Curso de Direito

A LICITUDE DA INTERCEPTAÇÃO TELEFÔNICA COMO PROVA DIGITAL

THE LEGALITY OF TELEPHONE INTERCEPTION AS DIGITAL EVIDENCE

Eduarda Sobral Monteiro e Lavígnia Felix Nakao [1], Carla Queiroz [2].
1 Alunos (as) do Curso de Direito
2 Professora Mestre do Curso de Direito

RESUMO

Atualmente a tecnologia está presente em toda parte, inclusive nos procedimentos processuais penais. A cadeia de custódia é um procedimento para o recolhimento de vestígios na cena do crime, e consequentemente colaborar com a investigação e a prova dos fatos. As provas digitais podem facilitar a elucidação do delito. A problemática consiste na análise da legalidade da interceptação telefônica como prova digital na cadeia de custódia. O presente estudo tem como objetivo analisar a licitude da interceptação telefônica. A pesquisa é bibliográfica, por meio de doutrinas e jurisprudências que versam sobre cadeia de custódia, provas digitais e interceptação telefônica.

Palavras-Chave: cadeia de custódia; prova digital; interceptação telefônica.

ABSTRACT

Nowadays, technology is present everywhere, including in criminal proceedings. The chain of custody is a procedure for collecting traces at the scene of a crime, and consequently collaborating with the investigation and proving the facts. Digital evidence can facilitate the elucidation of the crime. The problem consists of analyzing the legality of telephone interception as digital evidence in the chain of custody. This study aims to analyze the legality of telephone interception. The research is bibliographical, using doctrine and case law on chain of custody, digital evidence and telephone interception.

Keywords: chain of custody; digital evidence; telephone interception.

INTRODUÇÃO

O mundo passou por uma grande modernização em todas as áreas com o avanço tecnológico, incluindo o meio jurídico. Tal fenômeno trouxe ferramentas capazes de auxiliar e facilitar o trabalho de todo o sistema judiciário, em especial na colheita de vestígios do crime por meio da prova digital.

Recentemente, o Brasil introduziu a cadeia de custódia no procedimento penal, com o fim de melhorar as investigações tornando a apuração dos fatos mais precisos e dinâmicos. Assim, surge a problemática: a interceptação telefônica como prova digital é legítima?

Para responder a esse questionamento, a pesquisa tem como objetivo geral apontar a licitude e ilicitude da interceptação telefônica. E como objetivos específicos: citar as etapas da cadeia de custódia; conceituar provas digitais; e apontar os documentos digitais como meios de prova no processo penal. Logo, a pesquisa é bibliográfica com método dedutivo, por meio de doutrinas, com coleta de informações adquiridas de forma imparcial em face de um assunto que já possui determinada relevância para o mundo jurídico.

Elucidar a legitimidade da prova digital da interceptação telefônica dentro da cadeia de custódia pode garantir a preservação das provas, desde a sua coleta até eventual apresentação em tribunal. E comportar tais provas pode facilitar o trabalho dos agentes, além de acelerar consideravelmente o curso do processo com o uso da tecnologia.

REFERENCIAL TEÓRICO

1. Provas no Processo Penal

Prova é o conjunto de atos sobre um crime, que serve para influenciar a decisão judicial. As provas servem como materialização do fato delituoso, com a finalidade de comprovar os fatos sustentados pelo réu, pelo autor ou por qualquer outro envolvido no processo. As provas são necessárias para que o magistrado consiga compreender a versão dos fatos, a fim de tomar uma decisão, condenatória ou absolutória.

Aury Lopes Jr., (2020, p. 556) defende que a prova no processo penal tem como objetivo central a descoberta da verdade real, ou seja, a apuração fática dos acontecimentos que originaram a infração penal. No mesmo sentido, Nucci (2020, p. 684), define que o termo prova, no sentido objetivo, pode significar o “ato” ou o “meio” de demonstração da verdade sobre o fato discutido e, em sentido subjetivo, pode ser entendido como “o resultada da ação de provar”.

Quanto à forma ou aparência da prova, pode-se citar as provas testemunhais, e documentais e materiais (perícia, exame de corpo de delito). Os meios pelos quais pode-se coletar as provas podem ser por exame de corpo de delito, perícias, interrogatório/confissão, depoimento de testemunhas, declaração da vítima, reconhecimento de pessoas e coisas, documentos, busca e apreensão, e acareação.

Eoghan Casey define *digital evidence* como “qualquer dado armazenado ou transmitido usando um computador que confirma ou rejeita uma teoria a respeito de como ocorreu um fato ofensivo ou que identifica elementos essenciais da ofensa como intenção ou o álibi”. Logo, prova digital é qualquer tipo de informação, com valor probatório, armazenada em repositórios eletrônicos-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou rede de comunicações eletrônicas, privadas ou publicamente acessíveis. (Vaz, 2012, p. 63)

Provas digitais se referem aos vestígios digitais nos quais podem ser produzidos através de diferentes tipos de dispositivos como HD, disquetes, CD/DVD, pendrive,

tablets, cartões de memória, smartphones, assistentes digitais pessoais (PDA), dispositivos eletrônicos pessoais (PED), sistemas de navegação móveis (GPS), sistemas embarcados, câmeras digitais de vídeo e fotografias (incluindo CFTV), desktops, Notebooks, redes baseadas em TCP/IP e outros protocolos digitais, bem como dispositivos semelhantes acima (NETO, 2020 p. 08).

Vale ressaltar que, as principais características das provas digitais são (VAZ, 2012):

> **Imaterialidade:** As provas digitais não estão vinculadas a um único suporte específico e podem ser enviadas para outros dispositivos eletrônicos, sendo separados o suporte físico e os próprios dados;
> **Volatilidade:** Os dados digitais podem ser alterados e a perda ou alteração de informações pode interferir na integridade das evidências digitais. Tais alterações podem ser intencionais ou não, como a vulnerabilidade inerente de determinados dispositivos (como discos rígidos externos);
> **Suscetibilidade de clonagem, e facilidade de dispersão:** Os próprios dados e provas digitais permitem fazer múltiplas cópias de uma prova e transferi-la integralmente para outros dispositivos, não mais a versão original;
> **Necessidade de dispositivo para transmissão:** Toda prova digital consiste em uma série de algoritmos que geram um código digital. O código em si não apresenta uma aparência compreensível. Para interpretar este código e apresentar as evidências de forma externalizada (ex: imagem, som), é imprescindível um dispositivo constituído por um processador (ex: computador, celular) e muitas vezes determinados procedimentos de captação, leitura, extração e visualização, etc.

Outrossim, o fato de que uma prova que não seja originalmente digital (como por exemplo, documentos impressos), quando digitalizados e inseridos no processo, recebem uma individualização tecnológica que assegura a sua autenticidade e integridade. Ou seja, independentemente de sua natureza original, todas as provas juntadas, de certa forma, serão alcançadas à condição digital, garantindo assim uma maior seguridade e autenticidade no processo, tornando inclusive a busca de documentos mais fácil, visto que estará inserido no meio digital sem grandes riscos de se perder elementos importantes.

A prova digital comparada com a prova tradicional deve ser analisada de forma mais cautelosa, devido a sua linguagem, produção, instrumentos que são através de dados tecnológicos. Assim, “são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos” (STJ, Informativo 763 p. 26-28).

Por se tratar de um estudo novo e pouco falado, aqueles que executam o direito tiveram de se aperfeiçoar, devido a fragilidade das provas digitais, para evitar que a prova

obtida seja inadmitida (BADARÓ, 2021 p. 10). Visto que, a apreensão de computadores, celulares, sem a devida técnica, podem ser contaminados, por meio de manipulação ou adulteração daquela evidência.

Deve-se ter cautela quando se apresenta qualquer tipo de evidência no processo, pois assim como há provas permitidas, também há provas que são proibidas, que não podem ser juntadas ao processo. As provas proibidas podem ser ilegítimas e ilícitas.

As provas ilegítimas afrontam alguma norma processual. Neste sentido, Eugênio Pacelli destaca que "as provas ilegítimas por sua vez, não decorrem de violações a normas constitucionais ou de direito material, mas de inobservância das normas de caráter processual, como, por exemplo, a ausência de formalidades essenciais ou a prática de atos processuais por autoridade incompetente. Embora também possam ser excluídas do processo, não se confundem com as provas ilícitas, uma vez que sua irregularidade não implica, necessariamente, violação de direitos fundamentais."

Já as provas ilícitas, são aquelas obtidas por meio de crime ou contra a Carta Magna (confissão sob tortura, apreensão de documentos com violação de domicílio, captação de conversa sem autorização judicial, entre outros). À vista disso, Capez, (2001, p. 31), "as provas ilícitas são aquelas produzidas com violação a regras de direito material, ou seja, mediante a prática de algum ato ilícito penal, civil ou administrativo".

Portanto, quando a obtenção de prova derivada de mensagens existentes no aparelho celular é feita de forma direta pelos órgãos de persecução criminal, sem prévia autorização judicial, haverá a violação às normas legais, o que poderá gerar a nulidade da prova obtida por esse meio.

Agora, no que diz respeito às provas ilícitas juntadas ao processo e descobertas, tem-se então a teoria dos frutos da árvore envenenada ou provas ilícitas por derivação. Está prevista no art. 157 do CPP que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais" e sugere que todas as provas que decorrem de uma prova ilícita também estarão contaminadas, já que sua origem é ruim, logo, a ilicitude da obtenção da prova ilícita transmite-se às provas dela derivada sendo imprescindível a retirada destas no processo.

A utilização de fonte de prova independente não tem a capacidade de invalidar todo o conjunto fático e probatório. Não é possível declarar a ilicitude de todo o conjunto probatório produzido a partir da juntada do laudo pericial. Apenas são inadmissíveis as provas derivadas das ilícitas, salvo se não ficar evidenciado o nexo de causalidade entre umas e outras, ou se as derivadas puderem ser obtidas por uma fonte independente das

primeiras (art. 157, § 1º, do CPP).

2. Cadeia de custódia

No que tange a abordagem sobre provas, vale ressaltar que na sociedade atual com a inovação da tecnologia, o direito também precisou evoluir, adotando as provas digitais para melhorar as investigações. As provas físicas ou digitais fazem parte da cadeia de custódia.

A definição da cadeia de custódia encontra-se no Código de Processo Penal no artigo 158-A com o Pacote Anticrime (Lei 13.964/19):"Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Como se trata de um conjunto de procedimentos, é importante conhecer o conceito de vestígio e indício. No caso do vestígio é toda marca, objeto, sinal, rastro, substância ou elemento que seja detectado em local onde tenha sido praticado um fato delituoso. E "considera-se indício a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias" (Código de Processo Penal, art. 239). Ambos são meios de prova e encontram-se dentre as etapas da cadeia de custódia.

Conforme o Código de Processo Penal, a cadeia de custódia se realiza por uma série de etapas:

> **Reconhecimento:** ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
> **Isolamento:** procedimento para evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
> **Fixação:** descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;
> **Coleta:** recolhimento de vestígio que será submetido à análise pericial, respeitando suas características e natureza;
> **Acondicionamento:** processo por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;
> **Transporte:** transferência do vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;
> **Recebimento:** ato formal de mudança da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de

> procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;
> **Processamento:** exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;
> **Armazenamento:** refere-se à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraprova, descartado ou transportado, com vinculação ao número do laudo correspondente;
> **Descarte:** liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial. (BRASIL)

A coleta dos vestígios deverá ser realizada preferencialmente por perito oficial, que dará o encaminhamento necessário para a central de custódia. A responsabilidade do perito é documentar detalhadamente os vestígios. E a remoção de quaisquer vestígios de locais de crime antes da liberação do perito responsável, é tipificada como fraude processual.

Vale ressaltar que todos os recipientes deverão ser selados com lacres, com numeração individualizada, de forma a garantir a inviolabilidade e a idoneidade do vestígio durante o transporte. Também, é necessário individualizar o vestígio, preservar suas características, impedir contaminação e vazamento, ter grau de resistência adequado e espaço para registro de informações sobre seu conteúdo com autorização.

Por fim, após cada rompimento de lacre, deve se fazer constar na ficha de acompanhamento de vestígio o nome e a matrícula do responsável, a data, o local, a finalidade, bem como as informações referentes ao novo lacre utilizado, e o lacre rompido deverá ser acondicionado no interior do novo recipiente. E todas as pessoas que tiverem acesso ao vestígio armazenado deverão ser identificadas, onde todas as ações deverão ser registradas, consignando-se a identificação do responsável pela tramitação, a destinação, a data e horário da ação.

Todos os Institutos de Criminalística deverão ter uma central de custódia destinada à guarda e controle dos vestígios, e sua gestão deve ser vinculada diretamente ao órgão central de perícia oficial de natureza criminal. Quanto aos serviços das centrais de custódia todas devem possuir os serviços de protocolo, com local a para conferência, recepção, devolução de materiais e documentos, possibilitando a seleção, a classificação e a distribuição de materiais, devendo ser um espaço seguro e apresentar condições ambientais que não interfiram nas características do vestígio e as entradas e saídas de vestígios deverão ser protocoladas, consignando-se informações sobre a ocorrência de inquérito que a eles se relacionam. (BRASIL, Código de Processo Penal art 158-E).

Quando se fala em “cadeia de custódia” deve ser compreendida como “documentação da cadeia de custódia” e acrescentando que “a cadeia de custódia em si, deve ser entendida com a sucessão encadeada de pessoas que tiveram contato com a fonte de prova real, desde que foi colhida, até que seja apresentada em juízo” por isso deve ser feita com cautela para melhor autenticidade, veracidade e detalhada dos fatos. (BADARÓ, 2021 p. 7-9).

Vale ressaltar que a cadeia de custódia é quebrada quando comprovado prejuízo efetivo ao réu. A quebra da cadeia de custódia diz respeito à idoneidade do caminho que deve ser percorrido pela prova até sua análise pelo magistrado, sendo certo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade. Tem como objetivo garantir a todos os acusados o devido processo legal e os recursos a ele inerentes, como a ampla defesa, o contraditório e principalmente o direito à prova lícita”. (AgRg no HC 615.321/PR, Rel. Min. RIBEIRO DANTAS, Quinta Turma, julgado em 03/11/2020, Dje 12/11/2020 STJ).

3. A licitude da interceptação de conversas como provas digitais e mensagens

A ilicitude da prova digital ocorre quando não há a coleta e armazenamento adequado, contrariando as etapas da cadeia de custódia previstas no Código de Processo Penal. Pacelli (2021, p. 361) também alerta para a necessidade de observar rigorosamente a cadeia de custódia na manipulação das provas digitais, sob pena de sua contaminação e consequente inadmissibilidade.

A interceptação de conversas em aplicativos de mensagem, como WhatsApp, Telegram, e outros, como meios de prova no processo penal, tem sido um tema crescente em debates jurídicos, especialmente à medida que o uso desses aplicativos se tornou predominante na comunicação cotidiana.

Em 2017, o Supremo Tribunal Federal (STF) proferiu uma decisão importante sobre a interceptação de mensagens de aplicativos de comunicação, como o WhatsApp, no HC 118.770. Essa decisão foi crucial porque o STF reconheceu que as interceptações de mensagens (enviadas ou recebidas via aplicativos) estão sujeitas às mesmas regras e requisitos da interceptação telefônica estabelecida pela Lei nº 9.296/1996.

Para compreender melhor sobre a licitude e elucidar os fatos, o seguinte julgado trás de forma prática e válida em quais momentos a interceptação telefônica não será validada como prova:

> No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157§1°do CPP. (RHC 143.169/RJ - STJ).

O artigo 5º, inciso XII, da Constituição Federal diz que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Assim, mensagens e dados contidos no computador, notebook, celulares, só podem ser violados com ordem judicial.

É importante entender a diferença entre interceptação telefônica, escuta telefônica e gravação clandestina. Quando se fala em interceptação telefônica, nenhum dos interlocutores sabe que a conversa está sendo gravada por terceiro. Quanto a escuta, um dos interlocutores sabe que está sendo gravado por um terceiro. Já quando se fala em gravação, um dos interlocutores está gravando a conversa. Interceptação e escuta, precisam de autorização judicial para que sejam consideradas provas lícitas, por outro lado, quando se trata da gravação é dispensável a autorização do magistrado.

Fernando Capez (2001, p. 290), aborda a interceptação telefônica como um importante meio de prova no Direito Penal, mas que exige rigorosa observância aos preceitos constitucionais e legais para ser considerada legítima. De acordo com Capez, a interceptação telefônica é uma medida excepcional, regulamentada pela Lei nº 9.296/96, sendo permitida apenas nos casos e condições previstos em lei, com o objetivo de proteger direitos fundamentais e evitar abusos.

Inobstante, Nucci (2020, p. 459) também entende que "a interceptação telefônica constitui um meio extraordinário de obtenção de prova, utilizado em casos de excepcional gravidade, desde que haja indícios razoáveis da autoria ou participação em infração penal, cuja punição seja superior a pena mínima de um ano de reclusão."

De acordo com a Jurisprudência do STJ, a investigação somente será lícita quando se apoiar na obtenção de mensagens armazenadas em aparelho celular, quando houver autorização anterior proferida pelo juízo criminal competente, ou na hipótese do próprio investigado fornecer livre acesso ao conteúdo existente em seu aparelho celular.

Pode-se mencionar, por exemplo, o julgado abaixo para melhor entendimento:

> 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. (AgRg no HC 646.771/PR, relator Ministro João Otávio de Noronha, Quinta Turma, julgado em 10/8/2021, DJe de 13/8/21.)

Assim, é ilícita a prova obtida diretamente dos dados constantes de aparelho celular, decorrente de acesso às mensagens de textos SMS, conversas por meio de programa ou aplicativos como, por exemplo, o "WhatsApp", mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no momento do flagrante, sem prévia autorização judicial (HC 433930/ES, Rel. Min. Reynaldo Soares da Fonseca, 5ªT, julgado em 19/06/2018, Dje 2906/2018).

É válido salientar também que, prova obtida por meio de violação de mensagem em aparelho celular, quando a materialidade delitiva está incorporada na própria coisa (divulgar fotografia pornográfica envolvendo menores), a apreensão do celular do investigado independe de pretérita autorização judicial.

> Conforme consta dos autos, a *vexata quaestio* cinge-se a saber se a autorização judicial para a apreensão de elementos de prova é imprescindível em qualquer hipótese ou se haveria alguma situação em que tal expediente seria despiciendo, v. g., em razão de o aparelho celular constituir o próprio corpo de delito, como no caso vertente, em que o recorrente foi denunciado por divulgar, por meio do aplicativo Whatsapp, fotografia pornográfica envolvendo uma adolescente. Com efeito, nas hipóteses em que os meios de prova são obtidos por meio dos elementos encontrados em algum objeto pessoal, v. g., o aparelho celular, como in casu, a reserva de jurisdição é medida que se faz presentemente. Ao revés, nos casos em que a materialidade delitiva está incorporada na própria coisa, aqui a autorização judicial já se mostra prescindível, como é o caso do delito inserto no art. 241-A do Estatuto da Criança e do Adolescente. (RHC 108.262/MS, relator Ministro Antonio Saldanha Palheiro, Sexta Turma, julgado em 5/9/2019, e-STJ fl. 22)

Ademais, a corrupção da prova colhida não tem o condão de contaminar toda a instrução probatória, devendo apenas a prova ilícita ser desentranhada do processo.

> O prévio trabalho investigativo das autoridades policiais, que culminou com a identificação do fato e de seus autores, bem assim como o indiciamento do recorrente, não resta contaminado pelo posterior acesso não autorizado aos dados do aparelho celular, bastando o desentranhamento dos autos dos documentos extraídos do aparelho celular e a supressão do parágrafo final dos depoimentos policiais, que fizeram referência ao conteúdo das conversas via whatsapp. (RHC 76.324/DF, relatora Ministra Maria Thereza de Assis Moura, 6ªT, julgado em 14/2/17, DJe de 22/2/17)

A autorização judicial poderá ser feita de ofício ou por requerimento de autoridade

policial, a fim de corroborar para a investigação criminal. A ausência de autorização judicial para captação de conversas, ensejará na declaração de nulidade do ato, uma vez que constitui vício insanável.

No ano de 2011, a atriz da Globo Carolina Dieckmann teve seu computador hackeado e sua intimidade violada por um grupo de hackers, assim, divulgaram sem autorização, fotos íntimas da atriz pelas redes sociais. Além disso, ela chegou a receber ameaças para que as fotos não fossem vazadas. Não demorou para que a mídia e a justiça tomassem conhecimento. Houve mandado de busca e apreensão onde foram encontrados CDs, softwares e cinco computadores dentre eles, um laptop que estava aberto em uma página só com as fotos da atriz, nos quais foram usados como provas contra os réus. (Portal g1).

Em 2012, foi sancionada a lei nº 12.737 e com o apelido de "Lei Carolina Dieckmann" que mudou o Código Penal Brasileiro acrescentando os arts. 154-A e 154-B, incluindo, pela primeira vez na história do país, a tipificação de crimes virtuais e delitos informáticos que diz "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Dessa forma, caso haja a invasão do celular para obter conversas telefônicas, ou de whatsapp, sem autorização judicial, tipifica o crime de invasão de dispositivo informático alheio, conforme previsão do Código Penal.

E no caso da interceptação telefônica ter sido realizada sem autorização judicial, configura o crime do artigo 10 da Lei 9.296/96:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no **caput** deste artigo com objetivo não autorizado em lei.
> Art. 10-A. Realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 1º Não há crime se a captação é realizada por um dos interlocutores.
> § 2º A pena será aplicada em dobro ao funcionário público que descumprir determinação de sigilo das investigações que envolvam a captação ambiental ou revelar o conteúdo das gravações enquanto mantido o sigilo judicial. (BRASIL)

Como também caracteriza crime de abuso de autoridade, proceder à obtenção de

prova, em procedimento de investigação ou fiscalização, por meio manifestamente ilícito, com pena de detenção, de 1 (um) a 4 (quatro) anos, e multa. Incorre na mesma pena quem faz uso de prova, em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude (Lei 13.869/2019, artigo 25).

Portanto, a prova digital de interceptação telefônica sem autorização judicial, não é permitido no ordenamento processual penal brasileiro, sendo considerada prova ilícita. As provas ilícitas devem ser desentranhadas do processo. Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial. O juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão.

CONSIDERAÇÕES FINAIS

Diante do exposto, conclui-se que prova é todo e qualquer elemento material dirigido ao juiz da causa para esclarecer o que foi alegado pelas partes, especialmente circunstâncias fáticas. E com o grande avanço tecnológico, as provas digitais na cadeia de custódia são um grande meio facilitador com os quais hoje são trabalhados os processos.

A cadeia de custódia, como procedimento indispensável, assegura que vestígios coletados, armazenados e apresentados de forma que sua autenticidade e validade sejam preservadas. No entanto, a fragilidade das provas digitais demanda atenção redobrada, visto que qualquer falha em seu manuseio pode comprometer o processo judicial, resultando na inadmissibilidade das provas obtidas de forma ilícita.

Conclui-se que a interceptação telefônica é legítima apenas quando realizada com observância estrita às disposições legais, como a prévia autorização judicial, sendo este um mecanismo fundamental para equilibrar a eficiência investigativa e a proteção aos direitos fundamentais. Assim, o aprimoramento contínuo dos operadores do Direito, aliado a uma estrutura normativa robusta, é essencial para que as inovações tecnológicas possam ser plenamente incorporadas ao sistema jurídico sem prejuízo à justiça e aos direitos dos indivíduos.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Código de Processo Penal. Decreto-Lei 3.689, de 3 de outubro de 1941. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

BRASIL. Código Penal. Lei 2.848 de 07 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BRASIL. Lei 12.737 de 30 de novembro de 2012. Lei Carolina Dieckmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BRASIL. Lei 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Interceptação telefônica. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm

BRASIL. Lei 13.869 de 05 de setembro de 2019. Dispõe sobre crimes de abuso de autoridade. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869compilado.htm

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, ano, v. 29, p. 7-9, 2021.

CAPEZ, Fernando. Curso de Processo Penal. 26. ed. São Paulo: Saraiva, 2022.

CASEY, Eoghan. *Da prova penal: Tomo IV - Da prova-eletrónico-digital e da criminalidade informático digital.* Lisboa: Rei dos Livros, 2011, pág. 39. *Digital evidence and computer crime: forensic science, computers, and the Internet.* 2ª ed. San Diego/London: Elsevier Academic Press, 2004, pág 12. Tradução livre.

LOPES JÚNIOR, Aury. Direito processual penal. 17. ed. São Paulo: Saraiva Educação, 2020.

NETO, Mário Furlaneto; DOS SANTOS, José Eduardo Lourenço. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. Revista Em Tempo, [S.l.], v. 20, n. 1,nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130>. Acesso em: 04 june 2024. doi: https://doi.org/10.26729/et.v20i1.3130.

NUCCI, Guilherme de Souza. Curso de direito processual penal. 17. ed. Rio de Janeiro: Forense, 2020.

NUCCI, Guilherme de Souza. *Leis Penais e Processuais Penais Comentadas*. 13. ed. São Paulo: Editora Revista dos Tribunais, 2022.

PACELLI, Eugênio. Curso de Processo Penal. 25. ed. São Paulo: Atlas, 2021.

STJ. Superior Tribunal de Justiça. Informativo 763. Processo em segredo de justiça, Rel. O Ministro Messod Azulay Neto, Rel. Acd. Ministro Ribeiro Dantas, Quinta Turma, por maioria, julgado em 7/2/2023.

STJ. Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ, Embargos de Declaração no Agravo Regimental no Recurso em Habeas Corpus nº 143.169. Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 7 fev. 2023, publicado no DJe em 12 fev. 2023.

STJ. Habeas Corpus nº 433.930/ES, Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 19 jun. 2018, publicado no DJe em 29 jun. 2018.

STJ. Recurso em Habeas Corpus nº 76.324/DF, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 14 fev. 2017, publicado no DJe em 22 fev. 2017.

STJ. Agravo Regimental no Habeas Corpus nº 646.771/PR, Rel. Min. João Otávio de Noronha,

Quinta Turma, julgado em 10 ago. 2021, publicado no DJe em 13 ago. 2021.

STJ. Recurso em Habeas Corpus nº 89.385/SP, Rel. Min. Rogério Schietti Cruz, Sexta Turma, julgado em 16 ago. 2018, publicado no DJe em 28 ago. 2018.

VAZ, Denise; LEMOS, Diego Fontenele; CAVALCANTE, Larissa Homsi; MOTA, Rafael Gonçalves (*Apud* Denise Vaz, Provasi, 2012, pág. 20). A prova digital no direito processual brasileiro. In: Revista Acadêmica. Escola Superior do Ministério Público do Ceará. Ano 13, nº 1. Acesso em 15.09.2023. https://revistaacademica.mpce.mp.br/revista/article/view/147/137

https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 118.770, Relator Min. Dias Toffoli. Julgado em 2017. Disponível em: http://www.stf.jus.br. Acesso em: 15 dez. 2024.