

A INTERCEPTAÇÃO DE COMUNICAÇÕES NO PROCESSO PENAL BRASILEIRO: ANÁLISE À LUZ DA LEI Nº 9.296/96, DA LEI Nº 13.964/2019 E DA JURISPRUDÊNCIA

THE INTERCEPTION OF COMMUNICATIONS IN THE BRAZILIAN CRIMINAL PROCEDURE: ANALYSIS IN THE LIGHT OF LAW N. 9.296/96, LAW N. 13.964/2019 AND JURISPRUDENCE

Leonardo Pedriça Moreira

Pós-graduando em Direito Contemporâneo - Curso Jurídico FESP. Bacharel em Direito pela Universidade Tuiuti do Paraná. Vencedor do Prêmio Sydnei Lima Santos concedido pela Faculdade de Ciências Jurídicas da Universidade Tuiuti do Paraná como melhor aluno das turmas 2015-2019.

Resumo: Diante do estrondoso avanço tecnológico em diversas áreas do conhecimento nos últimos anos, em especial, na comunicação, tem-se por relevante perquirir a respeito dos mecanismos de captura de conversações postos à disposição dos operadores do processo penal. O tema das formas de interceptação de comunicações no processo penal brasileiro é importante porque a ideia de se obter provas, por meios tecnológicos, através, apenas, de interceptação telefônica estritamente considerada, em detrimento de outros mecanismos, **não** se revela como a medida mais eficaz no exercício da persecução criminal. Objetiva-se conceituar, analisar a natureza jurídica e delimitar a extensão da interceptação telefônica, *lato sensu*, investigar a evolução da teoria probatória no âmbito das comunicações e apresentar algumas das formas de interceptação de comunicações que vêm sendo admitidas no processo penal brasileiro. Em relação à metodologia, realizou-se pesquisa bibliográfica sobre tema, bem como procedeu-se a exame documental da Constituição da República Federativa do Brasil de 1988, das Leis Federais nº 9.296/96 e nº 13.964/2019, de outros textos legais e de acórdãos do STJ e do STF. Da análise de todo esse material, concluiu-se que, dado o avanço tecnológico da sociedade, bem como a evolução da legislação de regência e da jurisprudência, existe um evidente progresso do processo penal nacional no que diz respeito ao uso de ferramentas para a interceptação de comunicações por meios telefônicos, telemáticos e informáticos, tanto por meio da atuação normativa do Poder Legislativo quanto através do controle de legalidade exercido pelo Poder Judiciário.

Palavras-chave: Interceptação. Comunicações. Tecnologia. Prova. Processo penal brasileiro.

Abstract: Given the tremendous technological advances in several areas of knowledge in recent years, especially in communication, it is relevant to inquire about the available mechanisms for capturing conversations to operators of criminal proceedings. The issue of forms of interception of communications in Brazilian criminal proceedings is important because the idea of obtaining evidence, by technological means, strictly through telephone interception, in detriment of other mechanisms, does not prove to be the most effective measure in the exercise of criminal prosecution. The objective is to conceptualize, analyze the legal nature and delimit the extent of telephone interception, *lato sensu*, investigate the evolution of the proof theory in the field of communications and present some of the forms of interception of communications that have been admitted in the Brazilian criminal process. Regarding the methodology, bibliographical research was carried out on the subject, as well as a documental examination of the Constitution of the Federative Republic of Brazil of 1988, Federal Laws nº 9.296/96 and nº 13.964/2019, of other legal texts and of judgments of the STJ and the STF. From the analysis of all this material, it was concluded that, given the technological advances in society, as well as the evolution of the legislation and jurisprudence, there is an evident progress in the national criminal procedure regarding the use of tools for interception communications by telephone, telematic and computer means, both through the normative action of the Legislative and through the legality control exercised by the Judiciary.

Keywords: Interception. Communications. Technology. Proof. Brazilian criminal procedure.

1 INTRODUÇÃO

Em virtude do avanço tecnológico no âmbito da comunicação evidenciado nas duas primeiras décadas do século XXI, a mera interceptação de conversações telefônicas, nos moldes inicialmente propugnados por meio da Lei nº 9.296/96, editada ainda no fim do século XX, se

revela como medida dotada de pouca efetividade para fins penais, uma vez que cada vez mais as interações interpessoais se dão por novos meios, em especial, pelo uso da *internet*, e isso não é diferente quando se trata da prática de crimes.

Nesse contexto, a questão que se coloca é a seguinte: no âmbito probatório do processo penal brasileiro, além da interceptação telefônica, quais outros mecanismos de captura de comunicações podem ser utilizados?

Com o intuito de responder a essa indagação, objetiva-se: conceituar, bem como analisar a natureza jurídica e a extensão da interceptação telefônica, em sentido amplo; investigar a evolução da teoria probatória no âmbito das comunicações; e apresentar algumas das formas de interceptação de comunicações que vêm sendo admitidas no processo penal brasileiro.

Para tanto, buscou-se pesquisar as recentes inovações legais acerca do assunto, o que leciona a doutrina penal a respeito do tema e qual é o entendimento jurisprudencial das cortes superiores brasileiras sobre essa questão.

A escolha da temática se justifica sobretudo por razões práticas. No aludido cenário social de constante progresso tecnológico, no qual a comunicação se tornou instantânea, é inevitável que os mecanismos que facilitam essa interação interpessoal sejam utilizados para fins escusos. Diante disso, os operadores da seara penal devem ter ciência de quais ferramentas podem igualmente se valer, de conformidade com o Direito, em sua atuação na persecução criminal.

2 CONCEITO, NATUREZA JURÍDICA E EXTENSÃO DA INTERCEPTAÇÃO TELEFÔNICA: ART. 1º, CAPUT E PARÁGRAFO ÚNICO, DA LEI Nº 9.296/96

A título de conceituação, sobre a origem da palavra “interceptar”, bem como sobre sua significação jurídica, Gomes e Maciel (2018, p. 30) lecionam o seguinte:

[...] interceptar (de *intercepto* + *ar*) significa, etimologicamente, interromper no seu curso, deter, impedir na passagem, cortar, reter, empolgar. Do ponto de vista jurídico (mais precisamente na Lei 9.296/96), a palavra “interceptação” não corresponde exatamente ao seu sentido idiomático. Interceptar uma “comunicação telefônica” não quer dizer interrompê-la, impedi-la, detê-la ou cortá-la. Na lei, a expressão tem outro sentido, qual seja, o de captar a comunicação telefônica, tomar conhecimento, ter contato com o conteúdo dessa comunicação enquanto ela está acontecendo. É da essência da interceptação, no sentido legal, a participação de um terceiro. Interceptar comunicação telefônica, assim, é ter conhecimento de uma comunicação “alheia”.

Os citados juristas complementam a ideia exposta ao conceituar interceptação telefônica como sendo a “captação da comunicação telefônica por um terceiro, sem o conhecimento de nenhum dos comunicadores. Essa é a interceptação em sentido estrito (ou seja, um terceiro intervém na comunicação alheia, sem o conhecimento dos comunicadores)” (GOMES e MACIEL, 2018, p. 30).

No mesmo sentido, Cabette (2015, p. 31) assevera que “na interceptação, está ínsita a presença de um terceiro que não seja um dos interlocutores e que, ademais, não lhes seja de conhecimento”.

A questão central do conceito de interceptação telefônica se consubstancia, pois, no fato de que deve haver um terceiro alheio à comunicação feita por meio telefônico que passe a tomar ciência dela sem o conhecimento dos interlocutores e, por corolário, sem a autorização desses.

A interceptação telefônica possui natureza jurídica de medida cautelar processual. Nas palavras de Gomes e Maciel (2018, p. 63), sua natureza é de, “mais precisamente, medida coativa real (não pessoal), consistente numa apreensão imprópria”. Távora e Alencar (2018, p. 767) complementam essa ideia ao expor que “não há propriamente apreensão, mas gravação que viabiliza sua fiel reprodução, possibilitando assim seu conhecimento”. Ou seja, a interceptação apreende os elementos de prova de forma imprópria, indireta, porque seu procedimento ocorre por meio da captação, a distância, de comunicações. Diferentemente do que ocorre, por exemplo, com a busca e apreensão, que é medida cautelar própria, direta, realizada *in loco*.

Ademais, consoante a lição de Lima (2021, p. 538), a interceptação tem natureza cautelar porque visa conservar, para fins processuais, o conteúdo das comunicações capturadas tal como se deram no momento da conversação.

Tratando-se de medida cautelar, deverão estar presentes o *fumus comissi delicti* e o *periculum in mora*. Isto é, a realização de uma interceptação telefônica está condicionada à presença, no caso concreto, de indícios mínimos de autoria ou participação em infração penal do sujeito que terá suas comunicações devassadas. Ademais, deve-se considerar o prejuízo que a demora ou a não realização desse procedimento poderá trazer para a investigação ou para o processo, tendo em vista a produção probatória (LIMA, 2021, p. 538). Não se pode olvidar, é claro, da cláusula de reserva de jurisdição que recai sobre pedido de captura de comunicações, diante do contido no art. 5º, inciso XII, da Constituição da República. Assim, para além da presença dos requisitos acima referidos, a interceptação depende de prévia autorização judicial.

Conforme a lição de Gomes e Maciel (2018, p. 89) a interceptação telefônica é, ainda, medida cautelar *inaudita altera parte*. Isto é, antes de sua realização, não se ouve o sujeito passivo da captura. Do contrário, isto é, se houvesse prévia ciência do investigado acerca do procedimento, certamente não se obteria a prova, de modo que restaria frustrada a eficácia da repressão penal. Desse modo, aduzem os juristas citados, o contraditório acerca da prova obtida por meio da interceptação é diferido.

De acordo com o art. 1º, *caput*, da Lei nº 9.296/96, é possível a interceptação de comunicações telefônicas de qualquer natureza para prova em investigação criminal e em instrução processual penal. Ademais, o parágrafo único desse dispositivo dispõe que a normatização estabelecida pela lei se aplica à interceptação do fluxo de comunicações em sistemas de informática e telemática. É a partir desses contornos legais que se pode perquirir a respeito da extensão e dos limites de aplicação da interceptação telefônica.

Segundo Lima (2021, p. 525), em um passado não muito distante, quando se falava em comunicação telefônica, a única opção que se tinha à mão era uma conversa falada por telefone. Nesse sentido, aliás, o Código Brasileiro de Telecomunicações (Lei nº 4.117/62), em seu art. 4º, definia telefonia como “o processo de telecomunicação destinado à transmissão da palavra falada ou de sons”. Sucedeu que, desde a edição de tal código, houve, como se sabe, um estrondoso avanço tecnológico na vida humana, que aconteceu também, por evidente, em relação à comunicação. Por isso, quando da edição da Lei nº 9.296/96, o legislador optou por disciplinar a captura de comunicações por meios que vão além da comunicação telefônica tradicional, quais sejam, os meios informáticos e telemáticos. A esse respeito, consoante a lição de Jesus (1997, p. 462), “informática é a ciência relativa à informação por intermédio de equipamentos e métodos do sistema de processamento de dados” e, por sua vez, a “telemática é a ciência que versa sobre a informação por meio conjunto de computador e telecomunicação (“tele” de telecomunicação + “mática” de informática)”.

Ocorre que, em virtude da redação do art. 5º, inciso XII, da Carta Magna, desde a edição da

Lei nº 9.296/96, há divergência doutrinária a respeito da constitucionalidade da extensão da aplicação da interceptação telefônica aos meios telemáticos, nos termos do parágrafo único do art. 1º de tal lei.

Dispõe o art. 5º, inciso XII, da Constituição da República, que “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”. A controvérsia que surge a partir dessa redação é de caráter semântico e diz respeito ao alcance da expressão “salvo, no último caso”.

Gomes e Maciel (2018, p. 98) aduzem que a divergência na compreensão do dispositivo constitucional deu causa à criação de duas correntes antagônicas a respeito da compatibilidade, ou não, do parágrafo único do art. 1º da Lei nº 9.296/96 com a Lei Maior: a primeira reclama sua inconstitucionalidade; a segunda sustenta sua constitucionalidade restrita.

A corrente que sustenta a inconstitucionalidade do dispositivo aduz, em síntese, que a Constituição da República somente autorizou a quebra do sigilo das comunicações telefônicas, estritamente consideradas, e não das realizadas por meio de dados, o que envolve comunicações informáticas e telemáticas, sendo o sigilo dos dados, junto com o das correspondências e das comunicações telegráficas, absoluto, de modo que seria ilícita qualquer prova obtida com base na quebra desse último sigilo (GOMES e MACIEL, 2018, p. 98).

Já a corrente que milita pela constitucionalidade restrita do dispositivo argumenta, em resumo, que o parágrafo único do art. 1º da Lei nº 9.296/96 é válido em relação à comunicação telemática feita por telefone, uma vez que, considerando o *caput* da norma, é uma forma de comunicação telefônica, a qual não se limita apenas à conversa telefônica, isto é, a conversa falada entre duas pessoas, de modo que a comunicação de dados, relacionada com a telefonia, é passível de interceptação; porém, a lei não se aplicaria à comunicação que não seja feita através do telefone, como, por exemplo, por meio da *internet*, daí porque se fala de constitucionalidade restrita (GOMES e MACIEL, 2018, p. 98).

Nada obstante, cumpre destacar que, conforme a lição de Gomes e Maciel (2018, p. 98-99), a disposição do parágrafo único do art. 1º da Lei nº 9.296/96 é plenamente legítima, não havendo que se falar em inconstitucionalidade ou, ainda, em constitucionalidade restrita. Os citados autores ensinam que, de acordo com o constitucionalismo moderno, não se questiona se o legislador pode ou não restringir direitos, mas sim se a limitação criada observa os princípios da proporcionalidade e da razoabilidade.

É fato que existem normas constitucionais que indicam expressamente a necessidade de restrição do direito que asseguram – são as chamadas “reservas legais”, como é o caso, por exemplo do próprio art. 5º, inciso XII, da Carta Política – e outras que, por outro lado, nada explicitam a esse respeito. Isso não significa, porém, admitir, em relação a essas últimas, notadamente, que existam direitos absolutos. Isso porque, quando a norma constitucional não delimita restrição expressa ao direito que protege, subsiste a ideia de limites imanentes, isto é, de que para que prevaleça a convivência harmoniosa dos direitos, em particular, daqueles fundamentais, previstos na Constituição, sem que um tenha que deixar de existir para que outro possa valer, todos comportam limitações (GOMES e MACIEL, 2018, p. 99).

Por isso, não se sustentam as posições acima expostas, segundo as quais a Carta Magna autoriza somente a interceptação das comunicações telefônicas estritamente consideradas ou que permite a restrição das mesmas apenas nos meios telefônicos. Ainda que se admitissem essas ideias de limitação parcial do direito fundamental ao sigilo das comunicações, no que diz respeito às comunicações telefônicas, tem-se que o texto constitucional é expresso apenas nesse sentido. Em relação às comunicações por dados, telemáticas e informáticas, a

permissão é implícita, pois, como dito, a existência de limites aos direitos é imanente à ordem jurídica.

Ademais, diante do vertiginoso desenvolvimento da informática na atualidade, não se pode restringir a interceptação somente às comunicações feitas por telefone. A expressão “comunicações telefônicas” contida no *caput* do art. 1º da Lei nº 9.296/96 deve, necessariamente, abranger a transmissão de dados e informações de qualquer natureza por meio de telefonia estática ou móvel, conjugada, ou não, com meios informáticos. Essa posição tem fundamento em uma interpretação progressiva, segundo a qual a despeito das normas jurídicas ingressarem no ordenamento e nele permanecerem, no mais das vezes, com sua descrição inicial, o que de fato importa em uma lei é a *voluntas legis*, que evolui de acordo com a dinâmica dos fatos sociais (LIMA, 2021, p. 525-526).

Nesse sentido, ainda, a lição de Lima (2021, p. 526):

[...] quando a Constituição Federal autoriza a interceptação das comunicações telefônicas, refere-se não só às comunicações telefônicas propriamente ditas como também à comunicação de dados, imagens e sinais através da telemática. Não se pode ficar alheio aos avanços tecnológico-culturais, ampliando as formas de comunicações, privando os órgãos da persecução penal de um importante instrumento de investigação e busca da verdade. Logo, a nosso ver, a Lei nº 9.296/96 tem seu campo de incidência sobre qualquer forma de comunicação, seja telefônica ou não; versa não apenas sobre conversação telefônica, como também qualquer tipo de comunicação telemática (por telefone ou por via independente, sem uso da telefonia).

Desse modo, não admitir a validade do parágrafo único do art. 1º da Lei nº 9.296/96 não apenas representa uma interpretação retrógrada em relação ao avanço tecnológico-cultural do século XXI, como também importa retirar dos órgãos de persecução penal valioso instrumento de apuração de condutas ilícitas. Nesse contexto, precisa é a fala de Gomes e Maciel (2018, p. 94) quando aduzem que “não aceitar a interceptação na comunicação telemática por telefone representa, destarte, não contar com essa medida cautelar para a repressão do crime organizado. Dito de outro modo: o criminoso da era digital estaria fora do alcance do Estado”.

Na senda do exposto, também valendo-se de uma interpretação progressiva da Constituição, Jesus (1997, pg. 464) igualmente se manifesta pela validade da interceptação pelos meios informáticos e telemáticos:

Inclinamo-nos pela constitucionalidade do referido parágrafo único. A Carta Magna, quando excepciona o princípio do sigilo na hipótese de “comunicações telefônicas”, não cometeria o descuido de permitir a interceptação somente no caso de conversação verbal por esse meio, isto é, quando usados dois aparelhos telefônicos, proibindo-a, quando pretendida com finalidade de investigação criminal e prova em processo penal, nas hipóteses mais modernas. A exceção, quando menciona “comunicações telefônicas”, estende-se a qualquer forma de comunicação que empregue a via telefônica como meio, ainda que haja transferência de “dados”. É o caso do uso do modem. Se assim não fosse, bastaria, para burlar a permissão constitucional, “digitar” e não “falar”.

A constitucionalidade do parágrafo único do art. 1º da Lei nº 9.296/96 e, por conseguinte, a possibilidade de captura de comunicações feitas por via informática ou telemática é corroborada, ainda, pela Lei nº 12.965/2014, que instituiu o chamado Marco Civil da *Internet*.

Entre os direitos assegurados por essa lei, segundo Mendes e Pinheiro (2015¹), “restou assegurado aos usuários da *internet* no Brasil não apenas o sigilo do fluxo de comunicações, já regulamentado pela Lei nº 9.296/96, como também a inviolabilidade e o sigilo dos dados armazenados (art. 7º, II e III), tema até então sem legislação específica”.

1 As citações relativas à obra destes autores são feitas seguindo-se o modelo autor/data, porém, sem indicação do número da página do livro, haja vista tratar-se de um livro eletrônico, consultado por meio da plataforma Saraiva Digital, da Editora Saraiva.

Essa legislação, com efeito, em seu art. 7º, inciso II, ao mesmo tempo em que assegura a inviolabilidade e o sigilo do fluxo de comunicações das pessoas pela *internet* – em consonância com o disposto no art. 5º, inciso XII, da Constituição –, ou, em outras palavras, do fluxo de dados veiculados por meio digital, possibilita, por outro lado, a restrição de tais garantias, submetida à cláusula de reserva de jurisdição. Ora, se o marco regulatório para o uso da *internet* no país autoriza que as comunicações feitas por esse meio sejam, excepcionalmente, violadas, mediante autorização judicial, tem-se que subsistir mais um fundamento, previsto em lei, que autoriza concluir pela validade da interceptação de comunicações telemáticas e informáticas.

De acordo com Gomes e Maciel (2018, p. 96), no atual estágio de evolução tecnológica da sociedade, de pouco serviria, do ponto de vista da persecução criminal, autorizar apenas a interceptação de conversas telefônicas. Se assim fosse, conforme a lição de Jesus, acima citada, bastaria ao criminoso digitar ao invés de falar para se livrar da repressão penal, o que, evidentemente, não pode ser admitido, sob pena de se incorrer em gigantesco retrocesso no que diz respeito à tutela penal pelo Estado.

Nesse diapasão, Goldfinger (2021, p. 988-989) aduz que, desde que seja obtida autorização judicial, nos termos da Constituição, toda e qualquer forma de interceptação é possível, tendo em vista que se trata de valioso instrumento de que podem se valer os Estados modernos no combate às práticas criminosas hodiernas, que são facilitadas – como muitos outros aspectos da vida também são – pelo uso da tecnologia.

Analisando o direito comparado, Gomes e Maciel (2018, p. 97) destacam o seguinte:

Não é por acaso, aliás, que as mais avançadas legislações sobre interceptação telefônica preveem sua incidência nas “conversações”, bem como nas “comunicações” telefônicas ou nas “comunicações transmitidas por qualquer meio diferente do telefone” (v. arts. 187 a 190 do CPP português). O art. 266 do CPP italiano, por seu turno, dispõe: “a interceptação de conversações e comunicações telefônicas ou por outro meio de telecomunicação (...)”.

Nos países mais avançados, qualquer forma de comunicação, transmitida por qualquer meio de telecomunicação, pode ser interceptada, isso porque, diante de suas legislações, como nos exemplos acima, toda forma de telecomunicação conta com tutela penal, uma vez que, como se sabe, a informática passou a ser uma grande aliada do mundo criminoso (GOMES e MACIEL, 2018, p. 97).

No Brasil, é importante destacar que a jurisprudência dos tribunais superiores já se manifestou sobre a constitucionalidade do parágrafo único do art. 1º da Lei nº 9.296/96, ou seja, pela possibilidade de extensão da interceptação telefônica às comunicações por meios telemáticos e informáticos. Nesse sentido, destaca-se tanto a posição firmada pelo STJ no julgamento do HC nº 276.132/PR², em 2015, quanto a explicitada pelo STF, no ano de 2018, no julgamento do RHC nº 132.115/PR³.

Ao arremate, cabe salientar que, segundo Martins (1996, p. 97 *apud* Gomes e Maciel, 2018, p. 97), “tudo quanto foi dito em relação à interceptação telefônica tem exata aplicação para a telemática ou informática”, de modo que tanto a conceituação quanto a natureza jurídica alhures referidas, se aplicam, também, para a interceptação telemática e informática.

Portanto, a interceptação regulada pela Lei nº 9.296/96 se estende sobre qualquer forma de comunicação, seja telefônica, telemática ou informática, razão pela qual tem-se por plenamente constitucional o parágrafo único do art. 1º de tal lei.

² STJ, HC 276132/PR, Relator: Ministro Leopoldo de Arruda Raposo – Desembargador convocado do TJ/PE, T5 - Quinta Turma, Data do Julgamento: 18/08/2015, Data da Publicação: DJe 01/09/2015. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201302842937&dt_publicacao=01/09/2015>. Acesso: 10 jul. 2021.

³ STF, RHC 132115/PR, Relator: Ministro Dias Toffoli, Segunda Turma, Data do Julgamento: 06/02/2018, Data da Publicação: 19/10/2018. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=4905003>>. Acesso: 10 jul. 2021.

3 GERAÇÕES DE PROVAS: TRILOGIA OLMSTEAD-KATZ-KYLLO

A partir de três precedentes da Suprema Corte Norte Americana, a doutrina elenca uma classificação de gerações das provas que está ligada à necessidade, ou não, de observância da cláusula de reserva de jurisdição para a realização de certos procedimentos invasivos de investigação.

A primeira geração de direito probatório surgiu a partir do caso *Olmstead*, julgado pela Suprema Corte Norte Americana no ano de 1928. Na situação fática analisada, a polícia havia instalado um equipamento que permitia realizar interceptação telefônica diretamente na fiação da empresa de telefonia, ou seja, em via pública, e o fez sem prévia autorização judicial. Alegou-se que como não houve nenhum tipo de busca dentro da casa de *Olmstead*, não houve, por corolário, violação à sua privacidade. A Suprema Corte, nesse contexto, concluiu que não ocorreu violação de nenhuma propriedade do acusado, sendo, assim, lícita a prova obtida. Nesse primeiro momento, então, restou cunhada a chamada teoria proprietária (*trespass theory*), segundo a qual a proteção constitucional da privacidade das pessoas seria extensível apenas para áreas tangíveis e demarcáveis, de modo que somente a violação de um espaço privado configuraria afronta a tal direito, o que não ocorreu no caso *Olmstead*. Essa é, destarte, uma teoria de proteção de coisas concretas (LIMA, 2021, p. 527).

A segunda geração de direito probatório teve seu precedente no caso *Katz*, julgado em 1967. Nessa situação, a prova dos crimes investigados foi obtida por meio da instalação de um dispositivo de gravação colocado do lado de fora de uma cabine telefônica, que foi, então, utilizada pelo investigado. Partiu-se da premissa oriunda do caso *Olmstead* para assim se obter a prova, pois como a cabine telefônica era pública, não haveria invasão de propriedade privada do acusado, o que dispensaria prévia autorização judicial e tornaria lícita a prova. Contudo, a Suprema Corte, nesse caso, entendeu que apesar de o sujeito haver usado um telefone público, a partir do momento em que ele fechou a porta da cabine e pagou o valor que lhe autorizaria fazer a ligação, o investigado passou a possuir legítima expectativa de proteção de sua privacidade, sendo, pois, ilícita a prova obtida. Assim, a partir desse precedente, a Corte Maior americana alterou seu entendimento, concluindo que a proteção constitucional da intimidade e da vida privada das pessoas não deveria se limitar apenas à salvaguarda de coisas concretas, mas também ao resguardo de declarações orais (coisas imateriais). Houve, portanto, uma migração da teoria proprietária para a teoria da proteção constitucional integral, que ampliou a esfera de tutela da privacidade de apenas coisas tangíveis para pessoas e suas expectativas de não violação de intimidade e vida privada (LIMA, 2021, p. 528).

A terceira geração de direito probatório nasceu em 2001, quando a Suprema Corte Norte Americana se debruçou sobre o caso *Kyllo*. Na situação concreta, a polícia desconfiava que *Kyllo* cultivava maconha dentro de sua residência. Todavia, apesar da suspeita, os elementos informativos colhidos na investigação até então eram muito frágeis para embasar um pedido de expedição de mandado de busca e apreensão. Como a polícia sabia que o cultivo de maconha em ambiente fechado necessitava do uso de lâmpadas de alta intensidade, surgiu a ideia de, da via pública, utilizar um equipamento de captação de ondas térmicas para monitorar a emissão de calor de dentro da casa de *Kyllo*. A partir do uso desse equipamento, a polícia conseguiu obter as evidências necessárias para pedir a expedição de mandado de busca, em razão do qual foram apreendidos diversos pés de maconha dentro da residência do réu. Nesse contexto, a prova obtida poderia ser considerada lícita tanto à luz do caso *Olmstead* quanto do caso *Katz*, pois não houve invasão à residência de *Kyllo* e ele não manifestou nenhuma expectativa de proteção de sua privacidade, pois nada fez para impedir a emissão do calor. Nada obstante, a Suprema Corte Norte Americana concluiu nesse julgamento que os avanços tecnológicos não podem se impor descontroladamente sobre a esfera de proteção da privacidade. Assim, se o Estado pretende se valer de um dispositivo tecnológico que sequer

é de uso geral do público para explorar detalhes de dentro de uma casa que antes seriam totalmente desconhecidos sem uma invasão física (o uso de uma câmera térmica não pode ser comparado ao olhar nu de uma residência), esse uso da tecnologia deveria ser tido por desarrazoado acaso não precedido de autorização judicial. Desse modo, para que o uso do aparato tecnológico moderno não importe em devassa desproporcional à privacidade das pessoas, deve ser submetido à reserva de jurisdição, sob pena das provas obtidas serem taxadas de ilícitas (LIMA, 2021, p. 528).

4 FORMAS DE INTERCEPTAÇÃO DE COMUNICAÇÕES UTILIZADAS NO PROCESSO PENAL BRASILEIRO

Consoante destacado alhures, o art. 1º, *caput*, da Lei nº 9.296/96, explicita que as interceptações telefônicas de qualquer natureza deverão observar os preceitos nela estabelecidos, nisso incluídas as comunicações telemáticas e informáticas, nos termos do parágrafo único do dispositivo legal, cuja constitucionalidade se reafirma. A partir disso, a doutrina evidencia algumas formas diversas de interceptação de comunicações.

Interceptação telefônica, em sentido estrito, é a primeira forma de captura de comunicações que surge à mente quando se pensa sobre o tema. Segundo Lima (2021, p. 523), ela “consiste na captação da comunicação telefônica alheia por um terceiro, sem o conhecimento de nenhum dos comunicadores”. Como exemplo, tem-se a situação em que a autoridade policial realiza a interceptação de uma comunicação telefônica feita entre o líder de uma organização criminosa que explora o tráfico de drogas e um subordinado seu que está em um porto a preparar uma remessa de entorpecentes dentro de um dos contêineres que será enviado para outro continente.

Escuta telefônica, por sua vez, de acordo com Gomes e Maciel (2018, p. 31), “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, quando o pai de uma criança sequestrada autoriza que a autoridade policial intercepte a comunicação telefônica feita com o sequestrador para localizá-lo.

Gravação telefônica, conforme a lição de Lima (2021, p. 523), “é a gravação de comunicação telefônica por um dos comunicadores, ou seja, trata-se de uma autogravação [...]. Normalmente, é feita sem o conhecimento do outro comunicador, daí falar-se em gravação clandestina”. Ocorre, por exemplo, se a vítima de estelionato grava conversa telefônica que teve com o estelionatário durante a qual esse último confessa que praticou o crime.

Interceptação ambiental, por sua vez, consoante ensina Goldfinger (2021, p. 996), “ocorre quando alguém capta a conversa realizada entre duas ou mais pessoas, em qualquer lugar, público ou privado, porém, fora do telefone”. Imagine-se como exemplo a situação em que a autoridade policial instala um gravador em uma praça pública e capta as comunicações feitas por sujeitos que estão traficando drogas.

Escuta ambiental, segundo Gomes e Maciel (2018, p. 31), “é captação de uma comunicação, no ambiente dela, feita por terceiro, com o consentimento de um dos comunicadores”. Cita-se, por exemplo, caso em que a vítima de concussão, com ajuda da autoridade policial, grava conversa pessoal que tem com funcionário público no momento em que esse lhe pede uma vantagem indevida em virtude de sua função.

Gravação ambiental, de acordo com Lima (2021, p. 524), “é a captação no ambiente da comunicação feita por um dos comunicadores”. Ocorre, por exemplo, se o sujeito, ao trafegar

com seu veículo por rodovia acima do limite de velocidade, é parado por policial e grava a conversa que tem com o agente quando este lhe solicita vantagem indevida para não lhe aplicar multa de trânsito.

Segundo Gomes e Maciel (2018, p. 31), somente a interceptação telefônica e a escuta telefônica são objetos da Lei nº 9.296/96, pois somente nesses dois casos tem-se uma comunicação telefônica captada por um terceiro, de modo que as demais situações estão fora da esfera de abrangência da citada lei.

Para os referidos autores, como os demais casos (gravação clandestina e captações ambientais) não são regulamentados pela referida legislação especial, não haveria no Brasil uma lei expressa que os discipline. Assim, considerando que tais hipóteses envolvem, em regra, a quebra da privacidade e do sigilo das comunicações, seriam ilícitas tais formas de captação, por não possuírem base legal de regulação, e também porque a limitação de direitos e garantias fundamentais ou deve decorrer expressamente da Constituição da República, ou deve ser legalmente prevista (GOMES e MACIEL, 2018, p. 34).

No mesmo sentido, Cabette (2015, p. 32) leciona que a Lei nº 9.296/96 não tratou a respeito das gravações clandestinas nem sobre as gravações ambientais. Aduz o jurista que são permitidas as gravações perpetradas por terceiros com o consentimento de um dos interlocutores, isto é, as escutas telefônicas, mas, por outro lado, alega que são ilegais as interceptações ambientais, porque ferem o direito à privacidade (CABETTE, 2015, p. 33).

O posicionamento defendido pelos aludidos juristas foi o originalmente adotado pelo STF. A Corte Maior entendia que tanto as gravações telefônicas quanto as captações ambientais eram ilícitas, conforme restou decidido no âmbito da AP nº 307/DF, no ano de 1994⁴.

No entanto, em 2009, o Pretório Excelso mudou seu entendimento ao julgar o RE nº 583.937/RJ⁵, reconhecendo repercussão geral na matéria afeta à licitude da prova obtida por meio de gravações ambientais, fato que abriu caminho para o reconhecimento da licitude da gravação telefônica, bem como da interceptação e da escuta ambiental.

Destarte, o atual posicionamento jurisprudencial do Supremo Tribunal Federal, segundo Gomes e Maciel (2018, p. 37), é o seguinte: os casos de interceptação telefônica e escuta telefônica subsumem-se às regras da Lei nº 9.296/96 e aquelas só podem ser realizadas e seu conteúdo ser utilizado como prova se obedecerem ao disposto nesse texto legal. Por sua vez, as gravações clandestinas e as captações ambientais, por não estarem dentro do âmbito legislativo da mencionada lei, não dependem de autorização judicial e podem ser lícitamente usadas como prova, exceto se envolverem conversa íntima ou se existir causa legal de sigilo.

Esse entendimento da Corte Suprema vem se mantendo, tanto para a gravação telefônica quanto para as captações ambientais, conforme se constata a partir da análise de sua jurisprudência desde 2009, inclusive a mais recente, dando-se destaque aos julgamentos proferidos no HC nº 91.613/MG⁶, de 2012, e no HC nº 191.873/SE⁷, de 2021.

4 STF, AP nº 307/DF, Relator: Ministro Ilmar Galvão. Datas de Julgamento: 07/12/1994, 09/12/1994, 12/12/1994 e 13/12/1994. Este julgado foi acessado por meio da Revista Trimestral de Jurisprudência do Supremo Tribunal Federal (RTJ), v. 162, de out. 1997, pg. 7 e seguintes). Disponível em: <http://www.stf.jus.br/arquivo/cms/publicacaoRTJ/anexo/162_1.pdf>. Acesso: 15 jul. 2021.

5 STF, RE 583937/RJ, Relator: Ministro Cezar Peluso, Tribunal Pleno, Data do Julgamento: 19/11/2009, Data da Publicação: 18/12/2009. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=2610668>>. Acesso: 15 jul. 2021.

6 STF, HC 91613/MG, Relator: Ministro Gilmar Mendes, Segunda Turma, Data do Julgamento: 15/05/2012, Data da Publicação: 17/09/2012. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=2526322>>. Acesso: 17 jul. 2021.

7 STF, HC 191873/SE AgR, Relatora: Ministra Cármen Lúcia, Segunda Turma, Data do Julgamento: 17/02/2021, Data da Publicação: 18/02/2021. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=6012514>>. Acesso:

No mesmo sentido, vem reiteradamente decidindo o Superior Tribunal de Justiça ao longo dos últimos anos, consoante se denota, a título de exemplo, do HC nº 94.945/SP⁸, de 2010, e do AgRg no HC nº 549.821/MG, de 2019⁹.

Diante disso, verifica-se que, para além da interceptação telefônica, cuja realização e regulamentação é expressamente prevista em lei, e para além da escuta telefônica, que, de acordo com a doutrina, também se insere no contexto legal da interceptação, a utilização das demais formas de captura de comunicações é autorizada pela jurisprudência dos tribunais superiores, o que amplia os meios de obtenção de prova no contexto processual penal brasileiro.

Em relação às captações ambientais, sua aceitação pela jurisprudência dos tribunais superiores acabou por ser chancelada pelo legislador com o advento da Lei nº 13.964/2019 (o chamado “Pacote Anticrime”), que incluiu na Lei nº 9.296/96 regulamentação específica para a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos.

Segundo Lima (2021, p. 558), “a expressão captar deve ser compreendida como o ato de tomar conhecimento do conteúdo de comunicação alheia”. Quanto ao ponto, a escolha da expressão “captação”, pelo legislador, revela-se semanticamente mais precisa do que a “interceptação” aludida no art. 1º da Lei nº 9.296/96. Isso porque, como já visto, a palavra interceptar, na lei, não tem seu sentido idiomático de deter, cortar, interromper, mas sim de tomar ciência de uma comunicação alheia, isto é, captá-la, de modo que a terminologia da Lei nº 13.964/2019 mostra-se mais acurada.

Goldfinger (2021, p. 1082-1083) aponta uma divergência doutrinária acerca do fundamento constitucional das captações ambientais. Para a primeira corrente, como tais formas de intromissão em comunicação alheia são feitas em meio ao ambiente, isto, é, em recintos públicos ou privados, e não envolvem, pois, conversação telefônica, não lhes seria aplicável o regime insculpido no art. 5º, inciso XII, da Constituição, mas sim o regime geral de proteção da privacidade contido no art. 5º, inciso X, da Carta Magna, a partir do qual caberia a análise da licitude, ou não, de tais meios de obtenção de prova. Para a segunda corrente, por outro lado, as captações ambientais seriam inconstitucionais, ao argumento de que o art. 5º, inciso XII, da Lei Maior, autorizou apenas a quebra do sigilo das comunicações telefônicas, na forma da lei, razão pela qual não seria possível que o legislador infraconstitucional ampliasse os marcos traçados para o fim de criar limitações a direitos fundamentais que a Carta Política não previu.

Essa tese de inconstitucionalidade, *data venia*, consubstancia interpretação retrógrada como aquela afeta ao parágrafo único do art. 1º da Lei nº 9.296/96. Com efeito, admiti-la representaria outra forma de privação dos órgãos de persecução penal de importantes e modernos mecanismos de investigação. Aplica-se aqui aquilo já dito com relação à ideia de limites imanentes, ou seja, não se questiona se o legislador pode ou não restringir direitos, mas sim se o faz de forma a razoável e proporcional, a fim de que todos coexistam harmonicamente, pois todos os direitos comportam limitações.

Por outro lado, consoante a lição de Lima (2021, p. 561), diferentemente da captura de comunicações telefônicas, que sempre deve ser precedida de autorização judicial, nos termos do art. 5º, inciso XII, da Constituição, não é toda captura de comunicações ambientais que se submete à cláusula de reserva de jurisdição, tendo em vista que, nesse caso, por não se falar

17 jul. 2021.

8 STJ, HC 94945/SP, Relatora: Ministra Laurita Vaz, T5 - Quinta Turma, Data do Julgamento: 03/08/2010, Data da Publicação: Dje 23/08/2010. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200702745470&dt_publicacao=23/08/2010>. Acesso: 17 jul. 2021.

9 STJ, AgRg no HC 549821/MG, Relator: Ministro Jorge Mussi, T5 - Quinta Turma, Data do Julgamento: 17/12/2019, Data da Publicação: Dje 19/12/2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903632364&dt_publicacao=19/12/2019>. Acesso: 17 jul. 2021.

em comunicação telefônica, o direito em questão é o afeto à privacidade, conforme o art. 5º, inciso X, da Carta Magna.

De toda forma, o legislador optou por disciplinar a captação ambiental na mesma lei da interceptação telefônica, apesar dos fundamentos constitucionais diversos, o que, todavia, não inviabiliza a coexistência de ambos os institutos.

A captação ambiental pressupõe a participação de um terceiro, que passa a tomar conhecimento do conteúdo de uma conversa feita por duas ou mais pessoas, em geral, sem o conhecimento dessas. De acordo com Lima (2021, p. 559), existem diversas maneiras de se captar uma comunicação feita presencialmente entre duas pessoas, como, por exemplo:

[...] ingresso e permanência no local de pessoas que, portando instrumentos apropriados para a captação da comunicação, escondem a própria presença dos interlocutores; participação direta em conversa por operadores que portam consigo instrumentos apropriados para a captação da comunicação, oportunamente escondidos; ocultação no ambiente de dispositivos microscópicos ligados a aparelhos de captação e registros externos, instalados próximo ao local onde a interceptação for realizada.

Sobre a extensão da disciplina legal da captação ambiental, Lima (2021, p. 559) leciona que, de forma semelhante ao que ocorre com o art. 1º da Lei nº 9.296/96 em relação à interceptação e à escuta telefônica, o art. 8º-A inserido na Lei de Interceptação Telefônica pelo Pacote Anticrime abrange tanto a interceptação quanto a escuta ambiental, uma vez que ambas se consubstanciam em formas de captação de comunicação alheia por um terceiro.

Por outro lado, a gravação ambiental não é albergada pelo novo dispositivo da Lei nº 9.296/96, pois não envolve a intromissão de terceiro na comunicação, mas apenas a gravação da conversa por um dos interlocutores (LIMA, 2021, p. 559). Nada obstante, a gravação ambiental, conforme já dito, é tida pela jurisprudência das altas cortes brasileiras como meio lícito de obtenção de prova – ressalvadas as hipóteses de conversa íntima ou se existir causa legal de sigilo. A própria Lei nº 13.964/2019 corrobora esse entendimento, na medida em que ao incluir o crime tipificado no art. 10-A da Lei de Interceptação Telefônica estabelece no §1º desse dispositivo que não há crime quando a captação é realizada por um dos interlocutores.

Ainda sobre as captações ambientais, em virtude de sua base constitucional, assentada sobre o direito à intimidade e à vida privada, consoante acima referido, importa destacar que nem sempre será necessária autorização judicial para sua realização.

Com efeito, não é necessária autorização judicial prévia para realizar interceptação ambiental em local público, como, por exemplo, ruas, praças, parques etc., ou em local que apesar de particular é aberto ao público, como cinemas, teatros, *shoppings*, estádios de futebol etc. Ora, se os interlocutores desejassem privacidade ou certeza de que não seriam ouvidos por ninguém, deveriam recolher-se a ambiente privado. Se dois sujeitos estão a discutir em uma rua de seu bairro e um deles acaba por sacar uma arma e atirar contra o outro, sendo o fato filmado por uma câmera de segurança, há de ser reputada válida essa forma de captação ambiental, pois quem pratica um delito em via pública não possui nenhuma expectativa de proteção de privacidade. O mesmo vale para os ambientes particulares abertos ao público, pois esses, apesar de privados, não se destinam ao uso exclusivos dos proprietários, mas sim do público em geral. Admitir o inverso, isto é, que uma captura de comunicação ambiental nesse contexto dependesse de prévia autorização judicial importaria no absurdo de se exigir prévia autorização judicial para a instalação de câmeras de segurança em qualquer ambiente público ou aberto ao público, o que, por evidente, revela-se descabido (LIMA, 2021, p. 560-561).

Por outro lado, se o que se pretende é a captação ambiental de conversa mantida em ambiente estritamente privado, revela-se necessária prévia autorização judicial para tanto, porquanto

além de, nesse caso, haver violação da privacidade alheia, há também, por vezes, o ingresso em domicílio alheio, cuja inviolabilidade também é constitucionalmente assegurada (art. 5º, inciso XI, da Constituição). Assim, se a autoridade policial pretende interceptar comunicação feita entre os moradores de certa casa, sob a suspeita de que lá são mantidos entorpecentes para tráfico, deverá obter autorização judicial prévia para realizar a diligência, sob pena de a prova eventualmente obtida a partir desse recurso tecnológico ser taxada de ilícita (LIMA, 2021, p. 560-561).

A mesma ideia é aplicável à hipótese de captação de comunicação ambiental mantida em local público, porém quando uma das partes envolvidas pede sigilo à outra durante a conversação. Ou seja, nesse caso, também é necessária prévia autorização judicial para a captura. Isso porque trata-se de situação em que é exigida por uma das partes, expressamente, o respeito à privacidade, havendo, pois, legítima expectativa de que isso seja observado. Como exemplo dessa hipótese, cita-se o caso de uma entrevista concedida por uma investigada a um repórter de determinada emissora de televisão. A entrevistada concordou em realizar a gravação em local aberto ao público, porém, sucedeu que um diálogo privado entre a ela e seu advogado foi indevidamente captado pelo repórter da emissora. Diante da legítima expectativa da investigada de ter sua conversa com o patrono de modo privado, considerando, ainda, a prerrogativa para tanto de que goza a advocacia, essa gravação, que foi posteriormente usada como prova no processo, foi considerada ilícita (LIMA, 2021, p. 560-561).

Ainda no contexto de formas de captação de comunicações, importa destacar a possibilidade de acesso das autoridades penais aos dados e às comunicações feitas por meio do uso dos *smartphones*. À luz do parágrafo único do art. 1º da Lei nº 9.296/96, a captura dos dados transmitidos por meio de aplicativos, como o *Whatsapp*, revela-se plenamente possível no atual contexto probatório do processo penal brasileiro. Cumpre ressaltar, porém, que por se tratar de hipótese que também restringe a privacidade e o sigilo das comunicações, deve ser observada a cláusula de reserva de jurisdição.

Em relação a essa questão, é interessante notar que o STJ, em um primeiro momento, entendia que o acesso, pela polícia, às mensagens e dados armazenados em celular de pessoa investigada não constituía prova ilícita, pois para a Corte Superior não havia, em tais casos, propriamente, interceptação telefônica, de modo que não era exigida autorização judicial. Cita-se como exemplo desse entendimento o julgamento proferido no HC nº 210.746/SP¹⁰, de 2012.

Nada obstante, em um segundo momento, mais recente, o STJ mudou seu posicionamento, passando a não mais admitir que a polícia tenha acesso, sem prévia ordem judicial, aos dados e mensagens registrados no aparelho celular de pessoa investigada, conforme restou decidido, por exemplo, no bojo do RHC nº 77.232/SC¹¹, julgado em 2017.

Segundo Gomes e Maciel (2018, p. 53), a Corte Cidadã fazia uma distinção entre comunicação atual, isto é, que acontece no presente, e que, por isso, só podia ser interceptada mediante ordem judicial prévia, e comunicação antiga, ou seja, que já terminou e que estava armazenada em um aparelho qualquer, cujo acesso prescindia de autorização judicial. Todavia, ainda segundo os citados autores, “ocorre que agora o art. 7º, III, da Lei nº 12.965/2014 (Lei do Marco Civil da *Internet*) expressamente exige ordem judicial para o acesso das ‘*comunicações privadas armazenadas*’, não tendo mais cabimento a distinção outrora realizada pela Corte Superior”.

10 STJ, HC 210746/SP, Relator: Ministro Gilson Dipp, T5 - Quinta Turma, Data do Julgamento: 26/06/2012, Data da Publicação: Dje 01/08/2012. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201101442875&dt_publicacao=01/08/2012>. Acesso: 20 ago. 2021.

11 STJ, RHC 77232/SC, Relator: Ministro Felix Fischer, T5 - Quinta Turma, Data do Julgamento: 03/10/2017, Data da Publicação: Dje 16/10/2017. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201602706592&dt_publicacao=16/10/2017>. Acesso: 20 ago. 2021.

Desse modo, na atualidade, o STJ se posiciona no sentido de que são nulas as provas obtidas por meio de acesso aos dados e às conversas mantidas via *Whatsapp* pelo autor de determinado fato delituoso sem prévia autorização judicial.

Quanto à posição do STF sobre o tema, de acordo com Mendes e Pinheiro (2015), a jurisprudência do Pretório Excelso consagrava a orientação de que o uso de dados armazenados não configurava violação ao art. 5º, inciso XII, da Constituição, uma vez que o objeto de tutela desse dispositivo constitucional é a comunicação de dados e não os dados em si considerados. Nesse sentido: “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. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)¹²”.

Todavia, com o advento do Marco Civil da *Internet*, restou assegurado não apenas o direito ao sigilo do fluxo de comunicações – já objeto de regulação pela Lei da Interceptação Telefônica – como também a inviolabilidade e o sigilo dos dados armazenados, nos termos do art. 7º, inciso III, da Lei nº 12.965/2014, de modo que sua captação passou a depender de prévia autorização judicial.

Assim, ainda consoante a lição de Mendes e Pinheiro (2015):

[...] diante da clara proteção, pela nova lei, do sigilo dos dados armazenados em sistemas de tecnologia da informação e tendo em conta, por outro lado, o grande volume de informações sobre a vida privada armazenado nos mais diversos dispositivos com conexão à internet, como tablets e smartphones, entre outros, afigura-se necessário que o acesso aos dados armazenados em tais dispositivos seja precedido de autorização judicial específica e circunstanciada.

Como regra geral, portanto, tem-se que a devassa das comunicações e dos dados constantes de aparelho celular, como mensagens de texto e conversações por meio de aplicativos, é permitido, submetendo-se, porém, à cláusula de reserva de jurisdição, tendo em vista a proteção constitucional das comunicações por dados. Essa possibilidade é, na senda do exposto, reforçada pelas disposições do parágrafo único do art. 1º da Lei nº 9.296/96 e pelo art. 7º, incisos II e III, da Lei nº 12.965/2014.

Nada obstante, para determinados casos, a jurisprudência, notadamente do STJ, dadas as particularidades, apresenta soluções diversas da regra geral, fazendo a necessária distinção entre situações concretas que não devem receber a mesma abordagem.

Nesse sentido, não é necessária prévia autorização judicial para que se tenha acesso aos dados do telefone de pessoa falecida. Ora, se o detentor do direito ao sigilo de comunicações está morto, não há mais sigilo a ser tutelado. Se a pessoa foi vítima de homicídio, o acesso aos dados de seu aparelho celular não configura devassa indevida à sua privacidade, mas sim meio de investigação que pode levar à punição do culpado, razão pela qual não se exige autorização judicial para acesso aos dados nesse caso. (LIMA, 2021, p. 530). A esse respeito, já decidiu o STJ que não é ilegal a perícia feita pela polícia em telefone “na hipótese em que seu proprietário - a vítima - foi morto, tendo o referido telefone sido entregue à autoridade policial por sua esposa, interessada no esclarecimento dos fatos que o detinha, pois não havia mais sigilo algum a proteger do titular daquele direito¹³”.

12 STF, RE 418416/SC, Relator: Ministro Sepúlveda Pertence, Tribunal Pleno, Data do Julgamento: 10/05/2006, Data da Publicação: DJ 19/12/2006. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=2205705>>. Acesso: 25 ago. 2021.

13 STJ, RHC 86076/MT, Relator: Ministro Sebastião Reis Júnior, Relator para acórdão Ministro Rogério Schietti Cruz, T6 - Sexta Turma, Data do Julgamento: 19/10/2017, Data da Publicação: DJe 12/12/2017. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201701528146&dt_publicacao=12/12/2017>. Acesso: 04 ago. 2021.

A depender da situação fática analisada, havendo fundamento bastante que possa justificar a urgência da medida, em caráter excepcional, não se reputa ilícito o acesso imediato das autoridades policiais aos dados armazenados em telefone celular, isto é, feito sem prévia autorização do juízo competente (LIMA, 2021, p. 530). Essa hipótese, mais ampla, deve ser cuidadosamente analisada no caso concreto, pois somente se justifica em situações evidentemente excepcionais. Nesse caso, segundo a jurisprudência do STJ, a regra geral de submissão da quebra do sigilo de dados à cláusula de reserva de jurisdição é mantida, “se da hipótese não se depreende qualquer fundamento que possa justificar a urgência, em caráter excepcional, do acesso imediato das autoridades policiais aos dados armazenados no aparelho celular¹⁴”. Desse citado precedente extrai-se, inclusive, exemplo para elucidar a hipótese: em um caso de extorsão mediante sequestro, a polícia encontra celulares esquecidos no cativeiro recém-abandonado, de modo que o acesso imediato da autoridade policial aos dados e mensagens contidas no aparelho pode ser decisivo para a libertação dos reféns, circunstância essa, excepcional, diga-se, que justificaria a devassa do sigilo sem prévia autorização judicial.

Quando a materialidade delitiva resta incorporada no próprio telefone, não há necessidade de prévia autorização judicial para acesso aos dados (LIMA, 2021, p. 530). Nesse sentido, decidiu o STJ em caso envolvendo a transmissão de foto íntima de adolescente por meio do *Whatsapp* que “quando se tratar do próprio corpo de delito, ou seja, quando a própria materialidade do crime se encontrar plasmada em fotografias que são armazenadas naquele aparelho, como na espécie, a autorização judicial não será imprescindível¹⁵”, traçando, assim, outra hipótese de distinção da regra geral.

Havendo autorização do proprietário do aparelho celular, também não há que se falar em ilicitude da consulta pelas autoridades envolvidas na persecução penal aos dados contidos no telefone, pois se foi dada permissão para o acesso pelo próprio titular do direito, desnecessária se mostra a prévia autorização judicial (LIMA, 2021, p. 530). Em precedente firmado sobre a hipótese, o STJ destacou que “policiais acessaram as conversas telefônicas do aparelho celular do paciente sem autorização judicial, mas com a permissão do acusado, o que, de fato, não configuraria a ilegalidade¹⁶”.

Também há distinção da regra geral de submissão da quebra do sigilo de dados à cláusula de reserva de jurisdição na hipótese em que, por ocasião de uma abordagem policial, o sujeito abordado negue ser dono de um celular encontrado próximo dele, o qual, assim, é tido por abandonado em via pública, circunstância que autoriza os policiais a acessarem, de imediato, os dados do aparelho a fim de identificar a propriedade do bem (LIMA, 2021, p. 531). A esse respeito, decidiu o STJ que: “diante dessa específica particularidade do caso concreto (negativa do acusado de que o celular lhe pertencesse), deve ser mantido o afastamento da suposta ilicitude das provas obtidas a partir do acesso pelos policiais às informações contidas no referido aparelho celular apreendido¹⁷”.

Ainda, se o acesso a dados contidos em aparelho de telefone for restrito aos registros telefônicos, isto é, de ligações feitas e recebidas, e à agenda de contatos, não se configura

14 STJ, RHC76324/DF, Relatora: Ministra Maria Thereza de Assis Moura, T6 - Sexta Turma, Data do Julgamento: 14/02/2017, Data da Publicação: DJe 22/02/2017. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201602508220&dt_publicacao=22/02/2017>. Acesso: 04 ago. 2021.

15 STJ, RHC 108262/MS, Relator: Ministro Antônio Saldanha Palheiro, T6 - Sexta Turma, Data do Julgamento: 05/09/2019, Data da Publicação: DJe 09/12/2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201900423026&dt_publicacao=09/12/2019>. Acesso: 04 ago. 2021.

16 STJ, HC 537274/MG, Relator: Ministro Leopoldo de Arruda Raposo – Desembargador convocado do TJ/PE, T5 - Quinta Turma, Data do Julgamento: 19/11/2019, Data da Publicação: DJe 26/11/2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201902971596&dt_publicacao=26/11/2019>. Acesso: 04 ago. 2021.

17 STJ, AgRg no AREsp 1573424/SP, Relator: Ministro Reynaldo Soares da Fonseca, T5 - Quinta Turma, Data do Julgamento: 08/09/2020, Data da Publicação: DJe 15/09/2020. Disponível em: <<https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/>>

devassa ao direito ao sigilo, uma vez que esses dados não estão albergados pela cláusula de reserva de jurisdição do art. 5º, inciso XII, da Constituição da República (LIMA, 2021, p. 531). O STJ já decidiu nesse sentido: “a Corte local informou ter havido acesso aos registros telefônicos e à agenda do aparelho celular apreendido com um dos envolvidos, dados esses não abarcados pela reserva de jurisdição prevista no art. 5º, XII, da Constituição Federal, não podendo se falar em ilegalidade da referida prova¹⁸”.

Dentro de um contexto moderno envolvido pela terceira geração de direito probatório (precedente *Kyllo*), em que o uso da tecnologia pelo Estado para fins de investigação e instrução criminal, para ser legítimo, deve passar por prévio controle judicial, em virtude da tutela constitucional da privacidade e do sigilo das comunicações, a autorização legal contida no art. 1º, caput e parágrafo único, da Lei nº 9.296/96, para quebra do sigilo das comunicações telefônicas, telemáticas e informáticas, reafirmada e ampliada pelo legislador por meio da Lei nº 13.964/2019, e corroborada pela jurisprudência das cortes superiores – que, ainda, realiza as necessárias distinções em determinados casos concretos –, evidencia o avanço do processo penal brasileiro com relação ao uso dos modernos mecanismos de obtenção de provas. Este progresso demonstra que é possível aliar o respeito aos direitos e garantias fundamentais protegidos pelo texto constitucional com a evolução do direito probatório, em um cenário em que a tecnologia auxilia tanto a prática de crimes quanto a sua repressão.

CONSIDERAÇÕES FINAIS

O legislador constituinte foi muito perspicaz, ainda em 1988, ao assegurar como direito fundamental a proteção do sigilo das comunicações de forma ampla, abrangendo as realizadas por meios postais, telegráficos, telefônicos e por dados. À época, ainda eram mais comuns as interações através de cartas e telegramas e os telefonemas certamente representavam meio de comunicação extremamente eficaz. Não obstante, o futuro das comunicações por meio dos dados por certo já apresentava seus primeiros sinais.

Quando do surgimento da Lei nº 9.296, em 1996, as comunicações por meio de dados já se manifestavam de maneira incipiente, com o início da *internet* e o avanço da telemática com o surgimento dos primeiros celulares. Ainda assim, a lei foi editada em um período histórico no qual a sociedade permanecia muito vinculada ao uso dos aparelhos telefônicos tradicionais, representando, naquela época, pois, um importante mecanismo de obtenção de provas na seara penal.

Ocorre que, a partir do início dos anos 2000, a evolução da tecnologia em várias áreas do conhecimento humano foi tamanha que proporcionou uma revolução social. A comunicação foi uma dessas áreas incrivelmente afetadas. Com efeito, o avanço propiciado pela utilização da *internet* e dos *smartphones* trouxe a sociedade até o momento atual, em que as comunicações por meio de cartas, telegramas e até mesmo telefonemas se tornaram praticamente obsoletas. O que impera, hoje, são as interações feitas por meios telemáticos e informáticos.

E é certo que as modernas formas de comunicação não são usadas apenas para fins legítimos, mas senão, também, visando a prática de crimes. A criminalidade, enquanto parte integrante da sociedade, avança à medida que essa última também progride, e é evidente que não ficaria alheia às novas possibilidades que se abriam para o cometimento de ilícitos com o uso da tecnologia.

18 STJ, AgRg no AREsp 1853702/RS, Relator: Ministro Reynaldo Soares da Fonseca, T5 - Quinta Turma, Data do Julgamento: 23/06/2020, Data da Publicação: Dje 30/06/2020. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903748407&dt_publicacao=30/06/2020>. Acesso: 04 ago. 2021.

Por isso, não se pode admitir que o Estado, responsável, em última análise, pela manutenção da paz social, fique alheio ao avanço dos mecanismos tecnológicos, pois se de um lado eles podem ser utilizados para a prática de delitos, de outro, podem igualmente ser usados para sua investigação e punição. É nesse moderno contexto da persecução penal que tanto o Poder Legislativo quanto o Poder Judiciário vêm reconhecendo a importância de garantir aos agentes envolvidos com a repressão criminal uma maior gama de ferramentas de combate às infrações penais.

Nesse sentido, sob a perspectiva legislativa, a despeito da controvérsia semântica existente a respeito do art. 5º, inciso XII, da Constituição, isto é, se somente o sigilo das comunicações telefônicas poderia ser quebrado mediante ordem judicial ou se também seria autorizada a devassa do sigilo dos dados, o fato é que, por não existirem direitos absolutos, a discussão não deve se concentrar no ponto de determinado direito ser, ou não, passível de limitação, mas sim na questão atinente à proporcionalidade e à razoabilidade da restrição.

Malgrado a redação controversa, o art. 5º, inciso XII, da Carta Magna, é claro ao autorizar a quebra do sigilo de comunicações mediante prévia ordem judicial e para fins de investigação ou instrução processual penal, na forma que a lei estabelecer. A lei em questão é a Lei nº 9.296/96, que em seu art. 1º, *caput*, autorizou a interceptação de comunicações telefônicas de qualquer natureza e, ainda, em seu art. 1º, parágrafo único, expandiu as hipóteses de interceptação para as comunicações feitas por meios telemáticos e informáticos.

Diante disso, considerando que inexistem direitos absolutos e que o atual estágio evolutivo da sociedade baseia suas comunicações, justamente, em mecanismos telemáticos e informáticos, se revela razoável e proporcional que o legislador autorize, também, para além da mera – e já quase obsoleta – interceptação de conversas telefônicas, a captura de comunicações pelos meios modernos.

A ideia de que existem limites imanentes aos direitos e de que as leis devem ser interpretadas de forma progressiva é de suma importância, pois se a sociedade evolui de forma cada vez mais ampla e rápida, os direitos e as leis não podem permanecer engessados no tempo e no espaço, sob pena de sucumbirem e não mais atenderem aos fins a que se destinam.

Por isso é que se entende não só como constitucional, mas também como necessária, a previsão do art. 1º, parágrafo único, da Lei nº 9.296/96, isto é, de que são plenamente válidas perante o ordenamento jurídico pátrio as interceptações de comunicações feitas por meios telemáticos e informáticos. Acredita-se que adotar pensamento diverso, com o devido respeito, representa uma interpretação retrógrada não apenas em termos sociais, mas também com relação aos desideratos do Poder Constituinte Originário de 1988, uma vez que os direitos devem ser analisados sempre em uma perspectiva de evolução, dado que são estabelecidos para tutelar uma sociedade que está, igualmente, em constante mudança.

A atuação legislativa sobre o tema também progrediu, tendo em vista que, em 2019, com o advento da Lei nº 13.964/2019, adveio a regulamentação das capturas ambientais, incluída na Lei nº 9.296/96. Essas hipóteses de captura de comunicações, agora previstas em lei, vêm para corroborar a ideia de que todos os direitos comportam limitação, obviamente, dentro dos limites constitucionais e legais. E vêm, ainda, para reforçar as possibilidades de atuação das forças de persecução penal, tendo em vista que a existência de permissivo legal que autorize os agentes da seara criminal a, legalmente, realizar, por exemplo, interceptações de comunicações presenciais ou gravações ambientais ópticas de atividades criminosas, se coaduna muito melhor com os anseios por um processo penal moderno do que deixar que se valessem, ainda, apenas, de capturas de conversas telefônicas.

Sob a perspectiva judicial, por sua vez, os avanços já reconhecidos de forma normativa pelo Poder Legislativo são ampliados pela jurisprudência das altas cortes brasileiras. Com efeito, conforme explicitado, já de algum tempo são reconhecidas como válidas ferramentas como gravações telefônicas e ambientais. Ainda, a jurisprudência corrobora o entendimento de que são válidas as interceptações de dados – já autorizadas pela lei, repita-se –, em especial, no que tange aos aplicativos de troca de mensagens, como, por exemplo, principalmente, o *Whatsapp*, que pode se revelar como importante fonte de prova, notadamente no que diz respeito ao crime organizado e aos delitos cometidos pelos meios virtuais.

O Poder Judiciário, nesse contexto, ainda, exerce o controle de legalidade das capturas de comunicações, porquanto, embora permitidas em amplo espectro, ainda envolvem a quebra de direitos fundamentais, razão pela qual, devem ser precedidas, via de regra, de prévia autorização judicial. Até nesse ponto se revela fundamental a atuação judiciária, pois também são as cortes nacionais que firmam precedentes de distinção da hipótese geral, nas quais se possibilita a devassa de dados alheios sem a obrigatoriedade de observância da cláusula de reserva de jurisdição.

Portanto, não obstante a evolução tecnológica da sociedade gere, na mesma medida, a evolução de um dos fatores que tenta fragilizá-la, qual seja, o crime, é certo que é plenamente possível, dentro das regras do jogo constitucional, aparelhá-la com as ferramentas adequadas para combater as práticas lesivas ao seu desenvolvimento.

REFERÊNCIAS

- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso: diversos acessos entre mai. e ago. 2021.
- BRASIL. **Lei nº 4.117, de 27 de agosto de 1962**. Institui o Código Brasileiro de Telecomunicações. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L4117.htm>. Acesso: 20 mai. 2021.
- BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso: diversos acessos entre mai. e ago. 2021.
- BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso: 19 ago. 2021.
- BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso: diversos acessos entre jul. e ago. 2021.
- CABETTE, Eduardo Luiz Santos. **Interceptação telefônica**. 3. ed. São Paulo: Saraiva, 2015.
- GOLDFINGER, Fábio Ianni. Interceptação telefônica – Lei nº 9.296/96. In: CUNHA, Rogério Sanches; PINTO, Ronaldo Batista; SOUZA, Renne do Ó. **Leis penais especiais: comentadas**. 4. ed., rev. atual. e ampl. Salvador: Ed. JusPodivm, 2021.
- GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica e das comunicações de dados e telemáticas: comentários à Lei 9.296/96**. 4. ed. rev. atual. e ampl. São Paulo: Editora Thomson Reuters Brasil, 2018.
- JESUS, Damásio Evangelista de. Interceptação de comunicações telefônicas – notas à Lei nº 9.296/96. **Revista dos Tribunais**, vol. 735/1997, p. 458 – 473, jan. 1997.
- LIMA, Renato Brasileiro de. **Legislação criminal especial comentada: volume único**. 9. ed. rev., atual. e amp. Salvador: Editora JusPodivm, 2021.
- MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord). **Direito, inovação e tecnologia** [livro eletrônico]. v.1. São Paulo, Saraiva, 2015.
- TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 13. ed. rev. e atual. Salvador: Editora JusPodivm, 2.