

LEI N.º 9.296/1996 V

Retoma-se o estudo sobre interceptação telefônica, captação ambiental e demais temas relacionados à Lei n.º 9.296, de 1996, com destaque para assuntos atuais e julgados relevantes.

ACESSO A REGISTROS DE LIGAÇÕES E DE CHAMADAS TELEFÔNICAS

Obs.: um desses julgados trata do acesso aos registros de ligações telefônicas. Ressalta-se que não se refere ao conteúdo das ligações, mas apenas aos registros, como o número discado, o horário da chamada e sua duração. Importa destacar que comissões parlamentares de inquérito (CPIs ou CPMIs) não possuem competência para quebrar o sigilo do conteúdo das comunicações telefônicas, sendo esse acesso permitido apenas mediante autorização judicial. No entanto, podem acessar os dados externos das comunicações, como os registros de chamadas, sem necessidade de ordem judicial.

Esses dados compreendem, por exemplo, que o terminal X realizou uma ligação para o terminal Y, com duração de cinco minutos, em determinada data, e que os terminais estavam localizados em cidades distintas. Trata-se de informações exteriores à comunicação, cujo acesso é permitido às CPIs.

Por outro lado, o conteúdo das conversas continua protegido por sigilo, sendo o acesso condicionado à autorização judicial, conforme os requisitos legais previamente estudados.

RECURSO ESPECIAL. TRÁFICO DE DROGAS. USO DE DADOS CONTIDOS NA AGENDA TELEFÔNICA SEM AUTORIZAÇÃO JUDICIAL. VALIDADE. SITUAÇÃO NÃO ALBERGADA PELO SIGILO TELEFÔNICO OU TELEMÁTICO. RECURSO ESPECIAL PROVIDO. (...) 4. No caso, como autorizado pelo Código de Processo Penal – CPP foi apreendido o telefone celular de um acusado e analisados os dados constantes da sua agenda telefônica, a qual não tem a garantia de proteção do sigilo telefônico ou de dados telemáticos, pois a agenda é uma das facilidades oferecidas pelos modernos aparelhos de smartphones a seus usuários. 5. Assim, deve ser reconhecida como válida a prova produzida com o acesso à agenda telefônica do recorrido, com o restabelecimento da sentença condenatória, determinando-se que a Corte a quo continue a apreciar a apelação. 6. Recurso especial provido.

Obs.: em um caso específico, foi apreendido o telefone celular de um acusado preso em flagrante durante a prática de infração penal. A análise dos dados da agenda telefônica foi considerada válida, uma vez que tais informações não estão protegidas pelo sigilo telefônico ou pelo sigilo de dados telemáticos. A agenda, considerada uma funcionalidade oferecida pelos aparelhos celulares modernos, não goza da mesma proteção jurídica, sendo, portanto, lícita a prova obtida a partir de seu conteúdo.

O julgado em questão determinou ser possível o acesso, independentemente de autorização judicial, aos registros das ligações constantes da agenda telefônica.

ACESSO A CONVERSAS DE WHATSAPP

AGRAVO REGIMENTAL NO RECURSO ESPECIAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO PARA O TRÁFICO. DADOS DO APARELHO CELULAR. AUSÊNCIA DE MANDADO DE BUSCA E APREENSÃO. PROVA ILÍCITA. (...). 1. Os dados constantes de aparelho celular obtidos por órgão investigativo – mensagens e conversas por meio de programas ou aplicativos (WhatsApp) – somente são admitidos como prova lícita no processo penal quando há precedente mandado de busca e apreensão expedido por juiz competente ou quando há autorização voluntária de interlocutor da conversa (ut, AgRg no HC n. 646.771/PR, Relator Ministro JOÃO OTÁVIO DE NORONHA, Quinta Turma, DJe de 13/8/2021). 2. No caso concreto, consta do acórdão estadual que a devassa no aparelho celular do agravado não foi autorizada em momento algum pela autoridade judiciária competente, não havendo dúvidas, portanto, sobre a ilicitude dessas provas. (...). Incidência da Súmula n. 211/STJ. 4. Agravo regimental não provido.

Obs.: a menção ao mandado de busca e apreensão refere-se à autorização judicial que possibilita o acesso ao conteúdo do dispositivo. Assim, quando o juiz determina a apreensão do aparelho, compreende-se que está também autorizando o acesso às conversas ali contidas.

Outra possibilidade de acesso lícito ocorre quando o próprio proprietário do aparelho autoriza expressamente a análise do conteúdo. Nessa hipótese, cabe à autoridade policial ou ao investigador comprovar que tal autorização foi efetivamente concedida. Do contrário, estaria sendo exigida do investigado uma prova negativa — conhecida como prova diabólica —, o que configuraria uma exigência desproporcional e juridicamente inadequada.

Caso o acesso ao conteúdo do aparelho celular tenha ocorrido mediante autorização do investigado, tal consentimento deve estar devidamente demonstrado, preferencialmente por escrito ou por meio de gravação em vídeo.

ACESSO A CONVERSAS DE WHATSAPP

Se o telefone celular foi apreendido em busca e apreensão determinada por decisão judicial, não há óbice para que a autoridade policial acesse o conteúdo armazenado no aparelho, inclusive as conversas do whatsapp. Para a análise e a utilização desses dados armazenados no celular não é necessária nova autorização judicial. A ordem de busca e apreensão determinada já é suficiente para permitir o acesso aos dados dos aparelhos celulares apreendidos. STJ. 5ª Turma. RHC 77.232/SC, Rel. Min. Felix Fischer, julgado em 03/10/2017.



5m

Obs.: para a análise e utilização desses dados, não se exige nova autorização judicial, uma vez que a ordem de busca e apreensão já é suficiente para viabilizar o acesso às informações armazenadas no dispositivo. Esse entendimento foi consolidado pela Quinta Turma do Superior Tribunal de Justiça (STJ).

ACESSO A CONVERSAS DE WHATSAPP

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. Rogerio Schietti Cruz, julgado em 19/10/2017 (Info 617)

Obs.: nesse caso, não se trata do acesso ao dispositivo de um investigado, mas sim ao aparelho da vítima, entregue voluntariamente, o que afasta qualquer alegação de ilegalidade.

ESPELHAMENTO DO WHATSAPP (WHATSAPP WEB)

Obs.: além disso, destaca-se outro entendimento jurisprudencial recente, datado de 2023 e 2024, que representa uma mudança significativa na orientação do Superior Tribunal de Justiça. Até então, não se admitia a técnica do espelhamento de conversas via WhatsApp Web pela polícia, sob o argumento de que haveria acesso unilateral e possibilidade de manipulação de mensagens pelo agente público, dificultando o controle judicial da produção probatória.

Contudo, houve alteração nesse entendimento, e passou-se a admitir, no ordenamento jurídico brasileiro,

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 amparada por autorização judicial. STJ. 5ª Turma. AREsp 2.309.888-MG, Rel. Min. Reynaldo Soares da Fonseca, julgado em 17/10/2023 (Info 792).

O agente policial pode valer-se da utilização do espelhamento pela via do Whatsapp Web, desde que respeitados os parâmetros de proporcionalidade, subsidiariedade, controle judicial e legalidade, calcado pelo competente mandado judicial. STJ. 5ª Turma. AgRg no AREsp 2.318.334-MG, Rel. Min. Reynaldo Soares da Fonseca, julgado em 16/4/2024 (Info 810).

Obs.: a infiltração policial, prevista na Lei n.º 12.850/2013 (Lei de Organização Criminosa), estabelece regras específicas, mas que podem ser aplicadas de forma geral às situações que envolvam operações semelhantes. Entre os requisitos previstos, destaca-se a exigência de autorização judicial prévia para a sua implementação.

Dessa forma, mesmo quando a norma trata da infiltração no contexto de organizações criminosas, suas disposições são aplicáveis a qualquer situação que envolva a utilização de agentes infiltrados no ambiente digital, inclusive por meio do espelhamento do WhatsApp Web. Essa interpretação reforça o caráter de infiltração dessas ações e exige o cumprimento das formalidades legais previstas para sua validade.

Desde que a ação controlada esteja amparada por autorização judicial, sua utilização é admitida. Embora o julgado a denomine como “ação controlada”, tecnicamente, essa classificação não se aplica de forma precisa. Conforme o regramento da Lei n.º 12.850/2013, a ação controlada, como regra geral, não exige autorização judicial prévia, mas apenas a comunicação prévia ao juiz. Exceções existem, como na Lei de Drogas, que impõe a exigência de autorização judicial para essa medida.

No entanto, no caso do espelhamento via WhatsApp Web, exige-se expressamente a autorização judicial, nos mesmos moldes aplicados à infiltração policial.

Tal exigência fica evidenciada no julgado de 2024, o qual estabelece que o agente policial pode utilizar o espelhamento do WhatsApp, desde que respeitados os princípios da proporcionalidade, subsidiariedade, controle judicial e legalidade, sempre fundamentados em mandado judicial competente.

Nesse contexto, o meio de obtenção da prova deve ser proporcional, limitado ao tempo estritamente necessário e adotado apenas quando não houver outro meio menos invasivo para a obtenção da informação. Ademais, deve existir controle judicial contínuo quanto à legalidade do procedimento, bem como a exigência de autorização prévia por mandado judicial.

HABILITAÇÃO DE CHIP EM SUBSTITUIÇÃO AO DO INVESTIGADO TITULAR DA LINHA

É ilegal a quebra do sigilo telefônico mediante a habilitação de chip da autoridade policial em substituição ao do investigado titular da linha. A Lei n. 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)



10m

Obs.: nesse caso, o procedimento consiste na clonagem do chip para uso como se fosse o original do investigado. O Superior Tribunal de Justiça entendeu ser ilícita a quebra de sigilo realizada por meio da habilitação de chip por autoridade policial em substituição ao chip original do investigado. De acordo com o referido entendimento, a Lei n.º 9.296/1996 não autoriza a suspensão do serviço telefônico nem do fluxo de comunicação por meio dessa prática.

Assim, a prática de clonagem do chip do investigado com o intuito de se comunicar com outros integrantes da organização criminosa, simulando ser o próprio investigado, não é admitida. Embora atualmente se aceite o espelhamento via WhatsApp Web, a habilitação de chip clonado em substituição ao original do investigado ainda não é permitida, conforme os entendimentos vigentes.

QUEBRA DE SIGILO DE DADOS INFORMÁTICOS ESTÁTICOS

A determinação judicial de quebra de sigilo de dados informáticos estáticos (registros), relacionados à identificação de usuários que operaram em determinada área geográfica, suficientemente fundamentada, não ofende a proteção constitucional à privacidade e à intimidade. A quebra do sigilo de dados armazenados não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado. 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, não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos por tal diligência. STJ. 3ª Seção. RMS 61.302-RJ, Rel. Min. Rogerio Schietti Cruz, julgado em 26/08/2020 (Info 678).

Obs.: em outro julgado relevante, ocorrido no contexto das investigações sobre o assassinato da vereadora Marielle Franco, discutiu-se a quebra do sigilo de dados informáticos estáticos. Ressalta-se que dados armazenados em nuvem (cloud storage) não se confundem com comunicações em tempo real, pois tratam-se de dados estáticos.

A decisão analisada estabelece que a quebra de sigilo desses dados não exige a indicação prévia das pessoas investigadas, uma vez que o objetivo da medida é justamente possibilitar a identificação do usuário do serviço ou do terminal utilizado.

Por exemplo, em uma investigação que envolva um crime ocorrido em determinada área, como o assassinato da referida parlamentar, é possível requisitar informações sobre os aparelhos conectados às torres de telefonia na região ou sobre terminais que tenham realizado pesquisas relacionadas ao nome da vítima ou à sua agenda política. Tais dados, por serem armazenados e estáticos, não se equiparam ao fluxo de comunicações interceptadas em tempo real. Como o responsável pelo crime ainda não foi identificado, a medida visa justamente permitir a sua descoberta. Por esse motivo, é admitido o acesso a dados de maneira limitada a uma área geográfica e a um intervalo temporal específico, evitando a violação indiscriminada de dados da população. Ademais, por não se tratar de interceptação telefônica, não há exigência de identificação prévia e expressa dos indivíduos cujos dados serão acessados.

Não se aplicam os requisitos da interceptação telefônica quando se trata da quebra de dados informáticos estáticos. Nessa hipótese, é possível a aplicação do Marco Civil da Internet, o qual prevê que a parte interessada pode formar conjunto probatório a partir de registros de conexão ou de acesso a aplicações de internet.

Para que esses registros possam ser fornecidos, devem estar presentes determinados requisitos: existência de indícios fundados da ocorrência de ato ilícito, justificativa da utilidade dos registros para fins de investigação ou instrução probatória, e a delimitação do período ao qual os registros se referem.

MARCO CIVIL DA INTERNET (LEI N.º 12.965/2014)

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

- I. fundados indícios da ocorrência do ilícito;
- II. justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
- III. período ao qual se referem os registros.

Obs.: assim, desde que observadas essas condições, o Marco Civil da Internet autoriza tal solicitação.



DIRETO DO CONCURSO

15. (NC-UFPR/PC-PR/DELEGADO DE POLÍCIA/2021) Sobre a Lei n.º 9.296/1996, assinale a alternativa correta.



15m

a) A interceptação telefônica, preenchidos os demais requisitos legais, pode ser determinada quando o fato investigado isoladamente constituir infração penal punida com detenção ou reclusão, não sendo admitida nas hipóteses de prisão simples.

b) De acordo com o entendimento do STF, a interceptação telefônica poderá ser decretada pelo prazo de 15 dias, podendo ser renovada por uma única vez, por igual prazo.

c) Deferido o pedido de interceptação telefônica, a autoridade policial conduzirá os procedimentos de forma sigilosa, não sendo prevista nessa fase a participação do Juízo ou do Ministério Público.

d) De acordo com o STJ, é admissível a utilização da técnica de fundamentação *per relationem* para a prorrogação de interceptação telefônica quando mantidos os pressupostos.

e) As quebras de sigilo tanto de estação de rádio base (ERB) quanto de mensagens trocadas por e-mails ou por aplicativos de mensagens não dependem de prévia autorização judicial.



a) A interceptação telefônica somente pode ser determinada, mesmo quando preenchidos os demais requisitos legais, se o fato investigado constituir infração penal punida com reclusão. Portanto, não é admitida interceptação em crimes punidos apenas com detenção.

b) Conforme entendimento do Supremo Tribunal Federal, a interceptação telefônica pode ser decretada pelo prazo de quinze dias, sendo admitidas prorrogações sucessivas, desde que a medida continue sendo indispensável para a investigação.

c) Uma vez deferido o pedido de interceptação telefônica, a autoridade policial deverá conduzir os procedimentos de forma sigilosa. No entanto, há previsão de participação do juízo, responsável pelo controle de legalidade, bem como do Ministério Público, ao qual deve ser dada ciência da medida, sendo-lhe facultado acompanhar todo o procedimento.

d) De acordo com o Superior Tribunal de Justiça, é admissível a utilização da técnica de fundamentação “*per relationem*”, isto é, a fundamentação baseada em outros documentos ou decisões anteriores, para fins de prorrogação da interceptação telefônica. Contudo, não se admite que essa técnica se limite à mera citação da decisão anterior, sendo necessário demonstrar que os requisitos legais continuam presentes para justificar a renovação da medida.

e) Esse tipo de comunicação constitui fluxo de dados em tempo real, diferentemente dos dados armazenados, como aqueles presentes em serviços de nuvem, que são considerados dados estáticos. Assim, para que se proceda à interceptação de comunicações, é imprescindível a autorização judicial.

Em relação às Estações Rádio Base (ERBs), entende-se atualmente que a quebra de sigilo desses dados exige, como regra, autorização judicial. Embora exista uma flexibilização prevista no Código de Processo Penal para determinados crimes, trata-se de exceção. De modo geral, a autorização judicial é imprescindível para a obtenção dos registros de ERBs, os quais permitem identificar a geolocalização aproximada dos dispositivos ou terminais conectados às torres de telefonia, possibilitando assim a determinação da localização estimada do terminal telefônico investigado.

GABARITO

15. d

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Diego Alekes Fontes de Sousa.

A presente gravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.
