UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE NACIONAL DE DIREITO

INTERCEPTAÇÃO TELEMÁTICA: SUA ADMISSIBILIDADE COMO MEIO DE OBTENÇÃO DE PROVA NO DIREITO PROCESSUAL PENAL BRASILEIRO E A QUESTÃO DOS SISTEMAS CRIPTOGRAFADOS PONTO A PONTO

WAGNER DOS SANTOS GAGLIANO

Rio de Janeiro
2017/2º Semestre

WAGNER DOS SANTOS GAGLIANO

INTERCEPTAÇÃO TELEMÁTICA:
SUA ADMISSIBILIDADE COMO MEIO DE OBTENÇÃO DE PROVA NO DIREITO PROCESSUAL PENAL BRASILEIRO E A QUESTÃO DOS SISTEMAS CRIPTOGRAFADOS PONTO A PONTO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Nilo Cesar Martins Pompílio da Hora**.

.

Rio de Janeiro
2017/2º Semestre

CIP - Catalogação na Publicação

GAGLIANO, WAGNER DOS SANTOS
G135i INTERCEPTAÇÃO TELEMÁTICA: SUA ADMISSIBILIDADE COMO MEIO DE OBTENÇÃO DE PROVA NO DIREITO PROCESSUAL PENAL BRASILEIRO E A QUESTÃO DOS SISTEMAS CRIPTOGRAFADOS PONTO A PONTO / WAGNER DOS SANTOS GAGLIANO. -- Rio de Janeiro, 2017.
68 f.

Orientador: NILO CESAR MARTINS POMPÍLIO DA HORA.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. INTERCEPTAÇÃO TELEMÁTICA. 2. CRIPTOGRAFIA PONTO A PONTO. 3. LEI 9.296/96. I. HORA, NILO CESAR MARTINS POMPÍLIO DA, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

CDD: 341.2738

WAGNER DOS SANTOS GAGLIANO

INTERCEPTAÇÃO TELEMÁTICA: SUA ADMISSIBILIDADE COMO MEIO DE OBTENÇÃO DE PROVA NO DIREITO PROCESSUAL PENAL BRASILEIRO E A QUESTÃO DOS SISTEMAS CRIPTOGRAFADOS PONTO A PONTO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Nilo Cesar Martins Pompílio da Hora**

Data da Aprovação: __/__/____.

Banca Examinadora:

_____
Orientador **Professor Dr. Nilo Cesar Martins Pompílio da Hora**

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro
2017/2º Semestre

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, por ter me permitido chegar a momento tão significativo em minha vida com saúde e esperança na humanidade.

Meu agradecimento especial ao meu orientador, **Professor Dr. Nilo Cesar Martins Pompílio da Hora**, pelo acolhimento, direcionamento e constantes demonstrações de consideração e amizade.

À minha esposa Cynthia e filhas Katherine e Carolline, agradeço o amor, a amizade e o ambiente alegre e carinhoso com que vocês sempre me recebem em nosso Lar.

Aos amigos do seleto grupo "DarkeSideFND", pela demonstração de união e coesão que sempre nos manteve próximos durante todo o período de convivência na Nacional. Sem dúvida é um grupo de vencedores. Nossa amizade transporá com facilidade as barreiras impostas pelo tempo e muitas alegrias ainda virão.

E, por fim, agradeço por todos os momentos que desfrutei nos bancos escolares da nossa Faculdade Nacional de Direito.

A nossa maior glória não reside no fato de nunca cairmos, mas sim em levantarmo-nos sempre depois de cada queda.

Confúcio

RESUMO

GAGLIANO, Wagner dos Santos. *Interceptação Telemática: sua admissibilidade como meio de obtenção de prova no direito processual penal brasileiro e a questão dos sistemas criptografados ponto a ponto*. 2017. 68 páginas. Monografia (Graduação/Bacharelado em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

Este trabalho tem como objetivo analisar a admissibilidade da prova obtida por interceptação telemática no direito processual penal, bem como apresentar os questionamentos que envolvem os sistemas de comunicação criptografados ponto a ponto. Objetivando a melhor compreensão do tema a primeira parte volta-se à análise dos aspectos históricos e conceituais da interceptação telemática e da criptografia ponto a ponto. A segunda aborda os princípios constitucionais associados à interceptação telemática, com ênfase nos direitos fundamentais e, em adição, comentários sobre a legislação pátria correlacionada, partindo do inciso XII, do artigo 5º, da CRFB/88 e da Lei 9.296/96, que regula a interceptação telefônica, perpassando pela resolução nº 217/2016 que alterou a de nº 59/2008, ambas do Conselho Nacional de Justiça, encerrando o capítulo sob a ótica do direito comparado. A terceira parte está voltada para considerações sobre a validade da prova obtida por meio do procedimento em análise e sua admissibilidade no processo penal, considerando para tal a inter-relação do trinômio: prova obtida, investigação criminal e preservação da cadeia de custódia da prova.

Palavras-Chave: Interceptação Telemática; Lei 9.296/96; Criptografia ponto a ponto.

ABSTRACT

GAGLIANO, Wagner dos Santos. *TELEMATIC INTERCEPTION: its admissibility as a mode of obtaining evidence in brazilian criminal procedural law and the question of point-to-point encrypted systems*. 2017. 68 pages. Monograph. (Graduation/Bachelor in Law) - Federal University of Rio de Janeiro, Rio de Janeiro, 2017.

This work aims to analyze the admissibility of the evidence obtained by telematic interception in criminal procedural law, as well as to present the questions that involve the encrypted communication systems point to point. Aiming for a better understanding of the theme, the first part is devoted to analyzing the historical and conceptual aspects of telematic interception and point-to-point cryptography. The second deals with the constitutional principles associated with telematic interception, with emphasis on fundamental rights and, in addition, comments on the related national legislation, starting with item XII, article 5, CRFB / 88 and Law 9296/96, which regulates the telephone interception, passing through resolution 59/2008, amended by No. 217/2016, both of the National Council of Justice, closing the chapter from the point of view of comparative. The third part focuses on the validity of the evidence obtained through the procedure under review and its admissibility in criminal proceedings, considering for this the interrelationship of the trinomial: evidence obtained, criminal investigation and preservation of the chain of custody of the evidence.

Keywords: Telematic Interception, Law 9.296/96, Point-to-Point Cryptography

LISTA DE ABREVIATURAS E SIGLAS

UFRJ – Universidade Federal do Rio de Janeiro

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

CRFB – Constituição da República Federativa do Brasil

CNJ – Conselho Nacional de Justiça

DUDH - Declaração Universal dos Direitos do Homem da ONU

CPP- Código de Processo Penal

CP – Código Penal

EUA- Estados Unidos da América

MP- Ministério Público

FBI- Federal Bureau of Investigation

Sumário

INTRODUÇÃO

A Constituição da República Federativa do Brasil de 1988, em seu artigo 5º, inciso XII, prevê a possibilidade de restrição do direito fundamental à intimidade, estabelecendo, contudo, a necessidade de regulamentação legal da matéria.

Nesse sentido, de modo a limitar possíveis violações ao direito à inviolabilidade do sigilo das comunicações, bem como atender à previsão constitucional de reserva legal, foi editada a Lei nº 9.296 de 24 de julho de 1996, para regulamentar o artigo 5º, XII da CRFB/88, quanto ao instituto da interceptação telefônica nas investigações criminais.

Depois de decorridos mais de vinte anos da edição de sua lei regulamentadora, a interceptação telefônica continua sendo objeto de divergências doutrinárias, algumas remontam à sua gênesis, questionando, por exemplo, a construção gramatical do dispositivo constitucional que a originou, outras, por outro lado, são tão atuais, que ainda não permitiram a pacificação de jurisprudência sobre o assunto, inexistindo sequer doutrina que o contemple .

Nesse viés de incerteza figuram as implicações jurídicas da tecnologia de transmissão de dados ponto a ponto, usada no aplicativo *WhatsApp*, implementada em 2016, e que vem movimentando ainda mais as decisões judiciais, já deveras conturbadas em 2015.

No biênio 2015-2016, o aplicativo foi retirado do ar por quatro vezes, pelo descumprimento de ordens judiciais, relacionadas à disponibilização de dados de seus usuários, pela sociedade empresária *Facebook*, sua atual proprietária.

Foi nesse contexto jurídico, que mescla a evolução tecnológica e conceitual das comunicações com a obsolescência da Lei 9.296/96, que no lugar de se usar o tradicional tema interceptação telefônica, optou-se pelo tema interceptação telemática, em razão da gama de possibilidades relacionadas a esse espectro de maior abrangência. Visualizou-se que o tema escolhido permitiria mesclar, no decorrer da análise, tanto conceitos tradicionais passados, quanto presentes, em um enfoque voltado para desdobramentos futuros.

Dessa forma, o presente trabalho se propõe, em três capítulos, a estabelecer uma análise sobre a interceptação das comunicações telemáticas utilizando, para tanto, o método de

pesquisa bibliográfico e estabelecendo, sempre que possível, comparações entre a legislação pertinente e as diversas posições doutrinárias. Ao final, a presente produção acadêmica, traz, ainda, uma conclusão acerca da temática estudada.

Sendo assim, busca-se no capítulo 1, apresentar a interceptação telemática, a escuta e demais ferramentas, seus conceitos e variações admitidas. Iniciando com uma perspectiva histórica do tema, apontando as suas principais características e definições. Encerrando esse capítulo será comentada a arquitetura básica de comunicação do aplicativo *WhatsApp* e suas implicações jurídicas, principalmente, em relação às transmissões criptografadas ponto a ponto.

Já no capítulo 2, de maneira breve, introduz-se a temática relacionada ao ordenamento jurídico afeto à interceptação. Em seguida serão tecidas considerações sobre a legislação específica e comentados os princípios constitucionais selecionados como os mais significativos no contexto da admissibilidade da interceptação telemática como meio de obtenção de prova.

Na parte final deste capítulo far-se-á a apresentação de breves comparações da legislação alienígena a respeito da interceptação telemática, acompanhados de singelas observações do direito comparado.

Por fim, no terceiro capítulo, trar-se-á a temática das provas, particularmente as ilícitas, relacionando-as à admissibilidade das provas advindas da interceptação telemática, considerando a legalidade e a constitucionalidade dos procedimentos adotados frente ao exercício da ampla defesa e do contraditório. Encerrando o capítulo serão conduzidos comentários sucintos sobre a cadeia de custódia da prova e a investigação criminal na interceptação telemática.

Dessa forma, pretende-se analisar ao longo da monografia as especificidades das legislações brasileira e alienígenas, sendo o fulcro da produção acadêmica a análise da admissibilidade da prova obtida por interceptação telemática no devido processo legal.

1 INTERCEPTAÇÃO TELEMÁTICA

1.1 Aspectos históricos

A interceptação das comunicações remonta aos primórdios da organização e da vida em sociedade do homem. A busca por informações privilegiadas ou protegidas é uma marca indelével e intrínseca da natureza humana, que deu origem à máxima - "quem detém a informação detém o poder".

O homem avançou na organização de sua sociedade, chegando à idade moderna. No entanto, nesse período, déspotas exerciam sua autoridade de forma arbitrária e absoluta, governando de forma opressora, não existindo a mínima preocupação ou respeito aos direitos mais elementares de seus súditos.

Na França, por exemplo, foram instituídos locais por onde todas as correspondências obrigatoriamente deveriam passar. Nesses locais as correspondências eram violadas em busca de informações acerca de movimentos insurgentes contrários à coroa.

No século XVIII, a revolta crescente da população oprimida fez com que se sucedessem movimentos sociais por toda a Europa, culminando com a Revolução francesa em 1789. Alicerçada em ideias iluministas, foi anunciada a Declaração de Direitos do Homem e do Cidadão[1], em 26 de agosto de 1789, a qual contemplou no artigo 11, pela primeira vez, a liberdade e sigilo da comunicação.

> Art. 11. "A livre comunicação das ideias e das opiniões é um dos mais preciosos direitos do homem. Todo cidadão pode, portanto, falar, escrever, imprimir livremente, respondendo, todavia, pelos abusos desta liberdade nos termos previstos na lei".

A garantia da liberdade das comunicações na Declaração francesa de 1789 foi tão impactante na promoção dos direitos e garantias fundamentais que passou a influenciar

[1] FRANÇA. Declaração de Direitos do Homem e do Cidadão. Paris. 26 ago. 1789. Disponível em: https:<//br.ambafrance.org/A-Declaracao-dos-Direitos-do-Homem-e-do-Cidadao> acesso em 10 nov. 2017.

significativamente as legislações posteriores, culminando com a inclusão do artigo 12 na DUDH[2] da ONU, proclamada 159 anos depois.

> Art. 12 "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques".

A invenção do telefone, em 1876, pelo físico Alexander Graham Bell trouxe uma perspectiva diferenciada para as comunicações, estabelecendo uma nova dinâmica na troca de informações.

Além das óbvias vantagens trazidas pela invenção de Graham Bell, novamente via-se o direito obrigado a acompanhar tal evolução de modo a garantir o direito à livre comunicação e à intimidade.

No Brasil, a garantia constitucional ao sigilo das comunicações veio logo após a revolução francesa. Já em 1824[3], a "Constituição Política do Império do Brasil" trazia no art. 179 a inviolabilidade dos direitos civis, cujo inciso 27 contemplava o "segredo" das cartas.

As Constituições seguintes, de 1891[4], 1934[5], 1937[6] e 1946[7] traziam o mesmo teor quanto à inviolabilidade do sigilo da correspondência, sendo que as Cartas Magnas de 1937 e 46 continham dispositivos que previam a possibilidade de censura de todas as comunicações em casos emergenciais, como por exemplo, na de 1946, se decretado estado de sítio.

---

[2] Declaração Universal dos Direitos do Homem da ONU, proclamada, em 10 de dezembro de 1948. Disponível em: http://www.onu.org.br/img/2014/09/DUDH.pdf acesso às 14:05 de 10 nov. 2017.

[3] BRASIL. Constituição Política do Império do Brasil de 1824. **Coleção de Leis do Império do Brasil - 1824, Página 7 Vol. 1**, Carta de Lei de 25 de Março de 1824. Rio de Janeiro, RJ, 25 mar. 1824. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1824-1899/constituicao-35041-25-marco-1824-532540-publicacaooriginal-14770-pl.html>. Acesso em 10 nov. 2017.

[4] BRASIL. Constituição da República dos Estados Unidos do Brasil de 1891. **Diário [do] Congresso Nacional**, Rio de Janeiro, RJ, 24 fev. 1891. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1824-1899/constituicao-35081-24-fevereiro-1891-532699-publicacaooriginal-15017-pl.html>. Acesso em 10 nov. 2017.

[5] BRASIL. Constituição da República dos Estados Unidos do Brasil de 1934. **Diário Oficial [da] União - Seção 1- Suplemento**, Rio de Janeiro, RJ, 16 jul. 1934. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1930-1939/constituicao-1934-16-julho-1934-365196-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

[6] BRASIL. Constituição da República dos Estados Unidos do Brasil de 1937. **Diário Oficial [da] União - Seção 1**, Rio de Janeiro, RJ, 10 nov. 1937. Disponível em: http://www2.camara.leg.br/legin/fed/consti/1930-1939/constituicao-35093-10-novembro-1937-532849-publicacaooriginal-15246-pl.html 10/11/1937. Acesso em 10 nov. 2017.

[7] BRASIL. Constituição dos Estados Unidos do Brasil de 1946. **Diário Oficial [da] União - Seção 1**, Rio de Janeiro, RJ, 19 set. 1946. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1940-1949/constituicao-1946-18-julho-1946-365199-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

A Constituição de 1967, de acordo com a EC nº 1 de 1969[8], no art. 153, § 9º deixava claro não haver previsão de qualquer exceção à inviolabilidade das comunicações telefônicas.

Por último a Constituição de 1988 trouxe em seu art. 5º, inciso XII, a previsão da possibilidade de interceptação telefônica, desde que preenchidos certos requisitos, os quais foram estabelecidos somente em 1996, pela lei 9.296/96. Os desdobramentos advindos dessa lacuna temporal serão abordados a posteriore, no capítulo 2 do presente trabalho, que discorrerá sobre a legislação pertinente ao assunto.

1.2 Conceitos e características

1.2.1 Interceptação telemática ou Interceptação telefônica

Anote-se que não há consenso doutrinário em relação à previsão legal sobre a interceptação. Alguns autores posicionam-se favoravelmente à utilização do termo "telemática" em substituição ao vocábulo "telefônica".

Aqueles que são contrários alegam a inconstitucionalidade do p.u. do art. 1º da Lei 9296/96, enquanto que os favoráveis consideram ser possível, à luz da CRFB de 88, incluir, além da interceptação da comunicação telefônica, a interceptação do fluxo de comunicações em sistemas de informática e telemática, conforme previsão legal do p.u. do art. 1º da Lei 9296/96.[9]

> 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".

[8] BRASIL. Constituição do Brasil de 1967. EC nº 1, de 1969. **Diário Oficial [da] União**, Brasília, DF, 20 out. 1969. Disponível em: <http://www2.camara.leg.br/legin/fed/emecon/1960-1969/emendaconstitucional-1-17-outubro-1969-364989-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

[9] BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 26 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em 9 nov. 2017.

Dessa forma, no intuito de viabilizar uma abordagem mais ampla do tema, optou-se pela utilização do termo "telemática", em substituição ao vocábulo "telefônica". Na sequência serão apresentados conceitos estabelecidos por alguns doutrinadores, que servirão de alicerce para discussões futuras.

Da obra "Crimes de Informática e seus Aspectos Processuais"[10], de autoria de Carla Rodrigues, foram selecionadas algumas definições basilares para o tema escolhido:

> Interceptar é interromper o curso originário, impedir a passagem, sendo que na lei tem o sentido de captar a comunicação, conhecer seu conteúdo. Interceptar é ter contato com teor da comunicação, não impedindo que ela chegue ao seu destinatário.
> A telemática é uma ciência que trata da manipulação de dados e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não. Assim, qualquer comunicação feita através de sistema de informática é protegida pela lei; a título de exemplo, citamos as comunicações feitas na internet.

Damásio ensina que: "informática é a ciência relativa à informação por intermédio de equipamentos e métodos do sistema de processamento de dados. E telemática é a ciência que versa sobre a informação por meio conjunto de computador e telecomunicação".[11]

Do livro "Interceptação Telefônica – comentários à Lei 9.296/96"[12] retira-se a seguinte definição:

> "Interceptação telefônica (ou interceptação em sentido estrito): consiste na captação da comunicação telefônica por um terceiro, sem o conhecimento de nenhum dos comunicadores. Essa é a interceptação em sentido estrito (ou seja, um terceiro intervém na comunicação alheia, sem o conhecimento dos comunicadores)."

1.2.2 Conceitos correlatos

De modo a esclarecer as nuances do objeto da Lei 9296/96 serão apresentadas definições básicas, retiradas da obra "Interceptação Telefônica: comentários à Lei 9269/96"[13],

---

[10] ARAÚJO DE CASTRO. Carla Rodrigues. Crimes de Informática e seus Aspectos Processuais. Rio de Janeiro. Editora Lumen Juris, 2001, p.111 e 112

[11] JESUS, Damásio Evangelista de. Interceptação de comunicações telefônicas: notas à Lei nº 9296, de 24 jul. 1996. Revista dos Tribunais, São Paulo, n. 735, p. 458-473, jan. 1997.

[12] GOMES, Luiz Flávio e MACIEL, Silvio. Interceptação telefônica: comentários à Lei 9269/96. 3. Ed. rev. e ampl. São Paulo: Revista dos Tribunais, 2014. p. 24.

[13] Ibid. p. 25.

relacionadas às cinco situações cabíveis, além da já comentada “interceptação telefônica ou interceptação em sentido estrito”.

Tais conceitos são significativamente oportunos para o desenvolvimento do trabalho e entendimento das decisões do STF e do STJ, particularmente quando relacionadas ao termo “interceptação de comunicações telefônicas, de **qualquer natureza**”, como apresentado no caput do art. 1º da Lei 9296/96. (grifo nosso)

Cabe ressaltar que na opinião dos autores os objetos da Lei 9296/96 são apenas a interceptação em sentido estrito e a escuta telefônica, o que será adotado como uma das premissas básicas do presente estudo.

1.2.2.1 Escuta telefônica

“Escuta telefônica: é a captação da comunicação telefônica por terceiro, com o conhecimento de um dos comunicadores e desconhecimento do outro. Na escuta, como se vê, um dos comunicadores tem ciência da intromissão alheia na comunicação.”

1.2.2.2 Gravação telefônica

“Gravação telefônica ou gravação clandestina: é a gravação da comunicação telefônica por um dos comunicadores, ou seja, trata-se de uma gravação da própria comunicação. Normalmente é feita sem o conhecimento do outro comunicador, daí falar-se em gravação clandestina.”

1.2.2.3 Interceptação ambiental

“Interceptação ambiental: é a captação de uma comunicação no próprio ambiente dela, por um terceiro, sem conhecimento dos comunicadores.”

1.2.2.4 Escuta ambiental

“Escuta ambiental: é a captação de uma comunicação, no ambiente dela, feita por terceiro, com o consentimento de um dos comunicadores.”

1.2.2.5 Gravação ambiental

"Gravação ambiental: é a captação no ambiente da comunicação feita por um dos comunicadores (ex.: gravador, câmeras ocultas etc.). Também denominada gravação clandestina."

1.3 Sistemas criptografados ponto a ponto – "caso *WhatsApp*"

1.3.1 Conceitos e características

1.3.1.1 Peculiaridades do sistema

A cavaleiro das discussões sob as interceptações, que ainda apresentavam muitas divergências não pacificadas entre os doutrinadores, como, por exemplo, o questionamento sobre a constitucionalidade do p.u. do art. 1º da Lei 9296/96, ou a indefinição sobre quais procedimentos investigativos de comunicações estão abrangidos pela expressão "qualquer natureza", do caput do referido artigo, desponta a criação do aplicativo *WhatsApp* em 2009.

O aplicativo *WhatsApp* revolucionou a dinâmica das comunicações nas redes sociais. Em razão do significativo número de usuários no mundo e, particularmente no Brasil, foi selecionado como referência para o desenvolvimento e considerações sobre o controle e a possibilidade da interceptação telemática nas redes sociais criptografadas ponto a ponto, no escopo do presente trabalho.

Segundo o site techtudo:

> em maio de 2017, cento e vinte milhões de brasileiros possuíam o aplicativo *WhatsApp* instalado em seus dispositivos de comunicação. Foi realçado ainda que o processo de criptografia das mensagens, iniciado em abril de 2016, chegou a cem por cento de codificação do sistema em abril de 2017.[14]

[14] VELOSO, Thássius. WhatsApp em números: 120 milhões de brasileiros e 100% de criptografia. Techtudo, São Paulo, mai. 2017. Seção Redes Sociais. Disponível em: <https://www.techtudo.com.br/noticias/2017/05/whatsapp-em-numeros-120-milhoes-de-brasileiros-e-100-de-criptografia.ghtml.>. Acesso em 12 nov. 17.

O advento da criptografia ponto a ponto foi o combustível de retomada vigorosa do tema pelo judiciário gerando questionamentos e acirradas discussões entre os atores do judiciário, os peritos das polícias investigativas e os representantes do *Facebook*, atual proprietário do aplicativo.

1.3.1.2 Metadados

Do site metadados retira-se que: “metadados 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.” [15]

Os metadados são normalmente segregados do conteúdo literal da informação, ou seja, daquela que está relacionada diretamente com o teor da troca de informações.

No entanto, aplicando-se tecnologia própria, é possível, por meio dos metadados, selecionar dados de múltiplas fontes e consolidá-los em um banco de dados único. São exemplos de metadados os domínios e as especificações de segurança, dentre outros.

Tal possibilidade, no caso da interceptação de comunicações, pode ser um grande suporte para a investigação, pois, apesar de não apresentar o conteúdo da conversa propriamente dito, viabilizará a identificação das origens dos dados, de transferências, localizações etc..

1.3.1.3 Criptografia de ponto a ponto

Criptografia de ponto a ponto: as mensagens são embaralhadas ao deixar o telefone da pessoa que as envia e só conseguem ser decodificadas no telefone de quem as recebe.

Por ocasião do anúncio, em 2016, da criptografia integral de todas as comunicações, o serviço de mensagens *WhatsApp* afirmou: "Quando você manda uma mensagem, a única pessoa que pode lê-la é a pessoa ou grupo para quem você a enviou. Ninguém pode olhar

[15] METADADOS. Metadados, 2017. Braga, Portugal. Disponível em: <http://www.metadados.pt/oquesaometadados>. Acesso em 12 nov. 17.

dentro da mensagem. Nem cibercriminosos. Nem hackers. Nem regimes opressores. Nem mesmo nós."[16]

Esse sistema baseia-se em chaves que são distribuídas aleatoriamente para cada conversa e, **teoricamente**, somente os relacionados como emissores e destinatários terão acesso ao seu conteúdo. (grifo nosso)

1.3.2 Tráfego de dados criptografados nas redes sociais

A observação da arquitetura de rede empregada no aplicativo *WhatsApp* nos capacitará ao entendimento, mesmo que superficial, das nuances de um modelo de transmissão de dados criptografados ponto a ponto e os possíveis desdobramentos jurídicos a ele relacionados.

O aplicativo em questão pode ser habilitado em vários sistemas operacionais, tais como Android, BlackBerry, iOS, Nokia e Windows Phone. Seu principal diferencial para outros softwares de comunicação instantânea é o compartilhamento automático da agenda de telefones com a de contatos do *WhatsApp* do usuário e a vinculação a uma linha telefônica como elemento validador.

A comunicação criptografada se processa com o envio e recebimento de pacotes de dados, aos quais são atribuídas chaves de endereçamento e recebimento. Essas chaves são geradas, aleatoriamente, e armazenadas apenas nos celulares dos interlocutores, daí a denominação de criptografia ponto a ponto.

Todo fluxo de dados passa pelos servidores de gerenciamento do *WhatsApp* antes de atingir seu destinatário final. E é nesse ponto de interseção das comunicações que, segundo especialistas, reside a possibilidade da interceptação não do conteúdo das conversas, mas de metadados, possibilidade que é negada veementemente pelos proprietários do Facebook, atuais gerenciadores do aplicativo em discussão.

---

[16] COSTA, Camila. Quatro coisas que mudam com a criptografia no *WhatsApp* – e por que ela gera polêmica. BBC Brasil. Londres, abr. 2016. Seção Notícias. Disponível em: http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc, acesso em: 18 set. 2017.

O questionamento sobre a possibilidade ou não do fornecimento do conteúdo de conversas entre usuários do *WhatsApp*, ou pelo menos dos respectivos metadados, tem sido alvo de discussões acirradas no judiciário. Só no período 2015-2016, em decorrência de decisões judicias, o aplicativo foi retirado do ar por quatro vezes. A seguir será apresentado um resumo sucinto dessas decisões.

1.3.2.1 Bloqueios por decisões judiciais

As decisões judicias que tiraram do ar o aplicativo *WhatsApp* em 2015 e 2016, foram consequências descumprimento de ordem judicial para que a empresa fornecesse o conteúdo de conversas de investigados em crimes. Os proprietários afirmaram ser impossível cumprir as decisões, visto que as mensagens são criptografadas, procedimento já explanado acima.

Segue resumo dos casos de bloqueio ao aplicativo no território nacional, de acordo com a Folha de São Paulo:[17]

1º caso - 25 de fevereiro de 2015.

Em fevereiro do ano passado, um juiz do Piauí determinou o bloqueio do WhatsApp no Brasil, em razão de a empresa supostamente ter descumprido decisões anteriores relacionadas a investigações realizadas pela Polícia Civil do Estado. O motivo seriam crimes envolvendo crianças e adolescentes.

"Até pouco tempo atrás nós fazíamos interceptações telefônicas, mas hoje ninguém usa telefone [para falar], usa o *WhatsApp*. Para que se possa saber o que criminosos comunicaram, onde estão, é através dos apps", diz o juiz Luiz de Moura Correia, do Piauí.

A decisão, contudo, foi suspensa por um desembargador do Tribunal de Justiça do Piauí após analisar mandado de segurança impetrado pelas teles e o aplicativo não chegou a ser bloqueado.

[17] WIZIACK, Julio. Fundador do *WhatsApp* diz no STF que fornecer dados à polícia é impossível. Folha de S. Paulo, Brasília, jun. 2017. Seção Mercado. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/06/1889702-fundador-do-whatsapp-diz-no-stf-que-nao-e-possivel-interceptar-conversas.shtml>. Acesso em: 12 nov. 17.

2º caso – 17 de dezembro de 2015

O desembargador Xavier de Souza, da 11ª Câmara Criminal do Tribunal de Justiça de São Paulo pediu o bloqueio do app como represália após a empresa se negar a quebrar o sigilo de dados devido a uma investigação criminal. A medida foi determinada pela 1ª Vara Criminal de São Bernardo do Campo.

O pedido inicial, de 48 horas de bloqueio, durou cerca de 12 horas.

3º caso – 2 de maio de 2016

O juiz Marcel Montalvão, da comarca de Lagarto (SE), pediu o bloqueio do aplicativo por 72 horas. O magistrado queria que a companhia repassasse informações sobre uma quadrilha interestadual de drogas para uma investigação da Polícia Federal, o que a companhia se negava a fazer.

O bloqueio, no entanto, durou 25 horas. O desembargador Ricardo Múcio Santana de Abreu Lima, do Tribunal de Justiça de Sergipe, disse que a proibição do app no Brasil gerou "caos social em todo o território" e determinou o desbloqueio.

"A suspensão dos serviços do *WhatsApp* já dura 24 horas e certo é também que gerou caos social em todo o território, com dificuldade de desenvolvimento de atividades laborativas, lazer, família etc.", disse Santana.

O processo que culminou na determinação de Montalvão é o mesmo que justificou, em março deste ano, a prisão de Diego Dzodan, vice-presidente do Facebook, empresa dona do app, para a América Latina.

4º caso – 19 de julho de 2016

A juíza Daniela Barbosa de Souza, da 2ª Vara Criminal da Comarca de Duque de Caxias determinou o bloqueio. O motivo, assim como aconteceu em outras oportunidades no Brasil, envolve o fato de o aplicativo não compartilhar informações sobre investigações criminais.

A juíza determinou que o *WhatsApp* desabilitasse a criptografia que garante o sigilo das mensagens e permitisse o monitoramento das conversas de suspeitos de uma organização criminosa em Duque de Caxias em tempo real pelos investigadores. Ela já havia enviado três ofícios ao Facebook, dono do aplicativo, para que a ordem fosse cumprida. Mas a empresa se negou a atender à determinação, e foi por isso que a juíza mandou bloquear o serviço.

1.3.3 Possibilidades, limites e requisitos para monitoramento dos sistemas criptografados

A questão que envolve a criptografia de sistemas nas redes sociais, particularmente em relação ao aplicativo *WhatsApp* é significativamente complexa e requer uma análise detalhada e célere do assunto, tanto do Poder Judiciário, quanto do Poder Legislativo.

O primeiro, de modo a firmar jurisprudência sólida, robusta e definitiva, que tenha por base a CRFB/88 e a legislação pertinente ao assunto - interceptação telemática - e o segundo para que, tempestivamente, elabore leis mais modernas e abrangentes de modo a acompanhar a evolução das comunicações, e em paralelo preencha as lacunas deixadas pela legislação vigente.

Nesse viés, pode-se citar a audiência pública conduzida pelo STF em 2 de junho de 2017, cujo tema foi o aplicativo *WhatsApp*. A empresa que gerencia o referido aplicativo, o qual já foi retirado do ar por mais de uma vez no Brasil, está envolvida em numerosos processos que, de alguma forma, afetam uma porcentagem considerável da população brasileira.

A convocação foi do Ministro Edson Fachin, tendo como pauta a violação do preceito fundamental de liberdade de comunicação e expressão por ocasião dos bloqueios sofridos pelo *WhatsApp*. Participaram dessa audiência pública representantes da Polícia Federal (PF), da Procuradoria Geral da República (PGR), além de Brian Action, um dos fundadores do aplicativo.

Na ADPF, ajuizada pelo Partido Popular Socialista (PPS), foi invocada a violação da Lei 12.965/14 - Marco Civil da Internet, bem como da previsão constitucional relativa à privacidade.

Essa audiência pública foi o debate mais recente da Suprema Corte sobre o assunto. Nela, o representante do *WhatsApp* afirmou que o sistema de criptografia ponto a ponto impede que qualquer dado trafegado entre interlocutores ou grupos possa ser acessado por quem quer que seja. Somente os destinatários terão o acesso àquela informação. Afirmou ainda que nem mesmo a empresa que gerencia o *WhatsApp* consegue interceptar os dados.

No entanto, representantes da PF e da PGR discordaram do senhor Action quanto a essa limitação. O perito da PF citou a possibilidade do fornecimento de metadados pelo WhatsApp, os quais podem ter impacto decisivo nas investigações, como já explanado.

Essa possibilidade foi levantada em razão da obrigatoriedade de que o fluxo de comunicações do aplicativo passe pelos servidores do *WhatsApp*, interseção do sistema onde as chaves criptográficas poderiam ser permutadas. Com o referido procedimento não seria possível o acesso ao teor da conversa, no entanto, viabilizaria o acesso aos metadados.

Por sua vez, o representante da PGR afirmou ser a privacidade o fulcro do debate, argumentando que: "o Brasil não pode ser um paraíso digital, em que criminosos possam cometer infrações penais, violando direitos fundamentais tão importantes quanto o direito à privacidade".[18]

Cabe ainda ressaltar a discordância entre o STF e o STJ em relação a outro ponto polêmico, qual seja, o conteúdo do *WhatsApp* em celular apreendido, como podemos observar em decisão no julgado de 15 de março de 2016, cujo relator foi o Ministro NEFI CORDEIRO do STJ.[19]

Em resumo, foi decidido que o acesso ao conteúdo de conversas pelo *WhatsApp* em celular apreendido durante flagrante pela polícia precisa de autorização judicial para ser

[18] PAYÃO, Felipe. *WhatsApp* diz que é inviolável; Polícia Federal retruca o aplicativo no STF. **Tecmundo**, jun. 2017. Seção Software. Disponível em: <https://www.tecmundo.com.br/whatsapp/117364-whatsapp-diz-inviolavel-policia-federal-retruca-aplicativo-stf.htm>. Acesso em: 10 nov. 2017.

[19] BRASIL. Superior Tribunal de Justiça. Processual Penal. Recurso em Habeas-corpus. Constrangimento ilegal. **RHC** nº51.531/RO, da 6ª Turma do STJ, Brasília, DF, 19 de abril de 2016. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652>. Acesso em: 10 nov. 2017.

considerado como prova em processo judicial. A decisão foi da 6ª Turma do Superior Tribunal de Justiça no RHC 51.531/RO, sendo conflitante com posição anterior do STF.

O entendimento contrário apresentado pelo STF, e anterior à decisão da 6ª Turma do STJ, foi no julgamento do HC n. 91.867/PA, da relatoria do Ministro Gilmar Mendes, em que a 2ª Turma entendeu pela inexistência de coação ilegal na hipótese em que, após a prisão em flagrante, os policiais, ao apreenderem dois aparelhos de celular, procederam à análise dos registros telefônicos.

Em síntese, pode-se afirmar que o assunto ainda está longe de ser pacificado. Em adição aos questionamentos jurídicos, que envolvem princípios constitucionais, a Lei de interceptação telefônica e a Lei do marco civil da internet, aflora um grande entrave técnico, intrínseco à concepção do sistema de criptografia ponto a ponto, relacionado à possibilidade da interceptação de dados das conversas dos usuários do aplicativo.

Os representantes do *WhatsApp* afirmam ser impossível interceptar e fornecer dados em sua rede, entretanto, peritos afirmam ser possível realizar tal procedimento, já que a empresa proprietária possui o controle do processo de troca de "chaves".

Independente da discussão sobre possibilidade de quebra da criptografia vislumbra-se, pelo menos, quatro possibilidades de obtenção de dados[20] que não exigem a quebra da segurança do aplicativo nem a colaboração de seus proprietários e que poderão influenciar no curso do procedimento e invadir a privacidade do usuário.

Uma delas seria a instalação de vírus no computador ou no celular dos investigados, ao acessar o *WhatsApp* Web uma única vez todo o histórico poderia ser obtido por um software espião.

Outra forma seria a requisição do back up de conversas do Google Drive ou do iCloud, possível caso os usuários investigados tenham ativado essa facilidade.

[20] ROHR, Altieres. Como o governo teria grampeado terroristas no WhatsApp? G1.globo, São Paulo, jul. 2016. Seção Segurança Digital. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-o-governo-teria-grampeado-terroristas-no-whatsapp.html>. Acesso em: 09 nov. 17.

Uma terceira possibilidade seria a infiltração de agentes em grupos de *WhatsApp*, procedimento que, teoricamente, teria respaldado legal das Leis 12.850/2013 - sobre organização criminosa e 13.260/2016 – que trata de terrorismo.

A última e não menos importante seria a clonagem do número com colaboração da operadora, pois independente da cooperação do aplicativo as operadoras podem cooperar, esse metodologia encontraria respaldo na Lei 9.296/96 – que regulamenta a interceptação telefônica, desde que o procedimento fosse autorizado judicialmente.

2 A INTERCEPTAÇÃO TELEMÁTICA À LUZ DO ORDENAMENTO JURÍDICO

2.1 A interceptação telemática sob a ótica do direito brasileiro

2.1.1 CRFB/88 – dispositivo constitucional relacionado: art. 5º, XII

A opção por iniciar o presente capítulo com uma breve análise do dispositivo constitucional relacionado à interceptação deve-se ao entendimento de que qualquer discussão legislativa deve ser precedida da devida apreciação constitucional, de modo a que sejam delineados critérios interpretativos que garantam a intervenção mínima do direito penal e a máxima preservação da garantia dos direitos fundamentais.

Nesse viés, notabiliza-se o entendimento apontado pelo Ministro Luís Roberto Barroso:

> Como consequência do princípio da supremacia constitucional, nenhuma lei ou ato normativo - a rigor, nenhum ato jurídico - poderá subsistir validamente se for incompatível com a Constituição. Para assegurar essa superioridade, a ordem jurídica concebeu um conjunto de mecanismos destinados a invalidar e/ou paralisar a eficácia dos atos que contravenham a Constituição, conhecidos como controle de constitucionalidade. Assim, associado à superlegalidade da Carta Constitucional, existe um sistema de fiscalização judicial da validade das leis e atos normativos em geral.[21]

Dessa forma, o elemento constitucional estabelecerá o referencial necessário e adequado para alicerçar e balizar as considerações sobre a legislação infraconstitucional concernente ao tema em questão.

Nesse seguimento, traz-se a previsão constitucional sobre a inviolabilidade do sigilo das comunicações e a possibilidade de interceptação, contida no inciso XII, do artigo 5º:

> Art. 5º (...)
> (...)
> 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;

[21] BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010. p. 300.

A interpretação da previsão constitucional do inciso XII, art. 5º, CRFB/88, não é consensual. Os autores baseiam-se na interpretação gramatical do referido inciso para suscitar a dúvida.

Alguns sustentam que, de acordo com a redação do inciso, existiriam dois sigilos, um absoluto, relacionado exclusivamente à correspondência, e outro, relativo, associado às comunicações telegráficas, de dados e telefônicas, as quais se referem à expressão "no último caso".

Os demais autores sustentam que o sigilo seria absoluto, sendo relativo somente para as comunicações telefônicas, alegando que a expressão "no último caso" só é pertinente a ela. Essa divergência será trazida novamente para análise quando dos comentários sobre a Lei 9.296/96, que trata da interceptação telefônica.

2.1.2 Princípios constitucionais relacionados à interceptação telemática

Esse tópico trará considerações relativas aos princípios constitucionais selecionados como os mais significativos no contexto da admissibilidade da interceptação telemática como meio de obtenção de prova no processo penal.

Nesse sentido, cabe ainda ressaltar que muito além da exceção à inviolabilidade das comunicações prevista no dispositivo constitucional, a interceptação telemática, pode vir a representar uma preocupante violação das garantias instituídas por esses princípios.

2.1.2.1 Devido processo legal – contraditório e ampla defesa

A CRFB/88, em seu artigo 5°, inciso LIV, assegura que: "LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;"

Esse princípio se caracteriza como uma garantia, não da plena liberdade, mas de que, a privação dessa, somente se concretize quando os atos praticados pelas partes envolvidas tenham seguido todas os procedimentos previstos em lei.

O principal objetivo desse princípio é promover a paridade de condições de defesa e argumentação entre o Estado e o imputado, garantindo um equilíbrio processual entre as partes. Desmembra-se em outros dois princípios: o do contraditório e o da ampla defesa.

Em relação à interceptação telemática é cediço que parcela significativa dos doutrinadores considera que a invasão unilateral da privacidade e intimidade, sem sequer o conhecimento do investigado, contrapõe-se ao conceito do devido processo penal.

Outros, porém, consideram que, respeitada a imposição constitucional do inciso XII, 5º da CRFB/88 quanto à necessidade de ordem judicial, coexistindo os requisitos de *fumus boni iuris* e do *periculum in mora*, o procedimento de interceptação estaria harmonizado com o princípio do devido processo legal.

Em adição a CRFB/88, em seu artigo 5°, inciso LV, nos traz que: "LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;"

Em relação ao princípio do contraditório também inexiste o consenso em relação à interceptação telemática.

Parte da doutrina afirma que é incompatível com o princípio do contraditório, porque constitui meio de prova clandestino, utilizado para pesquisa prospectiva de indícios e/ou de autores, independente da existência de acusação oficial.

A outra vertente doutrinária defende tratar-se de medida cautelar probatória, conduzida na fase inquisitória do procedimento, sendo o contraditório apenas postergado para a fase da persecução judicial, ocasião em que as provas obtidas poderão ser descartadas.

No entendimento de Renato Brasileiro o contraditório nesse caso é assim definido:

> O contraditório sobre a prova, também conhecido como contraditório diferido ou postergado, traduz-se no reconhecimento da atuação do contraditório após a formação da prova. Em outras palavras a observância do contraditório é feita posteriormente, dando-se oportunidade ao acusado e seu defensor de, no curso do

> processo, contestar a providência cautelar, ou de combater a prova pericial feita no curso do inquérito.[22]

Ao comentar-se o princípio da ampla defesa deve-se ter em mente que a construção de qualquer defesa está fortemente ligada ao contraditório. No entanto, não se pode olvidar que o princípio do contraditório está afeto à proteção tanto do autor quanto do réu, enquanto que o da ampla defesa está voltado diretamente para o acusado.

Nessa linha de raciocínio aponta Renato Brasileiro:

> O exercício da ampla defesa só é possível em virtude de um dos elementos que compõe o contraditório – o direito à informação. Além disso, a ampla defesa se exprime por intermédio de seu segundo elemento: a reação.
> Apesar da influência recíproca entre o direito de defesa e o contraditório, os dois não se confundem. Com efeito, por força do princípio do devido processo legal, o processo penal exige partes em posições antagônicas, uma delas obrigatoriamente em posição de defesa (ampla defesa), havendo a necessidade de que cada um tenha o direito de se contrapor aos atos e termos da parte contrária (contraditório).[23]

Como se pode notar a interceptação telemática é um procedimento que, pelas especificidades das ações a serem empreendidas, pode, a qualquer momento, infringir o respeito ao contraditório, à ampla defesa e consequentemente ao devido processo legal. Tal situação pode caracterizar o cerceamento da defesa e acarretar a nulidade total ou parcial dos atos procedimentais.

2.1.2.2 Presunção de inocência

A CRFB/88, em seu artigo 5°, inciso LVII, nos traz que: “LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória;”

A mudança de entendimento do STF - trazida no informativo nº 814 – passou a considerar possível o início da execução penal condenatória após a prolação de acórdão condenatório em primeiro grau. Entretanto, esse posicionamento não atinge o princípio reitor do processo penal, a presunção de inocência.

---

[22] LIMA, Renato Brasileiro de. Manual de Processo Penal. 3. ed. rev. ampl. e atual. Salvador: JusPodivm, 2015. p. 51.
[23] Loc. cit.

A presunção de inocência ou não culpabilidade traz para a interceptação telemática um limite bastante tênue para a sua aceitabilidade. É cediço que para a instauração do procedimento faz-se necessário que sejam levantados "indícios razoáveis de autoria ou participação em infração penal", situação que seria antagônica a não incriminação prévia de um pretenso suspeito, o que na prática poderia traduzir-se como pretensão de culpa.

2.1.2.3 Proteção contra autoincriminação

Também conhecido como *nemo tenetur se detegere*, ou seja, ninguém é obrigado a produzir prova contra si mesmo. Esse princípio é extraído pela interpretação do inciso LXIII, art. 5º: "LXIII - o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado;".

O STF reafirmou a inteligência do princípio da inexigibilidade de autoincriminação, como se observa em trecho da decisão do Ministro Celso de Mello no HC 96982/DF:

> Esta Suprema Corte, fiel aos postulados constitucionais que expressivamente delimitam o círculo de atuação das instituições estatais, enfatizou que qualquer indivíduo "tem, dentre as várias prerrogativas que lhe são constitucionalmente asseguradas, o direito de permanecer calado. 'Nemo tenetur se detegere'. Ninguém pode ser constrangido a confessar a prática de um ilícito penal" (RTJ 141/512, Rel. Min. CELSO DE MELLO).
> Em suma: o direito ao silêncio - e o de não produzir provas contra si próprio (HC 96.219-MC/SP, Rel. Min. CELSO DE MELLO) - constitui prerrogativa individual que não pode ser desconsiderada por qualquer dos Poderes da República.[24]

Uma vez mais a interpretação telemática pode ser questionada, visto que em última análise quem tem a comunicação interceptada, acaba por produzir prova contra si mesmo.

2.1.2.4 Inadmissibilidade das provas obtidas por meio ilícito

A CRFB/88, em seu artigo 5°, inciso LVI, nos traz que: "LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;"

[24] BRASIL. Superior Tribunal Federal. Processual Penal. Informativo nº 530. Habeas-corpus nº: HC 96982/DF, In: SUPERIOR TRIBUNAL FEDERAL. Informativos. Brasília, DF, nov. 2008. Disponível em: <http://www.stf.jus.br/arquivo/informativo/documento/informativo530.htm.> Acesso em: 16 nov. 2017.

O entendimento desse inciso dá suporte ao sistema probatório pátrio na medida em que uma prova ilícita não fornecerá elementos sólidos e confiáveis o suficiente para respaldar a convicção do julgador, indicando a necessidade de descartá-la.

No entanto, parte da doutrina pondera que nenhuma liberdade pública é absoluta e por esse motivo, sustenta a possibilidade do uso da prova ilícita, em caráter de excepcionalidade, em benefício do réu, evocando os princípios da ampla defesa e do contraditório.

Nessa vertente, Renato Brasileiro, menciona que:

> Essa admissibilidade da prova ilícita *pro societate* somente seria possível em situações extremas, sob pena de se conferir ao Estado legitimidade ampla e irrestrita para violar direitos fundamentais, tornando letra morta o preceito constitucional que prevê a inadmissibilidade das provas obtidas por meios ilícitos.[25]

A outra postura sustenta, de maneira inegociável, ser inadmissível a utilização de qualquer prova obtida sem o devido respaldo legal. Esses doutrinadores consideram que o Estado não pode se permitir usar métodos que agridam a proteção de valores tutelados por lei, com a intenção de obter uma condenação penal.

Em consonância com o segundo entendimento, Alexandre de Moraes sustenta que:

> Os direitos e garantias individuais e coletivos não podem ser utilizados como um verdadeiro escudo protetivo da prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de total consagração ao desrespeito a um verdadeiro Estado de Direito.[26]

Aqueles que entendem pela inconstitucionalidade da interceptação telemática logicamente afirmam que a prova obtida por esse procedimento é ilícita e, portanto, só poderia ser aproveitada caso beneficiasse o investigado.

2.1.2.5 Do direito à intimidade

[25] LIMA, Renato Brasileiro de. Op. cit. p. 630.
[26] MORAES, Alexandre de. **Direito Constitucional**. 19. ed. São Paulo: Atlas, 2006. p.27.

Da CRFB/88, em seu artigo 5º, inciso X, temos que: "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

Percebe-se, numa leitura mais atenta do inciso, que a intimidade pode ser atingida em sua essência de dois modos principais, com a invasão propriamente dita – de um imóvel, por exemplo – , pela interceptação das comunicações entre dois ou mais interlocutores ou pela divulgação de informações obtidas pelos diversos meios de obtenção de prova.

Em relação à interceptação telemática, várias são as críticas que vem se desenrolando desde a promulgação da CRFB/88 e, posteriormente, com a edição da Lei 9.296/96, que deveria regulamentar o artigo 5º, inciso XII, mas que, no entanto, à época de sua promulgação, deixou lacunas quanto ao entendimento dos procedimentos a serem executados, que via de regra, poderiam violar a intimidade dos investigados.

Além disso, a violação do direito à intimidade não será restrita ao investigado. Deve-se ter a consciência de que terceiros que participem das conversações também sofrerão as consequências decorrentes do monitoramento.

Em seguimento, cabe uma ressalva sobre a extrema atenção que deve ser dada em relação à correta limitação do acesso e manuseio das provas mantidas sob custódia.

Nesse sentido, inúmeros dados coletados ficarão expostos a peritos, a autoridades policiais, ao MP, dentre outros revelando, ou melhor, expondo, por vezes, a indivíduos que não possuiriam a menor necessidade de conhecer do assunto, a intimidade de todos os interlocutores porventura monitorados.

2.1.2.6 Proporcionalidade

Em que pese não estar positivado explicitamente na CRFB/88, o princípio da proporcionalidade é essencial no contexto processual penal, estando sua essência intimamente ligada ao conceito de justiça, bem como ao devido processo legal, razão pela qual se optou, no presente trabalho, por introduzi-lo no contexto dos princípios constitucionais.

Nesse clivo, Barroso destaca que:

> Trata-se de um valioso instrumento de proteção dos direitos fundamentais e do interesse público, por permitir o controle de discricionariedade dos atos do Poder Público e por funcionar como a medida com que uma norma deve ser interpretada no caso concreto para a melhor realização do fim constitucional nela embutido ou decorrente do sistema. [...] O princípio pode operar, também, no sentido de permitir que o juiz gradue o peso da norma, em determinada incidência, de modo a não permitir que ela produza um resultado indesejado pelo sistema, fazendo assim a justiça do caso concreto.[27]

Este aspecto também é comentado por Alencar e Nestor Távora:

> O campo de atuação do princípio da proporcionalidade é polarizado. Tem-se admitido que ele deve ser tratado como um "superprincípio", talhando a estratégia de composição no aparente "conflito principiológico" (ex.: proteção à intimidade **versus** quebra de sigilo). Por sua vez, deve ser visto também na sua faceta da proibição de excesso, limitando os arbítrios da atividade estatal, já que os fins da persecução penal nem sempre justificam os meios, vedando-se a atuação abusiva do Estado ao encampar a bandeira do combate ao crime.[28]

Pode-se afirmar que, em razão da necessidade de harmonização dos princípios constitucionais, o princípio da proporcionalidade é imprescindível para conferir o equilíbrio entre as garantias do processo penal.

Será implementado como uma espécie de balança para a equiparação entre as garantias negativas, com a proibição de cometimento de excessos pelo Estado, e as positivas, nas quais o Estado é obrigado a agir, de modo a garantir uma proteção eficiente ao indivíduo e à sociedade.

Em relação à interceptação telemática entende-se que o princípio da proporcionalidade atuaria como um moderador à vedação de provas ilícitas, oferecendo um contraponto entre os direitos individuais, como a intimidade, e a proteção da sociedade, que teria preponderância. Dessa forma os princípios divergentes poderiam ser cotejados no intuito de qual deles seria prevalente.

---

[27] BARROSO, Luís Roberto. Op. cit. p. 305-306.
[28] TÁVORA, Nestor; ALENCAR Rosmar Rodrigues. Curso de direito processual penal. 11. ed. rev. ampl. e atual. Salvador: JusPodivm, 2016. p. 94.

2.1.3 Lei 9.296/96[29] - Interceptação Telefônica

A publicação dessa lei veio regulamentar o inciso XII, parte final, do art. 5° da CRFB/88, amenizando a lacuna legislativa que se arrastava desde a promulgação de nossa Carta Magna.

Em resumo, determinou a que a interceptação de comunicações telefônicas, de qualquer natureza, incluindo o fluxo de comunicações em sistemas de informática e telemática, para obtenção de prova em investigação criminal e em instrução processual penal. Dependeria de ordem judicial, para investigação somente de crime punível com reclusão, sendo mantido o procedimento sob segredo de justiça.

No entanto, a demora na regulamentação do referido inciso constitucional resultou em autorizações judiciais inconsistentes, no período de 1988 a 1996, gerando insegurança jurídica com o desrespeito a direitos fundamentais, como a intimidade individual.

Apesar do longo período de espera, cerca de oito anos, a lei de interceptação telefônica surgiu maculada em sua concepção. Alguns artigos não regulamentaram o inciso XII devidamente, ou o fizeram parcialmente, dando margem a uma quantidade significativa de recursos e severas críticas de diversos autores, particularmente, em relação à inobservância de princípios constitucionais.

Iniciando pelo artigo 1º, temos que:

> 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.

A primeira divergência sobre o artigo está relacionada ao caput. Diz respeito ao espectro abrangido pelo termo "interceptação telefônica", havendo posição majoritária na

[29] BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 26 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em 9 nov. 2017.

doutrina, que, dentre as modalidades apresentadas no item 1.2 do presente trabalho, estarão assim enquadradas, tanto a interpretação telefônica stricto sensu, quanto a escuta telefônica.

No entanto, também há o entendimento de que a Lei 9.296/96 aplica-se somente à interceptação telefônica stricto sensu, a qual necessitará, portanto, de autorização judicial.

As escutas e as gravações telefônicas não estariam enquadradas pela lei, por não existir a figura de um terceiro ator, externo à conversação, o qual faria a gravação. Por não corresponderem às definições apresentadas no item 1.2, sequer necessitariam de autorização judicial, sendo, portanto, lícita a prova assim obtida, desde que haja justa causa. Como exemplo pode-se citar o caso de uma família vítima de sequestro, que grava as conversações sobre os pedidos de resgate e ameaças sofridas.

A segunda divergência está relacionada a uma possível inconstitucionalidade do parágrafo único. Os que defendem essa posição alegam que a CRFB/88 no art. 5º, XII, traz textualmente: "comunicações telefônicas, salvo, no último caso" e que essa expressão limitaria que a interceptação fosse exclusivamente aplicada em comunicações telefônicas, ou seja, naquelas realizadas usando o aparelho telefônico.

Esse entendimento é minoritário e, data vênia, tenta sustentar-se no radicalismo do significado gramatical de uma expressão, relegando a segundo plano a capacidade interpretativa e a evolução de conceitos jurídicos básicos, fundamentais para o acompanhamento da transformação tecnológica dos modernos sistemas de comunicação e da sociedade como um todo.

Na verdade, esse apego gramatical de alguns autores se esvazia nos comentários de Ada Pellegrini, em relação ao texto constitucional original:

> O certo é que a Assembleia Nacional Constituinte aprovou texto diverso do que veio afinal a ser promulgado. A redação aprovada em segundo turno, no plenário, foi a seguinte: 'É inviolável o sigilo da correspondência e das comunicações de dados, telegráficas e telefônicas, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual'.[30]

[30] GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. Revista brasileira de ciências criminais. São Paulo: RT, nº 17, jan/mar, 1997, p. 113.

O acréscimo das palavras “comunicações”, “no último caso” e “penal”, ao texto constitucional original, pela Comissão de Redação da Assembleia Nacional Constituinte, alterou completamente o significado do conteúdo aprovado em plenário. Cabe ainda ressaltar que à comissão de redação competia, única e exclusivamente, rever, gramaticalmente, o texto aprovado.

Sendo assim, pode-se constatar que o artigo 5º, inciso XII da CRFB/88, como originalmente estruturado, facultava a possibilidade de quebra do sigilo, mediante autorização judicial, das comunicações telefônicas, das telegráficas e de dados, bem como quanto ao sigilo das correspondências em geral.

A comunicação telefônica, no passado, realmente restringia-se à transmissão única e exclusivamente de palavras e sons, no entanto, o conceito moderno de telefonia, particularmente com o advento de smartphones e tabletes, com capacidades de processamento cada vez maiores, traz o mundo da telemática para as mãos de qualquer usuário.

Nesse viés, é fundamental para a garantia de direitos fundamentais individuais e coletivos, que o Poder Judiciário lance mão de uma interpretação legislativa teleológica e progressiva, que se adeque à realidade do progresso da sociedade.

Encerrando as considerações a respeito do artigo 1º, cabe ainda destacar que já houve decisão unânime do pleno do STF na ADI nº 1.488-9, sendo relator o Ministro Néri da Silveira, que negou provimento na medida liminar. Pela decisão foi considerado constitucional o parágrafo único do referido artigo.

O artigo 2º nos traz que:

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

A lei veda a realização de interceptação de comunicação telefônica quando não houver indícios razoáveis da autoria ou participação em infração penal ou a prova puder ser feita por outros meios disponíveis, reafirmando a necessidade da presença do fumus boni iuris e do periculum in mora, condição *sine qua non* das medidas de caráter cautelar.

No artigo 10 temos:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena: reclusão, de dois a quatro anos, e multa.

A lei basicamente diz respeito ao direito processual penal, no entanto o art. 10º prevê a tipificação de crime.

Em relação aos demais artigos, cabe ressaltar: no artigo 5º, que a decisão deverá ser fundamentada, sob pena de nulidade, por período máximo de quinze dias renováveis por igual período, mediante comprovação da indispensabilidade; e no artigo 8º o sigilo dos procedimentos.

2.1.4 Lei 12.965/14 – Marco Civil da Internet

A Lei 12.965/14 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, além de proteger o sigilo das comunicações transmitidas via redes sociais em mensagens privadas.

A pertinência da lei do marco civil da internet com o presente trabalho deve-se à sua importância em relação ao item 1.3, que abordou a comunicação por sistemas criptografados ponto a ponto, particularmente, em relação ao aplicativo *WhatsApp*.

O artigo 7º, nos traz:

> "Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> [...]"

Pelos incisos do artigo 7º selecionados, pode-se depreender que a comunicação via redes sociais, no caso pelo aplicativo *WhatsApp*, deve ter tratamento similar ao dispensado aos demais tipos de comunicação, devendo a interceptação do fluxo de comunicação pelo aplicativo também ser submetida à prévia autorização judicial, nos moldes do que ocorre com a interceptação telefônica..

Outro artigo importante é o 9º, que trata da neutralidade da rede:

> Art. 9o O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
> [...]
> § 3o Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

O artigo 10 trata do sigilo, no tocante à proteção aos registros, aos dados pessoais e às comunicações privadas, nos seguintes termos:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.
> [...]

O artigo 11 trata da responsabilização de pessoa jurídica situada no exterior, que é o caso da empresa Facebook, proprietária do aplicativo *WhatsApp*:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os

> direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> [...]

O artigo 12 da Lei do Marco Civil da Internet respaldou as decisões judiciais de bloqueio do aplicativo em 2015 e 2016, já apresentadas em tópico próprio no presente trabalho.

Em Resumo, o grupo Facebook, empresa proprietária do aplicativo *WhatsApp*, não atendeu às determinações judiciais para colaborar em investigações criminais, ficando por quatro vezes suspenso no território nacional.

Apesar da Lei 12.965/14 necessitar de regulamentação em vários assuntos, nesse caso específico, tem previsão de bloqueio de páginas e aplicações de sanções às operadoras de telefonia móvel e provedores de acesso à internet que não cumpram ordem judicial, como detalhado abaixo no artigo 12:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> [...]
> III - **suspensão temporária das atividades que envolvam os atos previstos no art. 11**; (grifo nosso)
> [...]
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

2.1.5 Resolução 217/2016 do Conselho Nacional de Justiça (CNJ)

A Resolução nº 59/2008 do CNJ, havia sido editada para disciplinar e uniformizar as rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, especialmente no tocante à Lei nº 9.296/96.

O Conselho Nacional de Justiça, em fevereiro de 2016, motivado pelo Ofício 64/2016-GPR do Conselho Federal da OAB, atendeu requisição daquele órgão, na qual pleiteava o aperfeiçoamento da resolução pretérita.

Nesse sentido o CNJ decidiu alterar os artigos 10, que especifica os elementos que devem constar expressamente na decisão; o 14, que trata da prorrogação de prazo; o 17, que versa sobre sigilo; 18 que trata do controle da quantidade de interceptações em andamento e prorrogações; e o 19 que elenca as atribuições da Corregedoria Nacional de Justiça.

No entanto, na prática, as pequenas modificações continuaram sendo relacionadas basicamente ao procedimento do juiz quando da determinação de interceptação telefônica.

Cabe também citar que o CNJ confirmou na Resolução 217/2016 o entendimento da equiparação de voz e dados, já presente no artigo 2º da resolução de 2008, encerrando, dessa forma, a discussão, pelo menos no que se refere à prática forense.

Cabe ainda ressaltar a existência do Sistema Nacional de Controle de Interceptação Telefônica que reúne todas as informações concernentes às interceptações telefônicas impetradas no tribunal.

Nesse sistema o juiz deverá registrar todas as informações relacionadas à interceptação telemática. O banco de dados, que é alimentado pelos juízes e eletronicamente pelas operadoras, fica disponível no site do CNJ para livre consulta de qualquer cidadão, possibilitando a coleta de dados estatísticos e demais informações pertinentes.

2.2 A interceptação telemática sob a ótica do direito comparado

Os limites da licitude da interceptação telemática variam de acordo com o ordenamento jurídico de cada Estado soberano, no entanto, norteiam-se por diretrizes análogas, oriundas do Direito Internacional Público e da atuação das diversas organizações internacionais.

Como exemplo a essas normas internacionais, com interesse particular pelas relativas aos direitos humanos, cita-se, para o continente europeu, a Convenção Europeia dos Direitos

do Homem (CEDH) e para o continente americano a Convenção Americana sobre Direitos Humanos – Pacto de São José da Costa Rica.

Após breves considerações em relação à interceptação telemática sob a perspectiva do direito brasileiro, buscar-se-á, de forma expedita, abordar a adoção da aludida técnica na legislação alienígena, com o fito de expor alguns pontos da forma como esse procedimento é tratado por outros países, à luz de um viés comparativo com o direito brasileiro.

Dessa forma, para realizar a aludida exposição, os países foram selecionados, usando como critérios de escolha, o desenvolvimento científico-tecnológico de suas agências de investigação ou a proximidade com os usos e costumes brasileiros. Assim, versar-se-á, comparativamente ao direito brasileiro e em despretensiosa síntese, como é conduzida a interpretação telemática nos Estados Unidos da América (EUA), Inglaterra, Alemanha, Itália, França, Espanha e Portugal.

2.2.1 Estados Unidos da América

No entendimento da Justiça dos EUA, tanto na visão das agências de investigação federal (FBI, NSA etc.), quanto na dos Promotores de Justiça ou das polícias estaduais, é primordial para o combate ao crime, particularmente o organizado, o investimento substancial em material, equipamentos de investigação e especialmente no treinamento dos agentes.

Com a evolução e sofisticação do crime organizado e posteriormente, com as ameaças terroristas em seu território, agravadas pelo ataque às torres gêmeas em setembro de 2001, o "*U.S. Department of Justice*", bem como as companhias telefônicas, vêm fazendo vultosos investimentos, no intuito de evoluir seus meios investigativos. A criminalidade faz uso de todas as possibilidades oferecidas pela tecnologia das comunicações - senhas, misturadores de voz, mensagens criptografadas entre interlocutores (criptografia ponto a ponto) etc.

A IV emenda da Constituição dos EUA dispõe que:

> O direito do povo de estar seguro, na sua pessoa, nas suas casas, documentos e bens, contra desarrazoadas (não motivadas) buscas e apreensões, não pode ser violado; e nenhuma ordem deve ser emitida, exceto por uma causa (justificativa) razoável, embasada em declaração sob juramento ou afirmação e particularmente descrevendo o local a ser efetivada (a busca), e as pessoas ou coisas a serem apreendidas.

A interpretação da Suprema Corte Americana, tendo por base o disposto na IV emenda, formulou um espectro de amplitude mais abrangente para o termo busca (*search*). Sendo elencadas três possibilidades: razoável expectativa de privacidade, legítima expectativa de privacidade e justificável expectativa de privacidade.

Nesse sentido, a legislação americana passou a admitir a realização de investigação por meios eletrônicos, mediante ordem judicial, nos seguintes casos:

> 1 – Exista causa provável para acreditar que uma pessoa está praticando, tem praticado, ou vai praticar um dos crimes enumerados no 18 USC § 2516.[31]
> 2 – Exista causa provável para acreditar que comunicações particulares concernentes ao crime poderão ser obtidas através de interceptação.
> 3 – Procedimentos normais de investigação foram tentados e falharam, ou supostamente se afiguram insuficientes para o sucesso se forem realizados, ou são muito perigosos.
> 4 – Exista provável causa para acreditar que o local onde as interceptações devem ser realizadas está sendo utilizado ou será utilizado para a prática de crimes, está em nome de pessoa suspeita ou normalmente é utilizado por pessoa suspeita de prática de crimes.[32]

Para efeitos de licitude da interceptação telemática são considerados meios de investigação eletrônica os seguintes dispositivos:

> - *telephone tap*: extensão do número do telefone (interceptação telefônica);
> - *simple transmitter*: pequeno telefone instalado no local da escuta;
> - *telephone transmitter*: microfone instalado no aparelho de telefone;
> - *laser interceptors*: mecanismos que podem ser colocados, por exemplo, em uma janela e recepcionam a conversa de um ambiente fechado através da vibração de um vidro. O computador interpreta a vibração, decodificando-a nas conversas;
> - *satellite relays*: alguns microfones podem retransmitir por satélites especiais para um grande aparelho receptor maior; e
> - *fiber optics*: filamentos de fibra ótica são instalados dentro de paredes ou compartimento e transmitem a conversa através de um sistema elétrico especial.[33]

Pode-se mencionar ainda um instituto denominado investigação sequencial. Por entendimento da Suprema Corte, em havendo suspeito determinado e comprovação de que orbita em vários locais e utiliza meios de comunicação diversos, é possível a instalação de escutas nesses locais e/ou aparelhos de modo a obter a interceptação continua das conversações.

---

[31] United States Code
[32] MENDRONI, Marcelo Batlouni. **Crime Organizado**: aspectos gerais e mecanismos legais. 5. ed. São Paulo: Atlas, 2015. p. 396.
[33] Loc. Cit.

Cabe finalmente, comentário sobre procedimentos de algumas agências de investigação, particularmente, a Agência Nacional de Segurança (NSA), que após o atentado terrorista de 2001 passou a usar o programa de prospecção de dados denominado *Total Information Awareness* (TIA), que combinado com escutas variadas e com a colaboração das maiores companhias de telecomunicações visava, inicialmente, a prevenção de atentados.

O problema foi que a agência começou a ignorar as liberdades civis e não mais atender à obrigatoriedade de obtenção de autorização judicial para interceptação telemática da comunicação de cidadãos americanos.

Em 2013, Edward Snowden, ex-analista da NSA, foi a público denunciar abusos governamentais na realização de espionagem, envolvendo tanto o público interno quanto externo, inclusive chefes de governo de várias nações, como México, Brasil, França, entre outras.

2.2.2 Inglaterra

Apesar das evoluções tecnológicas e da preocupação crescente com a preservação dos direitos fundamentais do homem, a Inglaterra, seguidora do common law, continua observando sua concepção tradicional da admissibilidade da prova, desde que relevante para o embasamento do procedimento. (*admissibility-relevancy*).

O processo penal inglês busca a verdade material, não existindo a preocupação com exceções que possam acarretar a ilicitude do procedimento. Não há o instituto da prova obtida por meio ilícito, só importando a relevância da mesma para o processo.

A única exceção do ordenamento jurídico inglês em relação à ilicitude da prova obtida está relacionada à correspondência por cartas. No entanto, o direito inglês não usa a interceptação telefônica para a obtenção de provas, somente como meio de investigação.

Deve-se observar com atenção a evolução da jurisprudência inglesa uma vez que está cada vez mais pressionada pelas normas da CEDH, a qual foi ratificada pela Inglaterra em 1951.

2.2.3 Alemanha

A inteligência da Lei constitucional alemã prevê o sigilo das correspondências e das comunicações telefônicas. Interceptações, de qualquer natureza, são consideradas inconstitucionais, salvo em caráter excepcional quando houver a possibilidade do princípio da proporcionalidade.

De modo geral, o entendimento dos procedimentos a serem observados nas interceptações telemáticas em muito se assemelha ao do ordenamento jurídico norte-americano.

As infrações penais são enumeradas de modo taxativo, como a seguir:

> crimes contra o Estado, a segurança nacional, a ordem pública, ou contra a segurança das tropas dos Estados que aderiram ao Tratado do Atlântico Norte; crimes e homicídio voluntário premeditado, de falsificação da moeda, de sequestro, rapto, tráfico internacional de mulheres, estelionato e os crimes de perigo social, definidos no Código Penal alemão.[34]

2.2.4 Itália

Na Itália temos uma situação muito peculiar em virtude da forte presença do crime organizado na figura da máfia.

A Constituição italiana, em seu artigo 15, proclama a inviolabilidade do sigilo da correspondência e das comunicações, sob duas ordens de limitações: (a) limites impostos pelo juiz, por meio de ato motivado; e (b) garantias previstas pela lei.[35]

No entanto, devido à necessidade de regulamentar e dar respaldo para as ações investigativas contra a criminalidade mafiosa foi necessária a promulgação, à época em caráter emergencial, do Decreto-lei 356/92, que trouxe significativas modificações no Código de Processo Penal Italiano. Foram estabelecidas regras de prevenção quanto a interceptação telemática e a medidas cautelares de permanência.

---

[34] AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas**: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. rev. ampl. e atual. São Paulo: Revista dos Tribunais, 2015. p. 127.
[35] Loc. cit.

A referida lei trouxe a possibilidade, sob a denominação de "*intercettazione preventive*", de que o Ministério Público pudesse determinar diretamente a realização de interceptações telemáticas, em casos de urgência, devendo fazer a comunicação da instalação do procedimento em até 24 horas. O juiz, em até 48 horas, deverá ratificar ou anular o procedimento.[36]

Em relação aos princípios cabe comentar a possibilidade da aplicação do princípio do consenso, harmonizado com o princípio da legalidade, no intuito de flexibilizar os procedimentos, permitindo ao MP direcionar as providências legais de acordo com as especificidades de cada caso.

2.2.5 França

A Constituição francesa, apesar da atenção aos direitos do homem contidos na Declaração francesa, de 1789, não contempla em seu texto disposições específicas ao sigilo das comunicações.

A admissibilidade da interceptação telemática como meio de obtenção de prova trazia a nulidade dos atos instrutórios, em virtude da violação dos direitos de defesa, fato que acabava excluindo as provas do procedimento por serem consideradas ilícitas, podendo no máximo serem admitidas como indícios, para auxiliar o magistrado na formação de seu convencimento, se ele assim o entendesse.

Toda a polêmica girava em torno da previsão existente no art. 8º da Convenção Europeia dos Direitos do Homem (CEDH), a qual exige que os distúrbios da vida privada sejam previstos em lei específica, o que como já abordado anteriormente não acontecia no ordenamento jurídico francês.

A necessidade de previsão legal que atendesse o estipulado no artigo 8º da CEDH, levou a promulgação de Lei 91.646/91 que introduziu no CPP francês uma seção dedicada às interceptações de correspondências emitidas por vias de telecomunicações. O juiz pode

[36] MENDRONI, Marcelo Batlouni. Op. cit. p. 374.

determinar a interceptação nos crimes com previsão de pena maio do que dois anos de prisão.[37]

2.2.6 Espanha

A Constituição espanhola em seu art. 18, nº 1, garante o direito à honra, à intimidade pessoal e familiar e à própria imagem. O nº 3 estipula o segredo das comunicações, em especial, das postais telegráficas e telefônicas, salvo ordem judicial.[38]

Em 2003 entrou em vigor a Lei nº 32/2003, que regulamenta em seus artigos 33 a 36 o "*Secreto de las comunicaciones y protección de los datos personales*". Essa lei além de determinar os procedimentos técnico-investigativos, também fornece o regramento a ser observado pelas operadoras e sua obrigações perante o Poder Judiciário.

Segundo Mendroni, seus principais aspectos são:

> - obriga expressamente às operadoras que assumam o custo das operações judicialmente determinadas;
> - determina o sigilo das comunicações;
> - as operadoras devem adotar os meios técnicos necessários para garantir o sigilo das operações, bem como a proteção dos dados de caráter pessoal, adotando, para tanto, os meios técnicos necessárias; e
> - viabiliza, através das operadoras, que os dados da comunicação sejam cifrados, de forma a evitar leitura e/ou compreensão sem autorização.[39]

2.2.7 Portugal

Em relação à previsão da legislação portuguesa sobre a interceptação telefônica (para eles escutas telefônicas), Avolio nos traz que:

> Dos meios de obtenção da prova, revela-se, atualmente, um dos mais avançados textos legislativos sobre a matéria, cujas disposições sobre a sua admissibilidade (art. 187) e formalidades das operações (art. 188) abrange os demais meios invasivos das comunicações, aplicando-se, por extensão, 'às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrônico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceptação das comunicações entre presentes' (art.188.).[40]

---

[37] AVOLIO, Luiz Francisco Torquato. Op. cit. p. 133.
[38] AVOLIO, Luiz Francisco Torquato. Op. cit. p. 134.
[39] MENDRONI, Marcelo Batlouni. Op. cit. p. 427.
[40] AVOLIO, Luiz Francisco Torquato. Op. cit. p. 136-138.

3 A ADMISSIBILIDADE DA INTERCEPTAÇÃO TELEMÁTICA COMO MEIO DE OBTENÇÃO DE PROVA

3.1 Natureza jurídica da interceptação telemática

A prova, lato sensu, tem natureza jurídica de direito subjetivo de viés constitucional, sendo fundamental para a comprovação da veracidade dos fatos. Está diretamente ligada aos princípios da não autoincriminação (*nemo tenetur se detegere*), do devido processo legal, da inadmissibilidade das provas obtidas por meios ilícitos e da proporcionalidade.

Em decorrência, ao analisar-se as características da interceptação telemática chega-se a conclusão que tem natureza jurídica de meio de obtenção de prova.

Entretanto, à luz das condições estabelecidas nos artigos 2º e 3º da Lei 9.296/96, pode-se observar que também possui natureza jurídica de medida cautelar pela exigência de fumus boni iuris, advinda do art. 2º, I e do periculum in mora relacionado no inciso II, do mesmo artigo.

Em adição, cabe ainda ressaltar a natureza jurídica de medida cautelar preparatória, quando enseja a propositura da ação penal e de medida cautelar incidental, caso ocorra no curso do procedimento penal, sendo ambas extraída do art. 3º, incisos I e II, respectivamente.

Nesse sentido, Avolio aponta que:

> O provimento que autoriza a interceptação reveste-se de natureza cautelar, pois visa à fixação dos fatos, assim como de apresentam no momento da conversa. [...] A tutela cautelar penal surge, exatamente, como afirma Romeu Pires de Campos Barros, da impossibilidade de se fazer com rapidez e segurança jurídica o processo de conhecimento condenatório.[41]

A interceptação telemática, por apresentar natureza jurídica de medida cautelar, não permite a investigação de fatos futuros. Só é possível ser conduzida quando o suspeito já se encontre sob investigação criminal. Cabe ainda mencionar que pela sua natureza cautelar o suspeito deverá desconhecer a sua efetivação sob risco de insucesso do procedimento.

[41] AVOLIO, Luiz Francisco Torquato. Op. cit. p. 107.

3.2 Considerações sobre a prova advinda da interceptação telemática

Em observância ao art. 5º, XII da CRFB e à Lei 9.296/96, que o regulamenta, pode-se afirmar, em conformidade com o entendimento dos tribunais superiores, que preenchidos os requisitos legais previstos, entre eles a fundamentação da decisão e a competência do juiz que defere a medida, a prova obtida pela interceptação telemática é lícita, sendo meio hábil e legítimo de prova.

A inobservância de quaisquer dos requisitos legais estabelecidos acarretará a nulidade do procedimento.

Face ao desenvolvimento tecnológico e à sofisticação e evolução organizacional dos criminosos, em que pese a possibilidade de invasão da intimidade do indivíduo, não se pode prescindir de tão valioso meio de obtenção de prova.

No entanto, ao autorizar a instauração de procedimento sobremaneira invasivo da privacidade individual, não pode o magistrado, com o intuito de proteger interesses da sociedade, olvidar-se de preceitos relacionados às garantias e direitos fundamentais do indivíduo, imprescindíveis à preservação do estado democrático de direito.

3.2.1 Provas Lícitas e Provas Ilícitas

O art. 5º, LVI da CRFB/88, dispõe que: “são inadmissíveis no processo, as provas obtidas por meios ilícitos.”

Provas lícitas são aquelas que foram obtidas mediante integral observância do regramento jurídico.

A prova ilícita é aquela obtida com violação a regras de direito material, violação a direito da pessoa. Já a prova ilegítima é aquela obtida com violação de regras de ordem processual.

A prova ilícita é espécie do gênero das provas vedadas, proibidas ou inadmissíveis, como ensinam Alencar e Távora:

> A prova é taxada de proibida ou vedada toda vez que sua produção implique violação da lei ou de princípios de direito material ou processual. Por afrontar a disciplina normativa, não seria admitida ao processo. Temos assim, por classificação amplamente aceita, as provas vedadas, proibidas ou inadmissíveis, que é o gênero, do qual são espécies:
> a) As provas ilícitas: são aquelas que violam disposições de direito material ou princípios constitucionais penais. Ex.: confissão obtida mediante tortura (Lei nº 9.455/1997); interceptação telefônica realizada sem autorização judicial (art. 10 da Lei 9296/1996).
> b) As provas ilegítimas: violam normas processuais e os princípios constitucionais da mesma espécie. Ex.: laudo pericial subscrito por apenas um perito não oficial (art. 159, § 1º, CPP).
> [...] [42]

É possível admitir outros meios de obtenção de prova além dos elencados no CPP, no entanto, apesar da existência do princípio da liberdade probatória, deve-se observar suas limitações.

Em consequência desses limites é essencial a cuidadosa seleção desses meios, de modo a impedir a geração de provas proibida as quais não poderão ser admitidas no processo.

São espécies de prova proibida: a prova ilegítima e a prova ilícita, cujos conceitos já foram explanados acima. Detalhando os desdobramentos ocasionados pelos efeitos da prova proibida tem-se que: caso a prova seja ilícita, stricto sensu, deverá ser desentranhada dos autos, se for ilegítima acarretará uma mera irregularidade, uma nulidade absoluta ou uma nulidade relativa.

Outro aspecto que requer atenção diz respeito à relatividade da prova ilícita. Observa-se uma divergência diametralmente oposta de alguns autores, ancorada por um lado no princípio constitucional da liberdade individual e no outro no princípio da segurança da sociedade.

Os defensores de que toda e qualquer prova ilícita deve ser descartada pautam-se no princípio da liberdade individual, enquanto que aqueles que defendem a relatividade da utilização de provas ilícitas o fazem alegando a defesa da segurança da sociedade.

A despeito das críticas enfáticas dos partidários da vertente garantista, a qual afirma constituir um autêntico vilipêndio aos direitos fundamentais a aplicação do princípio da

[42] TÁVORA, Nestor; ALENCAR Rosmar Rodrigues. Op. cit. p. 624.

proporcionalidade, entendemos que uma prova colhida sob o manto da ilicitude possa, excepcionalmente, e em situações específicas, servir de subsídio para a convicção do julgador.

Nesse sentido, defende-se a aplicação do princípio da proporcionalidade devendo o julgador sopesar a preponderância de um princípio conflitante sobre o outro, objetivando manter ou recuperar o equilíbrio no caso concreto em julgamento.

Procedendo dessa forma, evitam-se radicalismos de ambas as partes, pois serão mantidos os direitos fundamentais bem como a estabilidade da sociedade pelo afastamento do sentimento de impunidade.

No tocante a uma possível ilicitude da prova obtida por interceptação telefônica, temos em resumo o que dispõe o art. 2º, da Lei nº 9.296/96, por garantias negativas, que o juiz não pode autorizar a interceptação de ligação telefônica nas seguintes hipóteses:

> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

A interceptação que incida em uma das hipóteses acima ou não possua autorização judicial é prova ilícita, além de passar a constituir crime, nos termos do art. 10º da referida lei.

No seguimento das provas ilícitas há ainda o instituto da prova ilícita por derivação, relacionada à teoria norte americana dos frutos da árvore envenenada (*fruits of the poisonous tree*[43]), cuja validade será analisada no próximo tópico.

3.2.2 Validade da prova emprestada, da obtida por derivação ou por encontro fortuito

[43] A primeira decisão em que a Suprema Corte Americana adotou a teoria (no entanto sem usar seu nome) foi no caso Silverthorne Lumber Co. vs Estados Unidos, em 1920. Alguns anos depois, em 1939, ao julgar o Nardone vs Estados Unidos, O Tribunal se referiu explicitamente à exclusão de provas ilícitas utilizando a terminologia "frutos da árvore venenosa". CICCHI, Rafael. A teoria dos frutos da árvore envenenada - fruits of the poisonous tree, artigo, disponível em< https: //djfeco.jusbrasil.com.br/artigos/445150669/a-teoria-dos-frutos-da-arvore-envenenada-fruits-of-the-poisonous-tree>, acesso em 13 out 2017.

3.2.2.1 Prova emprestada

Entende-se por prova emprestada aquela que é produzida em um processo, fruto de uma investigação criminal e é conduzida para a utilização em outro.

Ao referir-se a tal assunto, Alencar e Távora nos trazem que:

> É aquela produzida em um processo e transportada documentalmente para outro. A prova pode assim ser importante a mais de um processo. [...]. Havendo justificativa plausível, o empréstimo será oportunizado. Pode ser patrocinado o empréstimo probatório, até mesmo de um processo cível a um criminal.[44]

Requisitos para a aceitação da prova emprestada:

- as partes devem ser as mesmas em ambos os processos;
- o fato demonstrado pela prova a quer emprestada deve ser relevante para os dois processos;
- o contraditório deve ter sido respeitado no processo que concede a prova; e
- os requisitos formais de produção probatória devem ter sido observados no processo cedente.

Em seguimento ressalta-se que não há hierarquia entre as provas. Uma prova emprestada pode mostrar-se tão ou mais importante que outra já existente no processo de destino, entretanto, considera-se insuficiente para formação da convicção do julgador, a prova emprestada, se for a única do processo de destino.

Em relação à interceptação telemática Alencar e Távora nos trazem que:

> Julgados do STF (HC-102293) e do STJ (MS 201102155278), se posicionam no sentido de que é possível o empréstimo de provas formadas no processo penal ou inquérito policial a procedimentos diversos do penal, notadamente aquelas reunidas através da interceptação telefônica.[45]

[44] TÁVORA, Nestor; ALENCAR Rosmar Rodrigues. Op. cit. p. 639.
[45] TÁVORA, Nestor; ALENCAR Rosmar Rodrigues. Op. cit. p. 642.

Entretanto, os autores discordam desse posicionamento das cortes superiores, por entenderem que a prova obtida pela interceptação telefônica deve ser restrita e exclusivamente afeta ao processo penal.

Por seu lado, Ada Pellegrine possui entendimento similar ao dos superiores tribunais, sustentando que:

> O valor constitucionalmente protegido pela vedação das interceptações telefônicas é a intimidade. Rompida esta, licitamente, em face do permissivo constitucional, nada mais resta a preservar. Seria uma demasia negar-se a recepção da prova assim obtida, sob a alegação de que estaria obliquamente vulnerado o comando constitucional. Ainda aqui, mais uma vez, deve prevalecer a lógica do razoável.[46]

A prova emprestada visa à economia e celeridade processual, e, desde que observados os preceitos, constitucionais opta-se pelo mesmo entendimento adotado pela professora Ada Pellegrini em relação à prova emprestada oriunda de uma interceptação telemática.

Nesse viés, entende-se que a vedação constitucional se dá em relação à utilização da interceptação telemática para apuração de fato no âmbito de matéria cível e não em relação à utilização da prova documental já devidamente consolidada e submetida ao contraditório.

Cabe ainda mencionar uma situação mandatória para utilização da prova emprestada tanto na área penal, quanto na cível ou administrativa. Enquadra-se nessa situação aquela prova que seja fundamental para o convencimento do julgador e impossível de ser repetida, só existindo por essa razão no processo de origem.

3.2.2.2 Prova ilícita por derivação

A prova ilícita por derivação é, por imposição lógica, aquela prova obtida de forma lícita, sendo, no entanto, oriunda de elementos fornecidos por uma prova ilícita.

No entendimento de Renato Brasileiro, tem-se que:

---

[46] GRINOVER, Ada Pellegrine (2007. p. 194. apud CRUZ, Raugir Lima. Artigo: Uma análise principiológica e legal das interceptações telefônicas: a produção probatória à luz do princípio da proibição da proteção deficiente, disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11434. Acesso em 14 nov. 2017.

> Provas ilícitas por derivação são os meios probatórios que, não obstante produzidos, validamente, em momento posterior, encontram-se afetados pelo vício da ilicitude originária, que a eles transmite, contaminando-os, por efeito de repercussão causal. Afirma ainda o supracitado autor que de nada adiantaria dizer que são inadmissíveis, no processo, as provas obtidas por meios ilícitos, se essa ilicitude também não se transmitisse às provas delas derivadas.[47]

A CRFB/88 não abordou a prova ilícita por derivação, no entanto, a reforma processual trazida pela Lei 11.690/2008[48], incluiu explicitamente a proibição no art. 157 do Código de Processo Penal[49], *in verbis*:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
> § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.
> § 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.

Após a entrada em vigor da Lei 11.690/2008, a teoria norte-americana dos frutos da árvore envenenada[50], também conhecida como teoria da ilicitude derivada ou teoria da mácula, passou a integrar expressamente o nosso CPP. Por essa teoria a prova ilícita originária (árvore), tem a potencialidade de contaminar todas as provas nela originadas (frutos).

Entretanto, a teoria dos frutos da árvore envenenada ou da ilicitude derivada não é absoluta, admitindo algumas limitações, são elas:

- prova absolutamente independente ou teoria da fonte independente – são as provas lícitas, totalmente independentes da prova ilícita produzida, não havendo vinculação nem dependência entre as mesmas, não serão contaminadas;

---

[47] LIMA, Renato Brasileiro de. Op. cit. p. 612.
[48] BRASIL. Lei nº 11.690 de 9 jun. de 2008. Altera dispositivos do Decreto-Lei no 3.689, de 3 out. 1941 – Código de Processo Penal, relativos à prova, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 10 jun. 2008. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm>. Acesso em: 9 nov. 2017.
[49] BRASIL. Decreto-Lei nº 3.689 de 3 out. 1941. Código de Processo Penal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 out. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em 08 out. 2017.
[50] V. nota de rodapé 43.

- descoberta inevitável ou exceção da fonte hipotética independente – aplica-se nos casos em que a prova derivada seria conseguida de qualquer modo por outros atos de investigação válidos;

- contaminação expurgada, conexão atenuada – existe o vínculo da prova derivada com a prova ilícita, no entanto essa ligação é tão tênue que se torna desprezável, descaracterizando a contaminação da prova derivada; e

- boa-fé ou exceção da boa-fé – quando o agente investigativo desprovido de dolo obtém prova por meio ilícito. A ilicitude pode ser afastada tendo que ser observada além da boa-fé subjetiva, o respeito às leis (boa-fé objetiva). O agente acredita que está agindo completamente dentro do ordenamento jurídico.

3.2.2.3 Prova por encontro fortuito

Também conhecida como teoria da serendipidade, significa para o processo penal o encontro acidental de provas advindas de delito diverso daquele esperado em determinada investigação criminal.

No entendimento de Renato Brasileiro, o encontro fortuito de provas se caracteriza da seguinte forma:

> A prova de determinada infração penal é obtida a partir de diligência regularmente autorizada para a investigação de outro crime. Nesses casos, a validade da prova inesperadamente obtida está condicionada à forma como foi realizada a diligência: se houve desvio de finalidade, abuso de autoridade, a prova não deve ser considerada válida; se o encontro da prova foi casual, fortuito, a prova é válida.

O encontro fortuito de provas é tema de fundamental importância no âmbito da interceptação telemática pelas características da grande imprevisibilidade inerentes ao procedimento.

Desde que cumpridos os requisitos legais e certificando-se de que não tenha ocorrido desvio de finalidade no decorrer da investigação criminal pode-se asseverar a validade dos indícios assim obtidos.

Duas situações podem ocorrer em relação às provas obtidas de modo fortuito no decorrer da investigação criminal: ser considerada como prova válida, desde que guarde conexão ou continência como o fato investigado, ou caso contrário, sendo inválida, servirá como notícia do crime para abertura de novo procedimento investigativo.

3.3 Preservação da cadeia de custódia da prova

A preservação da cadeia de custódia da prova vai muito além de um simples e mero armazenamento de arquivos de áudio relacionados a potenciais crimes, inclui procedimentos complexos que se estendem desde a correta maneira de obter, localizar e identificar as possíveis evidências na cena do crime até o seu destino final, no devido local para depósito, guarda e manutenção, passando por toda a sequência de obtenção, produção, manuseio e transporte.

A prova é o elemento nuclear estrutural da cadeia de custódia, pois é a partir da obtenção dela que se iniciam todos os procedimentos afetos ao estabelecimento do correto encadeamento de ações que tem como objetivo precípuo assegurar que a prova seja legítima. Dessa forma, busca-se que não se viole as regras processuais, ou melhor, que seja lícita a prova obtida, pautando-se na observância das normas constitucionais e infraconstitucionais.

Nesse contexto, considera-se que a prova pericial é a mais importante e complexa. De um modo geral é ela que alicerça a formação do convencimento motivado dos magistrados, devido ao sustentáculo conferido pela fundamentação científica e neutralidade que a caracterizam.

3.3.1 Particularidades da cadeia de custódia

Segundo a posição adotada por José Braz:

> A chamada cadeia de custódia da prova é o processo usado na investigação criminal para manter e documentar a história cronológica de um vestígio, garantindo a sua integridade e a possibilidade de permanente escrutínio do potencial probatório que o mesmo contém.[51]

[51] BRAZ, José. **Investigação Criminal**: a organização, o método e a prova: os desafios da nova criminalidade. 2. ed. Coimbra: Almedina, 2010. p. 224.

"O fato de assegurar a memória de todas as fases do processo constitui um protocolo legal que possibilita garantir a idoneidade do caminho que a amostra percorreu." (NÓBREGA).[52]

WATSON descreve a cadeia de custódia como "o processo pelo qual as provas estão sempre sob o cuidado de um indivíduo conhecido e acompanhado de um documento assinado pelo seu responsável, naquele momento."[53]

3.3.1.1 Peritos

Em relação ao preparo técnico faz-se necessário destacar a ação dos peritos.

No entendimento de José Braz:

> Procurando responder a cada um dos distintos e irrepetitíveis circunstancialismos que caracterizam a prática criminal, dir-se-á que todas as perícias são admissíveis, desde que respeitem o princípio da legalidade e legitimidade da prova, isto é, que o seu objecto, a sua natureza e os processos que utiliza, não sejam proibidos por lei nos termos dos arts. 125.º e 126.º do CPP.[54]

ESPÍNDULA cita que "todos os elementos que darão origem às provas periciais ou documentais requerem cuidados para resguardar a sua idoneidade ao longo de todo o processo de investigação e trâmite judicial."[55]

3.3.1.2 A preservação da cadeia de custódia e o problema da contaminação das evidências

Nesse viés, traz-se um breve comentário sobre a correlação entre a cadeia de custódia da prova, a teoria dos frutos da árvore envenenada e a quebra da preservação da cadeia de custódia no processo penal.

---

[52] NÓBREGA, 2006, apud FERRARI JÚNIOR, Ettore. **A cadeia de custódia e a prova pericial**, artigo, disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11434>, acesso em 11 out. 2017.

[53] WATSON, James D, et al. **DNA Recombinante: genes e genomas**. Artmed Editora. 3a Ed. 2009, apud FERRARI JÚNIOR, Ettore. A cadeia de custódia e a prova pericial, artigo, disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11434>, acesso em: 11 out. 2017.

[54] BRAZ, José. Op. Cit. p. 142.

[55] ESPÍNDULA, Alberi. Perícia Criminal e Cível: uma visão geral para peritos e usuários da perícia. 3. ed. Campinas, São Paulo. Millenium Editora, 2009, apud FERRARI JÚNIOR, Ettore. **A cadeia de custódia e a prova pericial**, artigo, disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11434>, acesso em: 11 out. 2017.

O modo de obtenção, bem como a preservação das provas produzidas são fundamentais para a evolução satisfatória do processo judicial. Nesse sentido a imprudência, imperícia ou negligência na aquisição e/ou no manuseio das evidências poderão ocasionar a quebra da preservação da cadeia de custódia no processo penal e levar a perda da função probatória dessas evidências.

Em adição podemos afirmar que a teoria dos frutos da árvore envenenada se aplica em absoluta sintonia em relação a qualquer ocorrência que venha a acarretar a quebra da preservação da cadeia de custódia, visto que, provas obtidas de forma ilícita ou invalidadas por condutas incorretas no decorrer do procedimento de custódia irão contaminar as demais provas que delas se originarem por derivação.

3.3.1.3 Considerações sobre a cadeia de custódia da prova na interceptação telemática

Em relação à preservação dos elementos de prova em custódia cabe citar que em virtude da evolução dos sistemas de comunicação digital, dos meios de obtenção de áudio e da facilidade de manipulação dos sistemas, pode-se afirmar que não existe mais a tradicional gravação original.

Por inconsistências do sistema a geração de backups pode falhar inviabilizando o contraditório e, dessa forma, acarretando o cerceamento da defesa, a qual estará privada do acesso aos áudios integrais, caso entenda necessário. Nesse aspecto, cabe ainda a ressalva de que a rotina de degravação é estabelecida somente em trechos do aúdio de interesse da acusação.

Ainda nesse viés da inconsistência dos sistemas, cabe a ressalva da possibilidade de apagamento lógico ou por sobrescrição, o que impossibilitaria qualquer ação no sentido de rastrear determinada fonte de prova, de modo a esclarecer, por exemplo, se aquela prova apresentada pela acusação é válida ou inválida por ser advinda de uma prova ilícita;

Ao referir-se a esse assunto Geraldo Prado nos traz os princípios da *mesmidade* e da desconfiança. A palavra *mesmidade*, tem origem na língua espanhola, não apresentando tradução exata para o português. Seu significado assemelhasse ao do vocábulo mesma, ou

seja, seria a certeza de que a prova apresentada para valoração do julgador é absolutamente a mesma que foi obtida pelo procedimento.[56]

Em síntese, pode-se dizer que inexiste uma cadeia de custódia das provas oriundas das interceptações telefônicas. O controle de prazos, bem como o de acesso pela autoridade policial que detém os arquivos é precário. Contribuindo negativamente para todo o processo estão os superpoderes atribuídos às operadoras telefônicas, teoricamente no intuito de otimizar os procedimentos, acaba por fragilizar o sistema.

3.4 A interceptação telemática na investigação criminal

A interceptação telemática é um meio fundamental para a obtenção de provas. A condução do procedimento segue normas bem específicas no intuito de preservar garantias individuais, particularmente, em relação ao direito à privacidade e ao segredo das comunicações.

Por ser um instituto afeto a reserva de jurisdição, o agente policial e/ou o MP requisitam ao juiz a permissão para instauração do procedimento. Segundo o art. 5º da Lei 9.296/96, o período de interceptação deve ter duração máxima de quinze dias, prorrogáveis por mais quinze, de acordo com a necessidade.

O juiz terá prazo máximo de vinte e quatro horas para autorizar ou negar o pedido, de acordo com o previsto no art. 4º, § 2º do mesmo dispositivo legal.

Nesse ponto apresenta-se a primeira controvérsia acerca da temática: o prazo acima citado pode ser prorrogado indefinidamente? Ou há um limite para o número de prorrogações? Conforme entendimento adotado pela doutrina e jurisprudência majoritária, admite-se a possibilidade de prorrogações sucessivas, desde que respeitados os requisitos legais.

[56] PRADO, Geraldo. “Ainda sobre a quebra da cadeia de custódia das provas”, in Boletim do IBCCrim, n. 262, setembro de 2014, p. 16-17, apud ROSA E AURY LOPES. Artigo. A importância da cadeia de custódia para preservar a prova penal. Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>. Acesso em 5 out. 2017.

Os áudios oriundos da interceptação ou escuta devem ser gravados, consolidados em arquivos e encaminhados para degravação pela autoridade policial. Após o áudio ter sido degravado é remetido ao juiz, em apartado dos autos do inquérito, de modo a preservar não só o caráter sigiloso do material, como também para evitar exposições desnecessárias da vida íntima dos envolvidos. O MP selecionará os indícios necessários ao oferecimento da denúncia.

Nesse ponto, depara-se com o maior questionamento relacionado à observação do devido processo legal. O áudio oriundo da interceptação, após ter sido degravado e posteriormente analisado e selecionado pelo MP para o oferecimento da denúncia, pode não ser fornecido na íntegra para a defesa e, desse modo, gerar, eventualmente, um problema relacionado ao cerceamento de defesa, uma vez que nosso ordenamento jurídico é guiado pelo princípio constitucional da ampla defesa.

Portanto, conclui-se que à luz do princípio da ampla defesa, pode-se facear situação em que a defesa encontre-se tolhida de seu pleno exercício, em razão da limitação do acesso a certos trechos do áudio, os quais podem ter sido inexpressivos para a acusação, mas se mostrem imprescindíveis para a argumentação da defesa.

3.5 A admissibilidade da interceptação telemática

3.5.1 Como meio de prova PRO REO

De um modo geral tanto a doutrina quanto a jurisprudência tem admitido a prova ilícita obtida por interceptação telemática caso esta seja a única maneira de comprovar a inocência do acusado na persecução criminal, em virtude de estar-se privilegiando bem maior do que o protegido pela norma, qual seja, a liberdade de um inocente.

Complementando esse entendimento Renato Brasileiro destaca que:

> A norma constitucional da inadmissibilidade da utilização no processo de provas obtidas por meios ilícitos (CF, art. 5º, LVI) representa uma limitação ao direito de punir do Estado, depreende-se que o juiz pode, com base em uma prova ilícita, proferir uma sentença absolutória.[57]

[57] LIMA, Renato Brasileiro Op. cit. p. 629.

3.5.2 Como meio de prova PRO SOCIETATE

A utilização da prova ilícita, obtida pela interceptação telemática, em prol da sociedade apresenta opiniões significativamente contrárias. Aqueles que defendem sua admissibilidade como prova baseiam-se no princípio da proporcionalidade. Essa vertente recebe pesadas críticas de seus opositores, os quais afirmam ser inadmissível que o direito à prova prevaleça sobre direitos fundamentais. Tal flexibilização abriria perigoso precedente no sentido de que passaria a ser impossível o estabelecimento de qualquer vedação probatória.

Renato Brasileiro traz o entendimento de Barbosa Moreira sobre o assunto:

> A aplicação do princípio da proporcionalidade também autoriza a utilização de prova ilícita em favor da sociedade, como, por exemplo, nas hipóteses de criminalidade organizada, quando esta é superior às Polícias e ao Ministério Público, restabelecendo-se, assim, com base no princípio da isonomia, a igualdade substancial na persecução criminal.[58]

Dessa forma, pode-se concluir afirmando que os entendimentos doutrinário e jurisprudencial acenam com uma efêmera possibilidade de aplicação do princípio da proporcionalidade em situações de extrema necessidade em caso de incontornável ameaça a direito fundamental de outrem.

[58] BARBOSA MOREIRA, José Carlos. **A constituição e as provas ilicitamente obtidas**. Revista Forense, v.337. p. 128, apud LIMA, Renato Brasileiro Op. cit. p. 630.

CONCLUSÃO

Por meio do presente estudo pretendeu-se demonstrar a importância da interceptação telemática, ao longo do tempo, no escopo do desenvolvimento da investigação criminal. A evolução tecnológica, aliada a novas técnicas de comunicação, trouxe um novo paradigma criminal a ser enfrentado pelos órgãos estatais.

É nesse sentido que se apresenta a defesa de uma evolução das normas e da inteligência jurídica de modo a viabilizar uma reprimenda estatal mais eficaz e de acordo com os parâmetros legais, a fim de mitigar possível mácula aos direitos e garantias fundamentais. O incomparável poder de transformação resultante do binômio poder de compra e tecnologia disponível à criminalidade, obriga a uma atuação estatal cada vez mais proativa.

Assim, pode-se afirmar, que o simples fornecimento de sofisticado aparato investigativo aos agentes estatais não resolverá o problema. É necessário que a legislação especial evolua em sintonia com as possíveis ameaças que a revolução tecnológica impõe. Como por exemplo, pode-se citar algumas situações enfrentadas pelo direito alienígena: na Itália, os problemas crônicos com a máfia; e nos EUA, dificuldades com o terrorismo e com a violação da intimidade do cidadão comum.

A Itália é um caso típico de reformulação significativa da legislação e flexibilização do entendimento doutrinário para opor-se ao crime organizado, no caso materializado na máfia italiana, de modo a mitigar a sensação de insegurança e impunidade que reinava no País na década de 1990. A Operação "*mani pulite* (mãos limpas)" só teve êxito pelas possibilidades investigativas advindas de reformas legislativas e da reestruturação do Poder Judiciário e demais estruturas como o MP.

Por outro lado, o governo dos EUA, apesar de toda a sua capacidade de mobilização tecnológica, não se ateve ao mais importante: a garantia de direitos fundamentais individuais, sob o falso pretexto de monitorar terroristas no exterior foram desenvolvidos sistemas de rastreamento e acompanhamento que interceptavam comunicações ao redor do mundo. Tal procedimento evoluiu e depois, por exagero das agências de investigação (FBI, NSA etc.) passaram a monitorar o cidadão comum americano, caracterizando total desrespeito à privacidade e a intimidade.

Ainda no escopo da tecnologia é importante comentar a situação do aplicativo *WhatsApp* no Brasil. A atual situação carece de uma rápida solução pois é inadmissível que um país tenha sua soberania maculada por uma sociedade empresária estrangeira, que tenha desrespeitado tanto uma decisão judicial quanto a legislação pertinente, no caso a Lei 12.965/14 – Marco Civil da Internet, que prevê multa e desligamento dos sistemas.

Já em relação à temática provas, ressalta-se a importância da preservação da cadeia de custódia da prova, particularmente em relação à interceptação telemática, pois, como é cediço, é uma atividade investigativa extremamente sensível e produtiva.

Nesse sentido, cabe ressaltar que todo o mecanismo relativo à cadeia de custódia da prova obtida pela interceptação telemática deve ser muito bem definido e controlado. Qualquer falha no decorrer do procedimento - obtenção do áudio, catalogação, armazenagem e preservação de arquivos - poderá levar à contaminação de determinada prova, tornando-a ilícita ou ainda acarretar, por exemplo, o cerceamento de defesa, no caso de apagamento parcial de um áudio.

A triste realidade brasileira revela a inexistência de uma cadeia de custódia da prova corretamente organizada de modo a prestar o devido suporte à prova originada em uma interceptação telemática. Os problemas são diversos: controles de prazos e de acessos aos arquivos ineficientes, possibilidade de apagamento lógico ou por sobrescrição, dentre outros.

Por fim, levando-se em conta os aspectos expostos ao longo do presente trabalho pode-se constatar a importância da interceptação telemática para o direito processual penal, particularmente como um dos mais eficientes meios de obtenção de provas, alertando-se ainda quanto à importância da preservação da cadeia de custódia da prova na preservação da licitude da prova. Observados os requisitos legais e constitucionais exigidos pode-se afirmar que a prova assim obtida é plenamente admissível em qualquer o processo penal.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 9 nov. 2017.

BRASIL. Constituição Política do Império do Brasil de 1824**. Coleção de Leis do Império do Brasil - 1824, Página 7 Vol. 1**, Carta de Lei de 25 de Março de 1824. Rio de Janeiro, RJ, 25 mar. 1824. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1824-1899/constituicao-35041-25-marco-1824-532540-publicacaooriginal-14770-pl.html>. Acesso em 10 nov. 2017.

BRASIL. Constituição da República dos Estados Unidos do Brasil de 1891. **Diário [do] Congresso Nacional**, Rio de Janeiro, RJ, 24 fev. 1891. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1824-1899/constituicao-35081-24-fevereiro-1891-532699-publicacaooriginal-15017-pl.html>. Acesso em 10 nov. 2017.

BRASIL. Constituição da República dos Estados Unidos do Brasil de 1934. **Diário Oficial [da] União - Seção 1- Suplemento**, Rio de Janeiro, RJ, 16 jul. 1934. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1930-1939/constituicao-1934-16-julho-1934-365196-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

BRASIL. Constituição da República dos Estados Unidos do Brasil de 1937. **Diário Oficial [da] União - Seção 1**, Rio de Janeiro, RJ, 10 nov. 1937. Disponível em: http://www2.camara.leg.br/legin/fed/consti/1930-1939/constituicao-35093-10-novembro-1937-532849-publicacaooriginal-15246-pl.html 10/11/1937. Acesso em 10 nov. 2017.

BRASIL. Constituição dos Estados Unidos do Brasil de 1946. **Diário Oficial [da] União - Seção 1**, Rio de Janeiro, RJ, 19 set. 1946. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1940-1949/constituicao-1946-18-julho-1946-365199-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

BRASIL. Constituição do Brasil de 1967. EC nº 1, de 1969. **Diário Oficial [da] União**, Brasília, DF, 20 out. 1969. Disponível em: <http://www2.camara.leg.br/legin/fed/emecon/1960-1969/emendaconstitucional-1-17-outubro-1969-364989-publicacaooriginal-1-pl.html>. Acesso em 10 nov. 2017.

BRASIL. Decreto-Lei nº 3.689 de 3 out. 1941. Código de Processo Penal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 out. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em 08 out. 2017.

BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 26 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em 9 nov. 2017.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do**

Brasil, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 9 nov. 2017.

PRADO, Geraldo Luiz Mascarenhas. **Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça**. 2. ed. Rio de Janeiro: Editora Lumen Juris, 2012.

BRAZ, José. **Investigação Criminal**: a organização, o método e a prova: os desafios da nova criminalidade. 2. Ed. Coimbra: Almedina, 2010.

JESUS, Damásio Evangelista de. **Interceptação de comunicações telefônicas**: notas à Lei nº 9296, de 24 jul. 1996. Revista dos Tribunais, São Paulo, n. 735, p. 458-473, jan. 1997.

GOMES, Luiz Flávio e MACIEL, Silvio. **Interceptação telefônica**: comentários à Lei 9269/96. 3. Ed. rev. e ampl. São Paulo: Revista dos Tribunais, 2014.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. 3. ed. rev. ampl. e atual. Salvador: JusPodivm, 2015.

TÁVORA, Nestor; ALENCAR Rosmar Rodrigues. **Curso de direito processual penal**. 11. ed. rev. ampl. e atual. Salvador: JusPodivm, 2016.

MENDRONI, Marcelo Batlouni. **Crime Organizado**: aspectos gerais e mecanismos legais. 5. ed. São Paulo: Atlas, 2015.

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas**: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. rev. ampl. e atual. São Paulo: Revista dos Tribunais, 2015.

MORAES, Alexandre de. **Direito Constitucional**. 19. ed. São Paulo: Atlas, 2006.

GRINOVER, Ada Pellegrini. **O regime brasileiro das interceptações telefônicas**. Revista brasileira de ciências criminais. São Paulo: RT, n. 17, jan/mar, 1997.

ESPÍNDULA, Alberi. **Perícia Criminal e Cível**: uma visão geral para peritos e usuários da perícia. 3a Ed. Campinas, São Paulo. Millenium Editora, 2009.

WATSON, James D, et al. **DNA Recombinante**: genes e genomas. Artmed Editora. 3a Ed. 2009.

PRADO, Geraldo. "**Ainda sobre a quebra da cadeia de custódia das provas**", in Boletim do IBCCrim, n. 262, setembro de 2014, p. 16-17.

ROSA E AURY LOPES. Artigo. **A importância da cadeia de custódia para preservar a prova penal**. Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>. Acesso em 5 out. 2017

FERRARI JÚNIOR, Ettore. Artigo: A cadeia de custódia e a prova pericial, disponível em http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11434, acesso em 11 out. 2017.

RABESCHINI, André Gomes. Criminalística Forense, artigo, disponível em: <http://www.conteudojuridico.com.br/artigo,criminalistica-forense,51390.html >, acesso em 12 out. 2017.

CICCHI, Rafael. A teoria dos frutos da árvore envenenada - fruits of the poisonous tree, artigo, disponível em< https: //djfeco.jusbrasil.com.br/artigos/445150669/a-teoria-dos-frutos-da-arvore-envenenada-fruits-of-the-poisonous-tree>, acesso em 13 out. 2017.

LOCARD Edmond, disponível em: <https://pt.wikipedia.org/wiki/Edmond_Locard >, acesso em 12 out. 2017.

VELOSO, Thássius. *WhatsApp* em números: 120 milhões de brasileiros e 100% de criptografia. **Techtudo**, São Paulo, mai. 2017. Seção Redes Sociais. Disponível em: <https://www.techtudo.com.br/noticias/2017/05/whatsapp-em-numeros-120-milhoes-de-brasileiros-e-100-de-criptografia.ghtml.>. Acesso em 12 nov. 17.

METADADOS. **Metadados**, Braga, Portugal. Disponível em: <http://www.metadados.pt/oquesaometadados>. Acesso em: 12 nov. 17.

COSTA, Camila. Quatro coisas que mudam com a criptografia no *WhatsApp* – e por que ela gera polêmica. **BBC Brasil**. Londres, abr. 2016. Seção Notícias. Disponível em: <http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc>. Acesso em: 18 set. 2017.

WIZIACK, Julio. Fundador do *WhatsApp* diz no STF que fornecer dados à polícia é impossível. **Folha de S. Paulo**, Brasília, jun. 2017. Seção Mercado. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/06/1889702-fundador-do-whatsapp-diz-no-stf-que-nao-e-possivel-interceptar-conversas.shtml>. Acesso em: 12 nov. 17.

PAYÃO, Felipe. *WhatsApp* diz que é inviolável; Polícia Federal retruca o aplicativo no STF. **Tecmundo**, jun. 2017. Seção Software. Disponível em: <https://www.tecmundo.com.br/whatsapp/117364-whatsapp-diz-inviolavel-policia-federal-retruca-aplicativo-stf.htm>. Acesso em: 10 nov. 2017.

ROHR, Altieres. Como o governo teria grampeado terroristas no *WhatsApp*? **G1.globo**, São Paulo, jul. 2016. Seção Segurança Digital. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-o-governo-teria-grampeado-terroristas-no-whatsapp.html>. Acesso em: 09 nov. 17.

BRASIL. Superior Tribunal de Justiça. Processual Penal. Recurso em Habeas-corpus. Constrangimento ilegal. RHC nº51.531/RO, da 6ª Turma do STJ, Brasília, DF, 19 de abril de 2016. Disponível em:< https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652>. Acesso em: 10 nov. 2017.

BRASIL. Superior Tribunal Federal. Processual Penal. Informativo nº 530. Habeas-corpus nº: HC 96982/DF, In: SUPERIOR TRIBUNAL FEDERAL. Informativos. Brasília, DF, nov. 2008. Disponível em: <http://www.stf.jus.br/arquivo/informativo/documento/informativo530.htm.>. Acesso em: 16 nov. 2017.