho celular, relativos a mensagens de texto, SMS, conversas por meio de aplicativos e obtida diretamente pela polícia, sem prévia autorização judicial.

Sendo que há uma distinção entre dados armazenados e comunicações privadas armazenadas. No caso de dados, basta a apreensão lícita do bem (aparelho telefônico ou computador), já as comunicações armazenadas demanda prévia autorização judicial, nos termos do art. 7º, III, da Lei 12.965/2014[10] (BRASIL, 2014).

No mesmo sentido, há precedente, do mesmo Tribunal, que considera ilícito o acesso pela polícia, sem ordem judicial, aos dados de celular apreendido no momento do flagrante.

De outro turno, o mesmo STJ entende que o acesso ao conteúdo armazenado em telefone celular ou *smartphone*, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos (BRASIL, 2016c).

Entretanto, essas alternativas estão se tornando inviáveis, uma vez que o próprio *WhatsApp* vem propagando que a privacidade está em seu DNA e que nunca vai parar de criar formas de proteger as conversas pessoais, destacando que além da criptografia ponta a ponta, desenvolveu novas camadas de privacidade, pontuando as seguintes:

a) criação de mensagens temporárias que se apagam sozinhas;
b) para guardar o histórico de conversa, *backups* criptografados de ponta a ponta;
c) verificação em duas etapas, criando necessidade de inserir uma senha para acessar o aplicativo.
d) promessa de implementar o bloqueio de captura de tela para mensagens de visualização única (NOVOS, 2022).

[10] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

5 O IMPACTO NA SEGURANÇA E DEFESA NACIONAL PELA DIFICULDADE DE RASTREIO NAS COMUNICAÇÕES

O repúdio ao terrorismo configura um dos princípios constitucionais fundamentais das relações internacionais contidos na Constituição brasileira, estando a definição legal de terrorismo no Brasil expressa no artigo 2º da Lei nº 13.260/16:

> Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública (BRASIL, 2016a).

Ao estabelecer os Objetivos Nacionais de Defesa, a Política Nacional de Defesa (PND) reafirma a repulsa ao terrorismo contida na Constituição Federal e reforça o compromisso do país em combatê-lo, na medida em que este representa risco à paz e à segurança mundiais. Além disso, o Brasil participa e apoia as resoluções da Organização das Nações Unidas (ONU) pertinentes ao tema, devendo, portanto, cooperar com as demais nações no intuito de prevenir e combater as ameaças terroristas.

A gravidade em torno da escalada do terrorismo internacional é tão grande que, no ano de 2005, a ONU instituiu o *Counter Terrorism Implementation Task Force*, estabelecendo a Estratégia Global contra o Terrorismo baseada em quatro pilares (identificação das condições que conduzem à disseminação do terrorismo, prevenção e combate ao terrorismo, capacitação estatal e fortalecimento do papel da ONU, assegurar os direitos humanos e a aplicação do direito).

Entre as ações estratégicas que devem orientar a implementação da Estratégia Nacional de Defesa (END), destaca-se a necessidade de cooperação entre todas as instâncias do Estado brasileiro visando ao incremento do nível de Segurança Nacional.

Assim, a END define como prioritárias, entre outras, as seguintes tarefas: a prevenção contra atos terroristas, a execução de operações de contraterrorismo como forma de se antecipar à ameaça terrorista e a definição de medidas para a segurança das áreas relacionadas a infraestruturas críticas.

Para mostrar a relação de causa e efeito no possível uso de mensagens em ataques terroristas faz-se um contraponto entre os casos já conhecidos e as possibilidades de interferência na Segurança e Defesa.

Nessa esteira, é sabido que a estrutura de Defesa Nacional trabalha diuturnamente para conter as ameaças de todos os níveis. Exemplo disso, foi a prisão de criminosos na Operação *Hashtag*, a qual identificou um grupo que articulava ataques terroristas em eventos de grandes vultos no Brasil: Segundo a sentença condenatória, no período de 17/03 a 21/07/2016,

criminosos dedicaram-se a promover a organização terrorista denominada Estado Islâmico do Iraque e do Levante.

Após a investigação do caso, ficou provado que os meliantes utilizaram o aplicativo *Telegram* para comunicar-se. Dentre as mensagens rastreadas estavam os possíveis alvos de ataques que eles realizariam no Brasil:

> Os terroristas objetivavam estrangeiros, homossexuais, muçulmanos xiitas e judeus, durante os Jogos Olímpicos, com a orientação sobre a fabricação de bombas caseiras, a utilização de armas brancas e aquisição de armas de fogo para conseguir esse objetivo (PARANÁ, 2016).

A investigação apontou que, apenas quatro dias antes de ser preso, um criminoso enviou um áudio no grupo *Telegram* “Defensores da Sharia” em que afirma "a minha *bayat* é para o Califa Abu Bakr al Baghdadi e meu apoio é para o Dawlat alIslamiyah", convocando a todos para agirem naturalmente de modo a não despertar suspeitas sobre as ações terroristas. Afirmou ter aprendido essas técnicas de dissimulação com a leitura de manuais da Al Qaeda, o que é alinhado com os registros históricos de estudo dessa organização e do próprio ISIS.

A sentença menciona que:

> Igualmente identificaram-se diversas manifestações de exaltação à organização e de fomento de suas ações criminosas nos grupos Telegram Jundallah e Defensores da Sharia. Também após a entrada em vigor da lei ele, mais uma vez reafirmando sua adesão aos ideais terroristas, apenas quatro dias antes de sua prisão, manifestou interesse em compor um embrião de célula terrorista no Brasil, tal como proposto pelo correu LEONID (PARANÁ, 2016).

O fato é que, por intermédio do aplicativo de troca de mensagens *Telegram*, foram observadas conversas extremistas dos criminosos.

5.1 BREVES CONSIDERAÇÕES SOBRE O PAPEL DO ESTADO NA REGULAÇÃO

Segundo Prosser (1999), o Estado deve desempenhar um papel regulador por meio da definição de amplas políticas setoriais de acordo o interesse público. Essa teoria parte do princípio de que a regulação é uma forma de intervenção do Estado que objetiva atingir fins públicos, de interesse coletivo, em antagonismo à teoria do bem-estar econômico, cuja regulação visa a corrigir as falhas de mercado, como setores de monopólio natural, corrigir externalidades, consertar as assimetrias de informação.

Dessa forma, compreende-se que o fenômeno regulatório deve ser composto por múltiplos atores, nesse sentido, o poder Judiciário tem um papel relevante.

Vermeule (2016) demonstra que a relação entre o Estado e a Lei evidencia a posição relativa do Judiciário frente à regulação de meios digitais. Para o autor, os meios digitais não podem prejudicar o cumprimento da lei.

Ademais, é inadmissível que empresas estrangeiras operem em território nacional sem se sujeitarem a legislação vigente, vindo a ser um ataque a soberania, sob pena de filiar a declaração de independência do ciberespaço, de John Perry Barlow, citada em artigo publicado na Revista GEOUSP[11] (ISRAEL, 2020), na qual entende que o espaço virtual, paralelo ao espaço geográfico, estaria acima dos Estados nacionais.

> Os governos derivam seu justo poder a partir do consenso dos governados. Vocês não solicitaram ou receberam o nosso. Não convidamos vocês. Vocês não vêm do espaço cibernético, o novo lar da Mente. Não temos governos eleitos, nem mesmo é provável que tenhamos um [...]. O espaço cibernético não se limita a suas fronteiras [...]. Estamos formando nosso próprio Contrato Social. Essa maneira de governar surgirá de acordo com as condições do nosso mundo, não do seu. Nosso mundo é diferente [...]. Nosso mundo é um mundo que está em toda parte e em lugar nenhum, mas não é onde moram os corpos (BARLOW, 1996 apud ISRAEL, 2020, n.p.).

É cediço que criminosos evitam a qualquer custo deixar rastro, seja para não terem seus planos descobertos nas fases de cogitação e planejamento, visando uma execução exitosa, seja para se manterem escondidos dos órgãos de persecução.

> (...)Terroristas sofisticados conhecem bem os riscos de deixar "marcas digitais" que podem ser rastreadas e identificadas, por isso a Inteligência americana demorou tanto tempo para descobrir onde Osama Bin Laden estava escondido, já que todas as mensagens e dados enviados e recebidos pelo líder da al-Qaeda eram entregues em mãos(...) (GARDNER, 2013, n.p.)

Conforme noticiado pelo portal “Observador”, após o atentado terrorista na cidade de Londres, o governo britânico defendeu que os serviços de informação e segurança devem ter algum tipo de acesso aos conteúdos das aplicações de mensagens encriptadas para evitar que este tipo de serviços possa ser usado por terroristas (CARRAPATOSO, 2017).

Segundo o mesmo portal, a tese foi defendida pela secretária de Estado da Administração Interna britânica, Amber Rudd, depois de ter sido tornado público que Khalid Masood, o autor do ataque em *Westminster*, tinha usado o aplicativo, minutos antes do atentado junto do Parlamento britânico. Para ela é “completamente inaceitável” que estes serviços de mensagens ofereçam este tipo de encriptação, o que dificulta, em muito, o trabalho da polícia e dos serviços de segurança.

A mesma notícia, apresenta que Amber argumentou que precisamos assegurar que organizações como o *WhatsApp* não proporcionem um lugar secreto para os terroristas se comunicarem uns com os outros.

---

[11] é uma publicação do Programa de Pós-Graduação de Geografia Humana (PPGH) e do Programa de Pós-Graduação de Geografia Física (PPGF) da Universidade de São Paulo.

Certa oportunidade, o diretor-geral do serviço de inteligência britânico afirmou “não existir um "oásis" digital onde infratores ou terroristas podem esconder mensagens e comunicar-se livremente, sem medo de vigilância ou interceptação”(GARDNER, 2013, n.p.).

6 CONSIDERAÇÕES FINAIS

A expansão do uso dos aplicativos de mensageria, *WhatsApp e Telegram*, é uma realidade, sendo indiscutível sua importância para toda a sociedade, principalmente como ferramenta de comunicação.

Inconteste que a utilização da criptografia ponta a ponta, para se ter um meio confiável de comunicação, é essencial para as atividades licitas diárias, protegendo de possível abuso de cibercriminosos, hackers ou Estados-pária.

Ocorre que aproveitando da privacidade apresentada pelas plataformas como fundamento e pilar de funcionamento, criminosos estão fazendo uso dessa funcionalidade para evitar monitoramento. A utilização desses aplicativos esbarra, portanto, numa clara dicotomia entre privacidade e segurança e tem adquirido uma ampla dimensão.

Essa celeuma não é nova e o judiciário nacional já vem se posicionando há algum tempo, desde 2015, pois mesmo antes da implementação da criptografia ponta a ponta, as empresas responsáveis pelos aplicativos já vinham se recusando a cooperar com a justiça em investigações de crimes graves, nesse sentido duas foram as decisões que determinaram o bloqueio do aplicativo *WhatsApp* que foram, rapidamente, reformadas sob a alegação de falta de proporcionalidade e grave lesão aos usuários.

As duas outras decisões que determinaram a suspensão do serviço, após a implementação da criptografia ponta a ponta, foram igualmente revistas com celeridade sob o entendimento da desproporcionalidade e caos gerado pelo bloqueio no território nacional, com a inovação de não saber ser possível o cumprimento da ordem judicial pelas empresas.

Certo que o caso está sendo discutido no Supremo Tribunal Federal em duas ações, tendo dois votos no sentido de ser inconstitucional a interpretação do art. 12 da Lei 12.965/14 que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta a ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet.

Com base nesses dois votos, o Superior Tribunal de Justiça entendeu que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela

impossibilidade de se coletar os dados das conversas dos usuários da tecnologia, devendo ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível.

Essa discussão ainda não terminou, seja pelo fato de as duas ações ainda estarem pendentes de julgamento, por causa de um pedido de vista, seja pelo fato de no início deste ano perante a falta de cooperação da plataforma *Telegram* com os órgãos judiciais, o Ministro Alexandre de Moraes ter determinado monocraticamente, em desacordo com a posição que vinha se delineando na própria Corte Suprema, a suspensão do serviço que foi retomado, dias após a empresa atender algumas determinações.

Certo que mesmo após várias discussões, tem prevalecido o entendimento que deve se preservar os direitos fundamentais, principalmente a intimidade, sendo isso fonte de disputa entre as plataformas de aplicativos de qual é mais confiável.

Nessa toada, as empresas responsáveis, além de alegarem a impossibilidade de interceptação do fluxo das comunicações, seguem dificultando o acesso aos métodos alternativos, criando novas barreiras até para os metadados.

A possibilidade de acesso a conversa travada nesses aplicativos tem sido possível quando se tem acesso ao telefone ou quando o usuário realiza *backup* na nuvem e, com ordem judicial se tem acesso a ela, entretanto com as novas camadas implementadas, isso também não será possível, uma vez que:

a) caso o usuário use o recurso que possibilita que a mensagem se apague sozinha, de nada adiantará ter acesso ao aplicativo;
a) caso o usuário habilite o recurso de verificação em duas etapas, mesmo tendo acesso ao aplicativo, caso tenha conseguido a senha do telefone, precisará da senha de acesso do próprio aplicativo;
b) com os *backups* criptografados de ponta a ponta, mesmo que se consiga acesso as nuvens (*iCloud ou Google Drive*) não será possível decifrar os dados.

O assunto é grave e deve ser melhor debatido e estudado, inclusive sobre a possibilidade de espelhamentos de dados, mesmo que seja necessário a criação de ponto de falha, não sendo válidos os argumentos de possibilidade de o investigado descobrir ou esse ponto ser utilizado por hackers.

A tecnologia está evoluindo e urge a necessidade de adequação a realidade e isso tem que ser melhor analisado, sendo certo que o argumento de preservação de direitos fundamentais,

importantes, sem dúvida, como as cláusulas de inviolabilidade da privacidade, intimidade e liberdade, não pode constituir instrumento de salvaguarda de práticas ilícitas.

É cediço que há posicionamento jurisprudencial e doutrinário sedimentado no direito pátrio no sentido de que os direitos fundamentais, por mais importantes que sejam, não são dotados de caráter absoluto. A segurança pública e a segurança nacional são direitos difusos de todos, ao passo que a intimidade e a privacidade são direitos individuais.

Grupos terroristas em ações pelo mundo, inclusive no Brasil, para preparar e executar seus atentados, se utilizaram de meios alternativos de comunicação como *hashtags* espalhadas pelo Twitter, *selfies* no Instagram, vídeos no *YouTube*, *chat* de jogos on-line, visando comunicar livremente e se livrar de interceptações e vigilâncias.

A impossibilidade de interceptação dos aplicativos de mensageria e a recalcitrância dessas plataformas em atender e se adequar a norma local facilitam sobremaneira a atividade criminosa, visto não ser mais necessário procurar meios tão alternativos e criativos para a comunicação.

Analisando a Operação *Hashtag*, fica patente o uso de mensagens de aplicativos, não somente para exaltar atos terroristas, como também para planejar ataques desse tipo, restando evidente a importância de ter acesso aos aplicativos de suspeitos.

Países que foram alvo de ataques terroristas já entenderam que os serviços de informação e segurança devem ter algum tipo de acesso aos conteúdos dos aplicativos de mensagens encriptadas para evitar que este tipo de serviços possa ser usado por terroristas.

Não só, a Estratégia Nacional de Defesa (END), impõe a necessidade de cooperação entre todas as instâncias do Estado brasileiro visando ao incremento do nível de Segurança Nacional, considerando que prevenção e combate ao terrorismo e a aplicação do direito são pilares da Estratégia Global contra o Terrorismo instituída com a criação do *Counter Terrorism Implementation Task Force*.

Nessa eterna "*briga de gato e rato*"[12], deixar aplicativos de mensagens funcionarem, sem respeitar a legislação pátria, prometendo comunicação livre e segura, sem preocupação de monitoramento, é uma segurança apenas paras os criminosos, colocando em risco a sociedade.

[12] Criminosos procuram meios e formas de executarem seus crimes e não serem descobertos pela polícia. Sendo que quando são descobertas suas maneiras de agir, rapidamente buscam outras que a polícia não sabe. Criando um ciclo recorrente que a polícia sempre está atrás dos bandidos.

A falta de monitoramento pode retardar ou até mesmo impedir uma ação eficiente dos órgãos estatais frente a ações terroristas. É improtelável definição jurisprudencial e legal acerca da possibilidade de interceptação e fornecimento dos dados por partes das empresas responsáveis pelas plataformas e aplicativos.

Essa definição é necessária e deve ser consolidada, precedendo a definição de ferramentas e modos de utilização para evitar um quadro de nulidade futura, uma vez que a falta de amparo pode comprometer a utilização dos dados obtidos como prova.

Diante de todo exposto, resta claro que a falta de monitoramento e uso descontrolado dos serviços de mensageria tem levado criminosos a fazer uso dessas plataformas para se comunicarem, encontrando um verdadeiro terreno fértil para planejar suas práticas delituosas e não serem alcançados pela Justiça, garantindo a execução de suas ações criminosas e impunidade de seus atos, fragilizando a segurança nacional.

Ademais, empresas estrangeiras, sob pena de grave violação à soberania nacional, não podem se estabelecer no país e resistirem em cumprir a legislação vigente, visto que o espaço virtual, definitivamente, não está acima dos Estados nacionais.

Parafraseando o Excelentíssimo Ministro Barroso, por uma questão de Soberania e muito mais de Segurança, no nosso país só entra quem queremos e desde que cumpram as nossas regras.

REFERÊNCIAS

AMARAL, B. decisão contra telegrama é o primeiro bloqueio com fundamento no marco civil. **Teletime**, São Paulo, 18 mar. 2022. Disponível em: https://teletime.com.br/18/03/2022/decisao-contra-telegram-e-o-primeiro-bloqueio-com-fundamento-no-marco-civil/. Acesso em: 24 set. 2022.

ARAÚJO, Gilcilene; ROMERO, Maria. Juiz do Piauí diz que WhatsApp foi 'arrogante' diante da Justiça do Brasil. **G1,** [*S.l.*], 26 fev. 2015. Disponível em: https://g1.globo.com/pi/piaui/noticia/2015/02/juiz-do-piaui-diz-que-whatsapp-foi-arrogante-diante-da-justica-do-brasil.html. Acesso em: 27 set. 2022.

BARROSO, L. R. Barroso considera a suspensão do Telegram uma medida viável durante as eleições deste ano. [Entrevista concedida a] Mariana Muniz. **O Globo**, Brasília, 13 fev. 2022. Disponível em: https://oglobo.globo.com/politica/barroso-considera-suspensao-do-telegram-uma-medida-viavel-durante-as-eleicoes-deste-ano-25392201?versao=amp. Acesso em: 20 set. 2022.

BOELTER, T. Especial: o que dizem especialistas em criptografia sobre o bloqueio do WhatsApp. [Entrevista concedida a] Dennys Antonialli, Francisco Brito Cruz e Mariana Giorgetti Valente. **Estadão,**. São Paulo, 21 jun. 2016. Disponível em: https://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/. Acesso em; 24 SET. 2022.

BOTTINO, Celina; ARCHEGAS, João Victor; PADRÃO, Vinicius. Polêmicas do bloqueio do Telegram: proporcionalidade, eficácia e fundamentação. Internet não comporta soluções fáceis para problemas difíceis. **Jota**, São Paulo, 18 de março de 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/bloqueio-telegram-proporcionalidade-eficacia-fundamentacao-polemicas-18032022. Acesso em: 7 set. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2022a]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em: 12 set. 2022.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Rio de Janeiro, RJ: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 26 set. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 set. 2022.

BRASIL. **Lei nº 13.260, de 16 de março de 2016.** Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília, DF: Presidência da República, 2016a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 24 set. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 14 set. 2022.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Recurso em Habeas Corpus nº 75.800 (2016/1239483-8).** A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96. Relator: Min. Felix Fischer. Brasília, DF: STJ, 26 set. 2016c. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/862575507/inteiro-teor-862575526. Acesso em: 27 set. 2022.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus nº 51.531 (2014/0232367-7).** Ilícita é a devassa de dados, bem como de conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização juducial. Relator: Min. Nefi Cordeiro. Brasília, DF: STJ, 226 set. 2016b. Disponível em:

https://www.jusbrasil.com.br/jurisprudencia/stj/340165638/relatorio-e-voto-340165682. Acesso em: 20 set. 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso em mandado de segurança nº 60.531- RO (2019/0099392-7).** Recurso em mandado de segurança. Interceptação de dados. Astreintes. Possibilidade em abstrato. Criptografia de ponta a ponta. Impossibilidade fática, no caso concreto, de cumprimento da ordem judicial. Recurso provido. Relator: Ministro Nefi Cordeiro. R.P/Acórdão: Ministro Ribeiro Dantas. Brasília, DF: STJ, 2019. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1206303565/inteiro-teor-1206303573. Acesso em: 10 set. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) nº 5527.** Suspensão ou interrupção dos serviços fornecidos por provedores de conexão ou aplicações de internet determinada por ordem judicial. Relatora:Min. Rosa Weber. Brasília, DF: STF, 2022b. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15350632175&ext=.pdf. Acesso em: 20 set. 2022.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403**. Decisão: Após o voto do Ministro Edson Fachin (Relator), que julgava procedente o pedido formulado na arguição de descumprimento de preceito fundamental para declarar a inconstitucionalidade parcial. Brasília, DF: STF, 17 jun. 2020. https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 12 set. 2022.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental.** Trata-se de arguição de descumprimento de preceito fundamental, ajuizada pelo Partido Popular Socialista – PPS, com pedido de medida cautelar, "contra decisão do Juiz da Vara Criminal de Lagarto (SE), Marcel Maia Montalvão, nos autos do Processo nº 201655000183, que bloqueou o aplicativo de comunicação WhatsApp". Rel. Min. Edson Fachin. Brasília, 19 jul. 2016d. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acesso em: 27 ago. 2022

BRASIL. Supremo Tribunal Federal. **Petição 9.935 Distrito Federal.** Determina a suspensão completa e integral do funcionamento do Telegram no Brasil, consignando que a medida persistiria até o efetivo cumprimento das decisões judiciais anteriormente proferidas. Relator: Min. Alexandre de Moraes. Decisão em 17 mar. 2022. Brasília, DF: STF, 2022c. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DecisaoTelegram20mar.pdf. Acesso em: 25 set. 2022.

CARRAPATOSO, M. S. WhatsApp não pode ser "um lugar secreto para os terroristas". **Observador**, Lisboa, 26 mar. 2017. Disponível em: https://observador.pt/2017/03/26/whatsapp-nao-pode-ser-um-lugar-secreto-para-os-terroristas/. Acesso em: 24 set. 2022.

COUTINHO, M. O que é criptografia de ponta a ponta? Entenda o recurso de privacidade. **Tectudo**, [*S. l.*], 12 de junho de 2019. Disponível em: br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o- recurso-de-privacidade.ghtml. Acesso em: 24 set. 2022.

CRIPTOGRAFIA de ponta-a-ponta. **Blog do whatsApp,** [*S. l.*], 5 de abril de 2016. Disponível em: https://blog.whatsapp.com/end-to-end-encryption. Acesso em: 10 ago. 2022.

EXCLUSIVO: grupos no app Telegram violam leis e abrigam negociações de drogas, armas, pornografia infantil e outros crimes. **G1 – Fantástico**, [*S. l.*], 2022. Disponível em: https://g1.globo.com/fantastico/noticia/2022/03/13/exclusivo-grupos-no-app-telegram-violam-leis-e-abrigam-negociacoes-de-drogas-armas-pornografia-infantil-e-outros-crimes.ghtml. Acesso em: 5 maio 2022.

GARDNER, F. Como os terroristas se comunicam? **BBC News Brasil**, [*S. l.*], 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/11/131103_terroristas_comunicam_an. Acesso em: 5 maio 2022.

GOMES, Helton Simões. Estado Islâmico usa de WhatsApp a Twitter para promover 'terrorismo viral'. **G1 – Tecnologia e Games**, [*S. l.*], 2015. Disponível em: https://g1.globo.com/tecnologia/noticia/2015/11/estado-islamico-usa-de-whatsapp-twitter-para-promover-terrorismo-viral.html. Acesso em 05 maio 2022.

GRUPO terrorista usa o chat do PS4 para se comunicar, segundo Ministro belga. **Combo Infinito,** [*S. l.*], 2015. Disponível em: https://www.comboinfinito.com.br/principal/grupo-terrorista-usa-o-chat-do-ps4-para-se-comunicar-segundo-ministro-belga/. Acesso em: 5 maio 2022.

INTRODUÇÃO ao iCloud. **Manual do Usuário do Icloud**. [*S. l.*]: Apple, 2022. Disponível em: https://support.apple.com/pt-br/guide/icloud/mm74e822f6de/icloud#:~:text=iCloud%20%C3%A9%20o%20servi%C3%A7o%20da,mais%20com%20amigos%20e%20familiares. Acesso em: 19 set. 2022.

ISRAEL, C. B. Território, Jurisdição e Ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet. **GeoUSP:** espaço e tempo**,**, São Paulo, v. 24, n. 1, p. 69-82, 2020. Disponível em: https://www.revistas.usp.br/geousp/article/view/161521. Acesso em: 5 maio. 2022.

MEIOS de comunicação. **Significados,** *[S.l.],* 2022. Disponível em: https://www.significados.com.br/meios-de-comunicacao/. Acesso em: 20 set. 2022.

MENDES, L. E. O acesso aos dados telemáticos do aplicativo whatsapp e a investigação policial: uma análise sob a ótica dos Tribunais Superiores. *In*: PEDRO, D. *et al.* (Org.). **Temas atuais no direito brasileiro sob uma abordagem jurisprudencial.** Fortaleza, CE: DINCE, 2022. 224p.

NOVOS recursos para mais privacidade, mais proteção e mais controle. **Blog do WhatsApp,** [*S. l.*], 2022. Disponível em: https://blog.whatsapp.com/. Acesso em: 28 set. 2022.

O QUE é uma VPN e como funciona? **Kaspersky,** [*S. l.*], 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 25 set. 2022.

PARANÁ. **Ação penal nº 5046863-67.2016.4.04.7000/PR.** 14º Vara Federal de Curitiba. O Ministério Público Federal, com fulcro nos elementos constantes do inquérito policial 007/2016-DPF/MJ (5023557-69-2016.4.04.7000), ofereceu denúncia. Curitiba, PR, 2016.

PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil:** mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Pág. 20 Disponível em: https://bit.ly/3kGTde3. Acesso em: 28 ago. 2022.

PFEFFERKORN, R. Especial: o que dizem especialistas em criptografia sobre o bloqueio do WhatsApp. [Entrevista concedida a] Dennys Antonialli, Francisco Brito Cruz e Mariana Giorgetti Valente. **Estadão.** Deu nos Autos. São Paulo, 21 jun. 2016. Disponível em: https://link.estadao.com.br/blogs/deu-nos-autos/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/. Acesso em: 24 set. 2022.

PIAUÍ. Tribunal de Justiça. **Mandado de Segurança nº 2015.0001.001592-4.** Mandado de segurança à decisão de magistrado que determina a suspensão do aplicativo WhatsApp em prol de investigação criminal. Relator: Des. Raimundo Nonato da Costa Alencar. Teresina, PI: TJ, 2015. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pi/386999708. Acesso em: 27 ago. 2022.

PROSSER, T. Theorising Utility Regulation. **Modern Law Review**, [*S.l.*], v. 62, p. 196-217, 1999.

RÚSSIA diz que Telegram é usado por terroristas e pede acesso a mensagem criptografada. **G1**, [*S. l.*], 2017. Disponível em: https://g1.globo.com/tecnologia/noticia/russia-diz-que-telegram-e-usado-por-terroristas-e-pede-acesso-a-mensagem-criptografada.ghtml. Acesso em 05 maio 2022.

SÃO PAULO (Estado). Tribunal de Justiça. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Acesso em: 27 ago. 2022.

SERGIPE. Tribunal de Justiça. **Mandado de Segurança nº 201600110899.** Reconsideração. Decisão concessiva liminar. Relator: Desembargador Ricardo Múcio Santana de Abreu Lima, Aracaju, SE: TJSE, 3 maio 2016e. Disponível em: https://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf. Acesso em: 26 ago. 2022.

VERMEULE, A. **Law's Abnegation**: from Law's Empire to the Administrative State. Cambridge: Harvard University Press, 2016.

WHATSAPP. **Sobre o WhatsApp**. [*S.l.]:* Whatsapp, 2022. Disponível em: https://www.whatsapp.com/about. Acesso em: 27 ago. 2022.