UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE DIREITO

CÁSSIO ROBERTO URUGA OLIVEIRA

A (IN)CONSTITUCIONALIDADE DA PROVA PENAL OBTIDA COM VIOLAÇÃO DA PRIVACIDADE NOS MEIOS DIGITAIS: UMA ANÁLISE SOBRE OS DADOS DE COMUNICAÇÃO EM APLICATIVOS DE MENSAGENS INSTANTÂNEAS

SÃO CRISTÓVÃO
2021

CÁSSIO ROBERTO URUGA OLIVEIRA

A (IN)CONSTITUCIONALIDADE DA PROVA PENAL OBTIDA COM VIOLAÇÃO DA PRIVACIDADE NOS MEIOS DIGITAIS: UMA ANÁLISE SOBRE OS DADOS DE COMUNICAÇÃO EM APLICATIVOS DE MENSAGENS INSTANTÂNEAS

Trabalho de Conclusão de Curso apresentado à banca examinadora do Departamento de Direito da Universidade Federal de Sergipe, como requisito parcial para obtenção do grau de bacharel em Direito, sob a orientação do Professor Doutor Carlos Alberto Menezes.

SÃO CRISTÓVÃO
2021

CÁSSIO ROBERTO URUGA OLIVEIRA

A (IN)CONSTITUCIONALIDADE DA PROVA PENAL OBTIDA COM VIOLAÇÃO DA PRIVACIDADE NOS MEIOS DIGITAIS: UMA ANÁLISE SOBRE OS DADOS DE COMUNICAÇÃO EM APLICATIVOS DE MENSAGENS INSTANTÂNEAS

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito da Universidade Federal de Sergipe (UFS) como componente curricular necessário à obtenção do título de bacharel em Direito.

Monografia aprovada em: ____/____/2021

BANCA EXAMINADORA

_____

Prof. Dr. Carlos Alberto Menezes

Orientador/Universidade Federal de Sergipe

_____

Profa. Ma. Ana Carolina Santana

_____

Prof. Me. Matheus Dantas Meira

SÃO CRISTÓVÃO
2021

AGRADECIMENTOS

Gostaria de agradecer a todos que me ajudaram na construção desse trabalho, especialmente ao professor Dr. Carlos Alberto Menezes pela orientação e pelos ensinamentos cuidadosamente repassados ao longo de todo o curso, ao professor Me. Matheus Dantas Meira e à professora Ma. Ana Carolina Santana pela avaliação e contribuições sempre pertinentes.

RESUMO

A globalização e o desenvolvimento de uma sociedade conectada, a sociedade em rede, gerou a necessidade atualização dos mecanismos de persecução penal, sobretudo na utilização de meios ocultos de investigação. Com a mudança das comunicações telefônicas para as comunicações virtuais, realizadas pela internet, houve a necessidade de se dotar os agentes da persecução penal de formas modernas de investigação, como a quebra do sigilo de dados de comunicação virtual e a interceptação dessas comunicações. Porém, o disposto no art. 5º, XII da Constituição Federal protege o sigilo de dados da ingerência do Estado, relegando a lei infraconstitucional as hipóteses e formas em que esse sigilo pode ser relativizado. Com a edição da Lei n.º 9.296/1996, regulou-se a parte final do dispositivo, prevendo a possibilidade das interceptações telefônicas e de comunicações utilizando sistemas de informática e telemática. Dessa forma, tem-se como plenamente possível e aceitável em nosso ordenamento jurídico a utilização da interceptação dos sinais de comunicação virtual, notadamente as ocorridas por aplicativos de mensagens instantâneas. Porém, os dados de comunicação virtual armazenados em dispositivos eletrônicos não possuem previsão expressa de quebra do seu sigilo, sendo a sua utilização no processo penal, apesar de aceita por nossos Tribunais, inconstitucional, até que sobrevenha lei regulamentando essa prática. A referida lei deve levar em consideração a necessidade de ponderação entre os bens jurídicos tutelados, evitando o sacrifício total da proteção ao sigilo das comunicações, dispondo sobre limites materiais, subjetivos e temporais para a utilização da quebra do sigilo de dados de comunicação virtual armazenados em dispositivos eletrônicos, na persecução penal.

Palavras-chave: sigilo das comunicações; comunicações virtuais; proteção a dados; inconstitucionalidade.

ABSTRACT

Globalization and the development of a connected society, the network society, generated the need to update the mechanisms of criminal prosecution, especially in the use of hidden means of investigation. With the shift from telephone communications to virtual communications carried out over the internet, there was a need to equip criminal prosecution agents with modern forms of investigation, such as breaking the confidentiality of virtual communication data and intercepting these communications. However, the provisions of art. 5, XII of the Federal Constitution protects the confidentiality of data from State interference, relegating to the infra-constitutional law the hypotheses and ways in which this confidentiality can be relativized. With the enactment of Law Nº. 9,296/1996, the final part of the device was regulated, providing for the possibility of telephone and communications interceptions using computer and telematics systems. Thus, it is considered fully possible and acceptable in our legal system to use the interception of virtual communication signals, notably those occurring by instant messaging applications. However, virtual communication data stored in electronic devices do not have an express provision for breach of confidentiality, and its use in criminal proceedings, despite being accepted by our Courts, is unconstitutional, until a law regulating this practice comes into being. The aforementioned law must take into account the need for consideration between the protected legal assets, avoiding the total sacrifice of protection to the confidentiality of communications, providing for material, subjective and temporal limits for the use of the breach of confidentiality of virtual communication data stored in electronic devices, in criminal prosecution.

Keywords: confidentiality of communications; virtual communications; data protection; unconstitutionality.

SUMÁRIO

INTRODUÇÃO

A dinâmica social impõe ao direito a necessidade de adequar suas disposições à realidade social sob pena de tornar a proteção intentada ineficiente ou ineficaz.

Nas últimas décadas, a sociedade tem passado por uma quarta revolução industrial, nas palavras de Schwab (2016), estabelecendo-se uma verdadeira sociedade em rede, como define Castells (1999), que é caracterizada pela integração entre os sistemas físicos, digitais e biológicos, provocando uma verdadeira simbiose destes sistemas.

Assim, neste ambiente virtualizado e digital, há uma mudança de comportamento humano que, consequentemente, determina uma mudança na forma como o direito é interpretado e aplicado. É o que ocorre com a proteção da privacidade.

O conceito de privacidade e a forma como sua proteção se cristalizou no ordenamento jurídico decorre de uma sociedade analógica, onde a velocidade e a complexidade dos sistemas de comunicação eram muito inferiores e, portanto, as disposições a ela aplicadas devem ser revistas para que a proteção constitucional da privacidade não seja reduzida a mero camafeu de um direito fundamental.

Essa questão pode ser observada ao analisar os institutos da quebra de sigilo de dados de comunicação e da interceptação das comunicações, ambos para fins de investigação criminal e persecução processual penal.

Nessa sociedade da informação, a maior parte das comunicações se dá por meio da internet, notadamente nos populares aplicativos de mensagens instantâneas, que possuem dados de complexidade infinitamente superior aos dados telefônicos.

Aliando esse aumento na complexidade dos dados com o aumento exponencial da capacidade de armazenamento dos dispositivos informáticos (notadamente os dispositivos móveis de comunicação), temos que o acesso aos dados armazenados das comunicações realizadas por esse meio constitui uma

violação direta e massiva ao direito constitucional de proteção à privacidade que não encontra respaldo nem no permissivo constitucional, nem nas normas infraconstitucionais que regulamentam o tema.

Dessa forma, o presente trabalho busca identificar os pressupostos teóricos e metodológicos que edificaram a proteção constitucional à privacidade, bem como as suas mutações devido à dinâmica social, identificando a forma como a jurisprudência pátria enfrenta o tema e aferindo a constitucionalidade da prova obtida por meio do acesso aos dados de comunicação virtuais.

Com esse desiderato, buscou-se no primeiro capítulo analisar as normas que veiculam os direitos fundamentais à privacidade, intimidade e o sigilo das comunicações, a partir da técnica de análise do suporte fático da norma proposta por Silva (2010), bem como identificar as matrizes teóricas da sociedade da informação e como as mudanças na sociedade influem no âmbito de proteção da norma constitucional.

No segundo capítulo, analisou-se os limites processuais penais à relativização da proteção da privacidade, destacando-se as distinções existentes entre os elementos das comunicações virtuais e como os dados de comunicação virtual armazenados em dispositivos eletrônicos não se encaixam nas definições dos permissivos legais de sua relativização.

Por fim, no capítulo 3, correlacionou-se a análise realizada nos capítulos anteriores, verificando a possibilidade de violação do sigilo de dados de comunicação virtual para fins processuais penais e apresentando os requisitos mínimos ou essenciais para o acesso a esses dados.

1 A PROTEÇÃO CONSTITUCIONAL À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

O constitucionalismo moderno surge, de acordo com as lições de Canotilho (2003), sobretudo na segunda metade do século XVIII, como uma forma de questionar os planos político, filosófico e jurídico dos esquemas tradicionais de domínio e possui como características marcantes a organização do Estado e a limitação do poder estatal por meio de uma declaração de direitos e garantias fundamentais.

Sarlet (2018) afirma que os direitos fundamentais, ao lado da definição e forma de Estado, do sistema de governo e da organização do poder, integram a essência do Estado constitucional, fazendo parte não só da Constituição formal, mas sendo elemento nuclear da Constituição material.

Estes direitos fundamentais, previstos nas constituições modernas, são frutos de uma histórica luta pela delimitação do poder estatal e por um conjunto mínimo de direitos que garantisse, ao menos em tese, a dignidade da pessoa humana (CUNHA JR., 2018).

Nesse ínterim, a Constituição da República Federativa do Brasil de 1988, em seu art. 1º, inciso III, elevou a dignidade da pessoa humana à categoria de fundamento da República e estabeleceu um Título destinado aos Direitos e Garantias Fundamentais, mesmo havendo outros espalhados topograficamente no texto constitucional.

Essa opção, no entender de Cunha Jr. (2018), permite inferir que o constituinte originário se preocupou prevalentemente com o ser humano, consagrando-o como o “fim” do Estado, que só existe para ser instrumento da realização da dignidade daquele.

Reforça-se esse entendimento ao analisar o disposto no § 1º do artigo 5º da Constituição Federal que expressa a opção do legislador constituinte em dotar os direitos e garantias fundamentais de aplicabilidade imediata.

Já em relação à eficácia, os direitos fundamentais, como normas constitucionais, podem ser classificados como normas de eficácia plena, normas de eficácia contida ou normas de eficácia limitada, de acordo com a classificação clássica de José Afonso da Silva.

De acordo com Silva (2003), as normas constitucionais de eficácia plena são aquelas que desde a entrada em vigor da constituição produzem todos os seus efeitos essenciais, incidindo direta e imediatamente sobre o seu objeto de regulação. Já as normas de eficácia contida, apesar de produzir todos os efeitos almejados, preveem mecanismos ou conceitos que permitem manter sua eficácia contida em certos limites. Por fim, as normas de eficácia limitada não produzem imediatamente os seus efeitos essenciais, porque o constituinte deixou a cargo do legislador infraconstitucional a tarefa de completar a normatividade necessária para a produção dos efeitos pretendidos.

Ao cotejar sua classificação tríplice com o disposto no § 1º do artigo 5º da Constituição Federal, José Afonso da Silva (2014, p. 182) esclarece que:

> A eficácia e aplicabilidade das normas que contêm os direitos fundamentais dependem muito de seu enunciado, pois se trata de assunto que está em função do Direito positivo. A Constituição é expressa sobre o assunto, quando estatui que as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata. Mas certo é que isso não resolve todas as questões, porque a Constituição mesma faz depender de legislação ulterior a aplicabilidade de algumas normas definidoras de direitos sociais, enquadrados dentre os fundamentais. Por regra, as normas que consubstanciam os direitos fundamentais democráticos e individuais são de eficácia contida e aplicabilidade imediata, enquanto as que definem os direitos econômicos e sociais tendem a sê-lo também na Constituição vigente, mas algumas, especialmente as que mencionam uma lei integradora, são de eficácia limitada, de princípios programáticos e de aplicabilidade indireta, mas são tão jurídicas como as outras e exercem relevante função, porque, quanto mais se aperfeiçoam e adquirem eficácia mais ampla, mais se tornam garantias da democracia e do efetivo exercício dos demais direitos fundamentais.

Dessa forma, para analisar a eficácia, aplicabilidade e efetividade dos direitos fundamentais torna-se necessário compreender o âmbito de proteção dessas normas, estabelecendo de forma segura o espectro de proteção dos direitos garantidos pela Constituição Federal.

Para a análise do âmbito de proteção das normas de direitos fundamentais, utilizar-se-á a proposta desenvolvida por Virgílio Afonso da Silva (2010) que busca definir o suporte fático da norma de direito fundamental.

Silva (2010) defende que se pode analisar as normas constitucionais de direitos fundamentais por dois aspectos ou modelos: o suporte fático amplo e suporte fático restrito.

Segundo o citado autor, suporte fático amplo são os atos ou fatos que são descritos por determinada norma e para cuja a realização ou ocorrência se prevê determinada consequência jurídica. Segundo o autor, para a caracterização deste suporte fático amplo são necessárias respostas a quatro perguntas: (1) O que é protegido? (2) Contra o quê? (3) Qual a consequência jurídica que poderá ocorrer? (4) O que é necessário ocorrer para que a consequência possa também ocorrer?

Em linhas gerais, o que é protegido costuma ser chamado de âmbito de proteção do direito fundamental e esse objeto é protegido contra uma intervenção, que na maioria das vezes é realizada pelo próprio Estado. Assim, por decorrência lógica, a consequência jurídica, que em regra é a exigência da cessação de uma intervenção, só pode ocorrer se houver uma intervenção no âmbito de proteção da norma (SILVA, 2010).

Nesse contexto, como o suporte fático só é preenchido em caso de intervenção do Estado na esfera de liberdade protegida pela norma constitucional, torna-se estritamente necessário analisar as formas de atuação do estado na restrição dos direitos fundamentais para se compreender, de forma ampla, o conteúdo e a abrangência da norma de direito fundamental.

Em contrapartida, o suporte fático restrito parte do pressuposto que algumas ações, estados ou posições jurídicas não estão subsumidas, em abstrato, no âmbito de proteção das normas constitucionais de direitos fundamentais (SILVA, 2010).

Assim, em que pese haver várias estratégias e conceitos para a definição do suporte fático restrito, Silva (2010) afirma que todas elas possuem dois pontos em comum: (1) a procura pela essência de determinado direito ou manifestação humana; e (2) a rejeição da ideia de colisão entre direitos fundamentais.

A partir desses modelos é possível estabelecer padrões de análise não só da abrangência da proteção da norma constitucional de direitos fundamentais em abstrato, mas, também, quais são as possibilidades de restrições dessas normas de direitos fundamentais.

Para a análise das restrições a direitos fundamentais Silva (2010) esclarece a existências de tuas teorias: a teoria interna, que parte do pressuposto de que a

definição dos limites de cada direito é algo intrínseco à própria norma, podendo-se falar em limites imanentes da norma; e a teoria externa que divide o objeto da norma no direito em si e em suas restrições.

A diferenciação que a teoria externa faz do objeto da norma, apesar de parecer mera retórica jurídica, apresenta consequências importantes, notadamente na aplicação da teoria dos princípios às normas constitucionais de direitos fundamentais.

Sendo a teoria dos princípios uma teoria que utiliza a estrutura do suporte fático amplo, a dinâmica social naturalmente evidencia a colisão entre direitos fundamentais, exigindo-se uma restrição à realização de um direito fundamental em detrimento de outro, no processo de sopesamento ou de ponderação proposto por Alexy (2001).

Essa ponderação entre normas de direito fundamental só é possível se as restrições ao direito estejam separadas do conteúdo da própria norma, como propõe a teoria externa, sob pena de ao se restringir um direito fundamental esteja-se, em verdade, suprimindo o próprio conteúdo da norma e, consequentemente, o próprio direito.

Portanto, a análise dos direitos fundamentais utilizada nesse trabalho pressupõe a utilização da teoria ampla do suporte fático das normas de direitos fundamentais aliada à aplicação da teoria externa das restrições aos mesmos direitos, para se compreender o conteúdo essencial dos direitos fundamentais.

José Afonso da Silva (2014) afirma que os direitos fundamentais possuem as características da historicidade, imprescritibilidade e irrenunciabilidade, o que caracteriza esse conjunto de direitos como núcleo duro da proteção do indivíduo frente ao arbítrio do Estado, e podem ser classificados em cinco grupos: direitos individuais; direitos à nacionalidade; direitos políticos; direitos sociais; direitos coletivos e direitos solidários.

No direito constitucional brasileiro, os direitos fundamentais individuais estão previstos, em sua maioria, no rol do artigo 5º da Constituição Federal, que dispõe sobre os direitos, deveres e garantias individuais. Entre eles encontram-se os direitos à privacidade, intimidade e ao sigilo das comunicações, além de outros que serão abordados ao longo desta análise.

1.1 Proteção da privacidade, da intimidade e do sigilo das comunicações como direito fundamental

A noção moderna de privacidade surge a partir do século XVI, em razão de sua oposição à esfera social. Assim, a noção de privacidade emerge da relação indivíduo-sociedade, na medida em que o estabelecimento de uma esfera privada, livre da ingerência estatal, surge como consectário lógico do desenvolvimento da personalidade humana (DONEDA, 2019).

Ainda segundo Doneda (2019), a privacidade assume um caráter relacional entre a própria personalidade de uma pessoa, às personalidades das demais pessoas e o mundo exterior, que possibilite o desenvolvimento destas personalidades sem a intervenção de mecanismos controle social, sejam eles formais ou informais.

De igual modo, Gomes e Maciel (2018, p.20) são enfáticos ao afirmar que "respeitar a privacidade alheia é reverenciar a dignidade do ser humano". Portanto, nada mais natural que, em um estado constitucional, a proteção da privacidade, com seus desdobramentos, seja elevada à dignidade de direitos fundamentais, estando positivada nas constituições modernas.

No constitucionalismo nacional, a proteção de uma esfera privada não é algo novo. Encontra-se em todas as Constituições brasileiras, desde a Constituição Imperial de 1824, o direito à inviolabilidade do domicílio e da correspondência, facetas notórias do direito à privacidade.

A Constituição da República Federativa do Brasil de 1988 foi além e em seu rol de direitos e garantias fundamentais, a proteção da privacidade encontra-se insculpida no artigo 5º, incisos X a XII:

> Art. 5º [...]
>
> 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;
>
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
>
> 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;

Os incisos X a XII do art. 5º da Constituição Federal buscam proteger a inviolabilidade do domicílio, a privacidade, a intimidade e o sigilo das comunicações dos indivíduos, garantindo que estes componentes do direito da personalidade tivessem proteção constitucional (ARAÚJO, 2009).

Cunha Jr. (2018) esclarece que esse conjunto de direitos fundamentais consubstanciam o direito à privacidade, expressão *lato sensu* que abrange todas as manifestações da esfera íntima, privada e da personalidade das pessoas.

O âmbito de proteção do direito fundamental à privacidade, em sentido amplo, encontra-se adstrito ao desenvolvimento da personalidade humana, como elemento de uma vida digna em sociedade.

Desse modo, utilizando a análise dos suportes fáticos proposto por Silva (2010), podemos identificar no inciso X do art. 5º da Constituição Federal de 1988 um suporte fático amplo que visa proteger a intimidade e a vida privada dos indivíduos, exemplificados nos atributos honra e imagem, contra qualquer ingerência externa à sua própria personalidade, gerando como consequência jurídica de sua violação o direito à indenização pelo dano material ou moral sofrido.

Observa-se, de uma análise literal, que o constituinte não estabeleceu qualquer suporte fático restrito, ou seja, na disposição literal da norma constitucional insculpida no inciso X do art. 5º da Constituição Federal de 1988, nenhuma ação, estado ou posição encontra-se abstratamente fora do âmbito de proteção à privacidade.

Assim, como bem identificado por Sarlet (2011), o respeito à privacidade, intimidade, honra e imagem estão umbilicalmente ligadas à dignidade da pessoa, gerando um reconhecimento e proteção à identidade pessoal, que engloba a autonomia, a integridade psíquica e intelectual.

Já o inciso XI do artigo 5º da Constituição Federal de 1988 possui como suporte fático amplo a proteção contra a violação do domicílio, gerando como consequência jurídica o cometimento de um crime (artigo 150 do Código Penal),

quando o agente ingressa em domicílio alheio fora das hipóteses constitucionalmente permitidas.

Dessa forma, o suporte fático restrito do inciso XI do art. 5º da CF/88 apresenta como hipóteses em que a proteção constitucional não está abrangida: a própria autorização do morador, os casos nos quais a entrada é necessária em decorrência de um desastre ou da ocorrência de um flagrante delito, quando a violação é necessária para se prestar socorro e por determinação judicial, havendo uma limitação nesta última hipótese para o ingresso apenas durante o dia.

Observa-se, assim, que diferente do inciso X, o constituinte estabeleceu diversas hipóteses nas quais a proteção à inviolabilidade do domicílio e, consequentemente, da vida privada, cede ao interesse social, como forma de equilibrar a balança entre o desenvolvimento da personalidade e o interesse na ordem social.

Importante destacar a observação feita por Ferraz Filho (2018, p. 20) em relação ao vocábulo casa:

> Para os gregos antigos, *oikos*, casa, era o espaço onde o indivíduo humano se realizava, onde gerava os meios de subsistência e onde, pois, podia satisfazer suas necessidades. Mesmo que em tese a ideia de casa esteja ligada ao direito de propriedade, a correta interpretação do termo “casa” está ligada ao espaço privado, ocupado pelo individuo sob qualquer título, onde ele faça moradia, dispondo de plena autonomia e liberdade.

Logo, nota-se que a proteção à inviolabilidade do domicílio está diretamente relacionada com a própria proteção à intimidade e à vida privada, sendo a casa o *locus* onde a personalidade do ser humano se desenvolve.

Portanto, uma análise mais abrangente do direito fundamental insculpido no artigo XI da CF/88 nos permite afirmar que o constituinte buscou proteger o local onde o indivíduo desenvolve sua personalidade, ocupando-o de forma permanente ou temporária, mas com liberdade e autonomia.

Por fim, o inciso XII dispõe sobre o sigilo das correspondências e das comunicações. O dispositivo tem, desde a promulgação da Constituição Federal de 1988, despertado debates acalorados na doutrina e na jurisprudência. Identifica-se,

ao menos, duas grandes correntes doutrinárias sobre a determinação do suporte fático do disposto no inciso XII da CF/88.

A primeira corrente, da qual pode-se citar Grinover (1986), Fernandes (2002) e Ferraz Filho (2018), defende o caráter absoluto ao sigilo da comunicação, salvo a telefônica, tendo em vista uma interpretação literal do dispositivo constitucional. Segundo essa corrente:

> O inciso é absolutamente claro e não permite nenhuma interpretação diversa. Salvo as comunicações telefônicas que podem ser restringidas e/ou interceptadas com autorização judicial, conforme regulado pela Lei n. 9.296/96, a correspondência de cartas, de comunicações telegráficas e de dados, inclusive modernamente por uso de internet, são bens absolutamente invioláveis, e essa inviolabilidade não pode ser suspensa, extinta ou de alguma forma relativizada nem mesmo por ordem judicial ou previsão de lei infraconstitucional. A exemplo do parágrafo anterior, essa regra da inviolabilidade não é absoluta, pois durante o estado de defesa poderá ser suspensa. Veja-se a propósito o art. 136, § 1° [da Constituição Federal de 1988] (FERRAZ FILHO, 2018, p. 20).

No tocante à proteção de dados, Fernandes (2002) defende que em uma análise restrita do dispositivo, dados estariam relacionados apenas aos registros constantes em meios eletrônicos e digitais. Em contrapartida, em uma visão ampla, seriam quaisquer anotações pessoais e reservadas. Em qualquer caso, o autor defende que os dados estariam protegidos, ou pelo inciso XII ou pelo inciso X do artigo 5º da CF/88.

Em que pese esta seja a interpretação que confere maior amplitude ao suporte fático amplo da norma e, consequentemente, maior proteção à privacidade e ao sigilo das comunicações, não é a posição majoritária na doutrina, tampouco na jurisprudência.

A segunda corrente, encampada pela jurisprudência dos Tribunais Superiores, afirma que a ressalva da parte final do inciso XII da CF/88, inclui o sigilo dos dados, afirmando que a posição da vírgula indica que o constituinte englobou os dados e as comunicações telefônicas no suporte fático restrito de reserva legal.

Defendendo essa corrente doutrinária, Greco Filho (2005) e Velloso (1998) afirmam que a própria previsão da possibilidade de quebra do sigilo das comunicações

telefônicas permite, mesmo não se tratando de uma interceptação propriamente dita, o acesso aos registros das comunicações existentes nas concessionárias de serviço público.

Contudo, incontroverso nas duas correntes doutrinárias é o fato da norma constante no inciso XII do art. 5º da CF/88 ser uma norma de eficácia limitada, submetida à reserva legal, sendo imprescindível a edição de norma regulamentadora para viabilizar a quebra do sigilo, seja das comunicações telefônicas, sejam dos dados de comunicação.

Fixada a análise sobre o suporte fático das normas constitucionais de direitos fundamentais atinentes à proteção da intimidade e da privacidade, torna-se necessário compreender as hipóteses constitucionalmente permitidas de relativização desses direitos, de modo a completar o panorama da proteção constitucional, estabelecendo as balizas para a quebra do sigilo de dados de comunicação que respeitem os direitos fundamentais e a dignidade da pessoa humana.

1.2 Limites e restrições à proteção da privacidade: hipóteses constitucionalmente permitidas.

O problema da colisão e da restrição de direitos fundamentais é decorrência natural, como afirmou Silva (2010), da adoção de um modelo que amplia a extensão do âmbito de proteção dos direitos fundamentais.

Antes de analisar as formas de restrições e relativizações de direitos fundamentais, é necessário estabelecer, de plano, a diferenciação entre limites imanentes e restrição.

Diferente da doutrina de Canotilho (2003), que afirma que os limites imanentes são produtos do sopesamento entre direitos colidentes, logo são limites apriorísticos revelados pelo intérprete, Vírgilio Afonso da Silva (2010), utilizando as teorias internas e externas, afirma que quando tratamos de um limite derivado de uma intervenção externa, estamos tratando de restrições e não de limites imanentes.

No mesmo sentido, Barcellos (2002) afirma que os limites imanentes são os limites lógicos, oriundos da própria natureza e estrutura do direito. Logo, os limites

imanentes estão contidos no próprio direito, não sendo fruto de uma intervenção externa.

Assim, quando se fala em limites imanentes da norma de direito fundamental, tratar-se-á de limites inseridos na própria estrutura do dispositivo que sustenta a norma e não decorrente de qualquer processo de interpretação ou sopesamento. Nestes casos de limitação externa, decorrentes de uma interpretação ou da ponderação de normas, estar-se-á diante de uma restrição ao direito fundamental.

Como os limites imanentes da norma de direito fundamental estão inseridos na própria estrutura do dispositivo de direito fundamental, o próprio constituinte operou com o juízo racional de ponderação, estabelecendo em quais hipóteses fáticas restritas o direito fundamental deve ceder em benefício de outro direito ou valor fundamental.

É o que ocorre, por exemplo, quando o inciso XI do art. 5º da CF/88 dispõe que nos casos de flagrante delito, desastre ou para prestar socorro não se aplica o direito fundamental à inviolabilidade do domicílio.

Em contrapartida, as restrições aos direitos fundamentais só ocorrem em um processo externo a eles, por meio de uma intervenção do intérprete do direito com a intenção de harmonizar ou compatibilizar normas aparentemente colidentes.

Silva (2010) indica que a principal forma de controle às restrições aos direitos fundamentais é a regra da proporcionalidade.

Considerada por Ávila (2018) como “postulado normativo aplicativo” e por Silva (2010) como “regra de segundo nível” ou “meta-regra”, a regra da proporcionalidade é destrinchada em três sub-regras: adequação, necessidade e proporcionalidade em sentido estrito.

A regra da adequação informa que a intervenção estatal que viola, restringe ou limita um direito fundamental deve ter um objetivo constitucionalmente legítimo. Por esta regra, a intervenção estatal somente será proporcional se, e quando, o objetivo a ser atingido pela medida tenha igual dignidade do direito fundamental violado (ALEXY, 2001).

Pela regra da necessidade, a legitimidade de um ato estatal que viola, limita ou restringe um direito fundamental só é alcançada caso não se possa promover o mesmo objetivo por meio de outro ato que limite em menor grau o direito fundamental atingido (ALEXY, 2001).

Por fim, a proporcionalidade em sentido estrito se vincula à intensidade e a importância da intervenção no direito fundamental. Nesse sentido, somente será proporcional àquela medida que em um juízo racional produza mais benefícios que restrições (ALEXY, 2001).

Dessa forma, um juízo racional de proporcionalidade pode estabelecer restrições à eficácia de um direito fundamental. Porém, para que essa restrição seja legítima, ou constitucional, é necessário observar o momento em que ela é operada, além dos objetivos e dos produtos dessa restrição.

O primeiro momento em que a proporcionalidade pode ser aplicada para gerar uma restrição a um direito fundamental é no momento da produção normativa infraconstitucional.

Nessas situações, diante da colisão entre direitos fundamentais, o legislador deve operar com a proporcionalidade entre os direitos fundamentais colidentes, gerando um resultado que é expressado pela norma de direito infraconstitucional.

As normas geradas pelo legislador infraconstitucional podem ser objeto de impugnação perante o controle de constitucionalidade. Nesse processo, o poder judiciário deve verificar se a norma produzida é, de fato, proporcional ao direito fundamental violado, avaliando a necessidade, a adequação e a proporcionalidade em sentido estrito da norma produzida (SILVA, 2010).

Silva (2010) sustenta que essa é a forma constitucional de se aplicar a regra da ponderação à maioria dos casos: estabelecer *a priori* e abstratamente as ponderações entre os direitos fundamentais em normas infraconstitucionais. Segundo o citado autor, somente em casos excepcionais e na ausência de qualquer ponderação por parte do legislador é que a ponderação deve ser aplicada no caso concreto.

Porém, na dinâmica jurídica nacional, principalmente em matéria penal, o que se observa é a aplicação desmedida da proporcionalidade em diversos casos concretos, estabelecendo verdadeiras restrições especiais e particulares para direitos fundamentais, muitas vezes em cotejo com valores abstratos como “segurança pública”, “paz social” ou “eficiência do processo penal”.

Nesse sentindo, feliz é a observação realizada por Marcante (2020, p. 143) ao afirmar que “a proporcionalidade foi concebida para combater a prática de atos arbitrários e, paradoxalmente, caso se verifiquem problemas em sua aplicação, acabará funcionando como subterfúgio para a própria prática de tais atos”.

Portanto, pode-se concluir que os limites imanentes são um recurso de autolimitação dos direitos fundamentais impostos pelo próprio constituinte. Porém, eles devem encontrar-se expressos no texto constitucional e sua interpretação deve ser restritiva, não havendo o que se falar em aplicação da proporcionalidade nesses casos, pois não há, internamente, qualquer conflito de valores constitucionais que não tenha sido valorado.

De igual forma, uma vez proporcionalizado pelo legislador infraconstitucional a colisão aparente de direitos fundamentais, deve o interprete e o aplicador do direito se limitar às hipóteses descritas nas normas, utilizando-se do recurso do controle de constitucionalidade sempre que se verificar que a produção normativa não respeitou os três corolários, ou sub-regras, da proporcionalidade.

Por fim, em casos específicos, não regulados nem pelos limites imanentes, nem pelas normas infraconstitucionais, o aplicador do direito pode, de maneira moderada, utilizar-se da proporcionalidade no caso concreto, observando-se, contudo, o conteúdo essencial dos direitos fundamentais.

Esse conteúdo essencial, segundo Silva (2010), é um fenômeno complexo, que envolve a análise daquilo que é protegido pelas normas de direitos fundamentais, a relação entre o âmbito de proteção e suas possíveis restrições e a fundamentação do âmbito de proteção e de suas possíveis restrições.

Assim, torna-se necessário compreender o texto normativo, relacionando-o com a dinâmica social, para se fixar de forma coerente o âmbito de proteção da norma e suas possíveis restrições.

É nessa tarefa de interpretação do texto normativo em consonância com a dinâmica social que o estudo da mutação constitucional se torna fundamental para a compreensão do âmbito de proteção dos direitos fundamentais, notadamente os direitos à intimidade e sigilo das comunicações em uma sociedade informacional e globalizada.

1.3 A mutação constitucional e a necessidade de redimensionamento da esfera privada

As constituições modernas possuem como traço característico sua tendência de permanência, de estabilidade, permitindo fundar o direito de um Estado durante um longo período (BARROSO, 2018).

Em decorrência desse estado de permanência, para evitar que o texto constitucional se torne petrificado, as constituições preveem mecanismos próprios para sua alteração, gerando, com isso, uma possibilidade de adequação de suas normas às realidades sociais (SARLET, 2011).

De acordo com Barroso (2018), existem dois mecanismos de alteração de uma constituição: o formal, que é disciplinado pela própria constituição, manifestando-se pela reforma da constituição; e o informal, representado pela mutação constitucional, que permite a alteração do sentido e do alcance das normas constitucionais sem que sejam alteradas as suas disposições.

Hesse (1992) afirma que a mutação constitucional foi concebida e conceituada pela doutrina e jurisprudência alemãs como uma modificação no conteúdo da norma por meio de uma significação diferença, ainda que esta norma permaneça redigida em seus termos originais.

Nesse sentido, Luís Roberto Barroso (2018, p. 91) define a mutação constitucional como uma:

> [...] alteração do significado de determinada norma da Constituição, sem observância do mecanismo constitucionalmente previsto para as emendas e, além disso, sem que tenha havido qualquer modificação de seu texto. Esse novo sentido ou alcance do mandamento constitucional pode decorrer de uma mudança na realidade fática ou de uma nova percepção do Direito, uma releitura do que deve ser considerado ético ou justo. Para que seja legítima, a mutação precisa ter lastro democrático, isto é, deve corresponder a uma

> demanda social efetiva por parte da coletividade, estando respaldada, portanto, pela soberania popular.

Da análise do conceito de mutação constitucional formulado por Barroso (2018), nota-se que o autor estabeleceu como requisito de legitimidade à correspondência com uma demanda social efetiva. Em outras palavras, somente aquela alteração do sentido que corresponda com a realidade fática vivida pela sociedade é passível de ser incorporada ao texto constitucional, sem que se rompa com os dogmas do Estado democrático de direito.

Essa mutação decorre, nas palavras de Barroso (2018, p. 92), porque “o direito não existe abstratamente, fora da realidade sobre a qual incide”. Logo, atento à dinâmica social e à passagem do tempo, o interprete altera o conteúdo da norma, sem alterar o seu texto, de modo a buscar uma correspondência entre o texto constitucional e a realidade social.

Porém, essa interpretação que altera o sentido do texto constitucional não pode ser operada de maneira ilimitada e acrítica. Nesse contexto, Hesse (1992) afirma que há dois limites a serem observados no processo de mutação constitucional: os sentidos possíveis e os princípios fundamentais.

Ainda de acordo com as lições de Hesse (1992), corroboradas por Barroso (2018), o interprete não pode estabelecer um novo sentido para norma que não esteja entre os sentidos possíveis do texto constitucional. Dessa forma, a mutação constitucional está restrita a seleção de um dos sentidos possíveis do texto formal, não havendo a possibilidade do intérprete inovar, dotando o texto de um sentido completamente novo e dissociado do texto formal.

De igual sorte, Hesse (1992) e Barroso (2018) estabelecem que a unidade constitucional, representada pelo conjunto de princípios fundamentais que regem as relações sociais por ela regulada, impede que o intérprete confira um sentido a um dispositivo constitucional que divirja do conjunto das disposições constitucionais.

Uma vez rompidos esses limites, as mutações constitucionais implementadas pelos intérpretes são, marcadamente, inconstitucionais, devendo ser rejeitadas pelos Poderes competentes e pela própria sociedade.

Ferraz (1986) esclarece que apesar da mutação constitucional ser normalmente empregada pelo poder público (legislativo, executivo e judiciário), a

mutação constitucional pode ocorrer decorrente do próprio costume constitucional ou de processos anômalos de mudança da Constituição.

Silva (2007) destaca que a mutação constitucional válida pode ocorrer por meio de três processos: i) atos de complementação constitucional (servem para complementar o sentido das normas constitucionais, notadamente daquelas que dependem de complementação infraconstitucional – normas de eficácia limitada); ii) interpretação e construção constitucionais; ou iii) práticas políticas e sociais revertidas em convenções constitucionais (criação de precedentes políticos ou sociais capazes de determinar o significado do texto constitucional).

Por fim, em relação ao substrato fático que permite a aplicação da mutação constitucional, Barroso (2018) afirma que o instituto pode ser aplicado em razão de uma nova percepção do direito, quando os valores de uma sociedade se alteram, ou pode ser aplicado quando, em razão das alterações da realidade sobre o sentido, o alcance ou a validade de uma norma.

Para os fins deste trabalho, importa analisar a mutação constitucional decorrente das alterações da realidade sobre o sentido, o alcance ou a validade de uma norma, pois a proteção à intimidade, à privacidade e ao sigilo das comunicações continuam a ser valores perseguidos pela sociedade brasileira.

Nesse ínterim, observa-se que a globalização e a evolução da tecnologia são mecanismos de alteração social que impactam sobremaneira o sentido e o alcance de determinadas normas constitucionais, de modo que o entendimento desses processos de modificação da realidade social são importantes para a compreensão do âmbito de proteção das normas, seja por meio de um processo de estabelecimento do suporte fático das normas, seja por uma análise da mutação constitucional decorrente da modificação da realidade social.

Dessa forma, passa-se a analisar os fundamentos e as características do da denominada “sociedade da informação” e quais os impactos à proteção da privacidade, da intimidade e o sigilo das comunicações.

1.4 A sociedade da informação e os novos desafios à proteção da privacidade

As características, formas e consequências das relações sociais são objetos de diversas ciências que buscam, na análise desses elementos, informações preciosas para o desenvolvimento de seus campos de estudo. Nessa tarefa, destacam-se os estudos da modernidade realizados por diversos sociólogos e antropólogos que buscaram descrever a estrutura da sociedade contemporânea, definida como sociedade da informação por Castells (1999), e seus reflexos nas relações entre os indivíduos e o meio que os cercam.

Segundo Lyotard (2011), a característica principal da sociedade contemporânea é a ruptura das grandes narrativas históricas, sendo a questão social radicada em um jogo de linguagens e interrogações que posicionam o emissor, o receptor e o referente em um contexto de imediatidade, tornando a estrutura social mais móvel e mais complexa. Nesse sentido, afirma o citado autor que as disputas pela hegemonia dos relatos sociais devem se dar em torno do conhecimento, elevando, assim, a informação ao objeto das disputas política e econômica da era por ele denominada como “pós-modernidade”.

Tratando o fenômeno descrito por Lyotard (2011) como consequência da modernidade (e não como uma nova fase do arranjo social), Giddens (1991) afirma que o momento em que vivemos é de uma modernidade reflexiva, pautada em um mecanismo de desencaixe das relações sociais. Esse desencaixe é, na verdade, um deslocamento da interação de um contexto local para uma extensão indefinida no tempo e no espaço. Esse deslocamento das relações sociais é observado quando tratamos de relações travadas no ambiente digital que, devido à sua instantaneidade e à sua descentralização, se subsumem perfeitamente à relação social descrita por Giddens (1991) e Lyotard (2011).

Ainda com base em Giddens (1991), pode-se afirmar que esse desencaixe social se dá através de dois mecanismos: as fichas simbólicas e os sistemas peritos. As fichas simbólicas são meios de trocas que podem ser circulados entre os indivíduos independentemente de suas características específicas. Já os sistemas peritos são sistemas baseados na excelência técnica ou competência profissional que organizam e validam grandes áreas dos ambientes material e social em que a sociedade se organiza.

Na concepção de Giddens (1991), as fichas simbólicas, como o dinheiro no exemplo do autor, estão intrinsecamente fundidas na estrutura social de modo que

não há um questionamento sobre a sua legitimação, ou mesmo sobre o seu uso de modo racional. O mesmo pode ser observado quanto a legitimação dos sistemas peritos.

Na sociedade da informação, podemos identificar nos dados pessoais um exemplo de fichas simbólicas e os sistemas informatizados como sistemas peritos, caracterizando, assim, a sociedade da informação como uma sociedade que se encontra na modernidade reflexiva proposta por Giddens (1991).

Os sistemas de desencaixe proposto por Giddens (1991) funcionam como meios para se garantir o afastamento da relação espaço-tempo necessário para se promover a ruptura das grandes narrativas que sustentam a organização social, fundando um novo sistema de legitimidade e uma nova estrutura organizacional.

Esse processo de fundação de uma nova estrutura organizacional é descrito pelos economistas como sendo a quarta revolução industrial. De acordo com Schwab (2016), essa quarta revolução industrial é caracterizada pela velocidade, amplitude e profundidade das transformações, além do impacto sistêmico das mudanças tanto na estrutura da sociedade, quanto nos modos e nas formas de relacionamento dos indivíduos com as novas tecnologias.

Schwab (2016) afirma que a quarta revolução industrial vai muito além da conexão entre sistemas e máquinas inteligentes, ela funde essas tecnologias em uma interação entre os domínios físicos, digitais e biológicos, provocando uma verdadeira simbiose desses sistemas que, historicamente, eram tratados de maneira distinta.

Na sociedade da informação, caracterizada como sociedade pós-moderna no conceito de Lyotard (2011), ou como reflexiva no conceito de Giddens (1991), a produção social de riqueza está vinculada, essencialmente, a produção social de riscos (BECK, 2011).

Beck (2011) destaca que a modernização, enquanto salto tecnológico de racionalização e de transformação do trabalho e da organização, não pode ocorrer sem a produção de riscos. Nas palavras do autor:

> Às questões do desenvolvimento e do emprego de tecnologias (no âmbito da natureza, da sociedade e da personalidade) sobrepõe-se questões do “manejo” político e científico – administração, descoberta, integração, prevenção, acobertamento – dos riscos de tecnologias efetiva ou potencialmente empregáveis, tendo em vista horizontes de relevância a serem especificamente definidos (BECK, 2011, p. 24).

Assim, tem-se que na sociedade contemporânea a gestão dos riscos se torna parte integrante e fundamental para a compreensão dos mecanismos sociais empregados na análise e no desenvolvimento tanto das novas tecnologias quanto na formação e manutenção da própria estrutura social, além do âmbito de proteção dos direitos fundamentais frente à realidade social.

A definição da sociedade da informação foi detalhada por Castells (1999) como um fenômeno-paradigma de transformação social e econômica pautado pelo desenvolvimento de sistemas tecnológicos aptos a agir com e sobre informações. Esses sistemas informacionais buscam a integração das relações sociais em uma lógica de redes e processos humanos que geram uma flexibilidade das formas e das instituições sociais.

Nessa sociedade da informação os ativos políticos e econômicos sofrem sensível transformação, sendo os dados e a informação alçados a ativos em disputa nos referidos campos.

Doneda (2019) faz um alerta sobre a utilização dos termos “dado” e “informação”. Segundo o autor, os conceitos veiculados nesses vernáculos se sobrepõem em diversos aspectos de forma que há certa promiscuidade em sua utilização. Porém, é certo que o “dado” se apresenta em uma conotação mais primária, fragmentada, uma espécie de “informação em potencial”, uma “pré-informação” anterior aos processos de interpretação e elaboração necessários para a caracterização da informação propriamente dita.

Ainda segundo Doneda (2019), uma classificação possível dos dados, proposta originalmente por Pierre Catala, divide os dados em: informações relativas às pessoas e seus patrimônios; as opiniões subjetivas; as obras do espírito e as informações sobre fenômenos, coisas ou eventos. O primeiro grupo de dados (informações relativas às pessoas e seus patrimônios) ficou conhecida como “dados pessoais”.

A disputa pelos dados pessoais e pela informação pessoal ganha destaque quando a evolução tecnológica permite a sistematização e tratamento de grandes quantidades de dados, gerando informações mais precisas sobre pessoas e mercados, sendo a base de novos negócios e da transformação de tantos outros. Esse protagonismo é normalmente vinculado a uma frase, do matemático e cientista

de dados britânico Clive Humby, já famosa no meio econômico: "*Data is the new oil*" (Dados são o novo petróleo, em tradução livre).

Dessa forma, conjugando a ascensão da informação ao núcleo das relações sociais na sociedade da informação (sendo os dados como elemento atômico deste núcleo) com a premência de uma sociedade pautada na interligação dos sistemas tecnológicos, físico e biológico nas linhas propostas por Schwab como quarta evolução industrial, pode-se conceber os dados e a informação como bens relevantes do ponto de vista jurídico e, portanto, dignos de proteção.

Essa proteção jurídica dos dados pessoais é devida em decorrência de um regime especial, diferenciado, haja vista o vínculo indissolúvel entre a informação pessoal e o indivíduo referente, que é uma representação direta de sua personalidade (DONEDA, 2019). Assim, em última análise, a proteção de dados pessoais pode ser inserida tanto na proteção dos direitos da personalidade, quanto na proteção do patrimônio do indivíduo.

Portanto, sendo os dados pessoais um bem jurídico relevante da sociedade da informação na qual estamos insertos, torna-se pertinente e necessário observar os mecanismos de proteção, as disposições constitucionais e a sua vinculação como direito da personalidade do indivíduo, observando-se, ainda, as características próprias do ambiente no qual ele é mais difundido e utilizado: a internet.

Nesse sentido, Araújo (2009) afirma que os dados, como atributos da privacidade e da intimidade poderiam ser respeitados como decorrência do direito à vida, mas o legislador constituinte preferiu dar destaque às especificidades em decorrência da ameaça tecnológica que já se fazia presente quando da elaboração do texto constitucional.

Para além da precisa observação feita por Araújo (2009), temos que a "ameaça tecnológica" por ele citada evoluiu, redimensionando as questões atinentes à tecnologia e à sua influência na própria vida dos indivíduos, demandando uma releitura dos incisos X e XII do artigo 5º da Constituição Federal, a luz da das novas formas de relações sociais que o ambiente moderno nos proporciona.

Essa releitura, em decorrência da própria velocidade da evolução tecnológica, deve ser realizada, primordialmente, por meio do mecanismo da mutação constitucional, respeitando-se, contudo, os seus limites, sob pena de se desvirtuar o

instituto, gerando inconstitucionalidades que desestabilizam o sistema constitucional e violam direitos e garantias fundamentais do indivíduo.

Essa violação aos direitos e garantias fundamentais, decorrente da não observação dos limites da mutação constitucional pautada em uma análise da sociedade da informação, é mais sentida no âmbito processual penal, notadamente quando são impostas restrições à direitos que, em sua essência, não constam nos limites imanentes das normas constitucionais, tampouco decorrem de um sentido possível quando cotejados com as características da sociedade atual.

2 OS LIMITES PROCESSUAIS PENAIS À RELATIVIZAÇÃO DA PROTEÇÃO À PRIVACIDADE E AO SIGILO DAS COMUNICAÇÕES DE DADOS

Como descrito por Castells (1999), vivemos hoje em uma sociedade em rede, onde a conectividade e o acesso a uma grande quantidade de dados e informações são características intrínsecas desse novo modelo de relação social.

As relações sociais na sociedade da informação se dão em um ambiente diferenciado: a internet. De acordo com Sydow (2021), a internet é um novo meio ambiente em que grande parte das atividades desenvolvidas pela humanidade passam a ocorrer.

Ainda segundo Sydow (2021), o ambiente informático passou a receber mais investimentos e mais confiança se tornando o parâmetro de comunicação, em decorrência do conforto e da velocidade que emprega às relações sociais.

Assim, torna-se necessário vasculhar o espaço digital para identificar em que medida o ciberespaço tem influenciado o processo penal, notadamente em relação ao direito probatório (JEZLER JR., 2019).

Jezler Jr. (2019) destaca que a convergência digital, típica da sociedade em rede, impõe a constatação da existência de equipamentos eletrônicos multifuncionais e da edificação de um regime jurídico próprio em matéria probatória, pois a pós-modernidade tecnológica não pode ser suprida pela aplicação analógica da lei das interceptações telefônicas (Lei n.º 9.296 de 24 de julho de 1996) e do Código de Processo Penal (Decreto-Lei n.º 3.689 de 3 de outubro de 1941).

Essa evolução tecnológica, aliada a crescente globalização implicam em uma sofisticação da atividade policial e nos meios de obtenção de provas, sendo os métodos ocultos de investigação cada vez mais utilizados (MARCANTE, 2020).

Diante dessas reflexões, Marcante (2020, p. 87) assevera que “a dignidade humana deve nortear os meios de obtenção de prova, os quais devem ser utilizados pelo Estado tendo como critério o menor gravame ao direito fundamental do investigado, o qual deve ser tratado como sujeito de direitos e não mero objeto da investigação”.

Esse respeito aos direitos fundamentais só pode ser perfectibilizado a partir de uma sistemática processual bem definida em relação às proibições de prova e às hipóteses de restrições de direitos fundamentais.

2.1 As restrições de direitos como instrumento da persecução penal e as proibições de provas

A análise realizada no presente trabalho parte da premissa que a verdade buscada no processo penal é a verdade material, ou processual, uma vez que a busca da verdade não pode ser um valor absoluto em nosso ordenamento jurídico.

Essa relativização da verdade processual decorre de um sistema constitucional que estabelece as diretrizes básicas da persecução penal, no qual se incluem uma série de direitos e garantias do sujeito investigado ou acusado.

Conforme bem observou Giacomolli (2014), o modelo constitucional brasileiro é o processo devido, que informa não só o “modo-de-ser” do processo, como também o “modo-de-atuar” dos agentes da persecução penal, sendo este um paradigma democrático e humanitário.

Esse devido processo constitucional é aquele que assegura a proteção aos direitos fundamentais, que estabelecem limites à intervenção estatal e a legitimam em todas as etapas da persecução penal (GIACOMOLLI, 2014).

Assim, no escopo estatuído para o presente trabalho, torna-se importante analisar como as restrições aos direitos fundamentais se compatibilizam com o devido processo penal, notadamente em relação às proibições de prova.

Marcante (2020) afirma que, no processo penal, o direito à prova deve ser limitado. Essa limitação decorre de uma análise em duas dimensões: na dimensão da admissibilidade e na dimensão da validade da prova produzida durante a persecução penal.

Ainda segundo Marcante (2020) as proibições de prova funcionam a partir de uma dupla proteção: a proteção aos direitos fundamentais do cidadão e a proteção do interesse social de que o processo penal funcione de acordo com as regras do Estado de Direito.

Freitas (2011) definiu de forma precisa o que são as proibições de prova, relacionando a sua dupla proteção com as dimensões em que ela atua. Nas palavras do referido autor:

> Quando falamos, portanto, em proibições de prova, estamos nos referindo a um conjunto de regras e princípios, de cunho material e processual, presentes nos diplomas constitucionais e infraconstitucional, que limitam ou vedam a produção probatória pelas partes e por todos que intervenham de qualquer

> modo no procedimento, notadamente os órgãos estatais incumbidos da persecução criminal, como forma de se tutelar as liberdades individuais, a lisura da atuação estatal e a própria integridade constitucional (FREITAS, 2011, p. 42).

A doutrina aponta dois modelos de proibições de prova: o modelo alemão e o modelo norte-americano.

O modelo alemão utiliza a teoria das esferas jurídicas, que delimitam três esferas jurídicas: a intimidade, a vida privada e vida normal (ou social). De acordo com Roxin (2003), no modelo alemão, a prova só não será valorada se a produção afetar a esfera jurídica da vida privada ou da intimidade do indivíduo, devendo este arguir o vício na medida de seu prejuízo.

Segundo Andrade (1992), no modelo alemão há uma diferenciação entre as "proibições de produção de provas" e as "proibições de utilização ou valoração de provas". Enquanto aquelas limitam o modo de obtenção da prova, estas limitam o uso judicial e a valoração na sentença.

Assim, o modelo alemão das proibições de prova é marcado pela não aplicação abstrata do princípio da contaminação, sendo aplicados diversos procedimentos para flexibilizar as proibições de provas (FREITAS, 2011).

O modelo alemão sofre diversas críticas da doutrina daquele país e no direito comparado. Segundo Marcante (2020) a contaminação do julgador pelo acesso a provas que não podem ser valoradas, mas não são desentranhadas do processo e a ausência de princípios aceitáveis para as consequências de cada um dos tipos de proibição são as críticas mais frequentes ao modelo alemão de proibições de prova.

No Brasil, o constituinte optou pela utilização do modelo norte-americano de proibições de prova, estabelecendo, no art. 5º, inciso LVI da Constituição Federal ("são inadmissíveis, no processo, as provas obtidas por meios ilícitos") a "regra de exclusão" (*exclusuinary rules*) do modelo norte-americano.

O entendimento pela exclusão da prova ilícita é reforçado pela regra específica de direito processual penal, insculpida no art. 157 do Código de Processo Penal (Decreto-Lei n.º 3.689 de 3 de outubro de 1941), com redação dada pela Lei n.º 11.690/2008, cuja redação prescreve que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais".

As regras de exclusão, segundo Freitas (2011, p. 43), "consistem em um conjunto de princípios, normas e práticas jurisprudenciais, assentado no modelo de

precedentes existente na *common law*, que compõe o que se refere como sistema americano de proibições de prova".

Dessa forma, a regra de proibição probatória incide quando um agente da persecução penal viola um dispositivo de cunho processual que regula a validade ou a admissibilidade de determinada prova.

Diferente do modelo alemão, o modelo americano não permite qualquer tipo de aproveitamento da prova obtida por meio de uma violação a uma regra de exclusão, de modo que nem mesmo as provas dela derivadas podem ser admitidas no processo (MARCANTE, 2020).

Essa vedação à admissibilidade da prova derivada da ilícita também foi prestigiada pelo legislador infraconstitucional que em 2008, através da Lei n.º 11.690/2008, incluiu o parágrafo primeiro ao artigo 157 do Código de Processo Penal, dispondo que "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".

Porém, hodiernamente, a jurisprudência americana vem aplicando a denominada "doutrina da atenuação", buscando mitigar a contaminação das provas derivadas. Essa doutrina da atenuação possui regras específicas que excepcionam a inadmissibilidade das provas ilícitas por derivação, como é o caso do nexo atenuado (*attenuated conection*), da descoberta inevitável (*inevitable discovery*), da fonte independente (*independente source*), entre outras (MARCANTE, 2020).

Da análise do parágrafo primeiro do artigo 157 do Código de Processo Penal, infere-se que o legislador infraconstitucional adotou a teoria da atenuação somente em relação ao nexo causal atenuado e a fonte independente.

Lopes Jr. (2020) adverte sobre a impropriedade de se falar em fonte independente, pois se há uma fonte independente não há o que se falar em prova derivada. Segundo o referido autor, ao abrir a possibilidade para admissão da prova ilícita por derivação sob o fundamento da existência de uma fonte independente, o legislador introduziu um conceito jurídico indeterminado que se torna perigoso na medida em que insere a admissibilidade de uma prova a um juízo de suposição sobre a sua fonte.

Essas "regras de atenuação" são, na verdade, verdadeiros métodos de flexibilização das proibições de prova e, consequentemente, métodos de flexibilização

da proteção constitucional do cidadão frente às investidas do poder público sobre sua intimidade e vida privada.

Como bem salientou Freitas (2011), apesar de serem aceitas acriticamente pela doutrina e jurisprudência nacional, o modelo constitucional do processo penal brasileiro não permite a flexibilização das proibições de prova, tampouco permite que o julgador fundamente sua decisão em fonte sobre a qual não tenha havido um efetivo contraditório.

Isso porque, a proibição prevista no art. 5º, inciso LVI da Constituição Federal e a regra do desentranhamento prevista no art. 157 do Código de Processo Penal não admitem interpretação restritiva, por tratar de direitos fundamentais do cidadão.

Rememorando a distinção realizada por Silva (2010) em relação aos limites imanentes e as restrições de direitos fundamentais, observa-se que limitação das proibições de prova não se enquadram no conceito de limites imanentes, pois a norma de direito fundamental não estabeleceu qualquer limitação de seu suporte fático amplo, tampouco pode-se falar em restrição, pois o legislador, ao realizar o devido juízo de ponderação, estabeleceu como ilícitas as provas derivadas, salvo as obtidas por fonte independente ou que não apresentem nexo causal com a prova ilícita.

Dessa forma, tem-se que uma análise constitucional dos dispositivos que estabelecem as proibições de prova no direito processual penal brasileiro não permite a aplicação irrestrita da teoria da atenuação para relativizar as proibições de prova e os direitos fundamentais dos cidadãos.

Como as provas ilícitas no processo penal brasileiro são conceituadas como legalmente como sendo as obtidas em violação as normas constitucionais ou legais (art. 1576, *caput*, do Código de Processo Penal), para a análise proposta neste trabalho, resta analisar os dispositivos constitucionais e legais relativos à proteção da intimidade, da vida privada e do sigilo das comunicações, buscando identificar as proibições de prova existentes nestas normas.

Para tanto, atento à mutação constitucional e ao desenvolvimento tecnológico da sociedade em rede, é necessário analisar os conceitos de comunicação e de dados, buscando aferir o suporte fático restrito das normas constitucionais e legais que regulam a disciplina.

2.2 Os elementos da comunicação virtual: uma distinção necessária

A análise proposta neste trabalho parte da compreensão do suporte fático da norma de direito fundamental do sigilo das comunicações, insculpida no inciso XII do artigo 5º da Constituição Federal. Em sua literalidade, o direito fundamental ao sigilo das comunicações envolve um suporte fático amplo e um suporte fático restrito:

> 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;

Da leitura atenta do dispositivo transcrito, nota-se que o constituinte buscou proteger o sigilo das comunicações, notadamente aquelas realizadas por cartas, por telégrafos, por dados e por telefone. Estabelecendo, assim, um suporte fático amplo que envolvia todos os meios de comunicação mais utilizados quando da elaboração do texto constitucional.

Porém, é preciso estabelecer qual o suporte fático restrito desta norma, sendo necessário verificar se o constituinte originário buscou proteger apenas a comunicação dos dados, ou protegeu, também, os dados em si.

Apesar de no senso comum os dados e a comunicação de dados serem tratados como sinônimos, tecnicamente há diferenças consideráveis, tanto na sua conceituação, quanto nas consequências da violação do sigilo de uns e de outros.

Analisando as atas da comissão de redação da Assembleia Nacional Constituinte, observa-se que a questão relativa à proteção dos dados ou da comunicação de dados foi debatida, sendo aprovada a redação que buscava proteger não só a comunicação de dados, mas os próprios dados:

> **O SR. CONSTITUINTE RICARDO FIÚZA**: – Muito obrigado, Sr. Presidente. O autor da proposta é o Constituinte Hilário Braun, o art. é o 4º; o inciso é o XII, e o destaque é 196, que está na página 11. Ele pede que se dê ao inciso XII do art. 4º a seguinte redação: "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial," etc. **Pretende S. Ex.ª fixar a inviolabilidade do sigilo de dados e não, precipuamente, o sigilo das comunicações de dados, tal qual estava redigido. Determina a inviolabilidade das comunicações de dados.** O texto está redigido assim: "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas, salvo, no último caso, por ordem judicial..." Portanto,

> pretende o Constituinte Hilário Braun acrescentar as expressões "de dados e das comunicações telefônicas." Entende S. Ex.ª e eu também que, **desta forma, prevê-se o sigilo dos dados**.
>
> **O SR. PRESIDENTE (Ulysses Guimarães):** – **Estão todos de acordo?** (Pausa.) **Aprovada** (original sem grifos) (BRASIL, 1988, p. 210)

Assim, houve a inserção da palavra “comunicações” antes da palavra “telefônicas” justamente para denotar que o direito fundamental ao sigilo das comunicações protegeria, também, os dados isoladamente considerados, não apenas a comunicação por meio de dados.

Diante da proposta de texto final apresentada pelo constituinte Ricardo Fiúza e aprovada pela comissão de redação, constante até o presente em nossa Constituição Federal, tem-se que não só a comunicação de dados possui o sigilo protegido pela Constituição Federal, mas os próprios dados em si ostentam a mesma proteção.

As normas de direitos fundamentais sobre a proteção do sigilo de dados e de comunicações, bem como as normas infraconstitucionais que as regulam, não dispõem expressamente sobre um conceito específico de comunicação e de dados, sendo necessário uma análise multidisciplinar sobre os referidos conceitos para aferir o âmbito de proteção destas normas.

A lei n.º 9.472 de 16 de julho de 1997, em seu artigo 60, §1º, conceitua telecomunicação como sendo “*a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza*”.

Guardia (2012) afirma que, embora uma interpretação abrangente e dilatada do conceito de telecomunicações permita incluir as comunicações no meio digital, os principais usos comunicativos da internet (comunicação instantânea e navegação) não possuem suporte normativo.

Os conceitos de informação e dados, objetos da comunicação no meio digital, são objeto de estudo de um ramo autônomo do conhecimento denominado Tecnologia da Informação. Apesar de muitas vezes serem utilizados como sinônimos, os dados diferem substancialmente da informação, devendo se estabelecer critérios objetivos para se identificar o que o constituinte denominou de dados.

De acordo com Forouzan (2010), os dados são parte da informação que podem ser apresentados em qualquer formato, desde que seja acordada entre as partes que criam e usam esses dados.

Doneda (2019) afirma que os dados apresentam uma conotação fragmentária, como uma espécie de “pré-informação”, uma informação em potencial, antes de ser transmitida, ou seja, o dado é uma informação anterior ao processo de elaboração e interpretação.

White (2012) vai além e diferencia os dados dos sinais ao tratar dos dados de comunicação digitais. Para o referido autor, os dados são entidades que possuem significado dentro de um computador ou sistema de computadores, eles capturam eletronicamente partes da informação e armazenam em determinado tipo de dispositivo. Para que esses dados sejam transmitidos de um ponto a outro, devem ser convertidos em sinais, que nada mais são que impulsos elétricos ou eletromagnéticos utilizados para codificar e transmitir dados.

Já a comunicação de dados, de acordo com Forouzan (2010), trata-se das trocas de dados entre dois dispositivos por intermédio de algum meio de transmissão. Para que isso ocorra nos meios digitais, deve haver a combinação de hardware (elemento físico) e software (elemento lógico).

Da combinação destes conceitos, pode-se inferir que os dados digitais são parte da informação capturada eletronicamente e armazenada em um dispositivo próprio, que para ser transportada ou comunicada com outro disposto necessita ser transformada em sinais (elétricos ou eletromagnéticos) que necessitam de um meio para serem transportados.

Isso significa que, no processo de comunicação digital, a informação é transformada em dados e, posteriormente, em sinais para serem transportados entre os terminais. Logo, no processo de comunicação, o fluxo observado entre os terminais são fluxos de sinais e não fluxos de dados.

Para que o fluxo de sinais seja transportado de um terminal a outro é necessário a utilização de um meio. O meio mais comum de transmissão de dados desta quadra histórica é a internet, rede mundial de computadores que ligam terminais em todo o mundo (CASTELLS, 1999).

Dessa forma, tem-se que os dados de comunicação digitais, ou virtuais, são partes da informação que se pretende comunicar entre terminais conectados à internet, que são transformados em sinais para serem enviados por meio de uma rede mundial de comunicação, a internet.

No contexto da comunicação pela internet, Guardia (2012) diferencia dados de comunicação e dados de tráfego. Para o autor, dados de comunicação são aqueles dados que o emissor pretende fazer chegar ao receptor, já os dados de tráfego são os elementos acessórios, externos à comunicação eletrônica, que permitem identificar sua origem, destino, momento e duração.

Ainda segundo Guardia (2012), os dados de tráfego possuem três características essenciais: o conteúdo formal, que dispõe que os dados de tráfego são destituídos de conteúdo; a funcionalidade, que permite a comunicação entre os terminais e a acessoriedade, que dispõe que os dados de tráfego são apenas acessórios à comunicação, sem possuir finalidade isolada.

Ainda sobre essa classificação, Guardia (2012) destaca que há três situações em que as particularidades exigem uma maior atenção: quando os dados de tráfego adquirem status de parte material da mensagem; nos casos em que dados de tráfego se refiram indiretamente ao conteúdo das informações; e diante da dificuldade de delimitar aquilo que o emissor realmente quis transmitir.

Nesses casos, em que há uma verdadeira simbiose entre os dados de comunicações e os dados de tráfego, torna-se necessário estender a proteção constitucional aos dados de comunicação para os dados de tráfego, notadamente em razão do acesso ao conteúdo da mensagem e a proteção à privacidade e à intimidade.

A partir dessa classificação, nota-se que os dados referentes à origem, destino, momento, duração, rota, modalidade e volume da comunicação são dados indubitavelmente de tráfego e que, portanto, não estariam abrangidos no escopo da inviolabilidade do sigilo de dados previstos no art. 5º, XII da Constituição Federal.

Em relação à comunicação por meio de aplicativos de mensagens instantâneas (Whatsapp, Telegram, Skype e outros), torna-se necessário observar a natureza dos dados, sendo imperiosa a distinção entre dados de comunicação – que

veiculam o conteúdo da mensagem – e dados de tráfego – que são auxiliares e permitem a identificação da comunicação.

Portanto, ao analisar a possibilidade de quebra de sigilo de dados de comunicação virtual em aplicativos de mensagens instantâneas, é preciso interpretar a norma de regência sob o prisma das distinções de dados, observando-se em quais situações o sigilo pode ser afastado e sobre quais dados essa relativização dos direitos fundamentais pode ser operada dentro dos limites constitucionais.

2.3 A normatização da violação da privacidade para fins processuais penais e sua adequação ao novo modelo de comunicação

Gomes e Maciel (2018) destacam que antes da Constituição Federal de 1988, malgrado ser uma prática recorrente no cotidiano das investigações criminais, a interceptação telefônica não possuía um estatuto próprio, específico e descritivo.

Com a previsão constante no inciso XII do artigo 5º da Constituição Federal de 1988, a preocupação passou a ser a de regulamentar a possibilidade de interceptação das comunicações telefônicas, de modo a dar legitimidade à prática investigativa, pois, segundo BARROS (1996) a única forma legítima de impor qualquer restrição a direitos fundamentais é pela via constitucional ou legal.

Diante dessa imposição resultante da interpretação do texto constitucional, conforme defendem Gomes e Maciel (2018), as interceptações telefônicas estão condicionadas a três requisitos: (i) lei regulamentadora, estabelecendo as hipóteses de cabimento e a forma de realização dessas interceptações; (ii) o uso exclusivo para fins penais das conversas interceptadas; e (iii) ordem judicial.

A necessidade de lei regulamentadora decorre da exigência expressa no texto constitucional. Diante dessa reserva legal qualificada, a interceptação telefônica somente poderá ser considerada lícita se pautada em uma das hipóteses descritas na norma regulamentadora. Logo, toda e qualquer interceptação de comunicação que não esteja regulamentada por lei torna-se ilícita e, portanto, inadmissível no processo penal brasileiro.

Para suprir essa reserva legal qualificada, o legislador infraconstitucional regulou a matéria através da Lei n.º 9.296 de 24 de julho de 1996. Publicada em 25 de julho de 1996.

O objeto da Lei n.º 9.296/1996 está expresso em seu artigo primeiro, que estabelece:

> 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.

Nota-se que o legislador infraconstitucional utilizou a expressão “qualquer natureza” para qualificar a expressão “comunicação telefônicas”. Interpretando esta qualificadora, Gomes e Maciel (2018) destacam que a expressão “qualquer natureza” engloba as interceptações propriamente ditas, escutas telefônicas, gravação telefônica, interceptação ambiental, escuta ambiental e gravação ambiental. Porém, no entender dos referidos autores, apenas as duas primeiras formas citadas de quebra do sigilo das comunicações telefônicas estão autorizadas em nosso ordenamento jurídico.

Posteriormente, a Lei n.º 13.964 de 24 de dezembro de 2019 incluiu o artigo 8º-A à Lei das Interceptações telefônicas, dispondo sobre a regulação da captação ambiental, dispondo em seu parágrafo quinto que se aplicam subsidiariamente à captação ambiental as regras previstas para a interceptação telefônica. Dessa forma, tem-se a captação ambiental como mais uma hipótese de intervenção nas comunicações regulada em nosso ordenamento jurídico.

Além disso, o dispositivo em análise restringe o uso das interceptações à persecução criminal, condicionando a realização da intervenção no direito fundamental à ordem judicial prévia e à manutenção do sigilo extraprocessual, por meio do segredo de justiça.

Essas condições buscam efetivar a proporcionalidade da medida invasiva, resguardando a intimidade e a vida privada do investigado ou acusado de uma exposição desnecessária e impondo um controle judicial ao uso da medida, de forma a evitar abusos.

Observa-se, também, que o legislador infraconstitucional ampliou o objeto da Lei n.º 9.296/1996 ao dispor no parágrafo único de seu artigo primeiro que as suas disposições aplicam-se, também, à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Assim, pode-se concluir que a lei das interceptações telefônicas aplica-se à interceptação em sentido estrito e à escuta de comunicações telefônicas, bem como do fluxo de comunicações em sistemas de informática e telemática.

Lima (2019) define e distingue as interceptações telefônicas em sentido estrito da escuta telefônica, destacando que em ambas existe a atuação de um terceiro que capta o conteúdo da comunicação. Nas palavras do autor:

> a) Interceptação telefônica (ou interceptação em sentido estrito): consiste na captação da comunicação telefônica alheia 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);
> b) 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. É o que ocorre, por exemplo, na hipótese em que familiares da pessoa sequestrada, ou a vítima de estelionato, ou ainda aquele que sofre intromissões ilícitas e anônimas, através do telefone, em sua vida privada, autoriza que um terceiro leve adiante a interceptação telefônica (LIMA, 2019, pg. 429).

Observa-se, a partir da análise do objeto da lei das interceptações telefônicas, que a intromissão do terceiro ocorre no momento em que a comunicação está ocorrendo, sendo, portanto, contemporânea à conversa travada pelos interlocutores.

Em relação ao âmbito de incidência da Lei de Interceptações telefônicas para os sistemas de informática e telemática, a partir das distinções realizadas sobre os dados de comunicação virtual, que são comunicações realizadas por meio de sistemas de informática, nota-se que o alargamento do objeto da lei das interceptações telefônicas abarca o fluxo de comunicações virtuais, que se dão por meio de sinais que são transmitidos entre terminais conectados à rede mundial de computadores.

Dessa forma, percebe-se que o legislador não incluiu os dados estáticos, que são aqueles que estão armazenados em dispositivos eletrônicos e que são fragmentos de uma informação num ambiente informático.

O artigo segundo da lei das interceptações telefônicas estabelece o caráter subsidiário e excepcional do meio de obtenção de prova invasivo à intimidade e a vida privada do cidadão:

> 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.

Infere-se da leitura do dispositivo que o legislador estabeleceu três hipóteses de inadmissão das interceptações telefônicas.

No inciso III, estabeleceu-se que as interceptações telefônicas só podem ser admitidas para apurar a suposta prática de crimes punidos com reclusão, ou seja, não se pode utilizar a interceptação telefônica para investigação dos crimes punidos com detenção e prisão simples, acompanhadas ou não de multa (LIMA, 2019).

Já no inciso I, conforme afirmam Gomes e Maciel (2018), estabelece a medida da interceptação telefônica como medida cautelar, seja preparatória (quando realizada na fase policial), seja incidental (quando promovida na fase processual), necessitando, assim, da existência do *fumus comissi delict* e do *periculum libertatis*.

Nesse sentido, afirmam os citados autores que o texto legal estabeleceu um *standard* probatório superior a simples suspeita para legitimar a utilização da interceptação telefônica, devendo haver "indícios razoáveis" de autoria ou participação na infração penal investigada.

Por fim, o inciso II estabelece o caráter excepcional da medida de interceptação telefônica, que deve ser aplicada apenas em *ultima ratio*, quando não disponíveis quaisquer outros meios para a obtenção da prova a ser obtida por meio das interceptações telefônicas (LIMA, 2019).

Sobre a excepcionalidade das interceptações telefônicas, Gomes e Maciel (2018) fazem uma observação importante sobre a vulgarização da medida invasiva aos direitos fundamentais, nas palavras dos autores:

> [...] embora esse requisito da indispensabilidade seja um dos mais importantes dispositivos da lei, é, talvez, o mais violado. De meio subsidiário de prova, na prática a interceptação é invariavelmente utilizada como primeiro mecanismo de investigação. E, como sói acontecer, requerido e autorizado muitas vezes sem as cautelas acima apontadas por nós. Prova disso é que só no ano de 2007 foram 4098 mil interceptações telefônicas ("grampos telefônicos"). Foram 1.200 interceptações por dia (GOMES e MACIEL, 2018, p. 109).

Outro aspecto que merece destaque encontra-se positivado no artigo 5º da Lei n.º 9.296/1996, que dispõe que "*a decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá*

exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova".

O art. 5º da Lei das Interceptações Telefônicas estabelece um conjunto de garantias procedimentais que buscam minimizar a intrusão do Estado na intimidade do investigado.

Inicialmente, respeitando o disposto no art. 93, IX da Constituição Federal, o legislador impôs que a decisão que autorize a interceptação telefônica seja devidamente fundamentada, sob pena de nulidade. Essa imposição, segundo Gomes e Maciel (2018) decorre do fato da interceptação telefônica ser medida *inaudita altera parte* e da necessidade do juiz expor o resultado do exame dos requisitos de admissibilidade, pois o contraditório será diferido.

Além de ratificar a necessidade de fundamentação da decisão que determina a interceptação telefônica, o art. 5º da Lei das interceptações telefônicas, determina que a decisão judicial que autoriza o meio invasivo da intimidade deve, expressamente, indicar a forma de execução da diligência, limitando, assim, o poder dos órgãos de persecução para devassar, por qualquer meio, a intimidade e a vida privada do indivíduo.

Por fim, o dispositivo dispõe sobre o prazo de execução da medida. Segundo o texto legal, a interceptação telefônica não poderá exceder 15 (quinze) dias, renovável por igual tempo, desde que comprovada a indispensabilidade do meio de prova.

A primeira questão que se põe é sobre o número de vezes que a interceptação pode ser licitamente renovada. Segundo Gomes e Maciel (2018), parte da doutrina, à exemplo de Paulo Napoleão Quezado e Clarisier Cavalcante e Altamiro Lima Filho, defendem que a medida pode ser renovada uma única vez; já Damásio de Jesus, Vicente Greco Filho e Antônio Scarance Fernandes afirmam que não há limites, podendo a interceptação telefônica ser renovada quantas vezes forem necessárias.

A jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça firmou-se no sentido de que pode o juiz autorizar sucessivas renovações, sem estabelecer qualquer limite, desde que os requisitos autorizadores permaneçam válidos e que haja pedido e decisão devidamente fundamentados (LIMA, 2019).

Diante do exposto, pode-se concluir que a Lei das Interceptações telefônicas, Lei n.º 9.296/1996, estabeleceu um conjunto de premissas e requisitos para a admissibilidade da interceptação telefônica:

1) Somente em casos de investigação criminal e instrução processual penal pode-se determinar a medida invasiva da privacidade;
2) A interceptação pode ocorrer tanto da comunicação telefônica, quanto do fluxo de comunicações em sistemas de informática e telemática;
3) Para a autorização da medida é necessária a existência do *fumus comissi delicti* e do *periculum libertatis*;
4) A interceptação telefônica é meio excepcional de obtenção de prova, não podendo ser autorizada quando a prova que se busca pode ser produzida por outros meios;
5) A medida só pode ser autorizada em casos nos quais o fato investigado constitui infração penal punida com reclusão;
6) A decisão que autoriza a medida deve ser devidamente fundamentada;
7) Na decisão de autorização da interceptação telefônica devem estar descritas as formas de execução da diligência;
8) O prazo máximo da execução da medida são quinze dias, prorrogáveis por igual período (em decisão fundamentada).

Esse conjunto de premissas e requisitos buscam, como dito, minimizar o impacto da medida da invasão à privacidade e à intimidade do investigado ou acusado, regulando a forma da quebra do sigilo das comunicações.

Porém, de uma análise sistemática à luz da sociedade da informação e dos novos meios de comunicação, nota-se que não há uma regulação específica para a quebra do sigilo de dados de comunicação realizados em meio digital, notadamente pelas suas diferenças em relação à comunicação telefônica.

Diante dessa constatação, parte da doutrina e da jurisprudência passou a olhar para o Marco Civil da Internet (Lei n.º 12.965 de 23 de abril de 2014) buscando soluções para a falta de regulação da quebra do sigilo de dados de comunicação virtual.

O Marco Civil da Internet, norma que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, já em seu artigo 7º, estabelece os direitos dos usuários da internet, assegurando o direito à inviolabilidade da intimidade,

da vida privada e do sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial e na forma da lei.

Observa-se que dispositivo, além de proteger à intimidade, vida privada e sigilo do fluxo de comunicações, determinou que a quebra deste somente poderia se dar por ordem judicial (reserva jurisdicional) e na forma que a lei estabelecer (reserva legal estrita).

Diante dessa proteção, o artigo 10 da referida lei estabelece que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como os dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes diretamente envolvidas, só sendo possível a disponibilização dos referidos registos, mediante ordem judicial, respeitado o disposto no artigo 7º.

Para regular essa disponibilização de dados de conexão de acesso a aplicação de internet e seus correlatos, o parágrafo único do artigo 22 do Marco Civil da Internet dispõe que o juiz deve ordenar que o responsável pela guarda forneça os registros, mediante requerimento que, além dos demais requisitos legais, deve conter: (i) fundados indícios da ocorrência do ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e (iii) período ao qual se referem os registros.

Observa-se, assim, que a quebra do sigilo dos dados de conexão e de acesso a aplicações de internet não podem se dar de maneira abrangente e indiscriminada, sendo necessário o preenchimento dos requisitos do *fumus comissi delicti* e do *periculum libertatis*, bem como a adequação da medida e, principalmente, de uma limitação temporal da quebra do sigilo.

Essa limitação temporal é de extrema importância uma vez que, diferentemente da interceptação telefônica em que a medida é concomitante com a comunicação, na quebra do sigilo de dados de conexão e acesso a aplicações de internet a quebra se dá em relação a registros de comunicações já ocorridas, não sendo proporcional uma quebra irrestrita do sigilo de uso da internet.

Importante destacar que o Marco Civil da Internet, assim como outras leis (como exemplos a Lei da Lavagem de Dinheiro e a Lei do Crime Organizado), excepcionam da reserva de jurisdição os dados cadastrais, que são o conjunto de informações referentes à data e hora do período de conexão com a Internet, sua

duração e registro do IP (*Internet Protocol*) utilizado pelos terminais envolvidos na comunicação (GUARDIA, 2012).

Esses dados, como se nota, não possuem qualquer conteúdo comunicacional, não havendo como se conhecer o conteúdo dos dados transferidos entre os terminais, ou seja, a informação comunicada permanece sob sigilo, pois o agente que tenha acesso a esses dados, tal qual nos dados de comunicação telefônica, apenas conhece da existência da comunicação, não do seu conteúdo.

Dessa forma, cotejando a disciplina da quebra do sigilo de dados armazenados em suportes eletrônicos com a legislação vigente, conclui-se que as principais diferenças entre os modos de obtenção de prova concernem ao modo e ao momento da obtenção da prova, não sendo possível uma aplicação direta dos institutos previstos em nossa legislação (GUARDIA, 2012).

Sendo assim, infere-se que apesar de ser uma prática corriqueira na persecução penal nacional, o acesso do conteúdo das comunicações pretéritas, realizadas por meio digital, malgrado tenham o seu sigilo protegido constitucionalmente, não possuem qualquer regulação infraconstitucional específica.

Essa questão não é desconhecida do legislador nacional, pois tramitam no Congresso Nacional 265 (duzentos e sessenta e cinco) projetos de lei para alteração da sistemática de quebra do sigilo das comunicações. Em alguns desses projetos, o objetivo do legislador é suprir a lacuna existente em relação à quebra do sigilo de dados de comunicação instantânea.

Porém, em que pese a grande quantidade de projetos de lei tramitando no Congresso Nacional em relação à disciplina da proteção da privacidade, intimidade e do sigilo das comunicações telefônicas, o que se observa é que o legislador busca incluir nos dispositivos já existentes a possibilidade de interceptação das comunicações realizadas no meio virtual, mas sem dispor, expressamente sobre a forma como ela deverá ser realizada a quebra do sigilo dos dados armazenados.

Nesse sentido, o Projeto de Lei n.º 6960/2017, de autoria do Deputado Federal Cleber Verde (PRB/MA), prevê a alteração do disposto nos artigos 5º e 7º do Marco Civil da Internet para dispor, expressamente, sobre a inviolabilidade do sigilo das comunicações privadas, armazenadas em terminais fixos ou móveis (celulares, smartphones, tablets ou similares), salvo por ordem judicial.

Já o Projeto de Lei n.º 3372/2021, de autoria do Deputado Federal Coronel Tadeu (PSL/SP), busca a alteração do disposto no parágrafo único do artigo 1º da Lei das Interceptações Telefônicas para constar, expressamente, a possibilidade de interceptação das comunicações em sistemas de envio de mensagens instantâneas e chamadas de voz.

O Projeto de Lei n.º 3372/2021 prevê, ainda, a inserção do art. 1º-A na lei das interceptações telefônicas, dispondo sobre os meios para se promover a interceptação telefônica. O artigo proposto possui a seguinte redação:

> Art. 1º-A. A interceptação do fluxo de comunicações em sistemas de envio de mensagens instantâneas e chamadas de voz poderá ocorrer por meio de:
> I - habilitação, pela operadora de telefonia, em horários determinados, de módulo de identificação de assinante (cartão "SIM") fornecido pela autoridade policial, em substituição àquele utilizado pelo investigado ou acusado;
> II - espelhamento, pela autoridade policial, em dispositivo próprio, das mensagens recebidas e enviadas pelo investigado ou acusado.
> Parágrafo único. A interceptação prevista neste artigo dar-se-á por meio de sistema que assegure a não interferência da autoridade policial nas comunicações travadas pelo investigado ou acusado, seja por meio da exclusão, da edição ou do envio de mensagens.

O cuidado tido para definir as formas de interceptação não foi observado para descrever as formas de quebra do sigilo dos dados de comunicação virtual armazenados, de modo que a disciplina permanece sem regulamentação e sem projetos de lei que disponham sobre o tema.

Diante dessa lacuna legislativa, a jurisprudência nacional vem se posicionando sobre a possibilidade e a forma da interceptação e da quebra do sigilo dos dados de comunicação virtual armazenados nos terminais.

2.4 O entendimento jurisprudencial sobre a violação da privacidade para fins processuais penais

A discussão sobre admissibilidade das provas produzidas com violação do sigilo da comunicação sempre foram objetos de discussão acalorada, tanto na doutrina, quanto na jurisprudência nacional.

Para os fins deste trabalho, importa iniciar a análise dessa questão a partir da promulgação da Constituição Federal de 1988 e seus reflexos no entendimento jurisprudencial sobre esses meios de obtenção de prova.

Como visto, a Constituição Federal de 1988 estabeleceu um regime jurídico de proteção à intimidade, a vida privada e ao sigilo dos dados de comunicação em geral e das comunicações telefônicas.

A partir dessa disciplina constitucional, a primeira grande discussão se deu em torno da recepção do artigo 57 do Código Brasileiro de Telecomunicações (Lei n.º 4.117 de 27 de agosto de 1962). O aludido dispositivo dispõe que não constitui violação de telecomunicação o conhecimento dado ao juiz competente, mediante requisição ou intimação deste.

O Supremo Tribunal Federal, em decisão paradigmática exarada nos autos do *Habeas Corpus* n.º 69.912/RS, julgado em 16 de dezembro de 1993, entendeu ser ilícita a interceptação telefônica em decorrência da ausência de lei que regulamentasse a parte final do art. 5º, XII da Constituição Federal de 1988.

Colhe-se do acórdão do Habeas Corpus n.º 69.912/RS lição esclarecedora do entendimento da Corte Constitucional em relação ao âmbito de proteção da norma e a necessidade de norma infraconstitucional para se estabelecer o suporte fático restrito da norma protetora de direito fundamental. No entender o ministro Celso de Mello:

> O art. 5º, XII, da Lei Fundamental da República, permite, agora, a interceptação das conversações telefônicas. Essa providência excepcional sujeita-se, no entanto, para efeito de sua válida efetivação, a determinados requisitos que, fixados pelo próprio ordenamento constitucional, condicionam a eficácia jurídica desse meio de prova.
> A derrogação desse princípio tutelar do sigilo telefônico somente legitimar-se-á, desde que a interceptação, sem precedida de ordem judicial, venha a realizar-se no campo exclusivo da persecução penal ne nas hipóteses a serem ainda definidas em numerus clausus pelo legislador, a quem incumbe prescrever, de outro lado, o modo e a forma de sua execução.
> O preceito constitucional em causa não se reveste, quanto à interceptação das conversações telefônicas, de densidade normativa suficiente. Ele impõe e reclama, para que possa válida e eficazmente atuar, a instauração de um processo de integração normativa de que derive a lei exigida pela Carta da República.
> Nessa matéria, a só existência de ordem judicial – que não se ajuste às hipóteses ou não observe as formas estipuladas pela lei – não constitui elemento bastante para autorizar a escuta telefônica para fins de persecução penal (BRASIL, 1993, p. 17/18).

Infere-se ao acórdão do *Habeas Corpus* n.º 69.912/RS que o Supremo Tribunal Federal entendeu que a autorização constitucional para a quebra do sigilo das comunicações telefônicas dependia de lei infraconstitucional que regulasse as hipóteses e as formas a serem aceitas em nosso ordenamento, configurando a norma

de direito fundamental como norma de eficácia limitada, conforme as lições de José Afonso da Silva.

Gomes e Maciel (2018), comentando o referido julgado, entendem que quando o direito fundamental reclama expressamente a existência de uma lei restritiva, como é o caso da quebra do sigilo dos dados de comunicações e da interceptação telefônica, sem a edição da referida lei o dispositivo constitucional não possui plena eficácia, logo, sem a lei exigida, a interceptação telefônica constitui-se prova ilícita e, portanto, inadmissível.

O mesmo entendimento deve ser dado à quebra do sigilo dos dados de comunicação digitais, uma vez que mesmo superando-se a discussão sobre a possibilidade da quebra do sigilo desses dados, admitindo como possíveis, não restam dúvidas sobre a sua vinculação à previsão da necessidade de norma regulamentadora e, como visto, não há em nosso ordenamento jurídico norma que se amolde à hipótese fática em questão.

Porém, com o advento da Lei n.º 9.296/1996 superou-se a questão relativa à admissibilidade das interceptações telefônicas, passando-se a discutir questões relativas ao procedimento específico da medida invasiva.

Em relação a essas questões, o entendimento dos Tribunais Superiores não foram tão garantistas quanto o entendimento fixado no *Habeas Corpus* n.º 69.912/RS. A Supremo Tribunal Federal e o Superior Tribunal de Justiça, em diversos julgados, relativizou o princípio da reserva legal, ampliando hipóteses permissivas, e até mesmo não aplicando hipóteses restritivas, o que não se coaduna com a disciplina constitucional da garantia da intimidade, da vida privada e do sigilo dos dados e das comunicações telefônicas.

No julgamento do Agravo Regimental no Agravo em Recurso Especial n.º 431.316/RJ, o Superior Tribunal de Justiça admitiu a utilização da técnica de fundamentação *per relationem* para a prorrogação de interceptação telefônica nos casos em que os pressupostos autorizativos da medida originária fossem mantidos (BRASIL, 2018).

O entendimento fixado pelo STJ e consolidado em diversos outros julgamentos da mesma Corte, viola a necessidade de fundamentação específica das

medidas de obtenção de prova invasivas aos direitos fundamentais, dificultado a efetivação do contraditório (diferido) e da ampla defesa em caos nos quais a interceptação telefônica é reiteradas vezes renovada.

Já no *Habeas Corpus* n.º 148.413/SP, o Superior Tribunal de Justiça inverteu o ônus da prova, determinando que a carga probatória recaísse sobre a defesa, quando esta arguir que houve violação ao art. 2º, II, da Lei n.º 9.296/1996, por não ser a interceptação telefônica utilizada como meio excepcional de obtenção de prova (BRASIL, 2014).

Mais uma vez a Corte Cidadã promoveu uma restrição do direito fundamental ao sigilo das comunicações, uma vez que o legislador infraconstitucional estabeleceu como requisito para admissibilidade da interceptação telefônica a sua subsidiariedade a outros meios de investigação. Logo, a carga probatória da indispensabilidade da medida é do órgão que a requisitou, não podendo recair sobre a defesa, notadamente por se constituir em verdadeira prova diabólica para a parte que não detém o conhecimento integral das provas e diligencias realizadas no curso da investigação.

No Recurso em *Habeas Corpus* n.º 56.744/RS, o STJ entendeu ser legítima a prova obtida por meio de interceptação telefônica para apuração de delito punido com detenção, se conexo com outro crime apenado com reclusão (BRASIL, 2015).

Nesse julgamento, houve a relativização da restrição objetiva inserida na Lei das Interceptações Telefônicas, que veda a sua utilização para a investigação de crimes que não estejam sujeitos à pena de reclusão.

Observa-se que apesar do STJ limitar a utilização do precedente para os crimes conexos, não são raras as situações em que há um alargamento do polo passivo das ações penais, para inserir acusados que supostamente cometeram apenas os crimes apenados com detenção, sendo a prova produzida pela interceptação telefônica utilizada, irrestritamente, para fundamentar a condenação desses corréus.

Outra decisão paradigmática, foi a exarada pelo Supremo Tribunal Federal no Recurso Extraordinário n.º 418.416/SC. Na oportunidade afirmou a Corte Suprema que não há violação ao art. 5º, XII, da Constituição no acesso aos dados de

comunicação em computadores apreendidos, pois "*não houve quebra do sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial*" (BRASIL, 2006).

Neste mesmo julgado, o Supremo Tribunal Federal afirmou que "*a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador*" (BRASIL, 2006).

O entendimento exarado pelo Supremo Tribunal Federal vai de encontro à pretensão do legislador ao alterar a proposta originária de redação do art. 5º, XII, da Constituição Federal, para incluir antes da palavra "telefônica" a palavra "comunicação", diferenciando, assim, a proteção à comunicação telefônica (fluxo de informação) dos dados em si próprios, estabelecendo uma proteção dos dados em si considerados e não apenas do fluxo destes (ver tópico 3.2 deste trabalho).

Já em relação à quebra do sigilo de dados de comunicação virtual armazenados em dispositivos de informática ou de comunicação móvel, as decisões ainda são incipientes e não permitem uma sistematização do entendimento sobre a matéria.

Em recente julgado, o Superior Tribunal de Justiça declarou nula a decisão judicial que autorizou o espelhamento do aplicativo de mensagens instantâneas *Whatsapp* para que a polícia acompanhasse as conversas do suspeito por uma plataforma online.

No julgamento do Recurso Ordinário em *Habeas Corpus* n.º 99.735/SC, o STJ afirmou que a prática, além de permitir o acesso ilimitado a todas as conversas do investigado, permitia que o "interceptador" interagisse com o ambiente, enviando ou excluindo mensagens. A ementa do referido julgado é paradigmática, pois pela primeira vez tratou-se da quebra de sigilo de dados de comunicação virtual com uma análise de suas especificidades em relação à interceptação telefônica:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES.

ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO.
1. Hipótese em que, após coleta de dados do aplicativo WhatsApp, realizada pela Autoridade Policial mediante apreensão judicialmente autorizada de celular e subsequente espelhamento das mensagens recebidas e enviadas, os Recorrentes tiveram decretadas contra si prisão preventiva, em razão da suposta prática dos crimes previstos nos arts. 33 e 35 da Lei n.º 11.343/2006.
2. O espelhamento das mensagens do WhatsApp ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado WhatsApp Web. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (Quick Response), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço.
Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico que se pretende monitorar.
3. Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras, a ferramenta WhatsApp Web foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da internet, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada. 4. Tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato.
Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários.
5. Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a exemplo de conversas mantidas por e-mail, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já registradas no aplicativo WhatsApp, com o propósito de periciar seu conteúdo.
6. É impossível, tal como sugerido no acórdão impugnado, proceder a uma analogia entre o instituto da interceptação telefônica (art.
1.º, da Lei n.º 9.296/1996) e a medida que foi tomada no presente caso.
7. Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via WhatsApp Web o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura.
8. O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar

> absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia end-to-end, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.
> 9. Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (ex nunc), o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (ex tunc).
> 10. Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indíviduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura - embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto -, acompanhada de afirmação falsa de que nada foi feito.
> 11. Hipótese concreta dos autos que revela, ainda, outras três ilegalidades: (a) sem que se apontasse nenhum fato novo na decisão, a medida foi autorizada quatro meses após ter sido determinado o arquivamento dos autos; (b) ausência de indícios razoáveis da autoria ou participação em infração penal a respaldar a limitação do direito de privacidade; e (c) ilegalidade na fixação direta do prazo de 60 (sessenta) dias, com prorrogação por igual período.
> 12. Recurso provido, a fim de declarar a nulidade da decisão judicial que autorizou o espelhamento do WhatsApp via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes, revogando, por conseguinte, a prisão preventiva dos Recorrentes, se por outro motivo não estiverem presos (BRASIL, 2018).

Em outro recente julgado, o Superior Tribunal de Justiça reafirmou seu entendimento no sentido de que o acesso aos referidos dados se submete à reserva de jurisdição.

No julgamento do Agravo Regimental no Recurso em *Habeas Corpus* n.º 154.529/RJ, o STJ apesar de afirmar que o exame do aparelho celular do investigado durante o flagrante não se encontra albergado no comando do art. 5º, XII, da Constituição Federal, determinou que os dados armazenados nesses dispositivos, decorrentes do envio ou recebimento de dados via mensagens de SMS, programas ou aplicativos de troca de mensagens, estão relacionadas com a intimidade e a vida privada do indivíduo, o que os torna invioláveis, nos termos do art. 5º, X, da Constituição Federal (BRASIL, 2021).

Apesar de em uma primeira leitura indicar uma evolução do entendimento jurisprudencial no caminho do reconhecimento da inconstitucionalidade da prova

obtida por meio da violação do sigilo de dados de comunicação virtual, uma análise mais atenta dos fundamentos da decisão permite concluir que não há qualquer avanço na referida decisão.

Ao transladar a proteção dos dados de comunicação do inciso XII para o inciso X do artigo 5º da Constituição Federal, a Corte da Cidadania designou uma norma cujo o suporte fático amplo não prevê a edição de norma infraconstitucional para a regulação do seu suporte fático restrito.

Dessa forma, abre-se a possibilidade de se reconhecer a quebra do sigilo dos dados de comunicação virtual armazenados em dispositivos, mesmo sem a edição de lei específica, pois a norma de proteção dos referidos dados (inciso X, do art. 5º, da Constituição Federal) pode ser relativizada pela técnica da ponderação de interesses e não pela técnica da subsunção, caso estes dados estivessem protegidos pela norma estatuída no inciso XII do art. 5º da Constituição Federal.

Esse movimento, apesar de sutil, pode favorecer uma prática cada vez mais recorrente na persecução penal brasileira: o acesso amplo e irrestrito aos dados de comunicação virtual por meio de aplicativos de mensagens instantâneas.

Da análise sistêmica de nossa jurisprudência, pode-se concluir que não há uma sistematização do entendimento referente aos dados de comunicação virtual, sendo as decisões exaradas ainda sob uma perspectiva analógica da comunicação, resultando em uma defasagem conceitual e uma proteção deficiente da intimidade, vida privada e do sigilo das comunicações.

É preciso que haja uma sistematização do conhecimento sobre a comunicação virtual, notadamente a comunicação em aplicativos de mensagem instantânea, sob uma perspectiva multidisciplinar, para que se identifique os limites de provas existentes em nosso ordenamento jurídico.

Para isso, além das diferenças conceituais sobre comunicação, dados e informação, já analisadas em tópico anterior, é preciso entender os meios e as formas pelas quais se dão o acesso aos dados armazenados para se compreender a extensão do dano causado aos direitos fundamentais pela sua utilização desregulada na persecução penal.

2.5 As principais formas de acesso aos dados de comunicação virtual na persecução penal

O desenvolvimento de uma sociedade conectada à internet desencadeou, nos órgãos de persecução penal, a necessidade de se aprimorar os meios de investigação para buscar a solução do conflito penal de forma mais condizente com a dinâmica social.

Esses novos meios de obtenção de prova, como afirma Jezler Júnior (2019), envolve não apenas o desenvolvimento de novas formas de obtenção de provas, mas também a criação de novos mecanismos, notadamente a prova digital.

De acordo com Thamay e Tamer (2020, p. 33), a prova digital é um "*instrumento jurídico vocacionado a demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de conteúdo*".

Ainda segundo Thamay e Tamer (2020), a utilidade da prova digital no processo brasileiro depende da observância de três requisitos de admissibilidade: (i) autenticidade; (ii) integridade; e (iii) preservação da cadeia de custódia.

No que tange ao acesso aos dados de comunicação virtual, como discutido, é preciso em um primeiro momento diferenciar o lugar e o momento em que esses dados são armazenados e produzidos, respectivamente.

Na quebra do sigilo dos dados de comunicação virtual armazenados em dispositivos eletrônicos é necessário observar o procedimento de busca e apreensão do dispositivo, a extração dos dados e a interpretação desses dados para a obtenção da informação perseguida, observando em todas as fases os já mencionados critérios de admissibilidade (THAMAY e TAMER, 2020).

De acordo com Badaró (2015), a busca e apreensão é um meio de obtenção de provas preparatório para a efetiva obtenção da prova desejada. Segundo o autor, após a eventual apreensão da coisa ou pessoa, é necessário a sua conservação e posterior produção da prova correspondente através da fonte apreendida.

Pitombo (2005) afirma que a medida de busca e apreensão afronta o direito à privacidade e intimidade, que possuem tutela e ampla proteção constitucional, devendo ser, portanto, meios excepcionais de produção de provas.

A busca e apreensão encontra-se prevista nos artigos 240 a 250 do Código de Processo penal e pode ser utilizada para apreender quaisquer tipos de aparelhos eletrônicos.

Como visto alhures, os Tribunais brasileiros, antes mesmo da entrada em vigor do Marco Civil da Internet, já consideravam como incluídas na apreensão dos aparelhos eletrônicos os dados nele armazenados, efetuando uma interpretação extensiva dos dispositivos legais.

Ocorre que ao tratar de dados de comunicação virtual, que veiculam não só os dados do tráfego de sinais telemáticos, mas também o conteúdo das comunicações travadas, impera analisar a possibilidade de acesso a esses dados não apenas como simples obtenção de dados armazenados em dispositivos eletrônicos, mas como verdadeira quebra do sigilo da comunicação por meio de dados, hipótese ainda não regulada em lei.

Após a apreensão do aparelho eletrônico, preservando-se a cadeia de custódia, passa-se a segunda etapa do processo: o acesso aos dados armazenados.

Diante dos mecanismos de segurança dos aparelhos eletrônicos modernos, esse acesso só pode ser realizado, ou com a autorização do proprietário do aparelho, oferecendo as chaves de segurança aptas a desbloquear o dispositivo, ou por meio de uma quebra dessas proteções (CASELLI, 2021).

Quando fornecidas as senhas de bloqueio e os padrões de acesso, o procedimento de extração de conversas de aplicativos de mensagens instantâneas é relativamente simples.

Alves e Lourenço (2021) descrevem o método utilizado em aparelhos cujo o sistema operacional é o Android:

1) Para preservar a integralidade do dispositivo, deve-se colocá-lo em “modo avião”, impossibilitando a sua conexão com a internet;
2) Após, deve-se desligar o aparelho e inserir um microSD (cartão de memória utilizado em smartphones) que contenha um APK de compactação (aplicativo de pacote destinado à compactação de arquivos do sistema Android);

3) Após a inserção do cartão de memória, liga-se o aparelho e inicia a instalação do APK, configurando o aparelho para permitir a instalação de aplicativos de fontes desconhecidas.
4) Na sequência, deve o perito ou investigador responsável transferir as conversas desejadas para o cartão de memória, exportando todo do conteúdo daquela conversa.
5) Por fim, acessa-se o cartão de memória em um computador, formatando a conversa e deixando-a inteligível para os investigadores ter acesso a todo o conteúdo daquela conversa.

Nota-se, da descrição do procedimento, que apesar de haver a preservação da cadeia de custódia, o mecanismo utilizado permite um acesso amplo e irrestrito a todas as conversas travadas pelo investigado, não havendo qualquer limite subjetivo ou objetivo.

Na prática, a utilização da extração de conversas por aplicativos de mensagens instantâneas permite um acesso universal à intimidade e a vida privada do investigado, sem qualquer limitação temporal, circunstancial e subjetiva, configurando verdadeira devassa da privacidade.

O procedimento descrito por Alves e Lourenço (2021) possui algumas limitações: só é aplicável aos dispositivos que funcionam com sistema operacional Android e é necessário o acesso às chaves e padrões de acesso para ser implementado. Essas limitações, no extremo, acabam por introduzir distinções entre os investigados, sendo que aqueles que possuem smartphones de outros sistemas operacionais (IOS, balckberry, entre outros) não podem ter os dados de comunicação virtual acessados por esse procedimento.

Outra forma de acesso ao conteúdo das comunicações realizadas pelo aplicativo de mensagens instantâneas Whatsapp (o mais utilizado no Brasil), é pela via da clonagem da conta ou do acesso remoto via dispositivo de acesso web (Whatsapp Web).

A sistemática consiste, basicamente, em clonar a conta do aplicativo de modo que o investigador tenha acesso, não apenas as conversas mantidas armazenadas pelo investigado, mas também as conversas que ocorrem em tempo real (GODOY, 2016).

Essa opção já foi rechaçada pelo Superior Tribunal de Justiça, pois permite ao investigador não apenas o acesso, mas o controle e a intervenção tanto na comunicação em tempo real, como nas conversas armazenadas, sendo, portanto inadmissível no processo penal brasileiro.

Dessa forma, resta ao investigador que não possui acesso às chaves e padrões de acesso ao dispositivo, tentar quebrar a proteção conferida ao dispositivo para acessá-lo de modo a extrair os dados.

Atualmente, o software mais utilizado para esse procedimento é o *Cellebrite Premium*, ferramenta desenvolvida pela empresa israelense *Cellebrite*, que, segundo a empresa, consegue desbloquear celulares com Android e iOS (FONTINATO, 2021).

Apesar do funcionamento do serviço ser um segredo comercial, especialistas afirmam que ele opera com uma combinação de softwares e hardwares que encontram brechas de segurança nos dispositivos e extraem dos dados do aparelho, não permitindo a manipulação desses dados para a preservação da cadeia de custódia (FONTINATO, 2021).

Esses procedimentos de acesso ao dispositivo decorrem da necessidade do investigador ter acesso a um dos terminais, pois as comunicações travadas por meio de aplicativos de mensagem instantânea utilizam-se de criptografia [1]ponta-a-ponta para garantir o sigilo das comunicações.

Caselli (2021) esclarece que todas as mensagens trocadas pelo aplicativo de mensagens instantâneas Whatsapp possuem criptografia na camada de transporte, ou seja, a mensagem é codificada no terminal de saída, sendo decodificada apenas no terminal de chegada. Esse método de criptografia dificulta a interceptação do fluxo de sinais utilizado por esse meio de comunicação.

Quando fala-se em acesso aos fluxos de sinais (comumente chamado de fluxo de dados) estar-se-á diante de uma interceptação do fluxo de comunicação digital, necessitando, por isso, de mecanismos e procedimentos aptos a colher esses sinais, converte-los em dados identificáveis e interpretar esses dados para obter a informação procurada, tudo isso sem descuidar dos requisitos de admissibilidade da

[1] A criptografia é uma ciência que estuda princípios e técnicas para uma comunicação segura, mas também é uma técnica que promove a construção e utilização de protocolos que impedem que terceiros tenham acesso ao conteúdo das mensagens. Existem diversos métodos de criptografia, nas aplicações de internet, devido a sua comunicação descentralizada, é comum o uso da criptografia de ponta-a-ponta, de modo que apenas os terminais de saída e de chegada tenham a possibilidade de decodificar os sinais recebidos convertendo-os em informação.

prova digital – integridade, autenticidade e preservação da cadeia de custódia (THAMAY e TAMER, 2020).

Dessa forma, para proporcionar uma interceptação do fluxo de sinais da comunicação por via de aplicativo de mensagens instantâneas seria necessário que o provedor de aplicação desenvolvesse um sistema paralelo, de acesso a terceiros autorizados às chaves criptográficas, o que não encontra um respaldo em nosso ordenamento jurídico (CASELLI, 2021).

Portanto, atualmente, o que se conhece como interceptação das comunicações de aplicativos de mensagens instantâneas é, na verdade, apenas a quebra do sigilo de dados de comunicação pretérita, que também não encontra respaldo em nossa legislação processual penal.

Assim, o uso indiscriminado de técnicas invasivas e de técnicas de quebra do sistema de segurança de aparelhos de telecomunicação móvel, além de não encontrar previsão legal e violar à proteção da intimidade, vida privada e o sigilo das comunicações, por vezes torna a prova produzida carente de integridade, autenticidade e confiabilidade, pois não se pode, através desses meios, garantir a cadeia de custódia e a reprodutibilidade do meio de investigação, notadamente devido ao segredo comercial dos softwares utilizados.

Com isso, realizada a distinção entre os tipos de dados, os métodos de acesso a esses dados e as bases normativas que regulam (ou não) o procedimento de acesso de terceiros ao conteúdo das comunicações realizadas por aplicativos de mensagens instantâneas, cumpre analisar se a prova produzida por esse meio invasivo se coaduna com as normas de direitos fundamentais analisadas no primeiro capítulo deste trabalho.

3 A (IN)CONSTITUCIONALIDADE DA QUEBRA GENÉRICA DO SIGILO DE DADOS DE COMUNICAÇÃO VIRTUAL

Delineados os parâmetros constitucionais da proteção da intimidade, da vida privada e do sigilo de dados e das comunicações, bem como as distinções entre os dados de comunicação virtual e os dados de comunicação telefônica, torna-se necessário analisar a proteção constitucional do sigilo dos dados e os permissivos constitucionais e legais para definir a possibilidade de utilização da quebra do sigilo de dados de comunicação virtual no processo penal brasileiro.

3.1 A (im)possibilidade de violação do sigilo de dados de comunicação virtual por aplicativos de mensagens instantâneas para fins processuais penais

O constituinte originário, tendo em vista a necessidade de inserir o ser humano no centro do ordenamento jurídico nacional, preservando a sua dignidade, incluiu no rol dos direitos fundamentais a proteção da intimidade, da vida privada e do sigilo das comunicações em sentido amplo.

A inserção dos incisos X, XI e XII no art. 5º da Constituição Federal plasmou em nosso ordenamento jurídico a proteção da esfera privada, local de desenvolvimento da personalidade do sujeito, dimensão de sua dignidade, impossibilitando que terceiros, incluindo o Estado, interfiram indevidamente nestes espaços.

Como discutido anteriormente, o inciso X do art. 5º da Constituição Federal protege a privacidade, intimidade, honra e imagem das pessoas de forma ampla, genérica, prevendo a indenização como consequência de sua violação.

De acordo com a análise do suporte fático da norma proposto por Silva (2010), nota-se que o disposto no inciso X do art. 5º da Constituição Federal não possui limites imanentes, tampouco restrições previstas para o seu âmbito de incidência, sendo o suporte fático amplo estabelecido pela norma qualquer violação aos bens jurídicos protegidos: privacidade, intimidade, honra e imagem.

De outro lado, ao estabelecer a proteção ao sigilo das comunicações, no inciso XII do art. 5º da Constituição Federal, o constituinte estabeleceu um suporte fático amplo, consubstanciado na proteção ao sigilo das correspondências, das comunicações telegráficas, dos dados e das comunicações telefônicas, mas também

incluiu um limite imanente – a possibilidade de restrição do direito para investigação criminal e instrução processual penal, na forma que a lei estabelecer.

Trata-se de norma de direito fundamental de eficácia contida, na definição de Silva (2014), que possui aplicabilidade integral e imediata, mas pode ter seu conteúdo restringido por norma infraconstitucional.

De acordo com Silva (2014) as normas de eficácia contida produzem seus efeitos de maneira integral até que o legislador infraconstitucional, por meio de lei formal, limite seu campo de eficácia. Na ausência da lei limitadora, a norma produz plenamente seus efeitos, não podendo haver qualquer limitação do seu âmbito de proteção.

Foi com base nesse entendimento que o Supremo Tribunal Federal, em diversos julgados (a exemplo do *Habeas Corpus* n.º 69.912/RS), fixou o entendimento de ser ilícita a interceptação telefônica em decorrência da ausência de lei que regulamentasse a parte final do art. 5º, XII da Constituição Federal de 1988.

Diante do entendimento fixado pelo Supremo Tribunal Federal sobre a indispensabilidade de edição de lei para prever as hipóteses de quebra do sigilo das comunicações telefônicas, o legislador infraconstitucional editou, em 1996, a Lei n.º 9.296/1996.

A Lei n.º 9.296/1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, dispõe sobre o instituto da interceptação telefônica, definida por Gomes e Maciel (2018) como sendo “a captação da comunicação telefônica por um terceiro, sem o conhecimento de nenhum dos comunicadores”. Logo, a interceptação telefônica ocorre no momento em que a comunicação está ocorrendo, sendo captado o fluxo da informação por um terceiro.

Logo, tem-se que interceptação telefônica é matéria cuja autorização depende de decisão judicial (reserva jurisdicional), que ela é efetivada no momento da comunicação entre os interlocutores e, sendo assim, só capta as conversas travadas após a decisão judicial autorizadora.

A referida lei, diante do crescente uso da internet e dos sistemas de computação, ampliou seu âmbito de incidência para abarcar à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Dessa forma, entende-se ser plenamente possível em nosso ordenamento jurídico a interceptação dos fluxos de comunicação por meio de aplicativos de

mensagens instantâneas (*Whatsapp*, *Telegram*, *Snapchat*, *Skype*, entre outros), uma vez que a norma regulamentadora previu, expressamente, essa possibilidade.

Para tanto, é necessário que o terceiro (agente da persecução penal) tenha acesso ao conteúdo das trocas de mensagens no momento em que elas ocorrem, uma vez que própria definição legal previu a interceptação do "fluxo de comunicações".

Ocorre que os aplicativos de mensagens instantâneas são programados para operar utilizando uma forma de criptografia de codifica os sinais que serão transmitidos entre os terminais, impossibilitando que um terceiro tenha acesso ao conteúdo das mensagens que estão sendo transmitidas.

Essa criptografia foi estabelecida, justamente, para garantir o sigilo das comunicações, permitindo que as conversas travadas por meio desses aplicativos sejam de conhecimento exclusivo de seus interlocutores.

Dessa forma, diante da criptografia ponta-a-ponta, como afirma Caselli (2021), torna-se necessário que o agente interceptador tenha acesso as chaves criptográficas, ou acesso a um dos terminais.

Segundo o Whatsapp (2020), aplicativo de mensagens instantâneas mais utilizado no Brasil, somente os usuários possuem acesso às chaves criptográficas utilizadas na comunicação, que são modificadas para cada sessão, não sendo possível que a empresa forneça as referidas chaves criptográficas, pois as chaves são criadas de maneira automática e sem registro pelo aplicativo.

Por conseguinte, a única forma da autoridade investigativa ter acesso ao fluxo da comunicação nos aplicativos de mensagens instantâneas é o acesso a um dos terminais envolvidos na comunicação.

Ocorre que, como bem decidiu o Supremo Tribunal Federal no *Habeas Corpus* n.º 99.735/SC, julgado em 27 de novembro 2018, caso o investigador tenha acesso a um dos terminais de comunicação por aplicativo de mensagens instantâneas, ainda que pelo espelhamento da conta em sistema on-line (*Whatsapp Web*), este poderia intervir na comunicação e no registro das mensagens, não sendo integra a prova produzida por este meio.

Portanto, tem-se que na atual conjuntura, a interceptação da comunicação por meio de aplicativos de mensagens instantâneas, apesar de prevista legalmente, é tecnicamente impossível, sendo necessário o desenvolvimento de aplicações de

internet, em colaboração com as empresas que disponibilizam esse serviço, para que o investigador possa ter o conhecimento das conversas em tempo real sem que possa interferir no registro dessas conversas.

Assim, superada a questão relativa a interceptação propriamente dita das comunicações via aplicativos de mensagens instantâneas, resta analisar a possibilidade de quebra do sigilo dos dados de comunicação armazenados nos dispositivos eletrônicos.

O texto do inciso XII do art. 5º da Constituição Federal foi editado para proteger não apenas o sigilo das comunicações, mas o sigilo dos dados em si considerados.

Essa é a conclusão obtida após analisar as atas da comissão de redação da Assembleia Nacional Constituinte, que aprovou a proposta do Constituinte Hilário Braun, apresentada pelo Constituinte Ricardo Fiúza, que inseriu a palavra "comunicações" antes da palavra telefônica justamente para denotar que o sigilo protegido pela Constituição Federal é o sigilo dos dados e não apenas o sigilo da comunicação. Diante dessa reflexão tem-se que para haver a quebra do sigilo dos dados de comunicação é necessária a edição de lei, disciplinando essa possibilidade.

Portanto, diferente do entendimento fixado pelo Supremo Tribunal Federal no Recurso Extraordinário n.º 418.416/SC, a proteção a que se refere o art. 5º, XII da Constituição Federal é a proteção aos dados em si mesmos, ainda que armazenados em dispositivos eletrônicos.

Como visto, a Lei n.º 9.296/1996 não previu a possibilidade de quebra do sigilo de dados de comunicação armazenados em dispositivos eletrônicos, regulou, apenas a interceptação do fluxo de comunicações em sistemas de informática e telemática.

Dessa forma, ausente legislação infraconstitucional que limite o âmbito de proteção da norma constitucional de eficácia contida, tem-se que a proteção conferida pelo legislador constituinte ao sigilo dos dados é plenamente eficaz, não sendo possível a sua violação para a produção de provas em investigação criminal e instrução processual penal.

Com isso, entende-se ser plenamente aplicável à quebra do sigilo de dados de comunicação virtual armazenados em aparelhos eletrônicos o mesmo raciocínio

jurídico exarado pelo Supremo Tribunal Federal quando julgou ilícitas as provas obtidas por meio da interceptação telefônica antes da edição da Lei n.º 9.296/1996.

É de se ressaltar que a dinâmica social atual não permite que se considere os dados de comunicação virtual armazenados em dispositivos eletrônicos como meros arquivos que podem ser acessados pelo investigador após a apreensão da base física na qual se encontravam os dados, como decidiu o Supremo Tribunal Federal no Recurso Extraordinário n.º 418.416/SC.

Na sociedade atual, definida como sociedade em rede por Castells (1999), a maior parte da comunicação é realizada utilizando dispositivos conectados na internet, sendo este o meio preferencial de comunicação. Não se pode, diante da mudança da comunicação telefônica para a comunicação por dados, relegar a esta proteção deficiente, sob o fundamento de que se estaria apenas periciando a base física regularmente apreendida.

Os dados de comunicação diferem substancialmente de outros dados e arquivos constantes nos aparelhos eletrônicos por diversas razões: i) os dados de comunicação possuem sigilo protegido pelo texto constitucional; ii) os dados de comunicação permitem ao investigador o acesso ao conteúdo da comunicação travada; e iii) os dados de comunicação são registros de uma conversa pretérita, cujos fragmentos podem ter sido apagados pelo interlocutor.

Sendo assim, não se pode comparar os dados de comunicação virtual armazenados em aparelhos eletrônicos com fotos, vídeos e outros documentos constantes no mesmo aparelho.

É imperiosa a edição de lei que preveja, não só a possibilidade, mas também as formas, procedimentos e limitações, da quebra do sigilo dos dados de comunicação virtual para que eles possam ser admitidos como provas no processo penal brasileiro.

Existem diversos projetos de lei tramitando no congresso nacional relativos ao sigilo das comunicações e a sua relativização. Dentre eles, o projeto de Lei n.º 6960/2017 prevê a alteração do disposto nos artigos 5º e 7º do Marco Civil da Internet para dispor sobre a possibilidade de quebra do sigilo dos dados de comunicações privadas armazenados em terminais fixos ou móveis.

Porém, não tramita no congresso nacional um projeto de lei que regule de maneira satisfatória a matéria, dispondo sobre as hipóteses permissivas, os requisitos e as formas da quebra do sigilo desses dados.

Sendo o sigilo dos dados um direito fundamental, é necessário que o legislador infraconstitucional estabeleça de forma clara e precisa os limites da relativização do sigilo dos dados, sob pena de esvaziar o preceito constitucional. Para isso, é importante realizar uma ponderação entre os bens jurídicos que se busca proteger, estabelecendo critérios que permitam que o direito fundamental não seja completamente esquecido frente à sanha persecutória do Estado.

3.2 Requisitos mínimos ou essenciais para a quebra do sigilo de dados de comunicação virtual: uma ponderação necessária.

Como visto, para a admissibilidade da prova produzida por meio da quebra do sigilo de dados de comunicação virtual armazenada em dispositivos eletrônicos é necessária a edição de lei formal, dispondo expressamente sobre as hipóteses de admissibilidade, bem como a forma de sua produção.

Porém, essa atividade legislativa não está imune a limites e controles, uma vez que a Constituição Federal, em seu art. 5º, inciso XII, insculpiu a proteção do sigilo dos dados como direito fundamental do cidadão.

Diante dessa premissa, tem-se que o legislador, ao atuar em seu mister de regular a relativização do direito fundamental ao sigilo dos dados, deve ter em vista que a inclusão de restrições aos direitos fundamentais não pode ser ilimitada, sob pena de esvaziamento da proteção conferida pelo constituinte.

Assim, impera que no processo legislativo haja observância do princípio da proporcionalidade, de modo que o sacrifício do direito fundamental se realize de forma adequada, na medida do necessário e respeitada à proporcionalidade em sentido estrito.

Marcante (2020) esclarece que o princípio da proporcionalidade *lato sensu* é um freio, um escudo, colocando limites na restrição de direitos, liberdades e garantias do cidadão.

Ainda em relação à aplicação do princípio da proporcionalidade em matéria de proibições de prova, Marcante (2020) destaca que o referido princípio deve ser utilizado no plano *lege ferenda*, pré-estabelecendo legalmente os crimes em que os meios invasivos aos direitos fundamentais serão admitidos e a forma como essas provas serão produzidas.

Dito isso, importa nesse momento propor uma reflexão sobre os limites da quebra do sigilo de dados de comunicação virtual armazenados em dispositivos eletrônicos, com o intuito de fixar premissas que devem ser observadas em um juízo de ponderação no momento de produção da norma permissiva da medida invasiva aos direitos fundamentais.

Em um primeiro momento, assim como previsto na Lei das Interceptações Telefônicas e em outras normas infraconstitucionais que preveem meios excepcionais de obtenção de provas, é necessário que o legislador fixe um rol de crimes nos quais serão admitidas as provas produzidas com a quebra do sigilo dos dados de comunicação virtual.

Esse rol de crimes deve respeitar a proporcionalidade em sentido estrito, não sendo razoável se permitir a utilização de meio tão invasivo aos direitos fundamentais em crimes de menor gravidade.

A lei das interceptações telefônicas previu a utilização da medida apenas para os crimes punidos com reclusão. Diante do caráter prospectivo da interceptação telefônica, que é menos invasivo que o caráter retrospectivo da quebra do sigilo de dados armazenados, tem-se como parâmetro inferior dessa limitação os crimes punidos com reclusão.

Não seria proporcional que o legislador admitisse que a quebra do sigilo de dados de comunicações virtuais para crimes punidos com detenção ou prisão simples, uma vez que limitou medida menos invasiva (interceptação telefônica) aos crimes punidos com reclusão.

A outro giro, diante do caráter plural das comunicações, onde o investigador terá acesso a todas as conversas do investigado, é necessário se estabelecer um limite subjetivo, definindo-se na decisão que autoriza a medida quais conversas poderão ser acessadas pelo investigador.

Essa limitação subjetiva evitará que se promova uma verdadeira devassa nas conversas do investigado, buscando-se elementos que não estejam em conexão com o crime investigado.

Além disso, essa limitação subjetiva também promove a proteção do sigilo dos dados de comunicação virtual de pessoas que não são alvo da investigação, ou mesmo pessoas com foro por prerrogativa de função, que necessitaria de uma decisão do juízo competente para ter seu sigilo quebrado.

Por fim, mas não menos importante, é necessário que se estabeleça uma limitação temporal. Como os dados de comunicação virtual armazenados em dispositivos eletrônicos guardam a informação de todo o histórico de conversas do indivíduo, não se mostra proporcional que o investigador tenha acesso a todo o período de conversas salvo no dispositivo, sendo necessário que a decisão que autoriza a medida preveja o período no qual o investigador pode acessar o conteúdo das comunicações.

Acredita-se que estabelecidas essas três limitações (material, subjetiva e temporal), haverá um respeito à proporcionalidade *lato sensu*, permitindo que a medida invasiva aos direitos fundamentais seja utilizada de maneira a não esvaziar o conteúdo mínimo do direito fundamental de proteção do sigilo dos dados.

Ressalte-se, ainda, que as limitações impostas na decisão de autorização da quebra do sigilo de dados virtuais não impedem que o investigador, a partir de uma quebra de sigilo válida, colha elementos de informação hábeis a subsidiar um novo pedido de quebra do sigilo, justificando-se a necessidade de ampliação do objeto investigado.

Dessa forma, somente com a edição de lei formal que, além de prever a possibilidade de quebra do sigilo de dados, estabeleça critérios seguros de proporcionalidade no plano abstrato, tem-se como admissível a utilização da prova obtida com violação do sigilo de dados de comunicação virtual, pois respeitados os ditames constitucionais sobre a matéria.

4 CONSIDERAÇÕES FINAIS

A dinâmica social impõe ao aplicador do direito um olhar atento às mudanças e evoluções das relações sociais. Na sociedade contemporânea, marcada pela globalização e pelo uso massivo da internet como meio de comunicação, a proteção constitucional à privacidade, intimidade e ao sigilo das comunicações devem ser observadas à luz dos fundamentos dessa nova forma social.

Diante disso, é preciso observar que os dados de comunicação virtual armazenados em dispositivos eletrônicos diferem substancialmente dos demais dados armazenados neste dispositivo.

Os dados de comunicação virtual, além de informar a existência e duração da comunicação, informam, também, o próprio conteúdo da comunicação, não podendo ser tradados como meros dados de registro de comunicações, como os dados de comunicação telefônica.

A constituição federal, em seu art. 5º, inciso XII, previu a proteção dos dados e das comunicações telefônicas. A inserção da palavra “comunicações” antes da palavra "telefônicas" foi uma opção do constituinte originário para denotar que não apenas as comunicações de dados estavam protegidas, mas os dados em si considerados, não havendo o que se falar que a proteção constitucional não alcança os dados armazenados nos dispositivos eletrônicos.

Porém, como a norma constante do art. 5º, inciso XII da Constituição Federal é uma norma de eficácia contida, o legislador infraconstitucional pode, mediante edição de lei, restringir o âmbito de proteção da norma, dispondo sobre hipóteses nas quais o sigilo pode ser afastado.

Com esse desiderato, o legislador editou a Lei n.º 9.296/1996, regulando a parte final do art. 5º, XII da Constituição Federal, disciplinando a utilização da interceptação telefônica para fins de investigação criminal ou instrução processual penal.

No parágrafo único do art. 1º da Lei n.º 9.296/1996, o legislador ampliou o âmbito de incidência da norma para incluir a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática.

Assim, tem-se como plenamente possível, do ponto de vista jurídico, a interceptação do fluxo de comunicações virtuais realizadas por meio da internet, notadamente com o uso de aplicativos de mensagens instantâneas.

Porém, a arquitetura da rede mundial de computadores e a programação dos aplicativos de mensagens instantâneas impossibilitam, ao menos por enquanto, a interceptação desse fluxo comunicacional, sem que o agente investigador possa influenciar no registro das mensagens, o que compromete a integridade da prova obtida, em decorrência da criptografia utilizada.

Por outro lado, não há em nosso ordenamento jurídico nenhuma disposição infraconstitucional que permita o acesso aos dados de comunicação virtual armazenados em aparelhos eletrônicos.

Apesar de ser uma prática comum e aceita em nossos tribunais, a quebra do sigilo de dados de comunicação virtual armazenados em aparelhos eletrônicos não encontra respaldo legal, sendo, portanto, inconstitucionais as provas obtidas por esse meio, até que sobrevenha norma regulamentadora da espécie.

Nesse sentido, existem projetos de lei tramitando no Congresso Nacional que preveem tanto a regulação da interceptação das comunicações por aplicativos de mensagens instantâneas, quanto a quebra do sigilo dos dados armazenados em aparelhos eletrônicos, mediante decisão judicial.

Apesar da previsão de inserção dos dispositivos autorizadores, não há nos projetos de lei analisados, uma regulação específica da matéria, sendo necessário que o legislador promova a adequada ponderação entre os bens jurídicos tutelados, a fim de se estabelecer rígidos controles do uso da medida, sob pena de se esvaziar o direito fundamental previsto na Constituição Federal.

Assim, é preciso que o legislador infraconstitucional, além de dispor um rol taxativo de crimes que permitam a utilização da medida, estabeleça um limite temporal, consubstanciado em um intervalo temporal das conversas que terão seu sigilo quebrado, bem como uma limitação subjetiva, não sendo possível a quebra do sigilo de dados reflexa, e uma limitação material, não sendo possível a utilização de conversas que não guardem relação direta com o crime investigado.

Acredita-se que somente após a edição dessa lei regulamentadora é que a quebra do sigilo dos dados de comunicação virtual armazenados em dispositivos eletrônicos passará à condição de provas constitucionais e, portanto, admissíveis no processo penal nacional.

REFERÊNCIAS

ALEXY, Robert. **Teoria da argumentação jurídica**. Trad. Zilda Hutchinson Shild Silva. São Paulo: Landy, 2001.

ALVES, Gustavo André; LOURENÇO, Marcus Vinicius**. Extração de mensagens do aplicativo Whatsapp**. In: JORGE, Higor Vinicius Nogueira (organizador). Tratado de Investigação Criminal Tecnológica. 2ª edição. Salvador: Juspodivm, 2021.

ANDRADE, Manuel da Costa. **Sobre as proibições de prova em processo penal**. Coimbra: Coimbra Editora, 1992.

ARAÚJO, Luiz Alberto David. **Artigo 5º, incisos X ao XII**. In: BONAVIDES, Paulo; MIRANDA, Jorge; AGRA, Walber de Moura (organizadores). Comentários à Constituição Federal de 1988. Rio de Janeiro: Forense, 2009.

ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. 18ª edição. São Paulo: Malheiros, 2018.

BADARÓ, Gustavo. **Processo Penal**. 3ª edição. São Paulo: Revista dos Tribunais, 2015.

BARCELLOS, Ana Paula de. **A eficácia jurídica dos princípios constitucionais**. Rio de Janeiro: Renovar, 2002.

BARROS, Suzana Toledo. **O princípio da proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais**. Brasília: Brasília Jurídica, 1996.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 7ª edição. São Paulo: Saraiva Educação, 2018.

BECK, Ulrich. **Sociedade de Risco: rumo a uma outra modernidade**. Tradução: Sebastião Nascimento. 2ª edição. São Paulo: Editora 34, 2011.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 3372**, de 29 de setembro de 2021. Disponível em: https://short.gy/BRgnl4. Acesso em 01 de novembro de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 6960**, de 20 de fevereiro de 2017. Disponível em: https://short.gy/CjXr1x. Acesso em 01 de novembro de 2021.

BRASIL. **Decreto-Lei n.º 3.689/1941**, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União de 24 de outubro de 1941.

BRASIL. **Diário da Assembleia Nacional Constituinte (Suplemento "B")**. 1988. Disponível em: https://www.senado.leg.br/publicacoes/anais/constituinte/redacao.pdf. Acesso em 04 de novembro de 2021.

BRASIL. **Lei n.º 11.690**, de 9 de junho de 2008. Altera dispositivos do Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e dá outras providências. Diário Oficial da União de 10 de junho de 2008.

BRASIL. **Lei n.º 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União de 24 de abril de 2014.

BRASIL. **Lei n.º 13.964**, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União de 30 de abril de 2021.

BRASIL. Lei n.º 4.117, de 27 de agosto de 1962. Institui o Código Brasileiro de Telecomunicações. Diário Oficial da União de 17 de dezembro de 1962.

BRASIL. **Lei n.º 9.296**, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial da União de 25 de julho de 1996.

BRASIL. **Lei n.º 9.472,** de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Diário Oficial da União de 17 de julho de 1997.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental em Agravo em Recurso Especial n.º 431.316/RJ**. Quinta Turma. Julgado em 06 de fevereiro de 2018. DJe de 16 de fevereiro de 2018.

BRASIL. Superior Tribunal de Justiça. ***Habeas Corpus* n.º 148413/SP**. Sexta Turma. Julgado em 21 de agosto de 2014. DJe de 01 de setembro de 2014.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em *Habeas Corpus* n.º 56744/RS**. Quinta Turma. Julgado em 02 de junho de 2015. DJe de 10 de junho de 2015.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em *Habeas Corpus* n.º 154529/SC**. DJe de 01 de outubro de 2021.

BRASIL. Supremo Tribunal Federal. ***Habeas Corpus* n.º 69.912/RS**. Tribunal Pleno. Julgado em 16/12/1993. Disponível em: https://url.gratis/0fHdtV. Acesso em 01 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n.º 418.416/SC.** Tribunal Pleno. Julgado em 10 de maio de 2006, DJ de 19 de dezembro de 2006.

CANOTILHO. José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7ª edição. Coimbra, Portugal: Almedina, 2003.

CASELLI, Guilherme. **Manual de Investigação Digital**. São Paulo: Editora Juspodivm, 2021.

CASTELLS, Manuel. **A sociedade em rede**. Tradução: Roneide Venancio Majer, 6ª ed. São Paulo: Paz e Terra, 1999.

CUNHA JR. Dirley da**. Curso de Direito Constitucional**. 12ª edição. Salvador: Juspodivm, 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados**. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019.

FERNANDES, Antônio Scarance. **Processo Penal Constitucional**. 4ª edição. São Paulo: Revista dos Tribunais, 2002.

FERRAZ FILHO, José Francisco Cunha. **Dos princípios Fundamentais**. In: MACHADO, Costa; FERRAZ, Anna Cândida da Cunha. Constituição Federal interpretada. 9ª edição. São Paulo: Manole, 2018.

FERRAZ, Anna Cândida da Cunha. **Processos Informais de Mudança da Constituição**. São Paulo: Editora Max Limonad Ltda., 1986.

FONTINATO, Giovanna. **Cellebrite: conheça o software usado na investigação do caso Henry**. TecMundo, 2021. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em 10 de novembro de 2021.

FOROUZAN, Behrouz. **Comunicação de dados e redes de computadores**. 4ª edição. Porto Alegre: AMGH, 2010.

FREITAS, Christiano Rodrigo Gomes de Freitas. **As proibições de prova em processo penal e a impossibilidade de sua flexibilização no processo constitucional**. Dissertação (Mestrado). Belo Horizonte: Pontifícia Universidade Católica de Minas Gerais, 2011.

GIACOMOLLI, Nereu José. **O devido processo penal: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica**. São Paulo: Atlas, 2014.

GIDDENS, Anthony. **As consequências da modernidade**. Tradução: Raul Fiker. São Paulo: Editora Unesp, 1991.

GODOY, Luiz Roberto Ungaretti. **A evolução tecnológica e o monitoramento de sinais: uma nova regulamentação jurídica**. Tese de Doutorado. Orientador: Marco Antonio Marques da Silva. São Paulo: Pontifícia Universidade Católica de São Paulo, 2016.

GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica e das comunicações de dados e telemáticas: comentários a Lei 9.296/1996**. 4ª edição. São Paulo: Thomson Reuters Brasil, 2018.

GRECO FILHO, Vicente. **Interceptação Telefônica. Considerações à Lei 9.296 de 24 de julho de 1996**. 1ª ed. São Paulo: Saraiva, 2005.

GRINOVER, Ada Pellegrini. **Liberdades públicas e processo penal – As interceptações telefônicas**. São Paulo: Saraiva, 1986.

GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações Eletrônicas e Dados Digitais no Processo Penal.** Dissertação (Mestrado). São Paulo: Faculdade de Direito da Universidade de São Paulo, 2012.

HESSE, Konrad. **Limites de la Mutación Constitucional**. In: Escritos de Derecho Constitucional. Madrid: Centro de Estudios Constitucionales, 1992.

JEZLER JR., Ivan. **Prova Penal Digital: tempo, risco e busca telemática**. Florianópolis: Tirant Lo Blanch, 2019.

LIMA, Renato Brasileiro de. **Legislação criminal especial comentada.** 7ª edição. Salvador: Juspodivm, 2019.

LOPES JR, Aury. **Direito Processual Penal**. 17ª edição. São Paulo: Saraiva Educação, 2020.

LYOTARD, Jean-François. **A condição Pós-moderna**. Tradução: Ricardo Corrêa Barbosa, 14ª edição. Rio de Janeiro: José Olympio, 2011.

MARCANTE, Marcelo. **Limites à atividade probatória: proibição de prova, conhecimentos fortuitos e compartilhamento de provas no processo penal**. Florianópolis: Emais, 2020.

PITOMBRO, Cleunice Bastos. **Da busca e da apreensão no processo penal**. São Paulo: Revista dos Tribunais, 2005.

PRADO, Geraldo. **Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça**. 2ª edição. Rio de Janeiro: Lumen Juris, 2006.

ROXIN, Claus. **Derecho Procesal Penal**. Buenos Aires: Del Puerto, 2003.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 13ª edição. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 9ª edição. Porto Alegre: Livraria do Advogado, 2011.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SILVA, José Afonso da. **Aplicabilidade das Normas Constitucionais**. 6ª edição. São Paulo: Malheiros Editores, 2003.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 37ª edição. São Paulo: Malheiros Editores, 2014.

SILVA, José Afonso da. **Mutações Constitucionais. In: Poder Constituinte e Poder Popular (estudos sobre a Constituição)**. São Paulo: Editora Malheiros, 2007. p. 288-296.

SILVA, Virgílio Afonso da. **Direitos Fundamentais: conteúdo essencial, restrições e eficácia**. 2ª edição. São Paulo: Malheiros Editores, 2010.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático: partes geral e especial**. 2ª edição. Salvador: Juspodivm, 2021.

THAMAY, Rennan; TAMER, Maurício. **Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie**. São Paulo: Thomson Reuters Brasil, 2020.

VELLOSO, Carlos Mário da Silva. **As comissões parlamentares de inquérito e o sigilo das comunicações telefônicas.** Revista Brasileira de Ciências Criminais, n. º 24, out-dez, p. 133-134, 1998.

WHATSAPP. Visão Geral da Criptografia do Whatsapp: documento técnico. 2020. Disponível em: https://2hsq.short.gy/2MEVdH. Acesso em 15 de novembro de 2021.

WHITE, Curt. **Redes de computadores e comunicação de dados**. São Paulo: Cengage Learning, 2012.