UNIVERSIDADE ESTADUAL DA PARAÍBA

CAMPUS I

PAULO HENRIQUE FELIX DOS SANTOS

LIMITES E CONTORNOS NA INTERCEPTAÇÃO TELEMÁTICA DAS COMUNICAÇÕES PELO *WHATSAPP* NA PERSECUÇÃO PENAL

CAMPINA GRANDE - PARAÍBA

2022

PAULO HENRIQUE FELIX DOS SANTOS

LIMITES E CONTORNOS NA INTERCEPTAÇÃO TELEMÁTICA DAS COMUNICAÇÕES PELO *WHATSAPP* NA PERSECUÇÃO PENAL

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Jurídicas, Campus I, Universidade Estadual da Paraíba, como requisito parcial à obtenção do Título de Bacharel em Direito.

Orientadora: Profª. Drª. Aureci Gonzaga Farias.

Área de concentração: Ciências Criminais e Novas Tecnologias.

CAMPINA GRANDE – PARAÍBA

2022

F224l Santos, Paulo Henrique Felix dos.
Limites e contornos na interceptação telemática das comunicações pelo Whatsapp na persecução penal [manuscrito] / Paulo Henrique Felix dos Santos. - 2022.
36 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2022.

"Orientação : Profa. Dra. Aureci Gonzaga Farias , Departamento de Direito Público - CCJ."

1. Novas tecnologias. 2. Comunicações instantâneas. 3. Criptografia. I. Título

21. ed. CDD 345.02

Elaborada por Kênia O. de Araújo - CRB - 15/649 BSCCJ/UEPB

PAULO HENRIQUE FELIX DOS SANTOS

LIMITES E CONTORNOS NA INTERCEPTAÇÃO TELEMÁTICA DAS COMUNICAÇÕES PELO *WHATSAPP* NA PERSECUÇÃO PENAL

Aprovado em: 09 / 03 / 2022

BANCA EXAMINADORA

Aureci Gonzaga Farias

Profª. Drª. Aureci Gonzaga Farias (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Rosimeire Ventura Leite

Profª. Drª. Rosimeire Ventura Leite (UEPB)

Rayane Félix Silva

Profª. Rayane Félix Silva (UEPB)

AGRADECIMENTOS

Agradeço a Deus e aos espíritos benfeitores pela força na vida, direcionando-me sempre ao melhor caminho, mesmo quando eu não enxergava a direção a ser seguida.

À minha mãe por me acompanhar em todas as adversidades com carinho, empatia e zelo. É, sem dúvidas, a pessoa mais admirável que conheço. Com infância de pouca comida e muito suor, é a quem vejo como demonstração de resiliência. É em quem confio e a quem amo.

Ao meu pai, embora não se encontre presente em vida, pois é a quem devo, em grande parte, a base de quem eu sou.

Aos meus irmãos Bruna e Pablo, por todo o carinho e amor em minha jornada.

A Raimundo Brito por todo o companheirismo, dando-me coragem e incentivo.

Ao meu amigo Lucas por dividir comigo todos os momentos bons e ruins.

Aos meus amigos mais próximos da universidade Juliana, Maria Luiza, Rafaela, Moisés, Luana e Sarah.

Ao meu querido cachorro por toda distração e carinho em momentos de estresse.

À professora Aureci, por toda dedicação, disponibilidade e empenho. Devo a ela diversos ensinamentos.

À Doutora Zedna Mara, pela revisão deste Trabalho de Conclusão de Curso.

Aos professores José Cavalcanti dos Santos e Lucira Freira Monteiro, por todo o auxílio prestado na monitoria e no projeto de extensão.

Aos demais docentes e funcionários da Universidade Estadual da Paraíba, os quais me auxiliaram imensamente até aqui.

Tornou-se chocantemente óbvio que a nossa tecnologia excedeu a nossa humanidade.

(Albert Einstein).

LIMITES E CONTORNOS NA INTERCEPTAÇÃO TELEMÁTICA DAS COMUNICAÇÕES PELO *WHATSAPP* NA PERSECUÇÃO PENAL

SANTOS[1], Paulo Henrique Felix dos

RESUMO

Este Trabalho de Conclusão de Curso tem como objetivo central identificar formas legais de interceptação das comunicações telemáticas, feitas por intermédio do *WhatsApp*, levando em consideração as limitações impostas pelos direitos fundamentais individuais, explicitados na Carta Magna brasileira. Para proporcionar as bases lógicas da investigação científica, a pesquisa utilizou os métodos observacional e indutivo. Em relação aos fins, a pesquisa foi exploratória e descritiva, de maneira a propiciar familiaridade com o objeto de estudo, fazendo a análise de exemplos que estimulem a compreensão do tema e a descrição das características da interceptação telefônica. Quanto aos meios, foi bibliográfica e documental, com emprego das técnicas de investigação teórica, utilizando documentos e doutrinas no âmbito jurídico, de maneira a aproximar-se do objeto de estudo. Por meio da técnica normativa, analisou-se a legislação pertinente e, através do uso da técnica da observação e investigação empírica foi efetuada a leitura, análise e interpretação de estudo de caso, livros, artigos e jurisprudências. Considerando que a jurisprudência, no Brasil, encontra grande impasse na interceptação das comunicações telemáticas do *WhatsApp*, em razão da sua criptografia ponta a ponta, questiona-se: como fazer a válida interceptação das comunicações telemáticas realizadas por meio do *WhatsApp* na persecução penal? Os resultados da análise feita demonstram a necessidade da criação de uma lei específica ou de modificação na Lei nº 9.296, de 24 de julho de 1996, com o intuito de, respectivamente, disciplinar ou ampliar as possibilidades de emprego de meios tecnológicos para a interceptação das comunicações feitas por intermédio do *WhatsApp*. Com isto, poder-se-ia fazer uso de um *malware*, de maneira a infiltrar-se no *WhatsApp* do acusado ou investigado, antes ou depois que ocorresse a criptografia das comunicações. A adoção das medidas legais e práticas sugeridas, ao garantir a efetivação da interceptação das comunicações realizadas através do WhatsApp, propiciaria ao Estado a capacidade investigativa necessária ao desempenho do seu papel no âmbito penal e processual penal.

Palavras-chave: Novas Tecnologias. Comunicações Instantâneas. Criptografia.

[1] Concluinte do Curso de Bacharelado em Direito pela Universidade Estadual da Paraíba (UEPB). Endereço eletrônico: <paulo.santos@aluno.uepb.edu.br>.

LIMITS AND CONTOURS IN THE TELEMATIC INTERCEPTION OF COMMUNICATIONS THROUGH WHATSAPP IN CRIMINAL PROSECUTION

SANTOS[2], Paulo Henrique Felix dos

ABSTRACT

This Course Conclusion Work has as its central objective to identify legal forms of interception of telematic communications, made through WhatsApp, taking into account the limitations imposed by individual fundamental rights, listed in the Brazilian Constitution. To provide the logical basis of scientific research, the research used observational and inductive methods. Regarding the purposes, the research was exploratory and descriptive to propitiate familiarity with the object of study, analyzing examples that stimulate the understanding of the theme and describing the characteristics of telephone interception. As for the means, it was bibliographic and documentary, adopting theoretical research techniques, using documents and doctrines in the legal sphere, in order to approach the object of study. Thus, through the normative technique, the relevant legislation was analyzed and, using the technique of observation and empirical investigation, the reading, analysis and interpretation of case study, books, articles and jurisprudence was performed. Considering that the Brazilian jurisprudence faces great impasse in intercepting telematic communications of *WhatsApp*, due to its end-to-end encryption, the following question must be answered: how to make the valid interception of telematic communications performed through *WhatsApp* in criminal prosecution? The analysis results show the need to create a specific law or modify law no. 9296 of July 24, 1996, respectively aiming at disciplining or expanding the possibilities of using technological means for the interception of communications made through *WhatsApp*. With this, one could use a malware in order to infiltrate the investigated subject's *WhatsApp*, before or after the encryption of communications occurred. The adoption of the legal and practical measures suggested, by ensuring the effective interception of communications made through *WhatsApp*, would provide the State with the investigative capacity necessary to perform its role in the criminal and criminal procedural spheres.

Keywords: New Technologies. Instant Communications. Cryptography.

[2] Completing the Bachelor's Degree in Law from the State University of Paraíba (UEPB). Electronic address: <paulo.santos@aluno.uepb.edu.br>.

SUMÁRIO

1 INTRODUÇÃO

O célere desenvolvimento tecnológico, no mundo atual, faz com que a investigação criminal adquira caráter dinâmico, sofrendo mudanças de maneira a adaptar-se à realidade. É que, embora crimes mais simples não tenham deixado de ocorrer, a ação criminosa tem sido aprimorada, passando por ampla preparação e utilizando instrumentos de alta tecnologia, o que demanda uma resposta estatal proporcional.

É cediço que a nova era da tecnologia marcou todas as dimensões da vida social. O sistema judiciário, por conseguinte, também sofreu essa influência, lidando atualmente com a necessidade de adequar seus princípios e normas criminais a esse novo panorama técnico-científico.

Nesse novo cenário eletrônico, observa-se que se parou, em um curto lapso temporal, de empregar tão somente as formas presenciais de escrita e fala como método de comunicação, cedendo-se espaço a novos sistemas mais eficazes e rápidos, por meio da conexão com a Internet, como, por exemplo, o uso do *WhatsApp*, um aplicativo de mensagens instantâneas para telefones celulares inteligentes ("*smartphones*"), que permite o envio e recebimento de mensagens de texto, imagens e arquivos multimídia.

Considerado como a plataforma de comunicação mais popular do planeta, o *WhatsApp*, no entanto, não é utilizado apenas para a comunicação convencional: o seu emprego se dá também para cometer vários delitos tipificados no Código Penal brasileiro, notadamente por organizações criminosas, sendo, portanto, um instrumento do crime cibernético. Nesse contexto, surgem dúvidas quanto às normas a serem aplicadas, a fim de disciplinar o uso dessa ferramenta no âmbito penal e processual penal.

Tendo em vista o exposto, o presente Trabalho de Conclusão de Curso, intitulado "Limites e Contornos na Interceptação Telemática das Comunicações pelo *WhatsApp* na Persecução Penal", tem, como objetivo geral, identificar formas legais de interceptação das comunicações telemáticas, feitas por intermédio do *WhatsApp*, levando em consideração as limitações impostas pelos direitos fundamentais individuais, explicitados na Carta Magna brasileira; e, como objetivos específicos, analisar as normas legais brasileiras existentes e a sua adequação à interceptação de comunicações efetuadas através do *WhatsApp*; e sugerir as medidas alternativas que

possam servir de solução a eventual dilema entre essa interceptação e a garantia de direitos individuais.

Para alcançar os objetivos propostos e de forma a proporcionar as bases lógicas da investigação científica, a pesquisa utilizou os métodos observacional e indutivo. O observacional, por servir de base para qualquer área das Ciências, de modo que foram captados os aspectos essenciais e acidentais do objeto da pesquisa. O indutivo, que consiste em partir da análise de dados particulares para que se obtenha noções gerais. Partiu-se, então, da análise da interceptação telemática de conversas, realizadas por meio do *WhatsApp*, que envolvam investigado ou acusado, chegando-se, ao final, a uma solução ao impasse no uso válido da interceptação destas conversas.

Em relação aos fins, a pesquisa foi exploratória e descritiva, de maneira a propiciar familiaridade com o objeto de estudo, fazendo a análise de exemplos que estimulem a compreensão do tema e descrição das características da interceptação telefônica. Quanto aos meios, foi bibliográfica, porque se buscou conhecer, analisar, explicar e discutir contribuições sobre o tema, fazendo uso de material acessível ao público em geral, como dicionários, teses, artigos, dissertações etc. Também se utilizou da pesquisa documental, porque foi feita a coleta, classificação, seleção difusa e utilização de informações, como das Leis nº 12.965, de 23 de abril de 2014, e nº 9.472, de 16 de julho de 1997.

Quanto aos procedimentos técnicos, fez-se emprego das técnicas de investigação teórica, utilizando documentos e doutrinas no âmbito jurídico, de maneira a aproximar-se do objeto de estudo. Isso foi feito por meio da técnica normativa, detendo-se à legislação pertinente, como por exemplo, a Constituição da República Federativa do Brasil, de 1988 e as Leis nº 9.296, de 24 de julho de 1996, e nº 12.965, de 23 de abril de 2014. Ademais, a fim de possibilitar maior contato imediato com a realidade estudada, também se fez uso da técnica da observação e de investigação empírica por intermédio da leitura, análise e interpretação de estudo de caso, livros, artigos e jurisprudências.

Justifica-se a escolha do tema como objeto de estudo, portanto, pela notória dinâmica estabelecida com o uso de novas tecnologias, que passaram a fazer parte do cotidiano, sendo utilizadas, não raras vezes, para o planejamento e prática de crimes, havendo a veiculação de notícias na mídia a respeito da interceptação e da quebra de sigilo das comunicações realizadas por meio do *WhatsApp*, especialmente

com a Comissão Parlamentar de Inquérito da Covid-19, o que despertou o interesse do autor pelo tema.

O trabalho está estruturado em cinco capítulos, incluindo esta Introdução. O Capítulo 2 aborda os dilemas causados pela introdução do *WhatsApp* na vida contemporânea, sendo feitas ponderações a respeito do direito à privacidade e da eficiência da persecução penal, bem como considerações acerca da criptografia. O Capítulo 3 apresenta os principais regimes jurídicos brasileiros aplicáveis à interceptação das comunicações telemáticas realizadas por meio do *WhatsApp*. O Capítulo 4 analisa medidas passíveis de serem aplicadas para possibilitar a solução do dilema causado pelo *WhatsApp*, a saber: espelhamento do *WhatsApp*, proibição da criptografia ou do aplicativo, uso de *backdoors* obrigatórios e emprego de um *software* malicioso. E o Capítulo 5 apresenta as considerações finais, indicando as conclusões e sugestões referentes aos objetivos geral e específicos definidos para este trabalho.

Embora já tenham sido realizados outros estudos sobre o assunto, sua abrangência ainda não foi exaurida. Os estudos anteriores carecem de melhor delimitação sobre o uso das comunicações realizadas por meio do *WhatsApp* na persecução penal, de maneira a permitir a sua interceptação para a elucidação do crime e, ao mesmo tempo, resguardar as garantias do acusado ou investigado. A jurisprudência no Brasil encontra grande impasse na interceptação das comunicações telemáticas do *WhatsApp* em razão da sua criptografia ponta a ponta. Outrossim, a sua análise é de extrema relevância científica, social e jurídica – tendo como público alvo a comunidade acadêmica, os aplicadores do Direito e a sociedade em geral – e demanda resposta ao seguinte questionamento: como fazer a válida interceptação das comunicações telemáticas realizadas por meio do *WhatsApp* na persecução penal?

2 NOVAS TECNOLOGIAS E O *WHATSAPP*

Este capítulo visa abordar os dilemas causados pela introdução do *WhatsApp* na vida contemporânea. Para tanto, serão feitas ponderações a respeito do direito à privacidade e da eficiência da persecução penal, bem como considerações acerca da criptografia.

A tecnologia, especialmente nos últimos anos, exerce importante atuação na área da comunicação, na medida em que possibilitou novas formas de contato que, até pouco tempo atrás, eram inimagináveis nas relações humanas. É difícil imaginar uma situação do dia a dia em que os meios tecnológicos não se façam presentes ou que sua utilização seja despicienda.

É frequente que, ao qualificar a sociedade contemporânea, esta seja denominada de sociedade da informação e da comunicação, isso porque as tecnologias fomentaram a obtenção, conservação, organização e compartilhamento de informações, especialmente por meio dos eletrônicos que fazem uso da Internet, os quais são utilizados nos âmbitos econômico, social e político. Nesse contexto, com o incremento na quantidade de informações e o aumento na possibilidade de acessá-las, tem-se uma sociedade voltada para o conhecimento.

Historicamente, a comunicação foi essencial para os homens, sendo, a bem da verdade, indispensável. Há muito tempo, predominam a linguagem oral e a escrita. A primeira por facilitar o contato presencial, e a segunda pelo seu teor mais duradouro e amplo, prolongando no tempo o acesso a informações e permitindo que se tenha acesso a dados sem o contato direto com o emissor.

Para o devido assento de informações no tempo, foram utilizadas anotações em paredes de cavernas, pedras, madeiras, dentre outros. O papel, no entanto, foi o principal meio escrito de transmissão conhecimentos, repassando informações para outras gerações além daquela que as transcreveu. Permitiu, inclusive, que os ausentes se comunicassem, fazendo o uso, por exemplo, de cartas.

Com o decurso do tempo, outras modalidades de intercomunicação foram criadas, sobretudo graças à eletrônica. O telefone fixo, o telefone móvel, rádio e televisão são exemplos disso. Com a telemática, esses meios de comunicação ganharam contornos modernos, permanecendo, contudo, a finalidade básica e comum de possibilitar o repasse de informações.

Segundo Andrade (2009, p. 155/156), as telecomunicações, hoje, abrangem um espectro enorme de procedimentos técnicos de transmissão incorpórea de notícias e de dados, de maneira a suplantar a realidade pretérita, na qual havia tão somente o telefone, o telegrama, o fax, o rádio e o teletexto ou telefoto, que, em conjunto, atualmente são responsáveis por um reduzido número de comunicações.

O *WhatsApp*, aplicativo inserido nesse contexto, é o mais utilizado pelos brasileiros como meio de comunicação, pois está disponível para celulares e é comumente empregado para efetuar ligações e para o envio de mensagens, vídeos e fotos, podendo esse conteúdo ficar armazenado no aparelho do emissor e receptor das mensagens. Nuvens (2018) o conceitua como "um aplicativo de troca de mensagens e comunicação em áudio e vídeo pela Internet, disponível para *smartphones Android, iOS, Windows Phone, Nokia* e computadores *Mac* e *Windows"*. Segundo esse autor, o programa tem mais de 1.500.000.000 (um bilhão e quinhentos milhões) de usuários ativos mensais, espalhados por mais de 180 (cento e oitenta) países.

Ressalta-se que o aplicativo, além de proporcionar a possibilidade de compartilhar a localização, contatos e enviar os históricos das conversas por *e-mail,* cria grupos. Em pesquisa realizada no ano de 2021, pela Panorama *Mobile Time/Opinion Box*, 98% (noventa e oito por cento) dos brasileiros usuários de *smartphone* possuem o *WhatsApp* instalado em seu aparelho. (SALGADO, 2021). Isso demonstra a forte incidência desse aplicativo como meio de comunicação, tendo diversos adeptos.

Quanto à escolha do nome *WhatsApp*, Nuvens (2018) assevera que era uma brincadeira com a expressão em inglês *What's Up*?[3] Acrescenta, ainda, que "o serviço foi criado em 2009 por Brian Acton e Jan Koum, dois ex-funcionários do *Yahoo*, que venderam sua criação ao *Facebook,* em 2014, por US$ 19 bilhões" (dezenove bilhões de dólares).

Em contrapartida, não é apenas para a comunicação convencional que o seu uso acontece. O seu emprego se dá também para cometer vários delitos tipificados no Código Penal brasileiro, notadamente por organizações criminosas, sendo, portanto, um instrumento do *cibercrime*. Em vista dessa nova realidade, remete-se à precisa descrição de Rodrigues (2002, p. 550): "processo muda com o mundo". Nesse

[3] E aí? Como vai? O que se passa? O que é que há? (Tradução do autor).

contexto, surgem dúvidas quanto às normas a serem aplicadas a fim de disciplinar o uso dessa ferramenta no âmbito penal e processual penal.

2.1 DIREITO À PRIVACIDADE E EFICIÊNCIA DA PERSECUÇÃO PENAL

É preciso levar em consideração que aparelhos como *tablets*, *smartphones* e computadores se alastraram nas mãos da população, de forma excepcional, nas últimas duas décadas. Esse aumento no número de portadores desses eletrônicos se deve à facilidade que trouxeram para o dia a dia, abrangendo atividades mais simples até as mais complexas, como por exemplo, compras, pagamentos, músicas e comunicação. Com a popularidade das comunicações telemáticas por meio de mensageiros eletrônicos instantâneos, como é o caso do *WhatsApp*, diversos direitos fundamentais ficaram sujeitos a serem violados, merecendo especial atenção o direito à privacidade. Entretanto, a Constituição da República Federativa do Brasil, de 1988, em seu artigo 5º, inciso X, assegura que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Conforme Doneda (2006, p. 126/127), há mais de um século a busca pelo refúgio da privacidade é vista como um meio instintivo de (sobre)viver, isto é, compreende-se que a casa é o espaço para o qual as pessoas se refugiam do escrutínio público. Modernamente, o *smartphone* pode ser considerado o asilo seguro do ser humano, comportando uma extensão da sua personalidade, com dados e informações dele e de terceiros. No caso do *WhatsApp*, as comunicações realizadas por meio dele costumam conter informações de cunho pessoal, podendo haver vídeos, mensagens e áudios com dados bancários, senhas diversas, informações embaraçosas sobre o emissor e receptor das mensagens ou das ligações, dentre outros elementos sigilosos.

Por outro lado, não se pode olvidar que o “direito à privacidade não se revela ilimitado e imune a intervenções restritivas” (SARLET, 2015, p. 43). O acesso às comunicações realizadas pelo *WhatsApp* é capaz de solucionar crimes, uma vez que, não raras vezes, são feitos comentários por meio dele sobre o planejamento e execução de delitos, trazendo a interceptação eficiência à investigação e ao processo criminal, de maneira a possibilitar, de forma excepcional, a restrição desse direito. A título de exemplo, pode-se citar o papel que o *WhatsApp* representa para o Primeiro Comando da Capital (PCC), pois, segundo Naísa (2016), o *WhatsApp* é empregado

para fins diversos, como o envio e recebimento de mensagens, registro de contabilidade e informações sobre o sorteio de rifas.

Portanto, verifica-se um impasse entre o direito constitucional à privacidade e a necessidade de obtenção de provas e elementos de investigação para elucidação dos crimes, garantindo eficiência na persecução penal. A solução desse conflito demanda um exame do caso concreto, devendo o Estado fazer uma análise dos interesses no caso real, por meio de uma decisão motivada sobre qual deve prevalecer.

2.2 CRIPTOGRAFIA E O *WHATSAPP*

A criptografia é uma ferramenta tecnológica importante na sociedade da informação e da comunicação, a qual, geralmente, impede que terceiros tenham acesso ao conteúdo criptografado. De forma frequente, ainda que sem perceber, as tarefas realizadas no dia a dia utilizam a criptografia, como por exemplo, em serviços bancários *online*, em compras pela Internet ou ao enviar mensagens privadas. Segundo Andress (2011, p. 63), a criptografia é considerada essencial para a segurança da informação e segurança no campo cibernético.

De forma geral, pode-se afirmar que esse instrumento tecnológico é imprescindível para resguardar direitos, a segurança, a privacidade e outros interesses dos cidadãos em um ambiente digital. Por outro lado, um impasse emerge quando se verifica que a capacidade da criptografia de proporcionar sigilo e segurança às informações e comunicações pode trazer consequências adversas, podendo ser um empecilho ou uma ameaça expressiva às diretrizes de segurança pública, quando utilizada para acobertar fins criminosos.

É necessário ressaltar que alguns governos empreenderam esforços para regulamentar a criptografia. Segundo Singh (1999, p. 314), as denominadas *Crypto Wars* (Guerras de Criptografia), dizem respeito a quando o governo dos Estados Unidos tentou, embora não tenha obtido sucesso, promulgar, formalmente, leis e regulamentos que proibissem ou limitassem o desenvolvimento e distribuição de tecnologia referente à criptografia.

Em 2017, a aliança Cinco Olhos – composta por Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos – solicitou, por meio de declaração internacional conjunta, a regulamentação mais firme da criptografia, pretendendo também o aumento na cooperação de empresas de tecnologia que incrementam e

utilizam a criptografia em seus sistemas. Em 2020, a referida aliança, com apoio da Índia e do Japão, divulgou uma declaração internacional sobre criptografia de ponta a ponta, na qual requereu que as empresas de tecnologia desenvolvessem ou alterassem seus serviços de mensagens criptografadas, para possibilitar que as autoridades interceptassem e ganhassem acesso aos dados criptografados ou cópias em texto simples das comunicações dos usuários. Essa solicitação foi respondida de forma negativa por empresas de tecnologia, especialistas em segurança cibernética e organizações da sociedade civil, por considerarem que é incompatível com a realidade técnica da criptografia.

Segundo o que está disposto no *site* do *WhatsApp*, as mensagens e ligações dos seus usuários são protegidas por criptografia "*end to end"* (ponta a ponta), de modo que apenas o emissor e receptor podem ler e escutar a comunicação, não tendo acesso a elas nem mesmo a própria empresa *WhatsApp Inc.* No entanto, em que pese o fato de que a criptografia de ponta a ponta padrão do *WhatsApp* tenha inovado na questão da privacidade, a interferência de *malwares* e, mesmo, de especialistas de segurança bem-intencionados demonstrou que as mensagens dos usuários não são à prova de interceptação. Por exemplo, conforme noticiado por Leetaru (2019), em maio de 2019, no *Site* da *Forbes*, uma empresa de *spyware* descobriu uma falha no sistema de criptografia do *WhatsApp* que lhes permitia instalar um *software* de vigilância simplesmente ligando para os usuários do *WhatsApp*.

3 LEIS BRASILEIRAS APLICÁVEIS À INTERCEPTAÇÃO DO *WHATSAPP*

O objetivo deste capítulo é apresentar os principais regimes jurídicos brasileiros aplicáveis à interceptação das comunicações telemáticas realizadas por meio do *WhatsApp*. Nesse passo, serão feitas conceituações para melhor entender a aplicação desse instituto.

De modo a compreender o que significa a comunicação telemática, é essencial entender o conceito de telecomunicação, uma vez que o termo “telemática” é uma aglutinação das palavras “telecomunicação” e “informática”.

Nesse sentido, destaca-se a definição de telecomunicação, prevista na Lei nº 9.472, de 16 de julho de 1997, em seu artigo 60, parágrafo 1°, como sendo “a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza”.

Já o conceito de telemática, segundo os dicionários, consiste nas tecnologias da comunicação e da informação decorrentes do agrupamento de meios peculiares das telecomunicações – telefone, satélites, cabos, dentre outros – com os meios de informática e seus componentes, tais como o os computadores e sistemas de redes. A junção desses campos possibilitou o transporte de enorme montante de dados, em diminuto espaço de tempo, conectando pessoas de diferentes locais.

A comunicação no *WhatsApp é* feita pela transferência de caracteres gráficos – que constituem mensagens escritas, vídeos, imagens e arquivos – ou por meio de ligações, sendo realizada com auxílio de softwares e da internet, tratando-se, então, de comunicação telemática.

A interceptação, por sua vez, pode ser definida como sendo a captação, por um terceiro, da interação em desenvolvimento entre o comunicador e o receptor, sem que, no entanto, haja o consentimento destes. Para Capez (2011, p. 15), a interceptação “provém de interceptar, intrometer, interromper, interferir, colocar-se entre duas pessoas, alcançando a conduta de terceiro que, estranho à conversa, se intromete a tomar conhecimento do assunto tratado entre os interlocutores”.

3.1 LEI Nº 12.965/2014 *VERSUS WHATSAPP*

A Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, estabeleceu, de acordo com sua ementa, princípios, deveres, direitos e garantias para o uso da Internet no âmbito brasileiro. Essa legislação surge da necessidade de controlar os impactos advindos do comportamento dos usuários no campo virtual, amoldando o Direito à modernidade.

O Marco Civil da Internet foi construído a partir dos pilares da: i) liberdade, que consiste na confecção, acesso e reprodução de conteúdo; ii) neutralidade, a qual obsta a discriminação sem motivação idônea independentemente do transmissor, espécie ou matéria; iii) privacidade, que, como o próprio nome indica, permite ao usuário ter seus dados e informações de cunho pessoal protegidos, limitando o acesso de terceiros. Destaca, portanto, com clareza, a importância de assegurar o direito à privacidade e à liberdade de expressão no âmbito digital, prevendo, em seu artigo 8º, que “a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet”. O legislador assentou conceitos e explanou o sentido de alguns termos, tais como a Internet, terminal e os demais termos dispostos em seu artigo 5º, a seguir colacionado:

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Esse método adotado pelo legislador, sob o ponto de vista hermenêutico, possibilita uma interpretação mais fiel à vontade do legislador, dificultando que se tenha uma interpretação diversa, de modo a dar segurança jurídica.

De forma similar à previsão contida no artigo 5º, inciso XII, da Constituição da República Federativa do Brasil, de 1988, o Marco Civil da Internet prevê, nos incisos II e III do seu artigo 7º, que são assegurados ao usuário, com exceção de ordem judicial, o direito de inviolabilidade e de sigilo do fluxo de suas comunicações pela Internet, bem como de suas comunicações privadas armazenadas. Ademais, o parágrafo 2º do artigo 10 da citada lei expressa que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do artigo 7º".

A partir do disposto na mencionada lei, infere-se que ela resguarda as comunicações feitas por meio do *WhatsApp*, uma vez que o dispositivo que acessa este aplicativo, seja um computador ou um *smartphone*, é um terminal, ocorrendo sua conexão por meio da Internet. Por sua vez, o *WhatsApp* é uma aplicação de Internet, porque o seu conjunto de funcionalidades é acessado por intermédio do referido terminal.

No Brasil, diversas decisões judiciais determinaram o bloqueio do *WhatsApp*. Entre os anos de 2015 e 2016, este aplicativo foi suspenso por três vezes: a primeira delas, em dezembro de 2015, por ordem de um dos juízos de 1º grau de São Paulo; a segunda, em fevereiro de 2016, por um dos juízos de 1º grau de Alagoas; e. em julho de 2016, por um dos juízos de 1º grau do Estado do Rio de Janeiro. Embora não tenham sido implementadas, pois instâncias superiores as tornaram sem efeito, outras ordens de bloqueios também surgiram, tal como as proferidas em fevereiro de 2015 e em maio de 2016, respectivamente, pela Justiça do Piauí e por um dos juízos de 1º grau de Sergipe. Tais suspensões ocorreram como sanção pela não disponibilização do conteúdo das mensagens de investigados que utilizam o aplicativo. O principal argumento para o descumprimento das decisões foi a incapacidade técnica de cumpri-la, tendo em vista a criptografia utilizada.

A Ação Direta de Inconstitucionalidade (ADI) Nº 5.527/DF, tendo por Relatora a Ministra Rosa Weber, foi proposta pelo Partido da República e busca verificar a constitucionalidade da Lei nº 12.965, de 23 de abril de 2014, em seu parágrafo 2º, artigo 10, e os seus incisos III e IV do artigo 12. Esses dispositivos legais foram utilizados para fundamentar sucessivas decisões judiciais estabelecendo a suspensão

temporária de serviços pelo descumprimento de ordem judicial que estipulava que a empresa *WhatsApp Inc.*, responsável pelo aplicativo de troca de mensagens por meio da Internet, providenciasse o acesso ao conteúdo das comunicações. A parte requerente pretende "ver declarada a inconstitucionalidade da penalidade de suspensão temporária e de proibição de exercício das atividades, decorrente de descumprimento de ordem judicial por parte da empresa responsável por fornecer mecanismo de troca de mensagens via Internet".

Segundo o demandante, por se tratar de serviço de comunicação bastante utilizado no Brasil, a suspensão acarretaria em ofensa ao princípio da continuidade do serviço público e à liberdade de comunicação, bem como à intranscedência e à individualização da pena. Sustenta, ademais, que os artigos questionados da Lei n° 12.965/2014 são contrários aos princípios da livre iniciativa, da livre concorrência e da defesa do consumidor, sendo a suspensão medida desproporcional e inadequada.

Por sua vez, a Arguição de Descumprimento de Preceito Fundamental (ADPF) Nº 403/SE, de autoria do Partido Popular Socialista (PPS), ajuizada em desfavor de decisões judiciais, sobretudo à da Vara Criminal da Comarca de Lagarto/SE, a qual determinou a suspensão do *WhatsApp* por 72 (setenta e duas) horas no Brasil, em razão da negativa da empresa em providenciar o acesso às comunicações de investigados nesse aplicativo. Em seus argumentos, o requerente aduziu que a mencionada decisão não observou as liberdades comunicativas sedimentadas no artigo 5º, inciso IX, da Constituição da República Federativa do Brasil de 1988, requerendo a sua suspensão liminar. No mérito, solicitou o reconhecimento de violação de preceito fundamental, de maneira a impedir outras decisões judiciais que suspendam a continuidade da função desempenhada pelo *WhatsApp*. Assim, como bem definido pelo Ministro Relator Edson Fachin em seu voto, a ADPF Nº 403/SE tem por objeto:

> (i) saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do artigo 7º, II, do Marco Civil da Internet; e, em sendo constitucional, (ii) saber se a sanção prevista no inciso III do artigo 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário.

Na referida ADPF, o Juízo da Vara Criminal da Comarca de Lagarto/SE informou que o Tribunal de Justiça de Sergipe cassou a tutela provisória, ordenando a liberação do funcionamento do *WhatsApp*. Por sua vez, a empresa *WhatsApp Inc.* concordou com o disposto na arguição, destacando que as ordens judiciais desse tipo

descumprem as liberdades de expressão e a comunicação, bem como encontram óbice no Marco Civil, impondo uma sanção desequilibrada à população brasileira usuária do aplicativo. A Polícia Federal, no entanto, expressou concordância com as decisões que suspendem, de forma provisória, o aplicativo por considerar que:

> [...] nenhum direito individual é absoluto, devendo sempre ser interpretado dentro do princípio da razoabilidade, de forma a garantir o reconhecimento da supremacia do interesse público sobre o particular, dotando as autoridades encarregadas da persecução criminal dos meios necessários para dar cabal cumprimento aos seus deveres no interesse da sociedade (ADPF nº 403/SE).

O Ministério da Justiça opinou pela falta de descumprimento de preceito fundamental, e a Procuradoria-Geral da República pela procedência do pedido.

Em 27 de outubro de 2016, foi convocada audiência pública na ADPF Nº 403/SE, para tratar das questões técnicas da suspensão do aplicativo *WhatsApp* por decisões judiciais no Brasil. Considerando a clara relação com o objeto da ADI Nº 5.527/DF, foi ampliada a Audiência Pública para incluir os objetos de ambas as ações. Para ela, contribuíram 30 (trinta) expositores, como membros do Ministério Público Federal e da Polícia Federal, representantes de entidades civis e um dos fundadores do *WhatsApp*. É importante frisar a pertinência da audiência pública, pois ela dá voz a diversos agentes, sendo uma das colunas que garantem o acesso à justiça. Destaca-se que, na audiência, conforme mencionado pelo Ministro Fachin em seu voto, os representantes do Ministério Público Federal foram perguntados sobre quais os crimes necessitam de investigação, preferencialmente ou unicamente, por meio de interceptações. Em resposta, informaram que são os crimes cometidos por organizações criminosas, bem com os de tráfico de drogas, pornografia infantil e tráfico de armas.

O Plenário do Supremo Tribunal Federal iniciou, em 27 de maio de 2020, o julgamento conjunto da ADI Nº 5.527/DF e da ADPF Nº 403/SE. Na fundamentação do seu voto, a Ministra Rosa Weber destacou que o artigo 10, parágrafo 2º, da Lei nº 12.965/2014 confere apoio normativo para determinação judicial que disponha sobre o fornecimento do conteúdo de comunicações privadas realizadas por meio de aplicativos de mensagens tão somente na investigação criminal ou na instrução processual penal. Ponderou, no entanto, que esse poder do Estado não leva à dedução de que é ilegal o oferecimento de serviço que use tecnologia que torne inacessível esse conteúdo ao próprio provedor da plataforma, não podendo o Estado

compelir este a ofertar um serviço mais vulnerável, sob o argumento de que poderá, eventualmente, utilizar essa vulnerabilidade para dar cumprimento a ordem judicial.

Para a Ministra, seria um retrocesso impedir o emprego da criptografia. Por outro lado, considerou que, no caso de ser possível cumprir a ordem judicial, ela deve ser executada pelo responsável pelo serviço ou pelos agentes estatais responsáveis por efetuar o acesso. Pontuou, ainda, que, pelo que dispõe a Lei nº 12.965/2014, não há amparo normativo na suspensão do serviço de aplicativo de comunicação pelo descumprimento da decisão judicial de disponibilização das comunicações. Em conclusão, votou pelo seguinte:

> (i) julgo improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014; (ii) julgo procedente o pedido de interpretação conforme a Constituição do art. 10, § 2º, da Lei nº 12.965/2014, a fim de assentar exegese segundo a qual "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º, e para fins de investigação criminal ou instrução processual penal"; (iii) julgo improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014, à compreensão de que não abrangido em sua hipótese de incidência o conteúdo que dele se pretende excluir; (iv) julgo parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) assentar que as penalidades de suspensão temporária das atividades e de proibição de exercício das atividades somente podem ser impostas aos provedores de conexão e de aplicações de internet nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, (b) ficando afastada qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação (ADI 5527 / DF).

Por sua vez, o Ministro Fachin, em seu voto, entendeu que o perigo da aplicação da criptografia ainda não é capaz de fundamentar o uso de soluções que se refiram ao acesso excepcional ou outro recurso que diminua a proteção assegurada por meio de uma criptografia forte. Considerou, então, inconstitucional obstar a utilização da criptografia ponta a ponta, tendo em vista que impactaria desproporcionalmente na vida das pessoas mais vulneráveis. Nesse passo, divergindo em parte do voto da Ministra Rosa Weber, julgou procedente a arguição de descumprimento de preceito fundamental 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.

Sobre a divergência do seu voto, o Ministro explicou que o *WhatsApp* não autoriza que o conteúdo das comunicações entre seus usuários seja fornecido, pois isso exigiria que o aplicativo alterasse seu sistema de criptografia de modo a incluir uma falha em seu sistema. Nesse contexto, pontuou que as ordens judiciais, mesmo que para fins de investigação criminal ou instrução processual penal, não são capazes de determinar que o aplicativo de Internet modifique seu sistema de criptografia.

No ponto de divergência, merece razão a decisão da Ministra Rosa Weber. O Estado precisa, sem esquecer dos direitos fundamentais do acusado, modernizar os seus aparatos investigativos, de modo a equilibrar seus recursos com aqueles utilizados pelos criminosos. Assim, embora se mostre ilegal a inserção de uma vulnerabilidade no aplicativo, se possível o cumprimento da ordem judicial, esta deve ser executada pelo serviço ou pelos agentes estatais responsáveis por efetuar o acesso.

Até a presente data, 21 de fevereiro de 2022, o julgamento se encontra suspenso devido ao pedido de vistas das duas ações feito pelo Ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF).

3.2 LEI Nº 9.296/1996 *VERSUS WHATSAPP*

A Constituição da República Federativa do Brasil, de 1988, prevê, em seu artigo 5º, inciso XII, que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Branco (2015, p. 293), ao analisar a Lei nº 9.296, de 24 de julho de 1996, sustenta que a interceptação telefônica só poderia acontecer no que se refere aos casos de comunicação telefônica, sendo impossível quebrar o sigilo quanto aos dados dispostos nas correspondências postais, telegráficas e comunicações telemáticas. No entanto, pondera o autor que a jurisprudência e a doutrina frisam que não há direitos absolutos, sequer os de correspondência e comunicação telemática, podendo se dar

a restrição dos direitos fundamentais, sem autorização do constituinte, desde que o caso respeite o princípio da proporcionalidade

A Lei nº 9.296/1996, que trata dos mais importantes temas do instituto da interceptação e regulamenta o inciso XII, parte final, do artigo 5º, da Constituição estabelece, em seu artigo 1º, parágrafo único, que o disposto na referida lei se aplica “à interceptação do fluxo de comunicações em sistemas de informática e telemática”. Embora o próprio texto da lei permita a aplicação dela em sistemas de informática e telemática, é necessário verificar a possibilidade de utilização desse regime jurídico nas diferentes formas de comunicação do *WhatsApp*, considerando as suas peculiaridades.

Importante pontuar interessante decisão do Superior Tribunal de Justiça (STJ) no *Habeas Corpus* nº 372.762, impetrado em face de acórdão proferido pelo Tribunal de Justiça do Estado de Minas Gerais. Segundo essa decisão, o artigo 5º, inciso XII, da Constituição da República Federativa do Brasil, de 1988, refere-se à interceptação telefônica ou telemática da comunicação de dados, mas não dos dados em si mesmo.

Quando a ligação se dá por meio do *WhatsApp*, Kist (2019, p. 339) defende que deve ser aplicado o regime jurídico estabelecido pela Lei nº 9.296/1996, isso porque se trata de hipótese em que as características são extremamente similares à conversação telefônica convencional. Nesse sentido, a interferência de diálogo em desenvolvimento por chamada de voz nesse aplicativo provoca a incidência das normas que tratam da interceptação telefônica. A maior dificuldade reside, na verdade, no fato de que o *WhatsApp* usa criptografia ponta a ponta, o que complica a interceptação das ligações e mensagens. No entanto, ainda que se vislumbrem dificuldades técnicas, isso não torna a norma inválida, devendo o seu teor ser considerado. Outra controvérsia, a ser debatida, diz respeito à aplicação da interceptação telemática no caso de comunicação pelo *WhatsApp*, com envio de mensagens escritas, imagens, áudios, vídeos e outros arquivos. Nesses casos, a divergência sobre a aplicação, ou não, do mesmo regime estabelecido para as ligações telefônicas se dá em razão da essência de cada comunicação.

Miranda e Medeiros (2010, p. 289-290) declaram que é direito daquele que profere a palavra de não a ter gravada para a consecutiva reprodução sem que permita. Seu caráter é eminentemente provisório, podendo gerar uma interpretação diversa da pretendida quando desprendida do contexto em que foi empregada, sendo legítima a expectativa de não a ver armazenada.

Kist (2019, p. 340), por sua vez, assegura que a intercomunicação por meio de mensagens escritas, imagens, áudios, vídeos e outros arquivos possui, em sua essência, caráter definitivo. Quem assim mantém a conversação, tenciona vê-la conservar-se no tempo, ficando sujeita à reprodução e divulgação. Há, então, uma dinâmica diversa de quando a palavra se dá por ligações telefônicas, o que justificaria um tratamento diferenciado entre elas.

Feitas essas considerações, não se pode olvidar que, tendo em vista que se trata de uma ferramenta de telecomunicação, o aplicativo *WhatsApp*, além de precisar do emissor e do receptor da mensagem, carece de um terceiro que estabeleça o vínculo entre o primeiro e o segundo. Seja em um curto ou longo período de tempo, há, em todas as ocasiões, um lapso entre a expedição e a recepção, o que leva a crer que a mensagem, nesse período, está com terceiro que a encaminha e, em razão disso, pode ser alvo de interferência com o propósito de interceptá-la.

Em outras palavras, assim como na interceptação de ligações, a interferência do envio de mensagens escritas, imagens, áudios, vídeos e outros arquivos se dá quando a mensagem segue pelos sistemas empregados para o deslocamento e a entrega, isto é, enquanto está na posse de terceiro, o que demonstra uma semelhança entre elas. Portanto, a interceptação das mensagens escritas, imagens, áudios, vídeos e outros arquivos segue o mesmo raciocínio, embora não nos mesmos modos técnicos, mas no que se refere às premissas e condições para a sua captura no decorrer do processo de comunicação (KIST, 2019, p. 341).

Vale ressaltar que, em geral, não há apenas a mera transmissão da comunicação pelo *WhatsApp*. Na verdade, esse conteúdo transmitido tende a ficar armazenado no próprio aplicativo, podendo haver relevância jurídica em tomar conhecimento dele. Assim, no caso de dados armazenados, já não se trata de interceptação telemática, mas de acesso a dados de diálogos pretéritos.

Pode-se afirmar, portanto, que a interceptação telemática do aplicativo *WhatsApp* deve seguir o estabelecido pela Lei nº 9.296/1996, seja no caso de ligações, seja no caso de mensagens escritas, imagens, áudios, vídeos e outros arquivos, aplicando-se, de forma análoga, o instituto da interceptação telefônica.

4 MEDIDAS ALTERNATIVAS PARA A SOLUÇÃO DO DILEMA

O presente capítulo visa analisar as medidas passíveis de serem aplicadas para possibilitar a solução do dilema causado pelo *WhatsApp*, a saber: espelhamento do *WhatsApp*, proibição da criptografia ou do aplicativo, uso de *backdoors* obrigatórios e emprego de um *software* malicioso, pois, conforme ressaltado antes, embora as disposições sobre o regime jurídico da interceptação telefônica e do Marco Civil da Internet sejam aplicáveis às comunicações em curso pelo *WhatsApp*, muitas vezes a interceptação resta inaplicável na prática, em razão da criptografia ponta a ponta do aplicativo. Com isso, o que se verifica é um impasse na possibilidade prática de acesso, em tempo real, das comunicações por meio *WhatsApp*, gerando preocupação na busca por uma alternativa de acesso a esses dados que não infrinja as garantias do acusado ou investigado.

4.1 ESPELHAMENTO DO *WHATSAPP*

Algumas investigações passaram a utilizar o *WhatsApp Web*, que permite ao usuário enviar e receber mensagens e mídias através do navegador do seu computador, por meio do *QR code*, que possibilita o acesso em tempo real das mensagens. Ocorre que essa prática dá um acesso ilimitado ao conteúdo disposto no aplicativo do aparelho, podendo os agentes, inclusive, participarem das conversas. Isso fere a privacidade do acusado ou investigado, bem como coloca em risco a veracidade da prova ou do elemento de investigação.

Em decisão do Superior Tribunal de Justiça (STJ), no *Habeas Corpus* de nº 99.735, contra acórdão proferido pelo Tribunal de Justiça do Estado de Santa Catarina, a ministra relatora Laurita Vaz, considerou nula a decisão judicial que autoriza o espelhamento do *WhatsApp*, via *QR* code, para acesso no *WhatsApp Web*, afirmando não ser possível a analogia com o instituto da interceptação telefônica. Em sua fundamentação, considerou a possibilidade de exclusão das comunicações, que não deixou vestígios quando feita, tendo em vista a criptografia de ponta a ponta utilizada pelo aplicativo. Destacou, ainda, que, diferentemente da interceptação telefônica, os investigadores podem atuar como participantes na conversa e ter acesso a todas as comunicações (*ex tunc*).

4.2 PROIBIÇÃO DA CRIPTOGRAFIA OU DO APLICATIVO

Por sua vez, o óbice ao uso de criptografia de ponta a ponta em serviços de mensagens – ou, mesmo, a proibição do próprio aplicativo – pode parecer medida extrema e impraticável, mas isso não impediu que outros países tenham elaborado tal proposta ou mesmo a efetivado. Segundo Chirisa (2020), a Coreia do Norte, China e Síria proibiram o aplicativo em razão da criptografia. Por seu turno, afirma Walker (2020) que a União Europeia considera a possibilidade de restringir o uso de criptografia de ponta a ponta.

No Brasil, a proibição de aplicativos de mensagens criptografadas ou a proibição desses aplicativos de implementar criptografia de ponta a ponta seria inviável. Seria medida desproporcional que afetaria o direito constitucional à livre iniciativa. Ressalta-se que o *WhatsApp* não é utilizado unicamente para acobertar crimes, mas, sobretudo, para comunicações legais cotidianas. Assim, a não ser que um serviço de mensagens criptografadas seja principal ou especificamente criado ou utilizado para a prática de crimes, os desenvolvedores e usuários são livres para desenvolver, distribuir, possuir ou usar esses aplicativos de mensagens dentro do país. Esse tipo de proibição infringiria a liberdade de expressão. Os usuários têm o direito de preservar suas conversações de terceiros. A criptografia só pode estar sujeita a limites razoáveis, prescritos por lei, que possam ser comprovadamente justificados em uma sociedade livre e democrática.

4.3 *BACKDOORS* OBRIGATÓRIOS

Outra forma mencionada com frequência, como solução para o impasse gerado pela criptografia, é a obrigatoriedade do *backdoor* (porta dos fundos), que consiste na criação de uma entrada vulnerável no sistema, permitindo um invasor no sistema comprometido. Na definição de Kiguolis (2016), no *Site* Sem Vírus, “é um programa malicioso usado para providenciar, ao agressor remoto, acesso não autorizado a um sistema operativo comprometido, explorando as vulnerabilidades de segurança”. Dessa forma, analisando a proposta no campo técnico, criar um *backdoor* na criptografia é similar a introduzir uma vulnerabilidade de segurança ou falha em um sistema. Com isso, o prejuízo à segurança expõe, de forma exponencial, as pessoas a riscos aumentados e indevidos, ameaçando a segurança da informação e privacidade de dados. *Backdoors* obrigatórios, portanto, não são uma opção viável

porque se opõem ao próprio propósito da criptografia, qual seja, assegurar a confidencialidade, integridade e autenticidade dos dados.

O caso *Apple versus FBI*, em que o *Federal Bureau of Investigation*[4] (FBI) dos Estados Unidos da América buscou uma ordem judicial para obrigar a *Apple* a criar uma versão de seu sistema operacional de smartphone que tornasse possível o acesso ao *iPhone* bloqueado do atirador de San Bernardino, demonstrou que as autoridades policiais não precisam de *backdoors* para acessar dispositivos criptografados e dados de suspeitos ou acusados, uma vez que podem obter acesso de outras maneiras. Um relatório posterior do Departamento de Justiça dos Estados Unidos da América concluiu que o pedido do *FBI* à *Apple* para criar uma porta dos fundos era injustificado, visto que a agência de aplicação da lei deveria primeiro ter exaurido outros métodos e meios disponíveis.

Segundo Albergotti e Nakashima (2021), foi confirmado que o *FBI* conseguiu invadir o *iPhone* bloqueado do atirador, com a ajuda de uma empresa australiana de segurança cibernética. Reed (2018) informa que, atualmente, existem dispositivos como o *GrayKey* que estão sendo vendidos para autoridades policiais para desbloquear *iPhones* criptografados. O caso *Apple versus FBI* ilustra que *backdoors* na criptografia não são apenas técnica e legalmente problemáticos, mas também desnecessários.

Tratando sobre a criptografia "*end to end*" e a impossibilidade do uso de um *backdoor* obrigatório, destaca-se o posicionamento de Aranha (2020, p. 144):

> A inviabilidade técnica de introdução de falhas intencionais para interceptação legal não significa que plataformas de comunicação segura estejam completamente imunes a esforços de investigação ou qualquer outra intervenção do aparato investigativo. Na verdade, o esforço de investigação deve se adaptar às características de plataformas para comunicação segura para exercer o seu papel. Equipar agentes e especialistas com informação técnica acurada sobre essas tecnologias é garantir o poder investigativo do Estado em longo prazo, à medida que tecnologias de preservação de privacidade se disseminam cada vez mais.

Desse modo, a impossibilidade de incluir um *backdoor* no *WhatsApp* não acarreta em um óbice automático a outros esforços investigativos que visem à interceptação desse aplicativo.

[4] Departamento Federal de Investigação (Tradução do autor).

4.4 *MALWARE*

O *malware* é uma das ferramentas que se pode levar em consideração para concretizar os esforços investigativos supramencionados por Aranha. É um termo abreviado da expressão em inglês *malicious software* (*software* malicioso). Para Ramalho e Vaciago (2016, p. 88), pode ser definido como um programa que se instala, de forma discreta, em um sistema de processamento de dados, não havendo o conhecimento ou concordância dos usuários, a fim de que seja posto em risco o sigilo e a integridade dos dados. Esses programas são capazes de burlar dispositivos de segurança como o antivírus e recursos como a criptografia.

Utilizar esse método na investigação impactaria, sobremaneira, nas garantias individuais do acusado, sendo, então, um método extraordinário de colheita de provas. Trata-se, ainda, de um método oculto, pois se dá sem o conhecimento do investigado, estabelecendo-se por um certo tempo, de modo a registrar o comportamento natural do indivíduo.

Andrade (2009, p. 164) há mais de dez anos já sinalizava para a problemática trazida pela criptografia em serviços de comunicação, destacando como solução a vigilância das fontes, segundo a qual se captaria as conversas antes da codificação ou após por meio de programas do tipo cavalo de Troia.

Analisando a legislação estrangeira, verifica-se que alguns países já regularam o *malware* como meio de investigação de prova em processo penal, principalmente na Europa.

Em 2017, a fim de melhorar o processo criminal com uso de tecnologia, a Alemanha emendou o *Strafprozeßordnung* (Código de Processo Penal). Na seção 100a, que trata da vigilância das telecomunicações, permitiu que estas sejam interceptadas e gravadas com meios técnicos para interferir nos sistemas de tecnologia da informação utilizados pelo investigado, se tal medida for, de fato, necessária para permitir a interceptação e o registro, ainda que façam o uso de criptografia. Outrossim, a seção 100b permite, mesmo sem o conhecimento do investigado, pesquisa remota secreta em sistemas de tecnologia da informação.

Segundo Batista (2018, p. 54), a jurisprudência alemã tem interpretado a seção 100a e seguintes do referido código, no que diz respeito à interceptação de telecomunicações, para permitir o uso de *malware*, nos casos em que seja preciso acessar conversas automaticamente criptografadas.

A Espanha também regulamentou o uso de medidas tecnológicas na investigação por meio da *Ley Orgánica* nº 13, *de 5 de octubre de 2015*, a qual alterou a *Ley de Enjuiciamento Criminal* (Código de Processo Penal). No texto de sanção da lei, foi destacado que a *Ley de Enjuiciamento Criminal* não conseguiu escapar ao passar do tempo, pois novas formas de criminalidade ligadas ao uso de tecnologias revelam a insuficiência de um marco regulatório concebido para tempos diferentes.

O texto da lei destaca que os fluxos de informação gerados pelos sistemas de comunicação telemática alertam para as possibilidades que estão à disposição do infrator, mas também fornecem ferramentas poderosas de investigação às autoridades públicas, ressaltando, ainda, a necessidade de encontrar um equilíbrio na capacidade do Estado de enfrentar essa nova fenomenologia criminal e que, por mais relevante que tenha sido o empenho de juízes e tribunais para delimitar os limites do Estado na investigação criminal, a delegação à jurisprudência do que deveria ser objeto de regulamentação legislativa tem acarretado um déficit na qualidade democrática do sistema processual do país.

O Capítulo IV da *Ley de Enjuiciamento Criminal* trata das disposições comuns à intercepção de comunicações telefônicas e telemáticas, à captura e gravação de comunicações orais por meio da utilização de dispositivos eletrônicos, o emprego de dispositivos técnicos de monitorização, localização e captura de imagens, o registo de dispositivos de armazenamento em massa de informação e registros remotos em equipamento de informática. Para o emprego de uma das medidas investigativas reguladas nesse capítulo, a mencionada lei prevê a necessidade de autorização judicial expedida em plena observância aos princípios da especialidade, idoneidade, excepcionalidade, necessidade e proporcionalidade da medida.

O Capítulo V refere-se à intercepção de comunicações telefônicas e telemáticas. Prevê, em seu artigo 588º a, que a autorização para a intercepção de comunicações telefônicas e telemáticas só pode ser concedida quando a investigação tenha por objeto crimes dolosos puníveis com um limite máximo de três anos de prisão, crimes cometidos no seio de grupo ou organização criminosa, crimes de terrorismo ou crimes cometidos por meio de instrumentos informáticos ou de qualquer outra tecnologia de informação e comunicação ou serviço de comunicação, prevendo a duração máxima inicial da intervenção, que será contada a partir da data da autorização judicial, de três meses, prorrogável por períodos sucessivos de igual duração até ao período máximo de dezoito meses.

Extinto o segredo e caducado o prazo de validade da medida de intervenção, a *Ley de Enjuiciamiento Criminal* define que será entregue, às partes, cópia das gravações e transcrições efetuada. Essa lei dispõe que na gravação em que houver dados referentes a aspectos da vida íntima das pessoas, somente será entregue a gravação e transcrição daquelas partes que não se referem a eles, sendo expressamente declarada a ausência de alguma parte da gravação na transcrição entregue.

Já o Capítulo IX aborda o uso de registros remotos em equipamentos de informática. Em seu artigo 588º *septs*, permite que o juiz competente autorize a utilização de dados e códigos de identificação, bem como a instalação de *software*, que possibilite, de forma eletrônica, o exame – à distância e sem que o proprietário ou utilizador tenha conhecimento – do conteúdo de um computador, sistema informático, instrumento de armazenamento massivo de dados informáticos ou base de dados.

Em outras palavras, a legislação espanhola permite a utilização do *malware*, limitando a aplicação do Capítulo IX da *Ley de Enjuiciamento Criminal* aos crimes cometidos no seio de organizações criminosas, crimes terroristas, crimes cometidos contra menores ou pessoas com capacidade judicialmente modificada, crimes contra a Constituição, traição e relacionados com a defesa nacional, crimes cometidos por meio de ferramentas informáticas ou qualquer outra tecnologia de informação ou telecomunicações ou serviço de comunicação, definindo que, quando os agentes que efetuarem a busca à distância e possuírem motivos para crer que os dados procurados se encontram armazenados em outro sistema informático ou em parte dele, informarão esse fato ao juiz, que poderá autorizar a prorrogação dos prazos da pesquisa. Destaca-se que a medida terá a duração máxima de um mês, prorrogável por igual período até o máximo de três meses.

Na França, foi promulgada a Lei 2019-222, *du 23 mars 2019*, que define as orientações e a programação dos meios de justiça do país até 2022 e trata da reforma da justiça, alterando artigos dos Códigos de Processo Penal, Civil e Comercial, dentre outros. Inserto no título dos procedimentos aplicáveis ao crime organizado do Código de Processo Penal, o artigo 706-102-1 permite a instalação de um dispositivo técnico cuja finalidade, sem o consentimento dos interessados, seja acessar, em qualquer lugar, a dados informáticos, registrá-los, armazená-los e transmiti-los, de acordo com sua exibição na tela do usuário em um sistema automatizado de processamento de

dados e conforme são inseridos ou são recebidos os caracteres, possibilitando a utilização do *malware*.

Feitas essas considerações, embora seja importante a análise da regulação do *malware* em outros países, não é possível importar o ordenamento jurídico exterior sem considerar as peculiaridades locais. Nesse passo, mostra-se oportuno mencionar os direitos fundamentais afetados pelo uso do *malware* para interceptar as comunicações telemáticas realizadas por meio do *WhatsApp* no Brasil. Dentre esses direitos, sobressaem-se o direito à não autoincriminação, à privacidade e ao sigilo e proteção das comunicações, que se confrontam com o direito à segurança. Todos esses são previstos na Constituição da República Federativa do Brasil, de 1988, e fixam princípios de observância obrigatória pelo Estado, possuindo, quando colocados em cotejo, peso abstrato equilibrado no ordenamento jurídico.

Nesse aspecto, é preciso ponderar que o empenho para garantir a segurança pública tem por pressuposto a violação de outros direitos fundamentais. Ainda assim, mostra-se vital que o emprego do *malware* seja uma medida subsidiária e que se dê de maneira excepcional, atuando quando outras medidas menos graves não sejam capazes de capturar prova imprescindível para apuração dos fatos.

Ademais, mesmo que se trate de uma ferramenta que pode estar sujeita a muitas mudanças, considerando a volatilidade das novas tecnologias, a tipicidade para o emprego do *malware* é essencial, ante o alto grau de invasão na esfera privada do investigado, de modo que se tenha estabelecido, em lei, com clareza, os seus requisitos e limites materiais e procedimentais, atendendo-se às suas peculiaridades, o que auxiliaria a evitar lesões aos direitos dos investigados. Deve ser estabelecido, por exemplo, o tempo de duração da medida, em quais crimes o seu emprego pode ser autorizado, o tratamento e descarte de dados que não tenham relação com a investigação e a necessidade de prévia autorização judicial. Portanto, desde que observadas as ponderações apontadas, o *malware* desponta como a medida que pode solucionar o impasse causado pelo *WhatsApp*, permitindo a válida interceptação das suas comunicações.

5 CONSIDERAÇÕES FINAIS

Da análise desse novo cenário eletrônico, pode-se considerar que os vestígios digitais são as impressões encontradas na cena física do crime, pois o uso de evidências eletrônicas se faz para localizar o criminoso, proteger a vítima, assegurar a persecução penal, dentre outros. Distingue-se da cena física por ter um caráter mais amplo, requerendo ferramentas distintas.

A modernização computacional alterou, inclusive, o acesso ao processo. Passou-se de manuscritos a autos datilografados, que, por sua vez, modificaram-se para a impressão por meio do computador. Hoje, o que se vislumbra é sua disponibilização no âmbito digital. Por outro lado, a criminalidade também não ignorou esses avanços, utilizando-se de ferramentas tecnológicas inovadoras para cometer crimes. O *WhatsApp* é um desses antros de incidência da criminalidade, deixando evidências digitais importantes para a investigação.

O *WhatsApp* é um aplicativo no qual criminosos aproveitam da sua criptografia, a qual, embora proteja a privacidade dos usuários, precisa ser contornada pelo Estado, a fim de que se esclareçam os fatos sob investigação. A inércia do Estado em casos como esse não deve ser admitida, sendo crucial que se empreendam esforços para garantir aparatos investigativos suficientes e adequados.

Com a análise das Leis nº 12.965/2014 e nº 9.296/1996, depreende-se que é possível a interceptação telemática das comunicações feitas por meio do *WhatsApp*. No entanto, apesar desse amparo legal, a criptografia de ponta a ponta, adotada pelo aplicativo, obsta a efetivação da interceptação autorizada.

Dentre as medidas alternativas para solucionar esse problema, o *malware* manifesta-se como a melhor. O uso de um *software* malicioso, contudo, não pode ser feito de maneira aleatória. É recomendado que haja uma legislação prévia, definindo seus limites e fixando seus contornos procedimentais. Não obstante, a análise do caso concreto também se revela significativa

Assim, levando em consideração a criptografia ponta a ponta do *WhatsApp*, é necessário que ocorra a criação de uma lei específica – disciplinando o emprego do *malware* – ou uma modificação na Lei nº 9.296, de 24 de julho de 1996, com o intuito de ampliar as possibilidades no emprego de meios tecnológicos para a interceptação das comunicações feitas por intermédio desse aplicativo. Após isso é que se poderia

fazer uso de um *malware*, de maneira a infiltrar-se no *WhatsApp* do acusado ou investigado antes ou depois que ocorresse a criptografia das comunicações.

Além do mencionado acréscimo legal, sugere-se que, na prática, sejam definidas as informações indispensáveis para a investigação e que se delimite quais são as opções para alcançar o objetivo da interceptação. Devem ficar definidos, ainda, a marca e o modelo dos itens sujeitos à investigação, o *hardware* e o *software* necessários, bem como as pessoas necessárias para realizar a investigação.

É elemento básico certificar-se que se trata de um ambiente limpo, de modo a evitar a contaminação dos dados e garantir a sua proteção contra invasores remotos. Para isso, pode-se fazer uso de um antivírus ou *firewall* atualizado. Necessário, ainda, documentar as noções sobre o início da investigação, os métodos usados, a autoridade policial que conduziu a investigação e as medidas tomadas para reduzir a interferência e contaminação.

Por fim, é preciso, também, extrema atenção na armazenagem do fluxo das comunicações interceptadas. Conforme as informações circulam entre emissor e receptor em tempo real, devem ser capturadas e registradas no tempo mais próximo da atualidade da conversa, de modo a evitar interferências. O aparelho que captura as conversas deve funcionar em plena capacidade, evitando falhas, tanto em termos de energia como em caso de eventual comprometimento do disco, devendo possuir capacidade de armazenamento suficiente para a interceptação almejada e ser célere o bastante para armazenar os dados em tempo real. Além disso, de modo a dar ainda mais segurança, as informações coletadas devem ser copiadas para um segundo local.

Adotadas essas medidas, legais e práticas, torna-se possível efetivar a interceptação telemática das comunicações realizadas através do *WhatsApp*, propiciando ao Estado a capacidade investigativa necessária ao desempenho de suas funções no âmbito penal e processual penal.

REFERÊNCIAS

ALBERGOTTI, Reed; NAKASHIMA, Ellen. The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm. **The Washington Post**, 2021. Disponível em: <https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/>. Acesso em: 25 nov. 2021.

ALEMANHA. **Strafprozeßordnung** (Código de Processo Penal de 1987). Portal Bundesministerium der Justiz. Disponível em: <https://www.gesetze-im-internet.de/stpo/BJNR006290950.html>. Acesso em: 19 jan. 2022.

ANDRADE, Manuel da Costa. **Bruscamente no verão passado, a reforma do código de processo penal**. Coimbra: Coimbra Editora, 2009.

ANDRESS, Jason. **The basics of information security:** understanding the fundamentals of infosec in theory and practice. Massachusetts: Syngress Press, 2011.

ARANHA, Diego de Freitas. **O que é criptografia fim a fim e o que devemos fazer a respeito?** São Paulo: Thomson Reuters Brasil, 2020.

BATISTA, Lydie Jorge. **O malware como meio de obtenção de prova em processo penal.** Dissertação de mestrado. Universidade de Lisboa: Lisboa, 2018.

BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 16. ed., São Paulo: Saraiva, 2015.

BRASIL. Constituição (1988). **Constituição**: República Federativa do Brasil. **Vade Mecum**. 32. ed., São Paulo: Rideel, 2021.

_____. Código Penal. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Vade Mecum**. 32. ed., São Paulo: Rideel, 2021.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Vade Mecum**. 32. ed., São Paulo: Rideel, 2021.

_____. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. **Vade Mecum**. 32. ed., São Paulo: Rideel, 2021.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Vade Mecum**. 32. ed., São Paulo: Rideel, 2021.

_____. Superior Tribunal de Justiça (STJ). Recurso em Habeas Corpus nº 372.762/MG, julgado em 03 de outubro de 2017. Ministro Relator Felix Fischer**. Portal do STJ**. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1631821&num_registro=201602540301&data=20171016&formato=PD>. Acesso em: 10 jan. 2022.

_____. Superior Tribunal de Justiça (STJ). Recurso em Habeas Corpus nº 99.735/SC, julgado em 27 de novembro de 2018. Ministra Relatora Laurita Vaz. **Portal do STJ**. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212&peticao_numero=-1&formato=PDF>. Acesso em: 10 jan. 2022.

_____. Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade (ADI) nº 5.527/DF. Ministra Relatora Rosa Weber**. Portal do STF.** Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Acesso em: 05 jan. 2022.

_____. Supremo Tribunal Federal (STF). Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403/SE. Ministro Relator Edson Fachin**. Portal do STF**. Disponível em: < http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500>. Acesso em: 10 jan. 2022

CAPEZ, Fernando. **Curso de processo penal.** 16. ed., São Paulo: Saraiva, 2011.

CHIRISA, Sharon. You Can't Use WhatsApp in These 6 Countries and Here's The Reason Why. **Iharare**, 2020. Disponível em: <https://iharare.com/countries-which-have-banned-whatsapp/>. Acesso em: 23 nov. 2021.

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

ESPANHA. Ley de Enjuiciamiento Criminal (Código de Processo Penal de 1882). **Portal BOE**. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em: 12 jan. 2022.

_____. Ley Orgánica nº 13, de 5 de octubre de 2015. Modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. **Portal BOE.** Disponível em: <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725>. Acesso em: 12 jan. 2022.

FRANÇA. Code de procédure pénale (Código de Processo Penal de 1959). **Portal Legifrance**. Disponível em: <https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/>. Acesso em: 15 jan. 2022.

_____. LOI n° 2019-222, du 23 mars 2019. De programmation 2018-2022 et de réforme pour la justice. **Portal Legifrance.** Disponível em: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038261631>. Acesso em: 12 jan. 2022.

KIGUOLIS, Linas. O que é backdoors e como removê-lo. **Sem Vírus**. 2016. Disponível em: <https://semvirus.pt/backdoors/>. Acesso em: 05 dez. 2021.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019.

LEETARU, Kalev. WhatsApp's Massive Security Flaw Serves To Remind Us The Limits Of Consumer Encryption Apps. **Forbes**. 2019. Disponível em: <https://www.forbes.com/sites/kalevleetaru/2019/05/24/whatsapps-massive-security-flaw-serves-to-remind-us-the-limits-of-consumer-encryption-apps/?sh=4d62e54e1e3e>. Acesso em: 05 dez. 2021.

MIRANDA, Jorge; MEDEIROS, Rui. **Constituição portuguesa anotada**. 2. ed., Coimbra: Coimbra Editora, 2010.

NAÍSA, Leticia. Dos 'salveiros' ao WhatsApp: como o PCC usou a comunicação para se expandir. **Vice**, 2016. Disponível em:<https://www.vice.com/pt/article/v b7dkb/como-o-pcc-usou-a-comunicacao-para-se-expandir>. Acesso em: 10 jan. 2022.

NUVENS, Eduardo. WhatsApp: história, dicas e tudo que você precisa saber sobre o app. **Olhar Digital**, 2018. Disponível em: <https://olhardigital.com.br/2018/12/20/noticias/whatsapp-historia-dicas-e-tudo-que-voce-precisa-saber-sobre-o-app/>. Acesso em: 01 set. 2021.

RAMALHO, David Silva; VACIAGO, Giuseppe. Online searches and online surveliIance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. **Digital Evidence and Electronic Signature Law Review**. London: University of London, 2016.

REED, Thomas. GrayKey iPhone unlocker poses serious security concerns. **Malwarebytes Labs**, 2018. Disponível em: <https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/>. Acesso em: 28 nov. 2021.

RODRIGUES, Anabela Miranda. A defesa do arguido: uma garantia constitucional em perigo no “admirável mundo novo”. **Revista Portuguesa de Ciência Criminal**. Coimbra: Coimbra Editora, 2002.

SALGADO, Danielle. Pesquisa sobre apps de mensagens no Brasil: confira dados exclusivos. Panorama Mobile Time/**Opinion Box**. 2021. Disponível em: <https://blog.opinionbox.com/apps-de-mensagens-no-brasil/>. Acesso em: 26 ago. 2021.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na constituição federal de 1988**. 10. ed., São Paulo: Livraria do Advogado, 2015.

SINGH, Simon. **The Code Book:** the secret history of codes and codebreaking. London: Fourth Estate, 1999.

WALKER, Dale. EU inches closer to ban on end-to-end encryption. **Itpro**. 2020. Disponível em: <https://www.itpro.co.uk/security/357699/leaked-memo-suggests-eu-ban-on-end-to-end-encryption-imminent>. Acesso em: 22 nov. 2021.