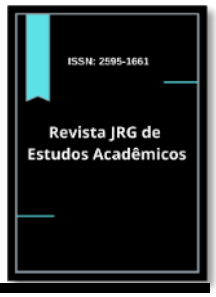
ISSN: 2595-1661

ARTIGO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



Interceptação telefônica, ambiental e *hacking* policial: equilíbrio ou abuso?

Telephone interception, environmental and police hacking: balance or abuse?

DOI: 10.55892/jrg.v8i19.2814
ARK: 57118/JRG.v8i19.2814

Recebido: 15/12/2025 | Aceito: 23/12/2025 | Publicado *on-line*: 26/12/2025

Thalles Renato Alcântara da Silva[1]
https://orcid.org/0009-0003-6741-7337
http://lattes.cnpq.br/4622219987537476
Universidade Federal da Bahia – Salvador/BA, Brasil
thalles-renato@live.com

Selma Pereira de Santana[2]
https://orcid.org/0000-0002-2597-4595
http://lattes.cnpq.br/1410037874765018
Universidade Federal da Bahia – Salvador/BA, Brasil
selmadesantana@gmail.com

Resumo

O presente artigo analisa os limites da investigação policial no contexto das interceptações ambientais e do *hacking*, como resposta ao crime organizado. Através do método de pesquisa bibliográfico, discute-se a compatibilidade dessas técnicas com os direitos fundamentais, especialmente o direito à privacidade e à intimidade. São abordadas as decisões da Suprema Corte Americana e do Supremo Tribunal Federal brasileiro sobre interceptações telefônicas, ambientais e o sigilo das comunicações, ressaltando os desafios impostos pela evolução tecnológica. Também se investiga a constitucionalidade da Lei de Interceptações (Lei nº 9.296/1996) e a possibilidade de adoção de *hacking* policial como alternativa à dificuldade de acesso a comunicações criptografadas. O estudo conclui que a modernização das técnicas investigativas é necessária, mas deve ser acompanhada de um controle rigoroso para garantir a proporcionalidade e a legalidade na aplicação dessas medidas.

Palavras-chave: Interceptação ambiental, *hacking* policial, privacidade, investigação criminal, crime organizado.

[1] Mestrando em Direito pela Universidade Federal da Bahia. Graduado em Direito e em Humanidades pela Universidade Federal da Bahia. Email: thalles-renato@live.com

[2] Professora Titular da Faculdade de Direito da Universidade Federal da Bahia. Procuradora de Justiça do Ministério Público Militar da União. Doutora em Ciências Jurídico-Criminais pela Faculdade de Direito da Universidade de Coimbra/Portugal (2006). Mestre em Ciências Jurídico-Criminais por esta última Faculdade (2002). Email: selmadesantana@gmail.com

Abstract
This article analyzes the limits of police investigation in the context of environmental interceptions and hacking as a response to organized crime. Using case law and bibliographic research, the article discusses the compatibility of these techniques with fundamental rights, especially the right to privacy and intimacy. The article addresses decisions by the American Supreme Court and the Brazilian Supreme Federal Court on telephone and environmental interceptions and the secrecy of communications, highlighting the challenges posed by technological developments. The article also investigates the constitutionality of the Wiretapping Law (Law No. 9,296/1996) and the possibility of adopting police hacking as an alternative to the difficulty of accessing encrypted communications. The study concludes that modernization of investigative techniques is necessary, but must be accompanied by rigorous control to ensure proportionality and legality in the application of these measures.

Keywords*: Environmental interception, police hacking, privacy, criminal investigation, organized crime.*

1. Introdução

A investigação criminal é um instrumento fundamental para o combate à criminalidade, especialmente no enfrentamento do crime organizado. A complexidade dessas infrações exige a adoção de técnicas investigativas sofisticadas, como interceptações telefônicas, ambientais e até mesmo o uso de *hacking* policial. No entanto, o uso dessas ferramentas levanta intensos debates jurídicos e doutrinários, especialmente no que tange à sua compatibilidade com os direitos fundamentais, como a privacidade, a intimidade e a inviolabilidade das comunicações.

Ao longo da história, diversas decisões judiciais influenciaram a interpretação desses direitos no contexto da investigação criminal. Nos Estados Unidos, a Suprema Corte analisou casos paradigmáticos, como *Olmstead v. United States* (1928), *Katz v. United States* (1967) e *Kyllo v. United States* (2001), estabelecendo a evolução do conceito de privacidade diante dos avanços tecnológicos. No Brasil, a Lei nº 9.296/1996 regulamentou a interceptação de comunicações, mas ainda há controvérsias quanto à sua aplicação e aos limites impostos pela Constituição Federal.

Além disso, a interceptação ambiental tem gerado debates acerca de sua legalidade e de sua utilização em investigações criminais. A legislação brasileira e decisões do Supremo Tribunal Federal demonstram uma flexibilização da inviolabilidade domiciliar quando há indícios de atividades ilícitas, como evidenciado no Inquérito nº 2.424/RJ. No entanto, há preocupações sobre a necessidade de um controle rigoroso para evitar abusos por parte das autoridades.

Outro tema controverso é a possibilidade de renovações sucessivas das interceptações telefônicas, a ausência de um prazo máximo e a (in)admissibilidade das interceptações preventivas. Enquanto a legislação vigente permite renovações mediante justificativa, a falta de um limite absoluto levanta preocupações sobre a duração excessiva dessas medidas, podendo comprometer direitos fundamentais.

No âmbito da tecnologia, a criptografia ponta-a-ponta tem dificultado o acesso de órgãos de investigação às comunicações de criminosos, levando à discussão sobre o uso do *hacking* policial como alternativa. Essa técnica, já adotada em alguns países, permite a interceptação de comunicações antes da criptografia,

mas também levanta questões éticas e jurídicas sobre sua legalidade e os riscos de abuso estatal.

A presente pesquisa adota uma abordagem qualitativa, de caráter exploratório, fundamentada em revisão bibliográfica e documental. Foram analisadas obras doutrinárias nacionais e estrangeiras, legislações pertinentes, jurisprudência dos tribunais superiores brasileiros e decisões paradigmáticas da Suprema Corte dos Estados Unidos. A investigação se desenvolve a partir da leitura crítica e interpretativa dessas fontes, buscando identificar os principais pontos de tensão entre os instrumentos investigativos modernos e os direitos fundamentais constitucionalmente garantidos.

Diante desse panorama, dividimos o presente artigo em dois principais capítulos com suas respectivas subdivisões. Buscamos relacionar, no primeiro capítulo, a interceptação das comunicações telefônicas frente aos direitos fundamentais. Inicialmente, discutimos os clássicos precedentes da suprema corte americana, como forma de contextualizar parte da origem desse tema. Em seguida, tratamos das limitações à interceptação ambiental no ordenamento jurídico brasileiro. Ao final desse primeiro bloco, apresentamos, especificamente, os principais pontos acerca da Lei de Interceptação Telefônica (Lei nº. 9.296/1996).

No segundo bloco, tornamos evidente, ainda que brevemente, as questões mais polêmicas sobre o tema, quais sejam: a) As renovações sucessivas de interceptações telefônicas e a (des)necessidade de um prazo máximo; b) A (im)possibilidade da interceptação preventiva; e c) A criptografia ponta-a-ponta e a técnica do *hacking* policial.

2. A interceptação de comunicações telefônicas frente aos direitos fundamentais: precedentes, limitações e debates acerca da lei nº. 9.296/1996

O estudo dos clássicos precedentes da Suprema Corte Americana – Olmstead (1928), Katz (1967) e Kyllo (2001) – evidencia a evolução da proteção à privacidade diante das investigações estatais. Inicialmente, a Corte adotava a teoria proprietária, considerando a invasão física como critério para ilicitude de provas. Posteriormente, passou a reconhecer a expectativa legítima de privacidade, independentemente do local. Com os avanços tecnológicos, estabeleceu-se que novas formas de vigilância também devem estar sujeitas a restrições constitucionais. Até os dias de hoje, tais precedentes influenciam debates sobre interceptações ambientais e sigilo das comunicações em diversos ordenamentos jurídicos, sendo fundamentais para equilibrar segurança pública e direitos fundamentais.

2.1 Os clássicos precedentes da Suprema Corte Americana

A busca pelo equilíbrio entre a legítima pretensão estatal de produzir provas e as entraves do direito à privacidade é antiga. Alguns doutrinadores, ao debater questões acerca da classificação do direito probatório, remontam a precedentes da Suprema Corte dos Estados Unidos: Olmstead (1928), Katz (1967) e Kyllo (2001). A essência desses julgados está na necessidade, ou não, de prévia autorização judicial que possa subsidiar diligências investigativas consideradas invasivas.

Quanto à primeira geração desse direito (oriunda do caso Olmstead), a polícia americana realizou uma interceptação telefônica através de instalação de equipamentos na rede da empresa, em via pública. Contudo, o procedimento foi adotado sem prévia autorização judicial, já que não havia ocorrido o ingresso na residência do suspeito. Para solucionar se essa interceptação telefônica era, ou não,

válida, a Corte Americana fundamentou a sua decisão com base na teoria proprietária (*trespass theory*).

Por esta teoria, deve-se proteger coisas, objetos e lugares como extensões da casa. Dessa forma, restando ausente a violação de um dos espaços da propriedade privada, o material probatório analisado deve ser considerado lícito. Como nenhuma propriedade de Olmstead foi defasada pelas autoridades, a interceptação telefônica, ainda que realizada sem autorização judicial, foi considerada válida. Nesse estágio inicial da trilogia, nota-se uma proteção constitucional de coisas, objetos e lugares (Lima, 2021, p. 695-696).

A segunda geração (o caso Katz), por sua vez, é marcada por uma interceptação telefônica, também sem autorização judicial, realizada em uma cabine de telefone público. Nesse caso, a Corte americana alterou seu entendimento e estendeu a proteção concedida à vida privada para além da teoria proprietária. Observou-se, que, a utilização da cabine telefônica, pelo cidadão, gerava uma expectativa de proteção ao direito à intimidade. Assim, se fosse empregada a teoria proprietária, a prova seria lícita, pois não houve qualquer violação ao domicílio do suspeito. Contudo, a Suprema Corte não adotou esse entendimento (*Ibidem*)

Ora, se o suspeito utiliza um telefone público e, portanto, paga por tal prestação de serviço, é de se esperar do Poder Público, no mínimo, uma expectativa de proteção da intimidade. Logo, tal prova deveria ser considerada ilícita. Adotou-se, aqui, a teoria da proteção constitucional integral, segundo a qual não se pode proteger apenas a propriedade do suspeito, mas também as expectativas de privacidade.

Em 2001, a Suprema Corte dos Estados Unidos julgou o caso Kyllo e acrescentou um novo entendimento ao tema. Esse precedente relata o caso da suspeita – por parte dos agentes de polícia – de que Danny Kyllo estava cultivando maconha em sua residência. Para tanto, conhecendo a necessidade de lâmpadas de alta intensidade para esse cultivo, as autoridades utilizaram um equipamento de captação térmica e constataram, sem invadir qualquer espaço atrelado ao domicílio, a presença de forte emanação de calor da residência da suspeita (*Ibidem).*

Se analisarmos este último caso sob a lente da primeira e da segunda geração, poderíamos concluir pela inexistência da ilicitude da prova, já que não houve a invasão da propriedade da suspeita, e, tampouco, a violação da expectativa de privacidade. Contudo, a Suprema Corte Americana fixou o entendimento de que os avanços tecnológicos não poderiam limitar a proteção concedida ao direito à privacidade e ao direito à intimidade. Não se pode equiparar a observação a "olho nu" à utilização de equipamentos de captação térmica, tornando, assim, a prova ilícita (Knijnik, 2016, *apud* Guaragni; Tamborlim, 2024, p. 2386-5229).

Danilo Knijnik (2016) resume essa trilogia da seguinte maneira:

> A trilogia Olmstead-Katz-Kyllo põe à luz que o paradigma da "intrusão física", reclamando uma coisa ou o ingresso em ambiente alheio (teoria proprietária), como ocorreu com Olmstead, evoluiu para uma noção de expectativa legítima de privacidade, associada ao reconhecimento que lhe conferiu Katz. Mas a penetração da tecnologia nos mecanismos investigatórios fez notar que, mesmo sem intrusão física de espécie alguma, ou mesmo à base de observações em espaços públicos nos quais não haveria nem pretensão, nem reconhecimento da expectativa à privacidade, a proteção constitucional ainda ali merece respeito, sob pena de tornar a sociedade refém, a ponto de ser, em última instância, reduzida a níveis intoleráveis, eliminando qualquer laivo de privacidade" *(Ibidem)*.

Não há dúvidas de que o avanço tecnológico continua gerando desafios complexos para a preservação dos direitos fundamentais, especialmente o direito à privacidade. No caso ora apresentado, houve uma preocupação da Suprema Corte dos Estados Unidos diante da utilização de dispositivos tecnológicas por autoridades de segurança, destacando a necessidade de um controle judicial mais rígido, voltado para defesa da proporcionalidade na aplicação de ferramentas invasivas.

Dessa forma, com a introdução de novos mecanismos de coleta de provas, também deve haver uma adaptação das normas jurídicas e uma reformulação das interpretações judiciais, de modo a assegurar um sistema justo e compatível com a modernidade tecnológica.

2.2 Limitações à interceptação ambiental no ordenamento jurídico brasileiro

Ao tratarmos sobre as interceptações ambientais, três direitos constitucionais previstos no art. 5º são ressaltados: a proteção da intimidade e da vida privada (inciso X); a inviolabilidade do domicílio (inciso XI) e o sigilo das comunicações (inciso XII). Muito se questiona se essas interceptações são conciliáveis com esses direitos.

Inicialmente, segundo José Afonso da Silva (2016), a intimidade foi considerada um direito diverso dos direitos à vida privada, à honra e à imagem das pessoas. Para o renomado autor, não é fácil distinguir “vida privada” de “intimidade”. Enquanto aquela integra a vida íntima da pessoa, percebida como repositório de segredos e particularidades do foro moral e íntimo, esta deve ser considerada como sinônimo de direito à privacidade, sendo compreendida como “o conjunto de informação acerca do indivíduo, que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito (Silva, 2016, p. 208-210)".

José Afonso da Silva explica, ainda, que:

> A tutela constitucional visa proteger as pessoas de dois atentados particulares: (a) ao segredo da vida privada; e (b) à liberdade dei vida privada. O segredo da vida privada é condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada; sem perturbação de terceiros. São duas variedades principais de atentados ao segredo da vida privada, nota Kayser: a divulgação, ou seja, o fato de levar ao conhecimento do público, ou a pelo menos de um número indeterminado de pessoas, os eventos relevantes da vida pessoal e familiar; a investigação, isto é, a pesquisa de acontecimentos referentes à vida pessoal e familiar; envolve-se aí também a proteção contra a conservação de documento relativo à pessoa, quando tenha sido obtido por meios ilícitos[3] (Kayser, 1984, p. 208 *apud* Silva, 2016, p. 209).

O que os autores buscam evidenciar, com isso, é o fato hoje notório de que a vida privada é cada vez mais suscetível à violação por investigações e divulgações ilegítimas a partir de captações eletrônicas registradores de imagem, sons e dados.

A segunda proteção constitucional interligada à interceptação telefônica gira em torno do direito à segurança. O art. 5º, XI[4], consagra o direito à segurança domiciliar como uma garantia de inviolabilidade do lar. O referido inciso está intimamente conectado ao anterior, afinal a casa é local em que se desenvolve a

[4] A Constituição protege o domicílio, estabelecendo, no art. 5º, XI, que: “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”.

vida privada. Essa proteção dirige-se basicamente contra as autoridades, visando impedir que estas invadam o lar. Mas também se dirige aos particulares. “O crime de violação de domicílio tem por objeto tornar eficaz a regra da inviolabilidade do domicílio” (Silva, 2016, p. 441).

Embora a Constituição empregue o termo “casa”, a proteção vai além do ambiente doméstico, alcançando, inclusive, quartos de hotel enquanto habitados. Além disso, os espaços profissionais também estão sujeitos à proteção constitucional, sendo considerados como “compartimento privado não aberto ao público, onde alguém exerce profissão ou atividade (CP, art. 150, § 4º, III), compreendendo, observada essa específica limitação espacial (área interna não acessível ao público), os escritórios profissionais” (Mendes, 2023, p. 1014).

Sobre o tema, é importante destacarmos o precedente do Supremo Tribunal Federal (STF) ao julgar Inquérito nº 2.424[5], do Rio de Janeiro, cuja investigação visava desarticular organização criminosa para a prática de crimes de corrupção passiva e prevaricação, envolvendo magistrados, um procurador regional da República e um advogado. *In casu,* foi autorizado o ingresso em escritório de advocacia, no período noturno, a fim de colher informações e instalar equipamento de captação ambiental.

Cabe aqui, pela pertinência, transcrevermos parte do trecho do Informativo 529 do STF[6]:

> Escuta Ambiental e Exploração de Local: Escritório de Advogado e Período Noturno – 4. Prosseguindo, rejeitou-se a preliminar de ilicitude da prova de escuta ambiental, por ausência de procedimento previsto em lei. Sustentava a defesa que a Lei 9.034/95 não teria traçado normas procedimentais para a execução da escuta ambiental, razão pela qual a medida não poderia ser adotada no curso das investigações. Entendeu-se não proceder a alegação, tendo vista que a Lei 10.217/2001 deu nova redação aos artigos 1º e 2º da Lei 9.034/95, definindo e regulando meios de prova e procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo. *(...) Asseverou-se, ademais, que a escuta ambiental não se sujeita, por motivos óbvios, aos mesmos limites de busca domiciliar, sob pena de frustração da medida, e que, não havendo disposição legal que imponha disciplina diversa, basta a sua legalidade a circunstanciada autorização judicial* (BRASIL, STF. Inq. Nº 2.424/RJ. Rel. Min. Gilmar Mendes. Julgado em 26 nov. 2008)

Em um segundo momento do julgamento:

> Afastou-se, de igual modo, a preliminar de ilicitude das provas obtidas mediante instalação de equipamento de captação acústica e acesso a documentos no ambiente de trabalho do último acusado, porque, para tanto, a autoridade, adentrara o local três vezes durante o recesso e de madrugada. Esclareceu-se que o relator, de fato, teria autorizado, com base no art. 2º, IV, da Lei 9.034/95, o ingresso sigiloso da autoridade policial no escritório do acusado, para instalação dos referidos equipamentos de captação de sinais acústicos, e, posteriormente, determinara a realização de exploração do local, para registro e análise de sinais ópticos. (...) *Considerou-se, entretanto, que tal inviolabilidade cederia lugar à tutela constitucional de raiz, instância e alcance superiores quando o próprio advogado seja suspeito da prática de crime concebido e consumado, sobretudo no âmbito do seu escritório, sob pretexto de exercício da profissão.* Aduziu-se que o sigilo do advogado não existe para protegê-lo quando cometa crime, mas proteger seu cliente, que tem direito à ampla

[5] Ver Inq. 2424/RJ. Relato: Min. Cezar Peluso. Julgamento: 26/11/2008. Publicação: 26/03/2010. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search/sjur175031/false> Acessado em: 09 fev. 2025.
[6] Disponível em <http://www.stf.jus.br/arquivo/informativo/documento/informativo529.htm> Acessado em 08 fev. 2025.

> defesa, não sendo admissível que a inviolabilidade transforme o escritório no único reduto inexpugnável de criminalidade. *Enfatizou-se que os interesses e valores jurídicos, que não têm caráter absoluto*, representados pela inviolabilidade do domicílio e pelo poder-dever de punir do Estado, devem ser ponderados e conciliados à luz da proporcionalidade quando em conflito prático segundo os princípios da concordância (BRASIL, STF. Inq. Nº 2.424/RJ. Rel. Min. Gilmar Mendes. Julgado em 26 nov. 2008).

É possível extrairmos da decisão supracitada que houve uma relativização de dispositivos que tratam da busca domiciliar e da inviolabilidade do escritório de advocacia (art. 7º, II, da Lei nº 8.906/94). Ponderou-se, que, as peculiaridades do caso concreto, como o fato de o próprio advogado ser suspeito da prática de crime e a utilização de escritório de advocacia para protegê-lo de possíveis investigações, devem prevalecer em face de determinados direitos fundamentais. Trata-se, portanto, de uma inovação no instituto da intimidade e vida privada, bem como do direito à segurança domiciliar, que demonstra que a insuficiência de técnicas tradicionais de investigação (como depoimentos de testemunhas; registros de câmeras de circuitos de segurança; acareações; reconhecimento de pessoas) e a necessidade de novos mecanismos implicam maior grau de afetação no campo dos direitos e garantias fundamentais.

O art. 5º, XII[7], da Constituição Federal, por sua vez, cuida de dois institutos: i) correspondência e comunicações telegráficas; e ii) dados e comunicações telefônicas. Vê-se, que o objeto de proteção desse inciso é o sigilo da correspondência e da comunicação. E, da redação pouco clara, sendo fonte de inúmeros debates acerca do seu alcance, surgem basicamente duas importantes questões interpretativas: a) qual é o objeto de proteção do sigilo? e b) qual(-is) grupo(-s), dentre os quatro listados no inciso (correspondência; comunicações telegráficas, de dados; e comunicações telefônicas) podem ser excepcionalizado de modo a permitir a quebra do sigilo (“salvo, no último caso...”)? (Abreu; Antonialli, 2017, p. 15).

Essas questões se tornaram referência doutrinária em 1993, quando Tércio Sampaio Ferraz Júnior publicou o artigo “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”. A partir disso, o Supremo Tribunal Federal (STF) passou a considerar que a proteção do sigilo de dados se aplica apenas às informações em trânsito, ou seja, ao fluxo de dados entre o emissor e o receptor no momento da comunicação telefônica ou telemática. Contudo, essa proteção não se estende aos dados que já tenham sido transmitidos anteriormente (Queiroz; Ponce, 2020, p. 67).

Jacqueline Abreu e Dennys Antonialli, alertam que o entendimento doutrinário predominante, com fundamento também em precedente do Supremo Tribunal Federal[8], é o de que a proteção prevista pelo referido inciso constitucional se refere ao “fluxo” das comunicações enquanto ocorrem, e não o conteúdo em si das informações. Além disso, apenas o sigilo da comunicação por telefonia (quando está em fluxo), poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas Abreu; Antonialli, 2017, p. 16).

[7] Afirma ser “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”.

[8] Recurso Extraordinário 418.416-8/SC, de 10/05/2006, o Min. Rel. Sepúlveda Pertence. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790 Acessado em: 8 fev. 2025.

Segundo Luciana Fregadolli, citando Vicente Greco Filho, as comunicações "telefônicas" não se confundem com as comunicações "por meio de linha telefônica", uma vez que telefone é aparelho de comunicação de voz, e, por essa razão, somente os instrumentos que se utilizam da linha telefônica podem ser a ele equiparados. Para a autora, se a Constituição quisesse uma extensão, de modo a alcançar às comunicações de dados, teria usado a expressão "comunicação por linha telefônica" (Fregadolli, 1998, p. 99-102).

A contrário *sensu*, há jurisprudência[9] e doutrina argumentando em favor de novas interpretações acerca desse dispositivo, seja em razão do avanço tecnológico e da enorme quantidade de conteúdo registrado, seja em razão da adaptação de novas tecnologias por organizações criminosas para o cometimento de crimes. Nesse sentido, endossamos aquilo que apresenta Gustavo Badaró ao expor outra interpretação dada à ressalva "no último caso". Segundo o autor, entende-se que o inciso XII teria apenas duas partes (1) "o sigilo da correspondência e das comunicações telegráficas"; e (2) "de dados e das comunicações telefônicas". Partindo dessa premissa, a ressalva "no último caso" estaria se referindo aos "dados" (comunicação de dados) e às comunicações telefônicas (Badaró, 2012, p. 4).

Assevera o Badaró que:

> Uma interpretação realista e adequada da norma constitucional não pode deixar de prever a possibilidade, com ressalvas, da interceptação das comunicações de dados. *Não se está propondo uma interpretação ampliativa das hipóteses que excepciona os direitos individuais, ou seja, em norma que exige interpretação restritiva. Todavia, não se pode considerar uma norma constitucional isolada de seu contexto histórico, social e político, mormente em temas que envolvem a evolução tecnológica*. Heleno Fragoso já advertia que "o desenvolvimento da técnica conduz à necessidade de mais eficiente tutela jurídica de esfera de intimidade". Todavia, em 1988 era inimaginável o avanço da *internet*. A própria comunicação por correspondência epistolar vem sendo substituída pelo *e-mail*, que nada mais é do que uma correspondência eletrônica. A comunicação telefônica vem sendo substituída por programas de computador que permitem troca de vozes, de forma absolutamente idêntica àquela que ocorre por linha telefônica convencional. Finalmente, a troca de dados por sistemas de computadores é uma realidade com enormes potenciais. Nesse contexto, o inciso XII deve ser interpretado em seu real escopo de tutela da liberdade de comunicação do pensamento, enquanto mecanismo de salvaguarda do direito à liberdade de manifestação do pensamento de forma reservada, isto é, a *riservatezza*, de que fala a doutrina italiana (*Ibidem, p. 5)*.

Dessa forma, negar o risco de uma interpretação puramente literal do inciso XII da Constituição Federal, ignorando os avanços tecnológicos, pode abrir caminho para uma criminalidade moderna, especialmente no caso de crimes sofisticados, como delitos que são planejados e executados por meio de transferência de dados via sistema telemáticos. Diante dessa evolução tecnológica, interpretar o dispositivo constitucional de forma limitada e descontextualizada resultaria em uma liberdade irrestrita para comunicações informáticas e telemáticas, impossibilitando qualquer tipo de interceptação ou restrição.

Portanto, ao interpretarmos o inciso XII devemos considerar o avanço tecnológico, de modo a preservar sua essência, qual seja: garantir o direito à

[9] Ver, por exemplo, STF. Mandado de Segurança 24.817/DF, Min. Celso de Mello, julg. em 03.02.2005, que associa quebras de sigilo de fiscal, bancário e telefônico a restrições ao art. 5, X. Disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418. Acesso em: 08 fev. 2025.

comunicação privada, sem a interferência de terceiros, independentemente da tecnologia empregada.

2.3 Debates acerca da lei de interceptação telefônica

No Brasil, o primeiro marco legal que discutiu a figura da interceptação ambiental foi a Lei nº. 9.034/1995, que se dispôs a tratar da organização criminosa. Entre as ferramentas de combate a essa espécie de crime se destacava a "captação ambiental". No entanto, a referida lei não regulamentou os meios de obtenção de prova nela indicados. A questão foi resolvida, ainda que com severas críticas, com o advento da Lei nº. 9.296/1996 (Lei de Interceptação Telefônica), que passou a tratar da matéria conforme exigido pelo texto constitucional.

Um dos principais debates acerca da referida Lei gira em torno da (in)constitucionalidade do seu artigo primeiro, que, na íntegra, diz o seguinte:

> 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 (BRASIL**.** *Lei nº 9.296/96, de 24 de julho de 1995*. Lex: legislação federal, 1996. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L9296.htm. Acessado em 9 fev. 2025).

Conforme debatido no capítulo anterior, a divergência doutrinária persiste na tentativa de reconhecer, ou não, a extensão da exceção prevista no inciso XII do art. 5º da Constituição Federal. A Lei das Interceptações surge para regular essa exceção constitucional ao sigilo das comunicações, determinando as circunstâncias em que os representantes do Estado podem ter acesso a comunicações telefônicas e telemáticas enquanto estejam em fluxo. Segundo Nelson Nery Jr. e Rosa Maria de Andrade Nery, o artigo primeiro da referida Lei é inconstitucional por estender, sem autorização judicial, às comunicações de informática e telemática, a exceção prevista apenas para comunicações telefônicas (Nery Júnior; Nery, 2001, p. 2170-2172).

Diverge de Nelson Nery Jr. e Rosa Maria de Andrade Nery as doutrinas de Lenio Streck e Alexandre de Moraes, que defendem a constitucionalidade do parágrafo único do art. 1º da Lei nº 9.926/1996. Segundo Streck, o parágrafo único, ao estender a possibilidade de interceptação também ao fluxo de comunicações em sistemas de informática e telemática, apenas especificou que a lei também atingirá qualquer variante de informações que utilizarem a modalidade "comunicação telefônica". Entende-se, dessa forma, pelo sentido amplo da expressão comunicações telefônicas pelo constituinte, o que permite, por exemplo, que as comunicações por meio de informações digitais de um computador para outro, via internet, sejam englobadas na previsão de telemática (Streck, 2001, p. 46).

No mesmo sentido, aduz Alexandre de Moraes que deve prevalecer o posicionamento da constitucionalidade do parágrafo único da referida lei, por três motivos:

> 1. A interpretação das normas constitucionais exige que a uma norma constitucional seja atribuído o sentido que maior eficácia lhe conceda (Canotilho), sendo vedada a interpretação que lhe suprima ou diminua a finalidade (Jorge Miranda). 2 Assim, apesar de a exceção constitucional (CF, art. 5", XI, in fine) expressamente referir-se somente à interceptação telefônica, nada impede que nas outras espécies de

> inviolabilidades haja possibilidade de relativização da norma constitucional, por exemplo, na permissão da gravação clandestina com autorização judicial (RT 692/370), pois, entende-se que *nenhuma liberdade individual é absoluta*, sendo possível, respeitados certos parâmetros, a interceptação das correspondências, das comunicações e de dados, sempre que essas liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas, pois como salienta o Tribunal de Justiça do Estado de São Paulo, "afirmar que um direito é absoluto significa que ele é inviolável pelos limites que lhe são assinalados pelos motivos que o justificam" (TJSP - Cam. Esp. MS 13.17fr0/2-SP - rel. Des. Denio Garcia). 3 Finalmente, o fato da ementa da lei afirmar que "Regulamenta o Inciso XII, Parte Final, do art. 5 da Constituição Federal*", de forma alguma impede que o texto legal discipline outros assuntos, uma vez que a lei que veicula matéria estranha ao enunciado constante de sua ementa, por só esse motivo, não ofende qualquer postulado constitucional*, não vulnerando tampouco as regras de processo legislativo constitucional, pelo que excluída da possibilidade de declaração de inconstitucionalidade (STF - Pleno - ADin. nó 1.096-4 - medida liminar - rel. Min. Celso de Mello, Diário da Justiça, Seção I, 22 set. 1995, p. 30.589), *pois inexistente no vigente sistema de direito constitucional brasileiro regra idêntica à prevista pelo art. 49 da Constituição Federal de 1934.* ("Os projectos de lei serão apresentados com a respectiva ementa, enunciando, de forma succinta, o seu objectivo, e não poderão conter matéria estranha ao seu enunciado (1998, p. 154-155) ".

Para tanto, a Lei das Interceptações, em seu artigo 2º, estabeleceu regras rigorosas para o preenchimento de requisitos (i) a configuração de indícios razoáveis da autoria ou participação em infração penal; (ii) a inexistência de outros meios de prova; e (iii) o envolvimento em crimes de maior gravidade.

De forma mais detalhada, Norberto Avena explica que, além dos requisitos supracitados, é indispensável a observância das seguintes regras: a) determinação exclusiva do juiz da causa para prova em investigação criminal e em instrução processual penal (vedadas em causas cíveis); b) determinada de ofício ou a requerimento da autoridade policial (na fase do inquérito); c) serão realizadas sob segredo de justiça, devendo o ato permissivo ser fundamentado, sob pena de nulidade; d) deverá ser realizado no prazo de 15 dias, renovável por igual período, se comprovada a indispensabilidade desse meio de prova; e) a Autoridade Policial poderá requisitar serviços técnicos especializados às concessionárias de serviço público; f) Será preservado o sigilo das diligências, gravações e transcrições respectivas . (Avena, 2023, p. 941-945).

Com o avanço significativo da criminalidade organizada, fez-se necessário a elaboração da Lei nº 12.850/2013, que ab-rogou a Lei nº. 9.034/1995 e trouxe uma nova regulamentação com novas técnicas de investigação – como a ação controlada e a infiltração de agentes. Contudo, originalmente, a referida lei não regulamentou a captação ambiental, embora já houvesse previsão legal no art. 3º, inciso II, da Lei nº. 12.850/2013, como meio de obtenção de prova no âmbito das Organizações Criminosas, sendo esta lacuna preenchida pela Lei nº. 13.964/2019 (Pacote Anticrime), que detalhou seu procedimento na lei de interceptação telefônica.

Dessa forma, em harmonia com a posição doutrinária e jurisprudencial, a captação ambiental passa a ser regulamentada diretamente na Lei nº. 9.296/1996, que até então somente tratava sobre interceptações telefônica. Agora, tornou-se uma verdadeira “lei geral de interceptação” (Ribeiro, 2020, p. 89). Dentre as diversas inclusões e modificações trazidas pela Lei nº. 13.964/2019, vale destacar a inclusão dos artigos 8º-A e 10-A na Lei nº. 9.296/1996, que trataram da interceptação entre

pessoas presentes. No entanto, antes disso, para fins de melhor compreensão sobre o tema, é preciso distinguirmos, ainda que brevemente, as classificações de captações telefônicas.

Segundo leciona Norberto Avena, as "captações telefônicas" (ou interceptações telefônicas *lato sensu*) correspondem a um gênero que se subdivide em três espécies, quais sejam: i) Interceptação telefônica *stricto sensu;* ii) Escuta telefônica; e iii) Gravação telefônica. A primeira, trata-se de hipótese na qual um terceiro capta o diálogo ou as imagens envolvendo duas ou mais pessoas, sem que nenhum dos alvos saiba. A segunda (escuta), ocorre quando há tais registros, envolvendo também duas ou mais pessoas, porém, um dos alvos sabe que está sendo realizada a escuta. Por fim, na gravação telefônica, também chamada de "gravação ambiental clandestina[10]", um dos interlocutores é o autor dos registros (Avena, 2023, p. 919).

Nos termos do artigo 8°-A, tem-se que:

> Art. 8º-A. Para investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando:
> I - a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e
> II - houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas.
> § 1º O requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental.
> § 2º (VETADO).
> § 3º A captação ambiental não poderá exceder o prazo de 15 (quinze) dias, renovável por decisão judicial por iguais períodos, se comprovada a indispensabilidade do meio de prova e quando presente atividade criminal permanente, habitual ou continuada.
> § 4º (VETADO).
> § 5º Aplicam-se subsidiariamente à captação ambiental as regras previstas na legislação específica para a interceptação telefônica e telemática (BRASIL. *Lei nº 9.296/96, de 24 de julho de 1995.* Lex: legislação federal, 1996. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L9296.htm. Acessado em 9 fev. 2025).

Jacqueline de Souza Abreu e Gianluca Martins Smanio criticam o referido texto, aduzindo que:

> O Projeto Anticrime não corrige esse problema e ainda propõe uma nova redação que aumenta o espectro de incidência para além dos crimes de organização criminosa. O texto legal proposto permite o uso dos meios de obtenção de prova lá previstos e, portanto, de interceptações ambientais, não apenas na investigação de infrações penais praticadas por organizações criminosas, mas também em todas aquelas cujas penas máximas sejam superiores a quatro anos, ou em infrações conexas. Da perspectiva aqui avançada, considerando-se o nível de restrição a direitos fundamentais que interceptações ambientais podem acarretar e o contexto da reforma, o dispositivo deveria ser revisto para se conter apenas a crimes praticados por organização criminosa. Na forma como está, a proposta tem potencial de multiplicar diversos outros problemas do projeto para diversas outras investigações. É o que se passa a ver (Abreu; Antonialli, 2017, p. 1496).

[10] O termo "clandestina" está empregado não na acepção de "ilícito", mas sim no sentido de "feito às ocultas".

Outro aspecto relevante gira em torno do termo “captação ambiental”. Parte da doutrina, representada por Renato Brasileiro, entende ter havido uma redundância na utilização do desse termo pelo art. 8º-A da Lei de Interceptações. Para ele, o referido artigo faz uso da expressão “captação ambiental” em sentido amplo, englobando a interceptação ambiental em sentido estrito e a escuta ambiental. Assim, a gravação ambiental não estaria contida no núcleo dessa proteção. Uma forte evidência disso é a tipificação trazida pelo artigo 10-A da Lei de Interceptações (acrescentado pela Lei Anticrime). Este artigo criminaliza a conduta de realização de captação ambiental sem autorização judicial, excepcionando, em seu parágrafo 1º, quando a captação for realizada por um dos interlocutores. Por isso, entende o autor, que a licitude da captação ambiental deve ser analisada no caso concreto, não estando submetida à proteção dada pelo art. 8-A (Lima, 2020, p. 852-854).

A questão não é nova, os precedentes mais recentes do STJ e do STF têm validado o uso das gravações clandestinas como meio de prova[11]. Um caso emblemático, decidido pelo Superior Tribunal de Justiça, foi o do médico anestesiologista, que, sem saber que estava sendo filmado, aproveitando-se da vulnerabilidade da paciente (em razão da dose excessiva de sedativa aplicada por ele), praticou estupro de vulnerável, dentro da própria sala de parto, ao introduzir seu pênis na boca da grávida que estava em trabalho de parto[12]. *In casu,* na colisão de interesses, prevaleceu os direitos fundamentais da parturiente em face da privacidade e da imagem do autor do crime.

Nesse caso, o STJ adotou a seguinte tese:

> Na colisão de interesses, é válida a captação ambiental clandestina sempre que o direito a ser protegido tiver valor superior à privacidade e a imagem do autor do crime, utilizando-se da legítima defesa probatória, a fim de se garantir a licitude da prova (BRASIL, STJ. 5ª Turma. HC 812.310/RJ, Rel. Min. Ribeiro Dantas, julgado em 21/11/2023 (Info. 16 – Edição Extraordinária).

Nesse sentido, embora a gravação clandestina, a princípio, pudesse estar adequada ao tipo previsto no art. 10-A da Lei de Interceptação, no caso concreto, ela é alcança pela excludente da antijuridicidade, pois, embora sua conduta tenha causado lesão a um bem jurídico constitucionalmente protegido (vida privada e intimidade), foi utilizada contra agressão injusta, atual e iminente, ajustando-se, assim, à legítima defesa probatória.

3. BREVE ANÁLISE ACERCA DE TEMAS POLÊMICOS ENVOLVENDO A INTERCEPTAÇÃO TELEFÔNICA E A INVESTIGAÇÃO CRIMINAL

No capítulo anterior, constatamos que alguns dos principais precedentes da Suprema Corte dos Estados Unidos, que refletem um dilema persistente no direito contemporâneo: o equilíbrio entre a proteção dos direitos fundamentais e a necessidade de métodos eficazes de investigação. No Brasil, esse debate se intensifica diante de temas polêmicos como a renovação sucessiva das interceptações telefônicas, a impossibilidade da interceptação preventiva e os desafios impostos pela criptografia ponta-a-ponta. Enquanto os tribunais americanos expandiram a proteção à privacidade diante do avanço tecnológico, o ordenamento

[11] Ver STF. Plenário.RE 583937 QO-RG, Rel. Min. Cezar Peluso, julgado em 19/11/2009 (Repercussão Geral – Tema 237).
[12] Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/9bed9658634281e6128aa6f2979a7944> Acessado em: 08 fev. 2025.

jurídico brasileiro ainda busca soluções para compatibilizar o sigilo das comunicações com a efetividade das investigações criminais.

3.1 Renovações sucessivas de interceptações telefônicas e a (des)necessidade de um prazo máximo

O primeiro tema polêmico acerca da interceptação das comunicações envolve a adoção de prazos absolutos. Conforme citado anteriormente, o juiz que autorize o procedimento de interceptação deve fundamentar devidamente sua resolução e assinalar a forma e o prazo máximo da diligência, que é de 15 dias, podendo ser prorrogado por igual período, desde que se determine a indispensabilidade desse meio de prova.

Não há obste para que o legislador adote um prazo máximo para as interceptações. Contudo, vincular a interceptação a prazos absolutos é de complexa adequação à realidade. No julgamento do Recurso Extraordinário 625.263/PR, o Ministro Relator Gilmar Mendes, em seu voto, explica que a dificuldade maior está no fato de tratar-se de medida investigativa em tempo real, que se presta a comprovar a autoria do crime que motivou a autorização, bem como a existência de outros crimes, anteriores ou posteriores à autorização, e mesmo a cogitação e preparação de crimes futuros[13]

Existe, inclusive, o Projeto de Lei 3.272/2008[14], de autoria da Presidência da República, que busca estabelecer um prazo máximo em abstrato. Segundo o parágrafo 1º do art. 5º, do projeto, o atual prazo de 15 dias seria substituído pelo prazo de 60 dias, até o máximo de 360 dias ininterruptos, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

Na íntegra:

> Art. 5º, §1º - O prazo de duração da quebra do sigilo das comunicações não poderá exceder a sessenta dias, permitida sua prorrogação por iguais e sucessivos períodos, desde que continuem presentes os pressupostos autorizadores da medida, até o máximo de trezentos e sessenta dias ininterruptos, salvo quando se tratar de crime permanente, enquanto não cessar a permanência (BRASIL, Projeto de Lei 3272/2008).

Ainda da análise do RE 625.263/PR, podemos extrair que, no direito comparado, a maior parte dos países não prevê cláusula de teto quanto ao prazo de prorrogação das interceptações de comunicações. A Corte Europeia de Direitos Humanos, por exemplo, já adotou o prazo de até 3 meses, renováveis por iguais períodos. Na Alemanha, conforme o Código de Processo Penal, a medida pode ser expedida para valer no máximo 3 meses. Prorrogações são possíveis, por igual período cada. Solução idêntica é adotada por Portugal, conforme art. 187º, 6, do Código de Processo Penal. Na Itália, adota-se o prazo de 15 dias, prorrogáveis por períodos sucessivos de idêntico prazo, enquanto permanecerem os pressupostos da medida (BRASIL STF. RE 655263/PR – Plenário do Supremo Tribunal Federal. Data do Julgamento: 17/03/2022, p. 8. Relator Min. Gilmar Mendes).

O fato de tratar-se de medida excepcional, envolvendo investigações mais complexas, faz com que o estabelecimento de um teto máximo seja inviável. Em muitos casos, as interceptações duram meses e até anos. Dessa forma, entendemos que a análise desse prazo deve ser guiada pelo princípio da proporcionalidade, com observância às regras da Lei de Interceptações.

[13] Ver STF. RE 655263/PR – Plenário do Supremo Tribunal Federal. Data do Julgamento: 17/03/2022, p. 5 Relator Min. Gilmar Mendes. Disponível em: <https://www.conjur.com.br> acessado em: 9 fev. 2025.
[14] Ver PL 3272/2008 – Disponível em: <www.camara.leg.br> Acessado em 09 fev. 2025.

3.2 Da (im)possibilidade da interceptação telefônica preventiva

Partindo do direito comparado, leciona Gustavo Henrique Righi Ivahy Badaró, que, na Itália, ainda sob o regime do CPP de 1930, o artigo 266, acrescido em 1978, admitia a interceptação telefônica preventiva para crimes graves. Contudo, os elementos de informações colhidos a partir desse modelo de interceptação, por expressa disposição legal, não podem servir como prova no processo penal. Nos Estados Unidos da América, após os atentados terroristas de 11 de setembro de 2001, foi editado o *Patriot Act*, que, com o fim de investigar organizações terroristas, permitiu a realização de interceptações preventivas por meio de Agências de Inteligência, sem a necessidade de autorização judicial (2012, p.9).

Nesse contexto, advoga Manuel da Costa Andrade, ao comentar o §100a do Código de Processo Penal Alemão, que dispõe sobre interceptação e gravação de telecomunicações, pela impossibilidade de utilização de interceptações telefônicas preventivas, ressaltando que a utilização de tal medida serve somente para "perseguição de crimes, dê guarita a meras medidas preventivas" (Badaró, 2012, p. 290).

Nesse debate, a doutrina questiona a possibilidade, diante do sistema constitucional legal brasileiro, de se realizar interceptação telefônica de forma preventiva, isto é, antes do cometimento do delito. O art. 5º, XII, da Constituição Federal não permite a adequação desse meio de obtenção de prova. Na verdade, somente no Estado de Defesa poder-se-ia, em tese, admitir uma interceptação telefônica preventiva, nos termos e limites do art. 136, §1º, da CF, que prevê a suspensão da garantia constitucional da liberdade de comunicação telefônica.

Assevera Gustavo Badaró, ainda, que:

> (...)a Constituição não permite a interceptação telefônica preventiva, mesmo que se pudesse superar o óbice constitucional, não seria possível, nos termos da Lei nº. 9.296/96, a obtenção de uma autorização judicial para a realização da interceptação telefônica preventiva. Primeiro, porque não haverá possibilidade de motivar a decisão judicial com relação aos indícios suficientes de cometimento de um delito, porque ainda não há delito.[55] O que se pretende é, exatamente, de forma preventiva, impedir a prática de tal crime. Em segundo lugar, o art. 1º, inc. II, caracterizando um princípio de subsidiariedade para a realização da interceptação telefônica, determina que a medida somente será cabível se "a prova não puder ser feita por outros meios disponíveis". Ora, prova de que? A resposta é dada pelo art. 4º, *caput*: o pedido de interceptação "conterá a demonstração de que a sua realização é necessária à *apuração de infração penal*". No caso de uma interceptação telefônica preventiva, ainda não há infração a se apurar! Ou seja, também sob tal ângulo, mostra-se impossível a interceptação telefônica preventiva, porque não há investigação a ser realizada, mas somente sujeitos que devem ser controlados. Por outro lado, é de se observar que, se admitida, tal atividade preventiva não deveria ser realizada por órgãos de polícia judiciária que, segundo o desenho constitucional, atuam após o cometimento do delito, mas a órgão da polícia preventiva ou de segurança (*Ibidem*, p. 10-11).

Com respeito ao que leciona o renomado autor, discordamos somente quanto ao órgão executor da medida de interceptação telefônica preventiva (caso fosse admitida). Em verdade, a polícia judiciária (Polícia Federal e Polícia Civil) é a instituição que possui como função a investigação criminal.

Assim, "Polícia Judiciária" não é função, mas sim a própria instituição. Conforme aduz o Delegado de Polícia Lucas Ferreira Dutra, o mais técnico é que a Constituição Federal explicitasse que a Polícia Federal e a Polícia Civil exercem

funções de investigação criminal para apurar infrações penais, possuindo essa função (de investigar) um caráter duplo: preventivo e repressivo (Dutra, 2022, p.1)[15].

3.3 A criptografia ponta-a-ponta e a técnica do *hacking* policial

Essa discussão parte da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403[16], cujo objeto é (i) saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internet; e, em sendo constitucional, (ii) saber se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário[17].

O voto do Relator Min. Edson Fachin recai sobre os argumentos acerca dos direitos envolvidos, bem como da intensidade da interferência neles causados a partir de possíveis alterações no modelo de criptografia adotado pelo *WhatsApp.* Doutro lado, órgãos da segurança pública apontam que o acesso excepcional garante aos agentes de investigação um mecanismo indispensável para a consecução de suas atividades de investigação em crimes mais graves[18]. Isso porque "a implementação da criptografia de ponta-a-ponta impossibilita a realização de interceptações telemáticas, a captura das conversas de alvos específicos em tempo real, mesmo mediante ordem judicial (Abreu; Antonialli, 2017, p. 22).

Na decisão, o Ministro Edson Fachin, seguindo a opinião defendida em audiência pública, aduz que, na hipótese de concessão ao acesso excepcional à comunicação criptografada, faria com que os criminosos optassem por sistemas ainda mais restritos, de difícil rastreamento[19]. Entende-se, assim, que o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional.

Com respeito ao que sugere o Ministro, não se pode esquecer que as organizações criminosas estão cada vez mais especializadas em tecnologias, adotando, inclusive *drones* para a preparação e consumação de seus crimes. Dessa forma, negar esse acesso excepcional aos órgãos de investigação, sob a justificativa de que as organizações criminosas poderão migrar para outros aplicativos, é "fechar os olhos" para a atuação criminosa dos denominados crimes de colarinho branco[20]. Na hipótese de migração para outros aplicativos, caberá à Polícia e ao Ministério Público qualificar-se de modo a se especializar em novas medidas necessárias para o efetivo monitoramento.

Uma das possíveis respostas dos órgãos de investigação à negativa de acesso às comunicações criptografadas é a técnica denominada como *hacking* policial. Podemos definir o termo da seguinte forma: "*hacker* se refere a pessoas habilidosas em programação, administração e segurança, o que difere de *crackers* que praticam atividades criminosas usando técnicas de invasão de computadores, furto de informações, etc." (Ferreira, 2021, p. 26).

Aduz Caio Porto Ferreira, citando Skorvánek, que há seis funcionalidades para *hacking* policial: i) capturar tipos específicos de dados, como o usuário do

[15] Disponível em: www.conjur.com.br.
[16] Ver Arguição de Descumprimento de Preceito Fundamental (ADPF) 403, Relator Min. Edson Fachin, requerente Cidadania, Intimado Juiz de Direito da Vara Criminal da Comarca de Lagarto/SE, processo único 4000331-63.2016.1.00.0000.
[17] Ver STF. Arguição de Descumprimento de Preceito Fundamental: ADPF 403. Relator: Ministro Edson Fachin. STF, p. 53, 2020. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf> Acesso em: 09 fev. 2025.
[18] *Idem,* p. 55, 2020.
[19] Ver STF. Arguição de Descumprimento de Preceito Fundamental: ADPF 403. Relator: Ministro Edson Fachin. STF, p. 71, 2020. Disponível em:https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf> Acesso em: 09 fev. 2025.
[20] São assim denominados por possuir a participação de indivíduos de classes sociais privilegiadas, que gozam de prestígio social e até de fé pública, seja por sua profissão de alto escalão no mercado de trabalho ou por algum cargo público de renome.

computador e a sua localização; ii) buscar, remotamente, dados armazenados em computador ou em nuvem, podendo ocorrer o espelhamento desses dados; iii) realizar o monitoramento remoto do uso do computador que possibilitaria a captura de dados, a partir da inserção de *malwares*; iv) interceptar os conteúdos das comunicações eletrônicas, por exemplo, e-mail, mensagens de texto e *chats* via WhatsApp ou Telegram; v) "sequestrar" a *webcam* do investigado (observação visual) para identificar o usuário e determinar a sua localização; e vi) deletar remotamente dados ilegais, como pornografia infantil, ou remover vírus de computadores infectados como forma de prevenir ataques coordenados (*Ibidem,* p. 27-28).

Para a presente discussão, destacamos a possibilidade de interceptação dos conteúdos das comunicações eletrônicas pelo *hacking* policial. Os autores sintetizam que seria nesta modalidade a principal oportunidade de contornar a dificuldade em se acessar o conteúdo das comunicações criptografadas:

> Sice most of these services nowadays use end-to-end encryption, and interception through the service provider is often not possible, interception at the source before encryption (or at the destination after decryption) may be the only way to capture the contents of online communications" (Skorvanek; Koops; Newel; Roberts 2019, p. 11 *apud* Ferreira, 2021, p. 28.

Dessa forma, inexistindo outros meios de prova cabíveis, e, havendo indícios mínimos de autoria e participação, o direito à segurança deve sobressair aos demais direitos. Para tanto, considerando os entraves ao acesso excepcional ao conteúdo dos diálogos criptografados, consideramos que a técnica do *hacking* policial, seja por meio de *softwares* espião, ou, até mesmo, infiltração policial virtual, são meios que consideramos efetivos para determinados casos ou soluções pontuais.

CONSIDERAÇÕES FINAIS

Ao longo do estudo, analisamos a evolução da jurisprudência, tanto no Brasil quanto nos Estados Unidos, demonstrando que o conceito de privacidade tem se expandido ao longo do tempo para acompanhar as novas realidades tecnológicas. A trilogia *Olmstead-Katz-Kyllo*, julgada pela Suprema Corte Americana, exemplifica essa transformação, indicando a necessidade de um equilíbrio entre a eficiência da investigação criminal e a proteção da privacidade. No Brasil, a jurisprudência do Supremo Tribunal Federal também tem caminhado para relativizar direitos como a inviolabilidade domiciliar e o sigilo das comunicações em situações que envolvem crimes de grande complexidade. No entanto, ainda é preciso um olhar mais crítico e cauteloso quando da análise entre os bens liberdade coletiva e segurança pública.

A análise das interceptações telefônicas e ambientais revelou importantes pontos de controvérsia, especialmente no que tange à constitucionalidade da interceptação de comunicações telemáticas, ao prazo de duração das interceptações e à possibilidade de sua utilização em caráter preventivo. Enquanto há argumentos que defendem uma interpretação estrita da Constituição, limitando a interceptação apenas ao fluxo de comunicações telefônicas, há também uma corrente que sustenta a necessidade de uma interpretação mais ampla, que contemple os avanços tecnológicos e o uso crescente de comunicações digitais no planejamento de crimes. Sendo esta última corrente mais adequada, pois reconhece a necessidade de adaptação do Direito às novas estratégias utilizadas por organizações criminosas.

A constitucionalidade da Lei de Interceptações (Lei nº 9.296/1996) também foi objeto de debate, especialmente no que se refere à sua aplicação a comunicações telemáticas. A interpretação mais adequada é aquela que amplia a possibilidade de interceptação para além das comunicações telefônicas convencionais, englobando novas formas de troca de mensagens, como aplicativos e redes digitais. Limitar essa possibilidade enfraqueceria a atuação do Estado e permitiria que criminosos se aproveitassem de brechas legais para driblar as investigações.

Dentre os temas analisados, um dos pontos mais controversos é a possibilidade de estabelecimento de um prazo máximo absoluto para interceptações telefônicas. Embora o argumento em favor dessa limitação seja a proteção contra abusos estatais e vigilância permanente, essa restrição desconsidera a realidade das investigações criminais complexas, especialmente aquelas que envolvem organizações criminosas. Crimes dessa natureza frequentemente exigem monitoramento prolongado para identificar todos os envolvidos e coletar provas robustas que sustentem uma acusação formal.

Outro ponto de grande relevância é a dificuldade de acesso a comunicações criptografadas, que tem levado à busca por alternativas como o *hacking* policial. Apesar de sua eficácia, essa técnica exige uma regulamentação criteriosa para evitar que se transforme em um instrumento de vigilância descontrolada. O *hacking* policial pode ser uma solução viável quando não houver outros meios de obtenção de prova, mas seu uso deve ser excepcional, autorizado judicialmente e acompanhado por mecanismos de auditoria que garantam sua aplicação dentro dos limites legais.

Diante desse cenário, conclui-se que o enfrentamento eficaz da criminalidade contemporânea, especialmente em sua forma organizada e tecnologicamente sofisticada, exige do ordenamento jurídico uma constante atualização interpretativa e normativa. A proteção dos direitos fundamentais, notadamente da privacidade e da inviolabilidade das comunicações, não deve ser encarada como obstáculo absoluto à atividade investigativa, mas como parâmetro essencial para sua legitimidade. A análise realizada demonstra que é possível — e necessário — compatibilizar o uso de técnicas modernas de investigação com o respeito às garantias constitucionais, desde que submetidas a rígido controle judicial, respaldadas por legislação clara e aplicadas de forma proporcional e excepcional.

REFERÊNCIAS

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais**. São Paulo: InternetLab, 2017.

ANDRADE, Manuelda Costa. **Sobre as proibições de prova em processo penal**. Coimbra: Coimbra Editora, 2006.

ARANTES FILHO, Márcio Geraldo Britto. **A interceptação de comunicações entre pessoas presentes como meio de investigação de prova no direito processual penal brasileiro**. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2011.

AVENA, Norberto **Processo penal** / Norberto Avena. – 15. ed. – Rio de Janeiro: Método, 2023.

BADARÓ, Gustavo Henrique Righi Ivahy. **Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia**. In: LIMA, Joel Corrêa de (Coord.). Temas para uma perspectiva crítica do direito: homenagem ao professor Geraldo Prado. 2. ed. Rubens Roberto Rebello (Coord.) CASARA. 2. ed. Rio de Janeiro: Lumen Juris, 2012.
BANDEIRA, Gustavo. **A interceptação do fluxo de comunicações por sistemas de informática e sua constitucionalidade**. Revista da EMERJ, v. 6, n. 22, 2003.
DE SOUZA ABREU, Jacqueline; SMANIO, Gianluca Martins. **Compatibilizando o uso de tecnologia em investigações com direitos fundamentais: o caso das interceptações ambientais**. Revista Brasileira de Direito Processual Penal, [S. l.], v. 5, n. 3, p. 1449–1482, 2019. Disponível em: DOI:10.22197/rbdpp.v5i3.262.
DUTRA, Lucas Ferreira. **O erro na diferenciação entre as polícias judiciária e investigativa**. Revista Consultor Jurídico, 20 de outubro de 2022. Disponível em: www.conjur.com.br
FERRAZ JR., Tercio Sampaio. **Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado**. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 88, p. 439-459, 1993.
FERREIRA, Caio Porto. **Hacking e infiltração policiais em resposta ao uso de criptografia por organizações criminosas**. Dossiê - Investigação Criminal e Novas Tecnologias para obtenção de prova. Revista Brasileira de Ciências Policiais. Brasília, v.12, N. 5, P. 19-48, Mai/Ago, 2021.
FILIPPI, Leonardo. **Intercettazione di comunicazioni**. In: Enciclopedia Giuridica - Istitvto Enciclopedia Italiana fondada da Giovanni Treccani. Roma: Instituto Poligrafico e Zecca dello Stato, 2001. Vol. XVII, p. 1-8
FREGADOLLI, Luciana. **O Direito à Intimidade e a Prova Ilícita**. Belo Horizonte: Del Rey, 1998.
GUARAGNI, Fábio André; TAMBORLIN, Fábio Augusto Hernandes. **A utilização de drones na investigação de infrações penais: uma análise à luz do direito à privacidade**. Cadernos de Direito Actual nº 26. Núm. Ordinário (2024), pp. 41-58ISSN 2340-860X -·ISSNe 2386-5229. 2024.
KAYSER, Pierre**. La protection de la vie privée**. Paris: Econômica, 1984. t. 1.
KNIJNIK, D. **A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI,** Revista da Escola da Magistratura do TRF da 4ª Região, ano 2, número 4,Porto Alegre/RS, 2016
LIMA, R.B.D**. Manual de processo penal**. Volume único, 9ºed., rev. ampl. e atual, JusPodivm, Salvador, 2021.
_____. **Manual de processo penal**, vol. I. Niterói-RJ: Impetus, 2020.
MENDES, Gilmar Ferreira **Curso de Direito Constitucional** / Gilmar Ferreira Mendes, Paulo Gustavo Gonet Branco. – 18. ed. – São Paulo: SaraivaJur, 2023. (Série IDP – Linha Doutrina)
MORAES, Alexandre de. **Direitos Humanos Fundamentais**. São Paulo, Atlas, 1998.
NERY JÚNIOR, Nelson e NERY, Rosa Maria de Andrade. **Código de Processo Civil Comentado**. Revista dos Tribunais, 2001.
ORLANDI, R. **O procedimento penal por fatos de criminalidade organizada: do maxi-processo ao «grande processo»**. Rev. Brasileira Direito Processual Penal [Internet]. 2021 Sep;7(3):2105–26. Available from: https://doi.org/10.22197/rbdpp.v7i3.634
QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. **Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função**

fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. Internet & sociedade, pág. 67, 2020. Acesso em 20 de janeiro de 2025, disponível em:

RIBEIRO, Pedro Melo. **A regulamentação da captação ambiental e o núcleo intangível da vida privada**. In: WALMSLEY, Andréa; CIRENO, Lígia; BARBOZA, Márcia Noll (orgs). Inovações da Lei nº 13.964, de 24 de dezembro de 2019. Brasília: MPF, 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo** José Afonso da Silva. -39. ed., rev. e atual. Até a Emenda Constitucional n. 90, de 15.9.2015. -São Paulo: Malheiros, 2016. 936 p.; 21 em.

STRECK, Lenio Luiz. **As Interceptações Telefônicas e os Direitos Fundamentais**. Porto Alegre, Livraria do Advogado, 2001.

ŠKORVÁNEK, Ivan; KOOPS, Bert-Jaap; NEWEL, Bryce Clayton; ROBERTS, Andrew. **My computer is my castle:new privacy frameworks to regulate police hacking**. Tilburg University. TILT Law & Technolog y, 2019.