

EXTENSIVO **2026** **DELEGADO** **DE POLÍCIA**

Legislação Penal Especial

Interceptação Telefônica – Parte 01
(Lei nº 9.296/1996)



Sumário

LEGISLAÇÃO PENAL ESPECIAL.....	3
<i>Lei de Interceptação Telefônica</i>	3
1. SIGILO DA CORRESPONDÊNCIA, DAS COMUNICAÇÕES TELEGRÁFICAS, DE DADOS E DAS COMUNICAÇÕES TELEFÔNICAS	3
2. O CONCEITO DE INTERCEPTAÇÃO TELEFÔNICA	5
3. COMUNICAÇÕES TELEFÔNICAS DE QUALQUER NATUREZA.....	8
3.1.4 (Des) necessidade de autorização judicial prévia para a extração de dados e de conversas registradas em aparelhos celulares apreendidos	9
3.1.4.1 Whatsapp web e prints de mensagem de Whatsapp	15
4. QUEBRA DO SIGILO DE DADOS TELEFÔNICOS	18
4.1 Requisição de informações acerca das estações rádio base (ERB's)	21
5. FINALIDADE DA INTERCEPTAÇÃO TELEFÔNICA: MEIO DE OBTENÇÃO DE PROVA EM INVESTIGAÇÃO CRIMINAL OU INSTRUÇÃO PROCESSUAL PENAL	25



LEGISLAÇÃO PENAL ESPECIAL

Lei de Interceptação Telefônica

Fala, futuras e futuros Delegados de Polícia, tudo bem com vocês? A Lei nº 9.296/1996, que dispõe sobre a **Interceptação Telefônica**, é sem dúvidas de altíssima relevância para as provas de Delegado de Polícia, inclusive para segunda fase e oral. Vamos nessa?

1. SIGILO DA CORRESPONDÊNCIA, DAS COMUNICAÇÕES TELEGRÁFICAS, DE DADOS E DAS COMUNICAÇÕES TELEFÔNICAS

A Constituição Federal, em seu art. 5º, assegura a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, dos dados e das comunicações telefônicas. A própria Carta Magna, contudo, estabelece exceção expressa quanto às comunicações telefônicas, permitindo a quebra do sigilo mediante ordem judicial, desde que para fins de investigação criminal ou instrução processual penal, nos termos da lei.

CF/88

Art. 5º (...)

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Apesar da redação literal parecer indicar apenas a relativização do sigilo telefônico, a doutrina e a jurisprudência consolidaram o entendimento de que não existem direitos fundamentais absolutos. Assim, garantias constitucionais devem ser interpretadas à luz da ponderação com outros valores constitucionais relevantes, especialmente quando em conflito com a ordem pública ou com direitos de terceiros.

Sobre tal assunto o Ministro Celso de Mello foi enfático ao afirmar que:

“(...) Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito



ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros. (...)”

(STF - MS: 23452 RJ, Relator.: CELSO DE MELLO, Data de Julgamento: 16/09/1999, Tribunal Pleno, Data de Publicação: DJ 12-05-2000 PP-00020 EMENT VOL-01990-01 PP-00086)

Esse entendimento permite hipóteses de mitigação do sigilo em situações específicas. No âmbito penitenciário, por exemplo, admite-se a interceptação de correspondências de presos pela administração carcerária, com fundamento na segurança pública e na disciplina interna, evitando que o sigilo seja utilizado como instrumento para práticas ilícitas.

Quanto à reserva de jurisdição, a regra geral é que a quebra de sigilo de dados bancários, fiscais, telefônicos, depende de decisão judicial fundamentada, sob pena de ilicitude da prova, em respeito ao direito fundamental à intimidade (art. 5º, X, da CF/88). Nesse viés, a jurisprudência do Supremo Tribunal Federal tem reafirmado que medidas investigativas que impliquem restrição a direitos fundamentais exigem fundamentação concreta e individualizada, como fez no seguinte julgado:

“(...)reconhecer a ilicitude das provas produzidas a partir da quebra dos sigilos fiscal, bancário e telefônico das pacientes, sem a devida fundamentação. Por conseguinte, determinou-se o desentranhamento dessas provas dos autos da Ação Penal 2004.83.00.026319-3, que tramita no Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado de Pernambuco, nos termos do voto do Relator. Decisão unânime.

(STF - HC: 96056 PE, Relator.: Min. GILMAR MENDES, Data de Julgamento: 28/06/2011, Segunda Turma, Data de Publicação: ACÓRDÃO ELETRÔNICO DJe-089 DIVULG 07-05-2012 PUBLIC 08-05-2012)

Ademais, o STJ no julgamento do AgRg na Rcl 47.883/RJ destacou que **informações meramente identificadoras de aparelhos telefônicos**, como marca ou modelo, não se inserem no âmbito de proteção do sigilo das comunicações previsto no art. 5º, XII, da Constituição, que tutela essencialmente **o conteúdo das mensagens, áudios e imagens armazenadas ou transmitidas**¹.

Desse modo, a proteção constitucional ao sigilo das comunicações exige constante ponderação entre direitos fundamentais individuais e interesses públicos relevantes, cabendo ao Poder Judiciário exercer controle rigoroso sobre as medidas restritivas, garantindo que sejam sempre proporcionais, fundamentadas e juridicamente justificadas.

¹ STJ - AgRg na Rcl: 47883 RJ 2024/0291763-6, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 09/10/2024, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 11/10/2024. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202402917636&dt_publicacao=11/10/2024.



2. O CONCEITO DE INTERCEPTAÇÃO TELEFÔNICA

No âmbito da Lei nº 9.296/96, o termo “interceptar” não deve ser compreendido em seu sentido etimológico comum, associado à ideia de interromper ou impedir a comunicação. Juridicamente, interceptação significa captar comunicação alheia, tomando conhecimento de seu conteúdo. O núcleo do instituto reside na intervenção de um terceiro estranho à conversa, que passa a ter ciência do diálogo travado entre outras pessoas.

A doutrina estabelece distinção precisa entre três modalidades que não se confundem:

- **Interceptação telefônica em sentido estrito** → Ocorre quando um terceiro capta a comunicação sem o conhecimento de qualquer dos interlocutores. Trata-se da hipótese paradigmática regulada pela Lei nº 9.296/96.
- **Escuta telefônica** → Envolve a atuação de um terceiro, mas com o conhecimento de apenas um dos comunicadores. É o que ocorre, por exemplo, quando vítima de extorsão ou familiar de sequestrado autoriza a autoridade policial a monitorar as ligações.
- **Gravação telefônica (também chamada de clandestina)** → É realizada diretamente por um dos próprios interlocutores, sem interferência de terceiro. Trata-se de autogravação, situação juridicamente distinta da interceptação.

A comunicação ambiental refere-se às **interações verbais** que ocorrem diretamente no meio ambiente, sem o emprego de meios físicos ou artificiais de transmissão, como redes telefônicas, cabos ou sistemas telemáticos. Trata-se, essencialmente, de conversas travadas presencialmente entre duas ou mais pessoas, em ambientes públicos ou privados.

Sob o ponto de vista constitucional, as comunicações ambientais submetem-se a regime jurídico distinto daquele aplicável às comunicações telefônicas. Enquanto a interceptação telefônica encontra fundamento específico no art. 5º, XII, da CF, a análise da licitude das captações ambientais tem como parâmetro principal o direito fundamental à intimidade e à vida privada, previsto no art. 5º, X, da Constituição.

A doutrina costuma subdividir a captação das comunicações ambientais em **três modalidades** principais (**isso é muito importante para as provas de Delegado**):

- **Interceptação ambiental** → Consiste na captação sub-reptícia feita por terceiro, sem que nenhum dos presentes tenha ciência. Exemplo recorrente é a filmagem policial de indivíduos praticando crimes em via pública sem ciência dos envolvidos.
- **Escuta ambiental** → Ocorre quando um dos participantes consente com a captação realizada por terceiro. Situação típica é a de vítima que, com apoio da polícia, registra o momento em que sofre exigência de vantagem indevida, como nos casos de concussão.



- **Gravação ambiental** → Consiste no registro realizado por um dos próprios interlocutores, mediante utilização de dispositivos como gravadores ou câmeras ocultas. Nessa hipótese, não há intervenção de terceiro, o que repercute diretamente na análise da licitude da prova.

A disciplina da Lei nº 9.296/96 incide primordialmente sobre a interceptação telefônica em sentido estrito e sobre a escuta. Já as gravações realizadas por um dos interlocutores não se submetem, em regra, ao sigilo das comunicações previsto no art. 5º, XII, da Constituição, mas à tutela da intimidade (art. 5º, X, da CF). Por essa razão, as gravações feitas por um dos participantes são consideradas, em regra, lícitas mesmo sem autorização judicial, desde que haja justa causa, como nas hipóteses de legítima defesa.

Lei nº 9.296/96

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 sigredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Além disso, também é válida a gravação realizada com o consentimento do genitor para proteção de filho absolutamente incapaz, pois o pai atua no exercício do poder-dever de proteção e vigilância. Por outro lado, a intervenção de terceiro na comunicação alheia exige, geralmente, autorização judicial prévia para que a prova seja admitida, sob pena de ilicitude. A exigência é ainda mais rigorosa quando o interlocutor que tem ciência da captação encontra-se sob custódia policial, sem plena liberdade de assentimento.

A **interceptação telefônica** em sentido **estrito** possui natureza jurídica de **meio de obtenção de prova**, mais especificamente, é classificada como **medida cautelar processual de natureza coativa**, voltada à captação de elementos informativos relevantes para a persecução penal. Trata-se de uma forma de apreensão imprópria, pois não recai sobre um objeto físico tradicional, mas sobre elementos imateriais, como os dados fonéticos que compõem a conversação telefônica. O objetivo da medida é viabilizar a captura e preservação desses elementos para futura utilização no processo penal.

- A **fonte de prova** corresponde às **comunicações telefônicas** propriamente ditas, das quais se extrai a comprovação da infração penal ou do vínculo do investigado com o fato delituoso.
- A **materialização da fonte** ocorre por meio da **gravação da interceptação**, que representa o resultado técnico da diligência.
- Já o **meio de prova** consiste na **transcrição do conteúdo captado**, documento que será efetivamente juntado aos autos e submetido à valoração judicial.

Em síntese, a **interceptação telefônica** tem como **finalidade a obtenção de prova** que se materializa em suportes documentais, como autos circunstanciados e transcrições, ou até mesmo em prova oral derivada.



Esses elementos permitem a fixação dos fatos no processo e servem de base para a formação do convencimento do magistrado, como afirma Gomes.²

CAIU NA PC/SP – 2011 – BANCA PRÓPRIA: Sobre a Lei nº 9.296/96 - Interceptação de Comunicações Telefônicas - é correto afirmar que o texto legal não abrange a interceptação do fluxo de comunicações em sistemas de telemática.³

CAIU NA PC/BA – 2013 – CESPE: Um delegado de polícia, tendo recebido denúncia anônima de que Milton estaria abusando sexualmente de sua própria filha, requereu, antes mesmo de colher provas acerca da informação recebida, a juiz da vara criminal competente a interceptação das comunicações telefônicas de Milton pelo prazo de quinze dias, sucessivamente prorrogado durante os quarenta e cinco dias de investigação. Kátia, ex-mulher de Milton, contratou o advogado Caio para acompanhar o inquérito policial instaurado. Milton, então, ainda no curso da investigação, resolveu interceptar, diretamente e sem o conhecimento de Caio e Kátia, as ligações telefônicas entre eles, tendo tomado conhecimento, devido às interceptações, de que o advogado cometera o crime de tráfico de influência. Em razão disso, Milton procurou Kátia e solicitou que ela concordasse com a divulgação do conteúdo das gravações telefônicas, ao que Kátia anuiu expressamente. Milton, então, apresentou ao delegado o conteúdo das gravações, que foram utilizadas para subsidiar ação penal iniciada pelo MP contra Caio, pela prática do crime de tráfico de influência. Com base nessa situação hipotética, julgue o item seguinte, a respeito das interceptações telefônicas.

A interceptação telefônica realizada por Milton é ilegal, porquanto desprovida da necessária autorização judicial.⁴

CAIU NA PF – 2018 – CESPE: Com referência à interceptação de comunicação telefônica, ao crime de tráfico ilícito de entorpecentes, ao crime de lavagem de capitais e a crimes cibernéticos, julgue o seguinte item. A interceptação da comunicação telefônica poderá ser realizada de ofício pela autoridade policial desde que o IP tenha como objetivo investigar crime hediondo, organização criminosa ou tráfico ilícito de entorpecentes.⁵

CAIU NA PC/SE – 2020 – CESPE: Acerca dos meios de provas, suas espécies, classificação e valoração, julgue o item a seguir.

Interceptação telefônica produzida regularmente no curso de inquérito policial constitui meio de prova nominada, voltada ao convencimento da autoridade judiciária sobre determinado fato.⁶

² LIMA, Renato Brasileiro de. **Manual de Legislação Criminal Especial Comentada: Volume Único**. 14 ed. São Paulo: Editora Juspodivm, 2026, p.845.

³ **ERRADO.** O texto da Lei nº 9.296/96 abrange sim a interceptação do fluxo de comunicações em sistemas de telemática, conforme descrito no artigo 1º.

⁴ **CERTO.** O item está certo, conforme artigo 1º da Lei 9.296/96

⁵ **ERRADO.** A CF traz em seu rol de direitos e garantias individuais que é inviolável o sigilo das comunicações telefônicas, salvo por **ordem judicial** nas hipóteses estabelecidas em lei e para fins de investigação criminal ou instrução processual penal. A Lei 9.296 de 1996 regulamentou a previsão constitucional e traz a necessidade de autorização judicial em seu art. 1º.

⁶ **ERRADO.** A interceptação telefônica é meio de obtenção de prova e não meio de prova.



3. COMUNICAÇÕES TELEFÔNICAS DE QUALQUER NATUREZA

A Lei nº 9.296/96 disciplina a interceptação de comunicações telefônicas “de qualquer natureza”. A interpretação dessa expressão deve ser **progressiva**, acompanhando a evolução tecnológica. Assim, o conceito não se limita à transmissão de voz humana, mas abrange também a circulação de símbolos, sinais, escritos, imagens e sons por meio de telefonia fixa ou móvel. Nesse contexto, incluem-se comunicações realizadas por fax, modem, internet e correio eletrônico, desde que caracterizado o fluxo comunicacional. A proteção jurídica recai sobre a comunicação em andamento, independentemente da tecnologia empregada.

A lei também alcança a interceptação do fluxo de comunicações em sistemas de informática e telemática, como prevê o parágrafo único do art. 1º da Lei nº 9.296/96. A telemática resulta da convergência entre informática e telecomunicações, permitindo a manipulação e transmissão de dados em redes digitais.

Embora haja posicionamentos doutrinário sustentando a inexistência de previsão constitucional expressa para essa ampliação, como é o caso de Vicente Greco Filho que afirmar que “*a garantia constitucional do sigilo é a regra e a interceptação a exceção, de forma que a interpretação deve ser restritiva quanto a esta (exceptiora non sunt amplianda)*” prevalece o entendimento de que a **proteção constitucional ao sigilo das comunicações não pode ser interpretada de forma restritiva a ponto de inviabilizar o combate a ilícitos praticados por meios tecnológicos modernos.**⁷

A jurisprudência tem considerado válida a interceptação das comunicações telemáticas. Em salas de bate-papo abertas na internet, por exemplo, o STJ entende que não há proteção de sigilo, pois se trata de ambientes virtuais de acesso irrestrito, voltados à interação pública e informal.

RECURSO EM HABEAS CORPUS. PENAL. ART. 241. INTERNET. SALA DE BATE PAPO. SIGILO DAS COMUNICAÇÕES. INVIABILIDADE. TRANCAMENTO DO INQUÉRITO POLICIAL. NECESSIDADE DE EXAME APROFUNDADO DO CONJUNTO PROBATÓRIO. INADEQUAÇÃO DA VIA ELEITA.

1. A conversa realizada em “sala de bate papo” da internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais.
2. O trancamento do inquérito policial em sede de recurso em habeas corpus é medida excepcional, somente admitida quando constatada, prima facie, a atipicidade da conduta ou a negativa de autoria.
3. Recurso que se nega provimento, com a recomendação de que o juízo monocrático determine a realização imediata da perícia requerida pelo parquet nos autos, sob pena de trancamento da ação penal.

⁷ LIMA, Renato Brasileiro de. **Manual de Legislação Criminal Especial Comentada: Volume Único**. 14 ed. São Paulo: Editora Juspodivm, 2026, p.846.



(STJ - RHC: 18116 SP 2005/0120859-5, Relator.: Ministro HÉLIO QUAGLIA BARBOSA, Data de Julgamento: 16/02/2006, T6 - SEXTA TURMA, Data de Publicação: DJ 06/03/2006 p. 443RSTJ vol. 201 p. 636)

No âmbito trabalhista, o Tribunal Superior do Trabalho firmou entendimento de que o **empregador pode monitorar e-mails corporativos**, por se tratar de ferramentas de trabalho disponibilizadas pela empresa, inexistindo expectativa legítima de privacidade plena por parte do empregado.

PROVA ILÍCITA. -E-MAIL- CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO.

(...)

5. Pode o empregado monitorar e rastrear a atividade do empregado no ambiente de trabalho, em e-mail- corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal.

(TST - RR: 613002320005100013 61300-23.2000.5.10 .0013, Relator.: João Oreste Dalazen, Data de Julgamento: 18/05/2005, 1ª Turma, Data de Publicação: DJ 10/06/2005.)

3.1.4 (Des) necessidade de autorização judicial prévia para a extração de dados e de conversas registradas em aparelhos celulares apreendidos

A controvérsia acerca da necessidade de autorização judicial para acesso a dados e conversas armazenadas em aparelhos celulares apreendidos insere-se no contexto da evolução para o direito probatório de terceira geração. O debate decorre da ampliação exponencial da capacidade tecnológica dos smartphones, que passaram a concentrar vasta parcela da vida privada do indivíduo.

Em precedente mais antigo, o STF considerou lícito o acesso direto, pela polícia, aos registros de chamadas e à agenda eletrônica de aparelho apreendido logo após prisão em flagrante. O fundamento foi o de que tal conduta não configuraria interceptação telefônica, mas mera colheita de elementos informativos relacionados à autoria e materialidade delitiva, nos termos do art. 6º do CPP.

HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA.

(...)



2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência.

2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados.

2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação.

(...)

(STF - HC: 91867 PA, Relator.: Min. GILMAR MENDES, Data de Julgamento: 24/04/2012, Segunda Turma, Data de Publicação: ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012)

Esse entendimento, contudo, estava ancorado em realidade tecnológica distinta, referente a fatos ocorridos em 2004, quando os aparelhos não possuíam internet de banda larga nem aplicativos de mensagens instantâneas. Com o advento dos smartphones, o acesso ao dispositivo passou a permitir a devassa ampla da intimidade do usuário, por meio de aplicativos como WhatsApp e Telegram, exigindo reinterpretação das garantias constitucionais à luz da proteção da vida privada e do sigilo das comunicações.

A 6ª Turma do STJ, no julgamento do RHC 51.531/RO, firmou entendimento de que o acesso a conversas de WhatsApp e a dados armazenados em aparelho celular **exige prévia autorização judicial, sob pena de nulidade da prova**. O fundamento reside na proteção conferida pelo art. 5º, XII, da Constituição Federal e pela Lei nº 9.296/96, haja vista que as mensagens do celular devem ser consideradas como um tipo de comunicação escrita imediata. Nesse viés, se há necessidade de autorização judicial para a quebra do sigilo do correio eletrônico, o mesmo entendimento deve ser aplicado as conversas dos aplicativos digitais.

“Sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante. STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Info 583).”



Segundo esse entendimento, é irrelevante que o aparelho tenha sido apreendido em flagrante. A autorização judicial é necessária tanto para a leitura de mensagens já existentes quanto para a eventual atuação policial simulando a identidade do titular em negociações. Logo, em razão da grande evolução tecnológica, o entendimento do STF acaba por ser inadequado.

No entanto, jurisprudência do STJ admite hipóteses específicas em que o acesso pode ocorrer sem mandado judicial, mediante distinção fundamentada. São elas:

- **Celular de vítima falecida** → Admite-se o acesso quando o aparelho pertence a vítima falecida e é entregue pela família para investigação do crime, inexistindo sigilo do titular a ser resguardado em favor do acusado.

Não há ilegalidade na perícia de aparelho de telefonia celular pela polícia, sem prévia autorização judicial, na hipótese em que seu proprietário - a vítima - foi morto, tendo o referido telefone sido entregue à autoridade policial por sua esposa. STJ. 6ª Turma. RHC 86076-MT, Rel. Min. Sebastião Reis Júnior, Rel. Acd. Min. Rogério Schietti Cruz, julgado em 19/10/2017 (Info 617).

- **Situação excepcional que justifique o acesso das autoridades policiais** → Também se reconhece a possibilidade de acesso imediato em situações de urgência excepcional, como nos casos de extorsão mediante sequestro, quando a demora na obtenção do mandado puder acarretar risco concreto à vida da vítima. Conforme entendimento previsto no RHC 76.324/DF.

“(…) Não descarto, de forma absoluta, que, a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativo recém-abandonado: o acesso incontinenti aos dados ali mantidos pode ser decisivo para a libertação do sequestrado.” (STJ - HC: 617232 SP 2020/0260299-8, Relator.: Ministro NEFI CORDEIRO, Data de Julgamento: 23/02/2021, T6 - SEXTA TURMA, Data de Publicação: DJe 26/02/2021)

- **Materialidade do crime incorporada no celular** → Outra hipótese ocorre quando o próprio aparelho constitui corpo de delito ou instrumento do crime, como em situações de compartilhamento de imagens ilícitas armazenadas no dispositivo. Como compreendeu a 6ª turma do STJ no RHC 108.262/MS.

“Como cedo, o entendimento prevalecente nesta Corte e no Supremo Tribunal Federal é o de que são ilícitas as provas obtidas de aparelhos celulares sem prévia e devida autorização, seja judicial seja do réu, ressalvados os casos excepcionais em que a observância de tal procedimento põe em risco a integridade de vítima ou traz prejuízos à investigação.” (RHC 108.262/MS, Rel. Ministro ANTONIO SALDANHA PALHEIRO, SEXTA TURMA, julgado em 5/9/2019, DJe 9/12/2019)



- **Autorização do proprietário** → É igualmente possível o acesso quando houver consentimento válido e voluntário do proprietário do aparelho. Da mesma forma, se o indivíduo nega a titularidade de celular encontrado em sua posse ou proximidade, admite-se a consulta aos dados para identificação do verdadeiro proprietário.

“(...) denota-se que os 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 ilegalidade.” (STJ - HC: 537274 MG 2019/0297159-6, Relator.: Ministro LEOPOLDO DE ARRUDA RAPOSO (DESEMBARGADOR CONVOCADO DO TJ/PE), Data de Julgamento: 19/11/2019, T5 - QUINTA TURMA, Data de Publicação: DJe 26/11/2019)

- **Localização de aparelho próximo ao flagranteado que nega a propriedade** → O STJ estabeleceu uma distinção (*distinguishing*) entre a extração de dados sem autorização judicial e a hipótese em que o indivíduo nega ser proprietário do celular encontrado próximo a ele. Se o aparelho estiver abandonado em via pública e o agente negar a sua propriedade, os policiais podem realizar uma breve consulta aos dados do dispositivo com o objetivo de identificar o verdadeiro proprietário. Nessa situação, afasta-se a ilicitude do acesso.

“O acesso a dados de celular abandonado em via pública afasta a ilicitude das provas obtidas.” (STJ – AgRg no AREsp n. 1.573.424 – SP, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 9/9/2020, DJe de 15/9/2020.)

- **Acesso exclusivo aos registros telefônicos e à agenda** → Embora a devassa de dados, como regra, exija autorização judicial, a 5ª Turma do STJ possui precedentes indicando que o acesso restrito aos **registros de chamadas e à agenda de contatos** não é ilegal. Segundo esse entendimento, tais dados específicos não estariam protegidos pela reserva de jurisdição prevista no art. 5º, XII, da Constituição Federal.

“Esta Corte Superior entende que a devassa nos dados constantes no aparelho celular, como mensagens de texto e conversas por meio de aplicativos, diretamente pela polícia, sem autorização judicial, constitui meio de prova ilícito e, consequentemente, os dados obtidos não podem constituir prova, devendo ser excluídos dos autos. No entanto, no presente caso, 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 prova. - Precedentes: AgRg no REsp n. 1.760.815/PR, Ministra Laurita Vaz, Sexta Turma, DJe 13/11/2018 e HC n. 91.867/PA, Ministro Gilmar Mendes, Segunda Turma, DJe 20/9/2012. (...)” (STJ - AgRg no REsp: 1853702 RS 2019/0374840-7, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 23/06/2020, T5 - QUINTA TURMA, Data de Publicação: DJe 30/06/2020)

- **Acesso a chip telefônico (SIMCARD) descartado** → Não há quebra de sigilo quando o chip telefônico é **descartado pelo acusado em via pública durante a fuga**. O STJ considerou lícita a conduta de policiais que, ao encontrarem um chip descartado, inseriram-no em outro aparelho apenas para identificar a vítima do crime, sem realizar exame de dados privados do acusado.



"(...)A hipótese de **acesso ao chip telefônico descartado pelo acusado em via pública, produto de roubo, objeto que inclusive possibilitou a identificação de uma das vítimas, não se qualifica como quebra de sigilo telefônico.** Estabelecida a autoria através de outras provas independentes, que não apenas o reconhecimento realizado em sede de inquérito e confirmado em juízo, **afasta-se a alegação de nulidade da condenação por violação do artigo 226 do Código de Processo Penal.** (...)" (STJ - HC: 720605 PR 2022/0023640-2, Data de Julgamento: 09/08/2022, T5 - QUINTA TURMA, Data de Publicação: DJe 16/08/2022)

- **Celular apreendido em cumprimento de mandado de busca e apreensão** → Quando o aparelho celular é apreendido durante o cumprimento de **mandado de busca domiciliar expedido por autoridade judicial**, não é necessária nova autorização judicial específica para analisar o conteúdo armazenado no dispositivo. Isso porque o próprio mandado de busca já confere legitimidade para o acesso aos dados necessários à investigação.

"(...) Se ocorreu a busca e apreensão dos aparelhos de telefone celular, não há óbice para se adentrar ao seu conteúdo já armazenado, porquanto necessário ao deslinde do feito, sendo prescindível nova autorização judicial para análise e utilização dos dados neles armazenados." (STJ - RHC: 77232 SC 2016/0270659-2, Relator.: Ministro FELIX FISCHER, Data de Julgamento: 03/10/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 16/10/2017)

- **Aparelho apreendido no interior de estabelecimento prisional** → O acesso aos dados de celulares encontrados em posse de presos **dispensa autorização judicial**. O STF entende que o dever da Administração Penitenciária de preservar a **segurança, a disciplina e a ordem no ambiente prisional** prevalece sobre a reserva de jurisdição, sobretudo porque a posse de aparelhos celulares em estabelecimentos prisionais é expressamente proibida.

"Não há no ordenamento, via de regra, direitos fundamentais de caráter absoluto. Assim, **não há nulidade diante do acesso aos dados de celulares apreendidos ilicitamente em interior de estabelecimento prisional, uma vez que, em tais hipóteses, a garantia da inviolabilidade dos dados e comunicações fica mitigada em função da expressa proibição contida no art. 50, VII, da Lei de Execução Penal**, sendo, portanto, tal garantia relativizada em favor das regras de disciplina prisional que norteiam as execuções penais." (STJ - AgRg no HC: 661489 MG 2021/0119909-9, Relator.: Ministro ANTONIO SALDANHA PALHEIRO, Data de Julgamento: 29/03/2022, T6 - SEXTA TURMA, Data de Publicação: DJe 04/04/2022)

"[...] se é prescindível decisão judicial para a análise do conteúdo de correspondência, a fim de preservar interesses sociais e garantir a disciplina prisional, com mais razão se revela legítimo, para a mesma finalidade, o acesso dos dados e comunicações constantes em aparelhos celulares encontrados ilicitamente dentro do **estabelecimento penal**, pois a posse, o uso e o fornecimento do citado objeto são expressamente proibidos pelo ordenamento jurídico. Tratando-se de ilicitude manifesta e incontestável, não há direito ao sigilo e, por consequência, inexistente a possibilidade de invocar a proteção constitucional prevista no art. 5º, inciso XII, da Carta da República. Por certo, os direitos fundamentais não podem ser utilizados para a salvaguarda de práticas ilícitas, não sendo razoável pretender proteger aquele que age em notória desconformidade com as normas de regência" (HC n. 546.830/PR, relatora Ministra LAURITA VAZ, SEXTA TURMA, julgado em 9/3/2021, DJe 22/3/2021).



- **Dados fornecidos por integrante de grupo de WhatsApp** → Não há ilicitude na prova quando **um dos integrantes de grupo de WhatsApp fornece espontaneamente as conversas à polícia**, mesmo sem autorização judicial. Esse entendimento aplica-se especialmente em situações nas quais há divulgação de conteúdo criminoso no interior do grupo.

“(…) No caso, as **conversas foram fornecidas, espontaneamente, por um dos integrantes do grupo, no qual foi divulgado o conteúdo criminoso (ameaça e injúria)**. 4. Ademais, a prática delitiva foi demonstrada também por outros meios de prova, robustos e independentes das mensagens de WhatsApp acessadas no celular apreendido, constando da sentença condenatória que "durante todo o procedimento o acusado reconheceu ser o autor das postagens, inexistindo qualquer questionamento sobre a veracidade dos áudios que embasam a acusação ou de sua autoria". (STJ - AgRg no AREsp: 1910871 RS 2021/0190019-1, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 19/10/2021, T5 - QUINTA TURMA, Data de Publicação: DJE 25/10/2021)

- **Número do IMEI** → A identificação do IMEI (**International Mobile Equipment Identity**) é considerada mera averiguação do objeto do crime, nos termos do art. 6º, III, do Código de Processo Penal, não estando protegida pelo sigilo de dados. Por se tratar de um código que pode ser visualizado externamente, de forma semelhante ao chassi de um veículo, sua obtenção não exige o acesso ou o desbloqueio de dados privados do usuário.

“(…) **Não haveria, tal violação quando há somente averiguação do próprio objeto do crime** (art. 6º, inciso III, do CP), como por exemplo, o IMEI, **que é mera identificação do aparelho celular** e, portanto, **não está abarcado pelo sigilo de dados**.” (STJ - AgRg no AREsp: 2340362 MG 2023/0128564-9, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 08/08/2023, T5 - QUINTA TURMA, Data de Publicação: DJE 14/08/2023)

A controvérsia em relação a essa matéria foi decidida pelo STF em 2025, ao julgar o ARE 1.042.075/RJ (**Tema 977 da Repercussão Geral**), fixando a tese vinculante sobre **a necessidade de autorização judicial para acesso a dados armazenados em aparelho celular apreendido**.

A Corte distinguiu a **mera apreensão** do aparelho do **acesso** ao seu **conteúdo**. A apreensão do celular, realizada nos termos do art. 6º do CPP ou por ocasião de prisão em flagrante, não está sujeita à reserva de jurisdição; trata-se de providência investigativa legítima no contexto da atividade policial.

Diversa, contudo, é a situação do acesso aos dados armazenados no aparelho, que envolve diretamente direitos fundamentais à intimidade, à vida privada, à proteção de dados pessoais e à autodeterminação informacional (art. 5º, X e LXXIX, da CF).

Em se tratando de celular apreendido com base no art. 6º do CPP ou em flagrante delito, o acesso aos dados depende de: consentimento expresso e livre do titular; ou prévia decisão judicial fundamentada. A decisão judicial deve demonstrar, com base em elementos concretos, a proporcionalidade da medida e delimitar sua abrangência, em consonância com o art. 7º, III, e o art. 10, § 2º, da Lei nº 12.965/2014 (Marco Civil da



Internet). O STF enfatizou que a celeridade é imperativa nesses casos, devendo a autoridade policial atuar com máxima eficiência e o Judiciário conferir tramitação prioritária aos pedidos, inclusive em regime de plantão.

A Corte também tratou da hipótese de encontro fortuito de aparelho celular. Nessa situação específica, o acesso aos dados, exclusivamente para identificar o proprietário ou esclarecer a autoria do fato supostamente criminoso, não depende de consentimento ou prévia decisão judicial. Contudo, exige-se justificativa posterior da medida, demonstrando sua finalidade restrita e necessidade.

Ademais, o STF reconheceu que a autoridade policial pode adotar providências técnicas destinadas à preservação de dados e metadados contidos no aparelho, antes da obtenção da autorização judicial. Essa atuação, entretanto, não autoriza a exploração do conteúdo. Deve haver posterior justificativa formal da medida adotada, preservando-se a cadeia de custódia e os direitos fundamentais envolvidos.

“1. A mera apreensão do aparelho celular, nos termos do art. 6º do CPP ou em flagrante delito, não está sujeita à reserva de jurisdição. Contudo, o acesso aos dados nele contidos deve observar as seguintes condicionantes:

1.1 Nas hipóteses de encontro fortuito de aparelho celular, o acesso aos respectivos dados para o fim exclusivo de esclarecer a autoria do fato supostamente criminoso, ou de quem seja o seu proprietário, não depende de consentimento ou de prévia decisão judicial, desde que justificada posteriormente a adoção da medida.

1.2. Em se tratando de aparelho celular apreendido na forma do art. 6º do CPP ou por ocasião da prisão em flagrante, o acesso aos respectivos dados será condicionado ao consentimento expresso e livre do titular dos dados ou de prévia decisão judicial (art. 7º, III, e art. 10, § 2º, da Lei nº 12.965/2014) que justifique, com base em elementos concretos, a proporcionalidade da medida e delimite sua abrangência à luz de direitos fundamentais à intimidade, à privacidade, à proteção dos dados pessoais e à autodeterminação informacional, inclusive nos meios digitais (art. 5º, X e LXXIX, CF/88). Nesses casos, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possíveis e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão.

2. A autoridade policial poderá adotar as providências necessárias para a preservação dos dados e metadados contidos no aparelho celular apreendido, antes da autorização judicial, justificando, posteriormente, as razões de referido acesso.

3. As teses acima enunciadas só produzirão efeitos prospectivos, ressalvados os pedidos eventualmente formulados por defesas até a data do encerramento do presente julgamento.” STF. ARE 1.042.075/RJ, Rel. Min. Dias Toffoli, julgado em 25/06/2025 (Repercussão Geral – Tema 977) (Info 1184).

3.1.4.1 Whatsapp web e prints de mensagem de Whatsapp

O STJ também fixou limites quanto ao uso de técnicas investigativas que extrapolam a mera observação do conteúdo armazenado. O Superior Tribunal, em um primeiro momento, considerou nula a utilização do chamado “espelhamento” por meio do WhatsApp Web, ainda que precedida de decisão judicial, pois tal



mecanismo permite atuação ativa do investigador, inclusive envio ou exclusão de mensagens, além de possibilitar acesso retroativo a conversas anteriores.

“É nula decisão judicial que autoriza o espelhamento do WhatsApp via Código QR para acesso no WhatsApp Web. Também são nulas todas as provas e atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes. Não é possível aplicar a analogia entre o instituto da interceptação telefônica e o espelhamento, por meio do WhatsApp Web, das conversas realizadas pelo aplicativo WhatsApp.” STJ. 6ª Turma. RHC 99.735-SC, Rel. Min. Laurita Vaz, julgado em 27/11/2018 (Info 640).

Contudo, mais recentemente, o STJ assumiu uma posição diversa, amparando-se na Lei nº 9.296/1996 (Lei das Interceptações Telefônicas) e na Lei nº 12.850/2013 (Lei das Organizações Criminosas), desde que observada a cláusula de reserva de jurisdição. Vejamos:

“É possível a utilização, no ordenamento jurídico pátrio, de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético, inclusive via espelhamento do Whatsapp Web, desde que o uso da ação controlada na investigação criminal esteja amparado por autorização judicial.” STJ. 5ª Turma. AREsp 2.309.888-MG, Rel. Min. Reynaldo Soares da Fonseca, julgado em 17/10/2023 (Info 792).

Outrossim, reputou-se ilegal a substituição do chip (SIM card) do investigado pelo da autoridade policial, uma vez que essa prática suspende o serviço do usuário e permite interação ativa nas conversas, medida não prevista na Lei nº 9.296/96.

“A Lei nº 9.296/96 não autoriza a suspensão do serviço telefônico ou do fluxo da comunicação telemática mantida pelo usuário, tampouco a substituição do investigado e titular da linha por agente indicado pela autoridade policial.” STJ. 6ª Turma. REsp 1806792-SP, Rel. Min. Laurita Vaz, julgado em 11/05/2021 (Info 696).

Para encerrar, um outro assunto de extrema relevância – validade dos “prints” de conversas do WhatsApp. A validade de capturas de tela de conversas do WhatsApp depende essencialmente de **quem realizou a coleta da prova e da forma como ela foi obtida**.

Quando os prints são fornecidos por **particulares**, como um familiar da vítima ou um integrante do grupo, e são apresentados espontaneamente às autoridades, a prova tende a ser considerada **lícita**, sobretudo quando confirmada em juízo e quando não há indícios de adulteração do conteúdo.

Situação distinta ocorre quando a coleta é realizada **pela própria polícia**. Nesse caso, o ônus de demonstrar a integridade da prova recai sobre o Estado. Assim, a utilização de métodos rudimentares, como simplesmente acessar o aparelho e realizar capturas de tela, sem o emprego de **ferramentas especializadas de extração de dados**, como máquinas extratoras, pode comprometer a **cadeia de custódia** da prova digital. Nesses casos, a ausência de rigor técnico na coleta pode levar ao reconhecimento da **inadmissibilidade da prova**.

No âmbito das provas digitais, a validade do material extraído de dispositivos eletrônicos depende da observância de **requisitos técnicos fundamentais**. Entre eles, destaca-se a **auditabilidade**, que exige que as



partes possam verificar se o método técnico utilizado foi corretamente aplicado. Há também a **repetibilidade**, que pressupõe que a aplicação do mesmo procedimento produza sempre o mesmo resultado. Soma-se a isso a **reprodutibilidade**, segundo a qual métodos distintos, quando aplicados ao mesmo material, devem conduzir à mesma conclusão. Por fim, exige-se a **justificabilidade**, que impõe que o método utilizado seja reconhecido como adequado pela melhor técnica disponível.

“1. O instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.

2. Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.

3. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.

4. A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital.

5. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRg no RHC n. 143 .169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).

6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital.

7. Agravo regimental provido a fim de conceder a ordem de ofício para que sejam declaradas inadmissíveis as provas decorrentes da extração de dados do celular do corréu, bem como as delas decorrentes, devendo o Juízo singular avaliar a existência de demais elementos probatórios que sustentem a manutenção da condenação.

(STJ - AgRg no HC: 828054 RN 2023/0189615-0, Relator.: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 23/04/2024, T5 - QUINTA TURMA, Data de Publicação: DJe 29/04/2024)



Nesse contexto, a utilização do **algoritmo hash** é apontada como técnica essencial para assegurar o chamado **princípio da mesmidade** da prova digital. O hash funciona como uma espécie de “impressão digital” do arquivo: qualquer alteração no conteúdo, ainda que mínima, modifica completamente o código gerado, permitindo identificar eventual manipulação do material probatório.

Em síntese, pode-se destacar que uso do **WhatsApp Web** foi considerado inválido pela **6ª Turma do STJ** em razão da possibilidade de alteração de mensagens e de efeitos retroativos. Por outro lado, a **5ª Turma do STJ** admite sua utilização como forma de **infiltração virtual**, desde que exista **prévia autorização judicial**. No que se refere aos prints obtidos pela polícia, exige-se rigor técnico na extração dos dados, sob pena de nulidade da prova por **quebra da cadeia de custódia**. Por fim, a cadeia de custódia tem justamente a função de garantir que o material analisado seja **exatamente o mesmo que foi originalmente coletado**, preservando a autenticidade da prova e o chamado **princípio da mesmidade**.

4. QUEBRA DO SIGILO DE DADOS TELEFÔNICOS

A doutrina estabelece uma distinção clara entre **interceptação das comunicações** e **quebra de sigilo de dados telefônicos**. Enquanto a interceptação telefônica tem por objeto a captação do fluxo das comunicações em tempo real, a quebra de sigilo de dados telefônicos refere-se a **informações relacionadas a chamadas já realizadas**, ou seja, comunicações pretéritas.⁸

Nesse contexto, a quebra de sigilo de dados não recai sobre o conteúdo das conversas, mas sobre registros documentais mantidos pelas operadoras de telefonia. Entre esses dados, destacam-se a data e horário das ligações, o número do telefone chamado, e a duração das chamadas.

Embora esses registros não revelem o conteúdo das comunicações, sua relevância probatória é significativa, pois permitem o **cruzamento de dados**, o que pode viabilizar a identificação de comparsas ou a reconstrução da dinâmica da empreitada criminoso investigada.

Diferentemente do que ocorre na interceptação telefônica, a **Lei nº 9.296/1996 não se aplica à quebra de sigilo de dados telefônicos**. Isso porque a referida lei disciplina exclusivamente a interceptação de comunicações telefônicas, voltadas à captação de comunicações **atuais e em curso**. A jurisprudência consolidada do STF e do STJ entende que a proteção prevista no **art. 5º, XII, da Constituição Federal** incide sobre a **comunicação de dados**, e não sobre os dados em si considerados.

“(…) A quebra do sigilo dos dados telefônicos contendo os dias, os horários, a duração e o números das linhas chamadas e recebidas, não se submete à disciplina das interceptações telefônicas regidas pela Lei 9.296/96 (que regulamentou o inciso XII do art. 5º da Constituição Federal) e ressalvadas constitucionalmente tão somente na investigação criminal ou instrução processual penal.” (STJ - RMS: 17732 MT 2003/0238137-5, Relator.: Ministro GILSON DIPP, Data de Julgamento: 28/06/2005, T5 - QUINTA TURMA, Data de Publicação: --> DJ 01/08/2005 p . 477)

⁸ LIMA, Renato Brasileiro de. **Manual de Legislação Criminal Especial Comentada: Volume Único**. 14 ed. São Paulo: Editora Juspodivm, 2026, p.858.



Ao contrário do que ocorre com a interceptação telefônica, que depende necessariamente de **ordem judicial**, a quebra de sigilo de dados telefônicos não está submetida a uma reserva absoluta de jurisdição. Assim, outros órgãos também podem requisitar esses dados.

As **Comissões Parlamentares de Inquérito (CPIs)**, por exemplo, possuem poderes próprios de investigação, previstos no **art. 58, §3º, da Constituição Federal**, podendo determinar a quebra de sigilo de dados telefônicos, desde que o ato seja devidamente fundamentado.

Da mesma forma, o **Ministério Público**, com base em seu poder de requisição previsto no **art. 129, VI, da Constituição Federal**, pode requisitar registros de ligações pretéritas sem necessidade de autorização judicial prévia, uma vez que tais registros são considerados **documentos**, não se confundindo com o conteúdo das comunicações.

CAIU NA PF – 2013 – CESPE: O presidente de uma comissão parlamentar mista de inquérito, após as devidas formalidades, ordenou, de forma sigilosa e reservada, a interceptação telefônica e a quebra do sigilo de dados telefônicos de testemunha que se reservara o direito de permanecer calada perante a comissão. Nessa situação, a primeira medida é ilegal, visto que a interceptação telefônica se restringe à chamada reserva jurisdicional, sendo permitida, por outro lado, a quebra do sigilo de dados telefônicos da testemunha, medida que não se submete ao mesmo rigor da primeira, consoante entendimento da doutrina majoritária.⁹

Além disso, informações como **dados cadastrais, horários de acesso e endereços de IP (Internet Protocol)** não estão protegidos pelo sigilo das comunicações previsto no art. 5º, XII, da Constituição Federal. No caso das **lan houses**, uma Lei Estadual de São Paulo (Lei nº 12.228/06) determinou que os estabelecimentos devem manter cadastro de seus usuários. O acesso a esses dados para identificação de autores de crimes não exige autorização judicial quando o próprio proprietário do estabelecimento permite a coleta das informações.

Nesse contexto, há precedente do STJ reconhecendo a legitimidade da requisição de informações relativas à origem de e-mails fraudulentos realizada diretamente por autoridade judicial à empresa de telefonia responsável.

HABEAS CORPUS. DIREITO PROCESSUAL PENAL. CRIMES CONTRA A HONRA. PROVA ILÍCITA. INOCORRÊNCIA. ORDEM DENEGADA.

1. A simples titularidade e o endereço do computador do qual partiu o escrito criminoso não estão resguardados pelo sigilo de que cuida o inciso XII do artigo 5º da Constituição da República, nem tampouco pelo direito à intimidade prescrito no inciso X, que não é absoluto.

2. É legítima a requisição do Presidente do Superior Tribunal de Justiça à empresa de telefonia local de informações sobre mensagem eletrônica amplamente divulgada, dando conta da existência de fraude em concurso

⁹ **CERTO.** O princípio constitucional da reserva de jurisdição incide sobre as interceptações telefônicas (CF, art. 5º, XII), mas não se estende à quebra de sigilo, pois, em tal matéria, e por efeito de expressa autorização dada pela própria Constituição (CF, art. 58, § 3º), assiste competência à CPI, para decretar, sempre em ato necessariamente motivado, a excepcional ruptura dessa esfera de privacidade das pessoas



público para provimento de cargos efetivos do quadro de pessoal do próprio Tribunal a que preside, cuja honrabilidade restou afetada.

(...)

(STJ - HC: 83338 DF 2007/0116172-1, Relator.: Ministro HAMILTON CARVALHIDO, Data de Julgamento: 29/09/2009, T6 - SEXTA TURMA, Data de Publicação: --> DJe 26/10/2009)

O Supremo Tribunal Federal, no julgamento da **ADC 51/DF**, reconheceu que empresas de tecnologia que atuam no Brasil sujeitam-se a jurisdição nacional. Portanto, tais empresas devem cumprir **ordens judiciais brasileiras para fornecimento de dados**, ainda que os servidores estejam localizados no exterior.

Essa compreensão também encontra respaldo no **Marco Civil da Internet (Lei nº 12.965/2014)**, que estabelece que qualquer operação de coleta, armazenamento ou tratamento de dados realizada em território nacional deve observar a legislação brasileira.

A decisão do STF também buscou garantir maior **agilidade na obtenção de provas digitais**, evitando a morosidade dos mecanismos diplomáticos tradicionais, que poderiam resultar na perda ou supressão de dados relevantes para a investigação.

“1. A controvérsia constitucional veiculada na ADC é, a rigor, mais ampla do que a simples declaração de validade do uso das cartas rogatórias e dos acordos MLAT para fins de investigação criminal. O escopo da ação declaratória compreende não apenas o exame de constitucionalidade dos dispositivos invocados pelos requerentes, como também da norma prevista no art. 11 do Marco Civil da Internet e art. 18 da Convenção de Budapeste.

2. O art. 11 do Marco Civil da Internet, que encontra respaldo no art. 18 da Convenção de Budapeste, é norma específica em relação às regras gerais do MLAT. O referido dispositivo assegura a **aplicação da legislação brasileira em relação a atividades de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações eletrônicas ocorridas em território nacional, desde que pelo menos um dos atos ou terminais se encontrem em território nacional, mesmo que a pessoa jurídica portadora dessas informações esteja localizada ou armazene tais informações no exterior.**

3. As hipóteses de requisição direta previstas no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste reafirmam os **princípios da soberania e da independência nacional, concretizando o dever do Estado de proteger os direitos fundamentais e a segurança pública dos cidadãos brasileiros ou residentes no país.**

4. Constitucionalidade dos dispositivos do MLAT, do CPC e do CPP que tratam da cooperação jurídica internacional e da emissão de cartas rogatórias, nos casos em que a atividade de comunicação ou a prestação de tais serviços não tenham ocorrido em território nacional.



5. Dispositivos que convivem com a possibilidade de solicitação direta de dados, registros e comunicações eletrônicas nas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste.

6. Pedido julgado parcialmente procedente para declarar a constitucionalidade dos dispositivos indicados e da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional.

(STF - ADC: 51 DF, Relator.: Min. GILMAR MENDES, Data de Julgamento: 23/02/2023, Tribunal Pleno, Data de Publicação: PROCESSO ELETRÔNICO DJe-s/n DIVULG 27-04-2023 PUBLIC 28-04-2023)

Lei nº 12.965/2014 (Marco Civil da Internet)

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

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

4.1 Requisição de informações acerca das estações rádio base (ERB's)

As **Estações Rádio Base (ERB's)** são antenas ou estações fixas que viabilizam a comunicação entre aparelhos de telefonia móvel e a rede das operadoras. Por meio dessas estações, é possível identificar a **localização aproximada de um aparelho celular ligado**, desde que o dispositivo esteja em uso, isto é, enviando ou recebendo chamadas ou mensagens.



As informações provenientes das ERB's possuem grande utilidade investigatória. Elas podem indicar, por exemplo, se determinado suspeito se encontrava nas proximidades do local do crime no momento da ocorrência, bem como servir como elemento de **confirmação de álibis apresentados durante a investigação**.

A base legal para a requisição dessas informações encontra-se no **art. 13-B do Código de Processo Penal**, introduzido pela Lei nº 13.344/2016. O referido dispositivo estabelece que,

CPP:

Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.

Entretanto, a redação do art. 13-B do CPP gerou intenso debate doutrinário, especialmente quanto à necessidade ou não de autorização judicial para a obtenção dessas informações. A controvérsia decorre do fato de que o dispositivo, em determinados trechos, parece exigir autorização judicial, enquanto em outros indica a possibilidade de requisição direta pela autoridade investigativa.

Nesse contexto, formaram-se duas correntes interpretativas.

A **primeira corrente** sustenta que a obtenção de dados de posicionamento de ERB constitui espécie de **dado telefônico externo**, não protegido pelo sigilo das comunicações previsto no art. 5º, XII, da Constituição Federal. Assim, **não haveria necessidade de autorização judicial prévia**. Nesse sentido, o Superior Tribunal de Justiça já reconheceu que a autoridade policial atua dentro de suas atribuições constitucionais ao requisitar registros de telefones que utilizaram o serviço em determinada localidade e horário relacionados ao crime investigado, não sendo necessária decisão judicial anterior.

" 1. O inc. XII do artigo 5º da CF garante o sigilo das comunicações dos dados, mas não dos dados em si. Interpretação no sentido de que o sigilo se estende aos dados, ou seja, informações, contidas em qualquer suporte, físico ou eletrônico, inviabilizaria a produção de prova em qualquer processo judicial ou administrativo, pois o dispositivo autoriza a flexibilização apenas em relação às comunicações telefônicas, para fins de investigação criminal ou instrução processual penal, em razão de sua instantaneidade e efemeridade.

2. Bem por isso, outras informações, como os dados cadastrais dos usuários, relações de chamadas e números que utilizaram determinada estação rádio base, não estão sujeitos à disciplina da Lei 9.296/96, que regula a parte final do inc. XII do art. 5º. 3. Com muito mais razão **não há falar em sigilo - com necessidade de prévia autorização judicial - nas hipóteses em que a informação obtida diretamente pela autoridade policial junto às companhias telefônicas restringiu-se aos números de telefones que foram utilizados em uma determinada localidade, não havendo sequer indicação do proprietário da linha, tampouco do teor das conversas efetivadas.**



4. A Constituição somente submete à **controle jurisdicional prévio**, a chamada reserva de jurisdição, medidas de três ordens, a saber: a **interceptação telefônica em sentido estrito** (CF, art. 5º, XII); o **ingresso em domicílio sem autorização do proprietário e fora dos casos de flagrante delito, desastre ou socorro** (CF, art. 5º, XI e CPP, art. 241) e a **prisão fora dos casos de flagrante delito, prisão militar ou crime militar** (CF, art. 5º, LXI). Há, ainda, casos em que a legislação impõe autorização judicial prévia, como se dá, por exemplo, com a infiltração policial (Lei nº 9.034/95, art. V; Lei nº 11.343/06, art. 53, I).

5. Os **demaís atos administrativos, incluindo aqueles praticados pela autoridade policial, estão sujeitos apenas a controle jurisdicional a posteriori, ainda que impliquem restrição de direito fundamental**. Afirmar que toda restrição a direito fundamental depende de prévia autorização judicial implicaria a paralisação da atuação policial e administrativa, e o banimento do poder de polícia do Estado.

6. Se toda e qualquer restrição da intimidade e da vida privada requeresse autorização judicial, seria necessário, sob pena de paralisação da atuação administrativa, que um juiz atuasse, exemplificativamente:

- a) em todas as patrulhas policiais, para autorizar eventuais buscas pessoais;
- b) em todos os postos aduaneiros, incluindo portos, aeroportos e alfândegas terrestres, para autorizar a abertura da bagagem dos viajantes;
- c) em todos os estabelecimentos prisionais, para examinar a legalidade de eventual revista em celas ou em visitantes.

7. Os **direitos fundamentais não são absolutos de modo que a medida tomada pela autoridade policial que implique sua restrição é permitida, desde que seja proporcional**, ou seja, necessária, adequada e proporcional em sentido estrito. (...)”

(STJ - HC: 247.331 RS, Relatora.: MINISTRA MARIA THEREZA DE ASSIS MOURA, Data de Julgamento: 21/08/2014, Data de Publicação: PROCESSO ELETRÔNICO DJe – 03/09/2014)

A **segunda corrente**, por sua vez, entende que o acesso ao posicionamento das ERB's afeta diretamente os direitos fundamentais à **intimidade e à vida privada**, uma vez que permite identificar a localização de uma pessoa. Segundo esse entendimento, o §4º do art. 13-B do CPP seria inconstitucional, pois **não seria admissível** que o simples decurso do prazo de doze horas pudesse **dispensar a prévia autorização judicial**.

A controvérsia foi enfrentada pelo **Supremo Tribunal Federal**, no julgamento da **ADI 5.642/DF**, concluído em abril de **2024**. Na ocasião, o Plenário da Corte fixou entendimento no sentido de que **a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB pode ser requisitada sem controle judicial prévio**, mas sujeita a um **controle judicial posterior**. Também se admitiu a requisição de sinais para localização de vítimas ou suspeitos após o decurso do prazo de doze horas previsto no §4º do art. 13-B do Código de Processo Penal.



O Supremo Tribunal Federal considerou a medida constitucional em razão da **urgência e da gravidade dos crimes que atentam contra a liberdade pessoal**, ressaltando que não há expectativa de privacidade para quem se encontra em situação de flagrante delito relacionado a crimes graves com vítimas submetidas à restrição de liberdade.

DISPOSITIVO E TESE

“1. Reconhecida a constitucionalidade do diploma impugnado e não vislumbrando dúvida sobre a interpretação constitucionalmente adequada da norma, pedidos contidos na presente ação direta julgados improcedentes.

2. Tese: “São passíveis de requisição sem controle judicial prévio, mas sempre sujeito ao controle judicial posterior, a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB por um período determinado e desde que necessário para os fins de reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do Código de Processo Penal; o extrato de ERB; os dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis; o extrato de chamadas telefônicas; o extrato de mensagens de texto (SMS ou MMS); e os sinais para localização de vítimas ou suspeitos, após o decurso do prazo de 12 horas constante do § 4º do art. 13-B do Código de Processo Penal.”

(STF - ADI: 5642 DF, Relator.: Min. EDSON FACHIN, Data de Julgamento: 18/04/2024, Tribunal Pleno, Data de Publicação: PROCESSO ELETRÔNICO DJe-s/n DIVULG 21-08-2024 PUBLIC 22-08-2024)

Além disso, o Superior Tribunal de Justiça, por meio de sua **3ª Seção**, também se manifestou acerca das ordens judiciais conhecidas como **“geofencing”**, que consistem na identificação de usuários localizados em determinadas coordenadas geográficas em um período específico.

Nesse contexto, prevaleceu o entendimento de que a quebra de sigilo de **dados informáticos estáticos**, quando delimitada por parâmetros objetivos de pesquisa e por período determinado, **não configura medida desproporcional**, distinguindo-se da interceptação de comunicações em fluxo.

Para a requisição desses dados armazenados, o magistrado deve verificar alguns requisitos, entre os quais se destacam: a existência de indícios da ocorrência do ilícito, a justificação da utilidade da requisição para a investigação, e a delimitação temporal dos registros a serem obtidos.

“Logo, a **ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes** cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura policial fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.

(STJ - RE no RMS: 61302 RJ 2019/0199132-0, Relator.: Ministro OG FERNANDES, Data de Publicação: DJ 07/12/2022)



5. FINALIDADE DA INTERCEPTAÇÃO TELEFÔNICA: MEIO DE OBTENÇÃO DE PROVA EM INVESTIGAÇÃO CRIMINAL OU INSTRUÇÃO PROCESSUAL PENAL

A interceptação telefônica constitui **instrumento de obtenção de prova**, cuja finalidade está expressamente delimitada tanto pela Constituição Federal (art. 5º, XII) quanto pela Lei nº 9.296/1996 (art. 1º). De acordo com esses dispositivos, sua utilização é restrita **à investigação criminal e à instrução processual penal**, não podendo ser empregada originariamente em processos de natureza cível, comercial, trabalhista ou administrativa.

Contudo, a decretação da interceptação telefônica **não depende necessariamente da instauração de inquérito policial**. A medida pode ser determinada sempre que houver outro procedimento investigatório legítimo conduzido, por exemplo, pelo Ministério Público ou por Comissões Parlamentares de Inquérito, que indique a existência de **indícios de autoria relacionados a crime punido com pena reclusão**.

“Este Superior Tribunal possui o entendimento no sentido de que, para que seja permitida a interceptação telefônica, não é imprescindível prévia instauração de inquérito policial ou de ação penal, bastando que haja, para a autorização da medida, indícios razoáveis de autoria ou participação do acusado em infração penal punida com reclusão.” (RHC 37.209/BA, Rel. Ministro ROGÉRIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 05/11/2013, DJe 21/11/2013)

Além disso, a interceptação pode assumir caráter **preventivo**, sendo decretada como medida cautelar preparatória, inclusive antes da formalização do inquérito policial. A interceptação telefônica também pode ser utilizada **durante a instrução processual penal**, fase destinada à colheita de provas em juízo. Esse período compreende o intervalo entre o oferecimento da peça acusatória e o encerramento da fase de diligências prevista no art. 402 do CPP. Nessa etapa processual, a interceptação pode ser determinada quando surgirem **circunstâncias novas e até então desconhecidas**, que justifiquem a adoção imediata da medida para esclarecimento dos fatos.

Como regra, a interceptação telefônica **não pode ser autorizada originariamente para processos de natureza não penal**. Contudo, a doutrina e a jurisprudência admitem a utilização da chamada **prova emprestada**. Uma vez que a intimidade foi legitimamente afastada por decisão judicial no âmbito de investigação ou processo penal, os elementos probatórios obtidos podem ser utilizados em outros procedimentos.

“A possibilidade de quebra do sigilo das comunicações telefônicas fica, em tese, restrita às hipóteses de investigação criminal ou instrução processual penal. No entanto, o ato impugnado, embora praticado em processo cível, retrata hipótese excepcional, em que se apuram evidências de subtração de menor, crime tipificado no art. 237 do Estatuto da Criança e do Adolescente.” (STJ - HC: 203405 MS 2011/0082331-3, Relator.: Ministro SIDNEI BENETI, Data de Julgamento: 28/06/2011, T3 - TERCEIRA TURMA, Data de Publicação: DJe 01/07/2011)



CAIU NA PC/GO – 2013 – UEG: Sobre a interceptação das comunicações, tem-se o seguinte: segundo o Superior Tribunal de Justiça, é possível a autorização de interceptação telefônica independentemente da existência de inquérito policial.¹⁰

Nesse sentido, os Tribunais Superiores admitem que os dados provenientes de interceptação telefônica regularmente autorizada possam ser utilizados em **processos administrativos disciplinares (PAD)**, tanto contra os mesmos servidores investigados quanto contra outros agentes cujas condutas ilícitas tenham sido reveladas durante a colheita da prova.

“A jurisprudência desta Corte admite o uso de prova emprestada em processo administrativo disciplinar, em especial a utilização de interceptações telefônicas autorizadas judicialmente para investigação criminal. Precedentes.” (STF - RMS: 28774 DF - DISTRITO FEDERAL 9929191-71.2010.1.00 .0000, Relator.: Min. MARCO AURÉLIO, Data de Julgamento: 22/09/2015, Primeira Turma, Data de Publicação: DJe-180 25-08-2016)

SÚMULA 591 do STJ: É permitida a “prova emprestada” no processo administrativo disciplinar, desde que devidamente autorizada pelo juízo competente e respeitados o contraditório e a ampla defesa.

A interceptação telefônica possui natureza de **medida cautelar conservativa**, destinada a preservar o conteúdo das comunicações quando ocorrem, impedindo que informações relevantes para a investigação se percam ou sejam modificadas com o passar do tempo. A utilização dessa medida **não viola o princípio do *nemo tenetur se detegere***, que assegura ao indivíduo o direito de não produzir prova contra si mesmo, pois o sujeito não se encontra em confronto direto com a autoridade estatal, não sendo compelido a responder perguntas nem submetido a pressões, razão pela qual o instrumento é utilizado em contexto de plena liberdade de comunicação.

Por se tratar de medida realizada ***inaudita altera parte***, isto é, sem a prévia oitiva da pessoa investigada, o contraditório não ocorre durante a execução da interceptação, mas apenas **posteriormente**, caracterizando o chamado **contraditório diferido**. Em razão deste fato, a defesa possui o direito de pleno acesso aos autos dos inquéritos policiais, bem como aos dados obtidos através das interceptações telefônicas. Esse entendimento foi consolidado pela **Súmula Vinculante nº 14**.

Súmula Vinculante nº 14: É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa.

Além disso, o Supremo Tribunal Federal admite a utilização do **habeas corpus** para impugnar interceptações telefônicas consideradas ilícitas, sempre que houver risco, ainda que indireto, à liberdade de locomoção do investigado.

CAIU NA PC/RN – 2021 – FGV: Tramita no âmbito interno da Polícia Civil do Estado do Rio Grande do Norte processo administrativo disciplinar (PAD) que apura eventual falta funcional praticada por certo delegado de polícia. Durante a instrução do PAD, foi verificada pela autoridade competente que o conduz a necessidade de

¹⁰ **CERTO.** Conforme entendimento do STJ no HC 203.405/MS e no RHC 37.209/BA.



obtenção de prova emprestada, consistente em interceptação telefônica realizada no bojo de processo criminal. De acordo com a jurisprudência dos Tribunais Superiores, o compartilhamento de prova pretendido é viável, desde que devidamente autorizada pelo juízo criminal competente e respeitados os princípios do contraditório e da ampla defesa.¹¹

¹¹ CERTO. Conforme entendimento do STF no RMS: 28.774/DF e de acordo com a Súmula 591 do STJ.

