

A LEGALIDADE DOS DADOS OBTIDOS DE APARELHOS CELULARES PELO DELEGADO DE POLÍCIA

THE LEGALITY OF DATA OBTAINED FROM CELLULAR DEVICES BY THE POLICE OFFICER

ALEXANDRE JUNIO DE PAULA ALVES¹
LUDMILA STEFANE DA SILVA FERNANDES²

RESUMO

O presente trabalho abordou o tema acerca da legalidade da quebra de sigilo de dados telefônicos pelo delegado de polícia e/ou autoridade policial. Cabe salientar inicialmente que o avanço da tecnologia tornou a comunicação mais efetiva, conectando as pessoas instantaneamente não importando a distância em se encontram. Ademais, este avanço possibilitou também a facilidade em troca e armazenamento de dados, tornando dispositivos móveis verdadeiros bancos de dados que contêm várias informações pessoais, e até mesmo se torna uma ferramenta na prática de ilícitos dada a sua praticidade. Neste ponto, os dispositivos móveis podem servir de ferramenta para viabilizar a prática de crimes, o que nos leva a questionar se a autoridade policial poderia de ofício determinar a busca nos celulares apreendidos com acusados, investigados ou em abordagens. Enfrentamos então pontos importantes que permeiam desde à garantia da inviolabilidade à vida privada, intimidade e sigilo de dados (expressos no art. 5º da Constituição Federal), e, noutro ponto, a garantia da segurança pública trazendo maior efetividade nas ações policiais que estariam aptas a agir de maneira imediata, caso constatassem irregularidades. O debate tem por objetivo evidenciar a necessidade de controle dos atos, para não admitirmos que arbitrariedades sejam cometidas contra cidadãos de bem, e que sejam preservadas a intimidade daqueles que possuem em seus

¹ Acadêmico do curso de Direito do Centro Universitário una – Betim.

Email :alexandrejuniodepaula@outlook.com

² Acadêmica do curso de Direito do Centro Universitário una – Betim.

Email :ludmilastefanesilva@gmail.com

dispositivos móveis uma verdadeira compilação da sua privada, evitando que terceiros o acessem sem o devido controle.

Palavras chaves: Dispositivos móveis, crime, inviolabilidade, direito, dados.

ABSTRACT

Initially, the advancement of technology has made communication more effective, connecting people instantly regardless of the distance among them. In addition, this advance has also made it easier to exchange and store data, making mobile devices true databases that store many personal information, and unfortunately, even become a tool in the practice of crimes. At this point, mobile devices can serve as a tool to make crimes possible, which leads us to question whether the police authority could, by themselves, determine the search on cell phones apprehended with accused, investigated or inspected. So, we face important points that permeate from the guarantee of inviolability to private life, intimacy and confidentiality of data (expressed in art. 5 of the Brazilian Federal Constitution of 1988), and, in another point, a national security, bringing effectiveness in the police actions that would be able to act immediately if irregularities were found. The purpose of the debate is to show the need to control acts. We don't have to admit that arbitrariness is committed in outrage of fundamental rights. The privacy of those who have on their mobile devices a true compilation of their lives is preserved, preventing others from accessing it without proper control.

Key words: Mobile devices, fundamental rights, privacy, confidentiality, data.

1 INTRODUÇÃO

Vários aparelhos eletrônicos permitem o acesso à internet e a outros sistemas de informação e comunicação, gerando uma verdadeira revolução nos meios de comunicação, seja através de conversas eletrônicas ou de trocas de mensagens escritas, gravadas, filmadas (vídeos), por meio de símbolos etc., ou mesmo das diversas formas de armazenagem dessas mensagens. Dentre esses aparelhos, merecem especial destaque os computadores tradicionais, *notebooks*, *tablets* e, particularmente, os celulares e *smartphones* (estes capazes de gerar a conversação entre os interlocutores, além de oferecer quase todas as funcionalidades de um computador).

Tais aparelhos, cada vez mais dotados de alta carga tecnológica que possibilita a sua múltipla aplicação como meio de comunicação falada e escrita; arquivo eletrônico de dados dos mais variados, inclusive relacionados com a intimidade do usuário e de terceiros; agenda de contatos; hospedeiro de aplicativos bancários, de registro viagens, de controle de finanças, de geolocalização etc., encontram-se disseminados dentre a população em geral, tornando-se comum a sua apreensão nas mais diversas situações de intervenção policial, bem como a utilização de sistema de geolocalização para encontrar pessoas foragidas, vincular suspeitos ao local do crime, rastrear o próprio aparelho quanto subtraído etc. A partir dessas apreensões, surgem alguns temas dignos de análise: i) a apreensão desses aparelhos está condicionada à prévia ordem judicial de apreensão? ii) os dados armazenados nesses aparelhos são protegidos pelo sigilo das comunicações? iii) os policiais estão autorizados a atender as chamadas efetuadas para o suspeito ou custodiado?

Tendo em vista os questionamentos acima expostos, o presente artigo objetiva abordar a legalidade dos dados obtidos de aparelhos celulares pelo delegado de polícia.

No Brasil, o assunto ainda é pouco explorado, o que, de certa forma, fomentou a presente pesquisa, deixando a advertência da necessidade de que o tema continue sob constante debate e reflexão não apenas por sua exploração científica, no âmbito acadêmico, mas também nos domínios político e jurídico.

Para a elaboração desta pesquisa, foi realizada uma revisão de literatura qualitativa e descritiva com base em doutrinas, artigos científicos, legislação e entendimentos jurisprudenciais pertinentes ao tema eleito para análise.

2 DAS PROVAS OBTIDAS POR MEIOS ILÍCITOS

Pelo art. 5º, inc. LVI, CF, “são inadmissíveis, no processo, as provas obtidas por meios ilícitos” (BRASIL, 1988, s.p).

Apesar da existência deste dispositivo, a proibição das provas ilícitas é uma decorrência implícita do sistema jurídico. Pode ser deduzida da garantia do devido processo legal (CF, art. 5º, inc. LIV) e de princípios gerais do direito (como o da boa-fé, do respeito à dignidade da pessoa humana etc.).

Nether (2018) ajuda a distinguir os conceitos de prova ilícita, ilegítima e inconstitucional. Segundo o doutrinador:

a) Prova ilícita: é aquela que viola regras e princípios de direito substancial; ofende valores e direitos constitucionais substanciais como a dignidade da pessoa humana, a liberdade, a intimidade, a integridade física, a inviolabilidade do domicílio, o sigilo profissional, de correspondência ou da comunicação telefônica (v.g., documento roubado; violação de sepultura para obtenção de um pedaço do cadáver com o intuito de realização de exame de DNA; infringência do sigilo de correspondência ou de interceptação telefônica; prova obtida mediante tortura ou de maus-tratos; constranger advogado a depor contra o seu cliente ou violar seu escritório, com o intuito de obter provas contrárias a ele).

b) Prova ilegítima: é aquela que ocorre no momento da produção da prova, infringindo regras, princípios e garantias de direito processual (v.g., prova obtida mediante mandado judicial, não fundamentado, de quebra do sigilo fiscal ou bancário, bem como interceptação telefônica autorizada por juiz incompetente, a requisição, feita diretamente aos bancos, de quebra de sigilo bancário, sem autorização judicial ou, ainda, o laudo assinado por alguém que se faz passar por perito).

c) Prova inconstitucional: trata-se de conceito mais abrangente, que busca dar tratamento sancionatório unitário à ilicitude, independentemente se o vício tem natureza substancial ou formal. Provas inconstitucionais são aquelas que violam direitos fundamentais, não podendo ser admitida ou utilizada em júízo, independentemente da ilicitude ter se originado dentro ou fora do processo.

Nesse sentido, corretamente prevê o art. 157, caput, do CPP (a partir da Lei 11.690/08) que são “inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas com violação a normas constitucionais” (BRASIL, 1941, s.p).

As provas inadmissíveis são excepcionais e devem estar baseadas ou em uma alta probabilidade de se obter informações falsas ou no conflito entre o valor da verdade e outros valores (como os da pessoa, da segurança jurídica e das instituições). Na primeira situação, a razão de não se admitir provas é proteger a verdade material. Já na segunda situação dá-se preferência a outros valores, distintos da verdade.

2.1 Provas ilícitas contrárias e favoráveis ao réu

A doutrina processual penal aceita, em sua ampla maioria, a aplicação da teoria da proporcionalidade quando a prova ilícita for produzida *pro reo*, uma vez que o bem jurídico a se tutelar, qual seja, a liberdade de um possível inocente, é assaz relevante, preponderante em relação à inadmissibilidade do uso da prova – e, por consequência, do próprio direito violado, como, por exemplo, a intimidade de outrem.

Cita-se o clássico exemplo do indivíduo que, vendo-se injustamente processado criminalmente, grava, sem autorização judicial, a interceptação telefônica de diálogo mantido entre o verdadeiro autor da infração e terceiro, e depois pretende fazer uso no processo-crime em que é acusado para demonstrar não ser o verdadeiro autor dos fatos apurados (ZANELLA, 2020).

Neste sentido os ensinamentos de Grinover, Scarance Fernandes e Gomes Filho (2011), para quem a ilicitude da prova em favor do réu é eliminada, seja por causas de justificação legal (estado de necessidade ou legítima defesa), seja pelo critério de proporcionalidade, diante da prevalência da ampla defesa, direito consagrado pela Constituição Federal.

Tourinho Filho (2017) observa que o princípio constitucional de inadmissibilidade das provas ilícitas não pode superar o direito de liberdade. Primeiro, porque a inadmissibilidade tem por escopo justamente a proteção de garantias e direitos do indivíduo; segundo, porque “é preciso que nos pratos afilados da balança sejam pesados os bens jurídicos envolvidos e, à evidência, a tutela do direito de liberdade do indivíduo é um valor mais importante para a sociedade que a tutela do outro bem protegido pela proteção ao sigilo” (TOURINHO FILHO, 2017, p.261-262).

Num balanço, o fundamento para permitir, em favor do acusado, a utilização da prova obtida ilicitamente é a consideração de que a garantia de ampla defesa (princípio constitucional) e, principalmente, o direito de liberdade (também consagrado constitucionalmente) superam, numa análise de proporcionalidade – adequação, necessidade e justa medida – a vedação (também constitucional) da inadmissibilidade da prova e, por consequência, o direito transgredido (intimidade, vida privada, entre outros) (MIRABETE, 2015).

Apesar de a teoria da proporcionalidade ser bem aceita pela doutrina e jurisprudência em favor do réu, minoritário é o entendimento no sentido de que ela também pode ser utilizada *pro societate*, ainda que a prova ilícita seja a única nos autos em desfavor do acusado (ZANELLA, 2020).

A razão para isso é que seu uso em favor do acusado preservaria o direito à ampla defesa no processo, em busca de sua (correta) absolvição e, por consequência, preservaria também sua liberdade. Já seu uso em favor da acusação e, portanto, como preceito, pelo Estado (a regra é que as ações penais são públicas), seria inconcebível, uma vez que este tem por obrigação pautar-se pela legalidade em todos os segmentos, inclusive na busca da prova. Este uso geraria descontrole e incentivaria atos funcionais abusivos.

Aury Lopes Junior (2016) sintetiza que o uso da teoria da proporcionalidade em favor da sociedade traria um perigo imenso, devido à amplitude do conceito (indeterminado e, portanto, “manipulável”) e o incorreto reducionismo binário do interesse público versus interesse privado, para justificar uma escolha do primeiro e assim legitimar restrições indevidas dos direitos fundamentais.

Nosso entendimento é de que por razões óbvias, a teoria da proporcionalidade não pode ser aplicada a qualquer ocasião em favor da sociedade. Ela o deve ser de forma bastante excepcional. Também é evidente que o conceito não deve ser manipulado, mas usado com extrema cautela e somente como *ultima ratio*³.

Compartilhando o posicionamento acima, Greco Filho (2015) afirma a possibilidade de guarida ao princípio da proporcionalidade *pro societate* e enfatiza – utilizando-se como exemplo a abertura de correspondência do preso integrante de organização voltada ao narcotráfico – que o direito ao sigilo (ou intimidade) do acusado não se choca apenas com o direito da acusação à prova, mas muito mais que isso: ele colide com a missão institucional do Ministério Público (que tem o ônus probatório), que é a de salvaguardar valores fundamentais para a coletividade, tutelados pela norma penal.

2.2 Métodos ocultos de investigação criminal e os limites impostos pelo direito probatório

Com o surgimento de novos delitos e, também, de novas formas de praticar os delitos já tipificados nos diplomas penais existentes, é necessário que o Estado tenha condições de investigar, processar, prevenir e reprimir estas infrações.

Excepcionalmente, a exemplo de situações que envolvem organizações criminosas, levando-se em conta que, muitas vezes, são constituídas por pessoas que

³ Expressão latina que se traduz como última razão.

gozam de prestígio e influência social, a investigação se torna difícil caso sejam empregados somente os meios convencionais de investigação.

Para esses casos, é possível que sejam empregados os meios investigativos ocultos, a exemplo das interceptações telefônicas, infiltração de agentes, informantes, acordos de colaborações premiadas, gravações ambientais, rastreamento de celulares, dentre outros, nos termos autorizados pela legislação vigente.

Ocorre que esses meios ocultos, que deveriam ser utilizados somente em casos excepcionais, às vezes são empregadas de maneira desregrada, em claro desrespeito aos princípios e garantias vigentes na lei brasileira e nos tratados internacionais dos quais o Brasil é signatário.

Não raro se tem notícias via mídia de interceptações telefônicas e acordos de colaboração premiada terem sido empregados como único meio de prova para fundamentar sentenças penais condenatórias, o que não é admitido em um Estado democrático de direito. Esses meios ocultos deveriam ser empregados somente em caráter excepcional, como formas para obter outras provas e, assim, em conformidade com o contexto probatório, poderiam ajudar a fundamentar uma condenação. Porém, o emprego de meios investigativos ocultos como única “prova” somente poderia ser utilizado para embasar sentenças absolutórias, mas não as condenatórias (VALENTE, 2017).

O Brasil, com o objetivo de prevenir e reprimir os delitos mais complexos de serem apurados, a exemplo da corrupção, tráfico de drogas e outros praticados por organizações criminosas, tem buscado exemplos em outros países, especialmente os países que adotam a *common law*, meios investigativos que, da maneira como vêm sendo utilizados, sem as necessárias adaptações ao ordenamento jurídico brasileiro, mostram-se claramente inconstitucionais, além de violarem tratados internacionais de direitos humanos (VALENTE, 2017).

O uso desses meios é de fundamental importância para a investigação e o processamento de casos complexos, mas é necessário que seja regulamentada pelo ordenamento pátrio, de maneira a evitar sua vulgarização, devendo ser empregados apenas excepcionalmente (em situações em que outros meios investigativos não puderem atingir as mesmas provas que se fazem necessárias) e sempre em consonância com os princípios e garantias, especialmente a ampla defesa, o contraditório, o devido processo legal e a presunção de inocência.

Nesta seção serão abordados os métodos ocultos de investigação criminal e os limites impostos pelo direito probatório. Inicia-se trazendo conceitos e as características dos referidos métodos.

2.2.1 Conceito e características

O desejo por uma justiça mais célere e veloz, que atenda ao clamor dos cidadãos, que se sentem amedrontados perante os fenômenos da criminalidade econômico-financeira, do crime organizado transnacional e do terrorismo, motivou os decisores políticos a implementarem meios especiais e excepcionais para a obtenção de prova, a saber:

[...] ampliação do âmbito das interceptações telefônicas, registro de voz off e imagem, gravações ambientais, gravações e fotografias por meio de câmaras de vídeo vigilância, agentes infiltrados física e digitalmente, rastreios e persecuções digitais, localizações celulares, controlo e monitoramento concreto de IP, IMEI e GPS, recurso a IMSI-Carther (IMEI), buscas e apreensões preventivas no sistema digital a nível nacional, regional e internacional sem qualquer conhecimento do visado, e a admissibilidade e utilização como meios de prova os relatórios elaborados pelos serviços secretos (VALENTE, 2017, p.474).

Estes meios são denominados métodos ocultos de investigação criminal, que são definidos como “aqueles métodos que representam uma intromissão nos processos de ação, interação, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência, conhecimento ou disso sequer se apercebam” (RODRIGUES, 2010, p. 37).

Embora já existissem, estes novos métodos de obtenção de provas, experimentaram um maior desenvolvimento nos últimos anos, motivado pelo progresso tecnológico, possibilitando a expansão daqueles métodos já existentes e tornando possível o surgimento de novos métodos (CAMBI, 2014). Aliado a este desenvolvimento, foi observada a existência de uma nova concepção “securitária” do direito penal, que segundo Cambi (2014) tem levado à redução das garantias dos cidadãos e, conseqüentemente, à violação de seus direitos fundamentais. No entanto, a cada dia, a prospecção para o emprego dos mesmos tem sido majorada, motivado pelo crescente desenvolvimento da criminalidade, de maneira a alcançar-se maior eficácia na investigação criminal.

2.2.1.1 Interceptação das comunicações

A título de exemplificação, a interceptação das comunicações, de um modo geral, e, em particular, a interceptação telefônica, situa-se no campo dos meios probatórios que têm elevado potencial de produzir danos individuais e coletivos ou sociais e, por isso, mereceu restrição em nível constitucional no art. 5º, inc. XII, que, protegendo a intimidade das pessoas, prevê:

Art. 5º, [...] inc. XII - é inviolável o sigilo das correspondências 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 (BRASIL, 1988, s.p).

Visando a regulamentar a exceção constitucional, no que diz respeito à possibilidade de autorização para a escuta telefônica, com vistas à persecução penal, foi editada a Lei 9.296/1996, que, ao contrário de legislações como a de Portugal e Alemanha, não trouxe um catálogo fechado de infrações penais que sujeitam os suspeitos a esse especial meio de captação de provas, preferido estabelecer, de forma negativa, as hipóteses de não cabimento da medida:

Art. 2º. Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: I – não houver indícios razoáveis de autoria ou participação em infração penal: II – a prova puder ser feita por outros meios disponíveis; o fato investigado constituir infração penal punida, no máximo, com pena de detenção (BRASIL, 1996, s.p).

Diante da opção do legislador, as infrações penais punidas com detenção, prisão simples ou exclusiva pena de natureza pecuniária, ou educativa, não autorizam a utilização da interceptação de comunicações telefônicas do investigado ou do réu respectivo e dentre essas infrações acham-se a ameaça (CP, art. 147), os crimes contra a honra (CP, arts. 138-140), a aquisição de drogas para consumo próprio (Lei 11.343/2016, art. 28) e outros, cujos meios de execução, não raro, envolvem esse tipo de comunicação.

Como existe expressa previsão que esse tipo de infração penal não autoriza o deferimento da medida probatória sob análise, não há dúvida de que, se houver uma interceptação telefônica com base em alguma dessas infrações penais, constituirá meio ilícito de captação de prova e inviabilizará a sua introdução e avaliação no processo, por força do disposto no art. 5º, inc. LVI da CRFB (“são inadmissíveis, no processo, as provas obtidas por meios ilícitos”).

Há também que se pontuar sobre o acesso aos dados armazenados em aparelhos de comunicação e às conversas que será mais bem detalhado à seguir.

3 AS PROIBIÇÕES DE PROVA ENQUANTO LIMITES AOS MÉTODOS OCULTOS DE INVESTIGAÇÃO CRIMINAL

Em um Estado Democrático de Direito, onde a matriz fundamental é a dignidade da pessoa humana, o Estado não pode se valer de qualquer método de obtenção de prova nem tampouco de certas provas que firam de morte as garantias fundamentais do cidadão.

Assim, a busca da verdade não se dá a qualquer custo, mas tão somente por meios justos e leais, conforme o Estado democrático de direito, ainda que eventualmente tenha que renunciar à descoberta da verdade para salvaguardar direitos intransponíveis. Nesse sentido, as proibições de prova funcionam como verdadeiros limites à descoberta da verdade e, como tal, limitam a atividade de investigação criminal e os métodos utilizados.

A CRFB/1988 impõe em seu art. 5º, inc. LVI que - são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

As limitações impostas pelo Direito Probatório refletem diretamente na atividade de investigação criminal e, mais especificamente, nos meios de obtenção de prova, não se admitindo ato investigativo criminal que não conduza a fonte de prova ou elemento que possa ser utilizado em juízo.

Conforme destacado em linhas pretéritas, a tecnologia está cada vez mais presente no cotidiano das pessoas, das empresas e das instituições públicas. Essa nova realidade impõe novos desafios, sobretudo, à segurança dos dados que circulam no ambiente digital, deixando mais vulneráveis a privacidade e a intimidade dos cidadãos. Por outro lado, também traz novos obstáculos à elucidação de condutas criminosas e de seus autores.

Nesse contexto de evolução tecnológica e de vulnerabilidade do ambiente digital, têm sido desenvolvidos “métodos de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses computacionais” (HENRIQUE, 2006), nos quais se incluem técnicas, *hardware* e programas informáticos. São o que se denomina de medidas antiforenses.

Essas medidas antiforenses podem se revestir de natureza legítima, quando utilizadas para proteção dos dados informáticos ou como meio de preservação da

intimidade e da liberdade de expressão. Mas, por outro lado, também são muitas vezes utilizadas como meios de esconder e camuflar a prática de crimes e frustrar potenciais atividades de recolha de provas nos sistemas informáticos (RAMALHO, 2017).

Nas palavras de Harris (2006, p. 45), as medidas antifoenses são:

[...] quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade.

Muitas são as medidas antifoenses por meio das quais objetivam-se evitar que as entidades de investigação alcancem dados digitais com potencial valor probatório (RAMALHO, 2017), o que não só tornam mais fácil a prática de crimes em ambiente digital e o seu anonimato, como, inversamente, tornam mais difícil a sua descoberta e a obtenção de provas. Em razão disso, algumas vezes demonstra-se imperiosa a utilização de métodos ocultos de investigação criminal para que o Estado possa ter acesso às fontes de provas digitais e, conseqüentemente, alcance a verdade no processo penal.

Evidentemente, os métodos ocultos de investigação criminal mitigam um conjunto de bens jurídicos e direitos fundamentais, notadamente os ligados à privacidade/intimidade do investigado. No entanto, enquanto forma de exercício do poder público, é impossível conceber-se um sistema processual penal eficaz sem qualquer ingerência nos direitos fundamentais dos cidadãos. Deve-se buscar na justiça penal o justo equilíbrio baseado na adequada ponderação dos interesses da persecução penal do Estado e dos direitos, garantias e liberdades individuais (RAMALHO, 2017).

Na busca desse equilíbrio, o Estado não deve ser, por um lado, um Estado-polícia com poderes ilimitados, sob pena de o combate à criminalidade gerar uma verdadeira “criminalidade de Estado”; e, por outro lado, não deve constituir-se também em um mero Estado-observador, omissivo (que em nada intervém), o que pode gerar a primazia da “lei do mais forte”. Assim, o sistema de justiça penal, no qual se inclui a investigação, deve encontrar uma solução intermediária entre o Estado débil e o Estado forte, fruto de uma adequada ponderação entre a necessidade da busca da verdade e realização da justiça, de um lado, e o respeito à inviolabilidade do núcleo essencial dos fundamentais do cidadão (RAMALHO, 2017).

Deve-se buscar, portanto, a concordância prática entre os propósitos paradoxais do processo penal da correta investigação dos ilícitos penais, da descoberta da verdade e subsequente realização da justiça, com o respectivo restabelecimento da paz jurídica, e, ao mesmo tempo, da proteção dos direitos individuais contra a atuação arbitrária do Estado.

Assim, a busca da verdade no processo penal em um Estado Democrático de Direito não pode ser realizada a qualquer preço, mas somente a partir de meios legítimos. Conforme a lição de Dias (2004, p. 194), a verdade processual não é absoluta ou ontológica, mas antes de tudo uma verdade judicial, prática e, sobretudo, não uma verdade obtida a todo o custo, mas processualmente válida, ou seja, obtida de acordo com as formalidades judiciais.

Como ensina Silva (2010, p. 82-83):

A justiça criminal é chamada a investigar atividades suspeitas, tanto de pessoas honestas como de malfeitores, mas todos são, pessoas. Por outra parte, não se compreende que aqueles que se dedicam a servir a justiça possam usar na luta contra os malfeitores meios análogos aqueles que lhes reprovam. A eficácia da justiça é também um valor que deve ser perseguido, mas, porque numa sociedade livre e democrática os fins nunca justificam os meios, só será louvável quando alcançada pelo engenho e arte, nunca pela força bruta, pelo artifício ou pela mentira, que degradam quem as sofre, mas não menos quem as usa.

Por mais grave que seja o ilícito criminal cometido e quão difícil seja se alcançar a verdade, o Estado jamais poderá se utilizar de meios que imponham a aniquilação do núcleo essencial dos direitos fundamentais. Por isso, a Constituição Federal brasileira estabelece expressamente que “são inadmissíveis, no processo, as provas obtidas por meios ilícitos” (SILVA, 2010, p. 80). A atuação do Estado na descoberta da verdade deve sempre estar adstrita ao princípio da lealdade. Esta postura do Estado é um dever essencialmente moral traduzindo “uma maneira de ser da investigação e obtenção de provas em conformidade com os direitos da pessoa e a dignidade da justiça” (SILVA, 2010, p. 80).

Assim, a salvaguarda do núcleo essencial dos direitos fundamentais e a obediência à postura leal impõem restrições aos meios de obtenção de prova no processo penal democrático, ainda que isso implique eventualmente renunciar à descoberta da verdade e conseqüentemente abdicar de condenar um criminoso quando a única prova da sua culpa apenas possa ser obtida a partir de meios, em abstrato, inadmissíveis num Estado de

Direito ou, em concreto, desproporcionais. Nesse sentido, segundo Ramalho (2017, p. 185):

[...] o Estado de Direito Democrático, assente na autonomia e dignidade da pessoa humana e no pluralismo, tem, forçosamente, de conviver com o fracasso e de reconhecer que, no caminho da prossecução da justiça, há, por vezes, um dever de recuar face à prevalência de direitos fundamentais.

Por outro lado, se é certo que essa orientação implica severas restrições ou limites à descoberta da verdade e à investigação criminal, “também é verdade que existem casos em que se justifica que o Estado vá mais longe do que noutros na procura da verdade, avançando paulatinamente em direção ao limite – a todos os títulos intransponível – da dignidade e integridade pessoal do visado” (RAMALHO, 2017, p. 185).

Na busca desse equilíbrio, o Estado deve decidir qual o preço está disposto a pagar para a prossecução penal de quem pratica um crime. Noutras palavras, o sacrifício que o Estado está disposto a fazer no que tange aos direitos fundamentais para o alcance da verdade. Esse sacrifício é materialmente executado, na fase de investigação, a partir da utilização “um *arsenal* de meios de investigação criminal progressivamente mais agressivos dos direitos dos cidadãos em função da gravidade e danosidade social do crime em causa ou da absoluta indispensabilidade do meio de prova em face das circunstâncias” (RAMALHO, 2017, p. 185-186).

Mesmo reconhecendo-se os enormes desafios para a descoberta da verdade oriundos da complexidade do ambiente digital e dos métodos desenvolvidos pelos recursos tecnológicos para esconder e camuflar a prática de crimes e obstaculizar o acesso às provas, o preço que o Estado se disponha a pagar não pode chegar ao ponto de corroer a liberdade de atuação do cidadão comum, por receio de uma ingerência estatal remota e secreta, preventiva ou repressiva, nas atividades de sua vida (RAMALHO, 2017).

É nesse âmbito que as proibições de prova funcionam como verdadeiros limites autoimpostos pelo Estado à descoberta da verdade, ancoradas no princípio da dignidade da pessoa humana, matriz fundamental do Estado Democrático de Direito, cuja violação atinge a própria legitimidade do exercício do poder punitivo do Estado.

A partir desse panorama inicial e resguardando-se principalmente a dignidade da pessoa humana, é que importa realizar os apontamentos necessários que permitam compreender as provas ilícitas por derivação.

4 A LEGALIDADE DOS DADOS OBTIDOS DE APARELHOS CELULARES PELO DELEGADO DE POLÍCIA

A apreensão de computadores, *smartphones*, *tablets* e celulares está sujeita às mesmas regras que regem a apreensão de bens em geral, exceto quando se tratar de objetos que tenham relação com o fato criminoso ou mesmo de objetos sujeitos a medidas assecuratórias ou cautelares patrimoniais, que possuem regramento específico. Assim, em se tratando de apreensão vinculada à produção de provas em geral, a regra é a de que deva ser precedida de ordem ou autorização judicial, pois se trata atividade constritiva com incursão sobre o patrimônio e a intimidade da pessoa afetada pela diligência e com reflexos na prova a ser produzida nas investigações extrajudiciais ou judiciais (SOUZA, 2020).

Importa destacar que eventuais excessos por parte dos agentes encarregados da investigação podem configurar, inclusive, desde que presente o elemento especial subjetivo do dolo (dolo específico) previsto no art. 1º, § 2º da Lei 13.869/2019, o tipo penal previsto no art. 25 da referida Lei de Abuso de Autoridade, desde que a prática ocorra no curso de procedimento de investigação (inquérito, sindicância, PIC etc.) ou fiscalização, havendo ainda a possibilidade da extensão do crime em questão àquela autoridade que: “[...] faz uso de prova, em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude”.

Os dados armazenados em quaisquer desses aparelhos (computador, *smartphone*, celular etc.) não se confundem com as comunicações das quais derivaram e, uma vez concluídas tais comunicações, desde que armazenadas, passam elas a ter a natureza de documentos guardados ou arquivados, podendo ser acessados e utilizados como prova, desde que observadas as mesmas restrições aplicáveis à apreensão de documentos em geral. Assim como um policial não está autorizado a acessar um escritório ou uma residência, fora das hipóteses legais ou da presença de concordância do responsável, e apreender documentos arquivados ou guardados, assim também não está autorizado a acessar o banco de dados desses equipamentos eletrônicos, exceto se tiver autorização judicial para tal diligência⁴.

⁴ STJ: Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial. 2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial,

Prática comum, mas nem por isso lícita, vem a ser aquela em que o policial realiza uma diligência ou mesmo uma prisão em flagrante e, sem autorização judicial ou do custodiado, atende as ligações destinadas a ele (suspeito ou investigado), acessa a sua agenda de contatos, o seu arquivo de fotos ou mesmo lê as mensagens ou e-mails do custodiado, sem o consentimento dele. Tal prática, apesar de contar com o apoio de alguma corrente jurisprudencial, é ilegal e fere o direito de privacidade das comunicações do indivíduo investigado (CRFB, art. 5º, XII) quando se trata de ligações ou mensagens em curso; ou a sua privacidade (CRFB, art. 5º, X), quando se refere a mensagens ou ligações armazenadas, movimentação bancária etc., neste caso concebidas como dados armazenados e não como dados interceptados, gerando prova ilícita.

Não obstante a posição aqui externada, há considerável corrente jurisprudencial, principalmente nos tribunais de 2ª instância, sustentando a tese da licitude da diligência policial consistente em acessar e ler ou decifrar os arquivos dos aparelhos celulares ou *smartphones*, sem consentimento de quem de direito, ao argumento de tal prática decorreria da autorização de apreensão prevista no art. 6º do CPP, o que parece decorrer de equívoco interpretativo, uma vez que as regras que dizem respeito a limitação de direitos fundamentais devem ser interpretadas restritivamente. No entanto, o acesso indevido aos dados armazenados não os invalida, tornando ilícitas apenas o uso do conteúdo acessado ilegalmente, mas permitindo que, invalidado aquele conteúdo, novas investigações possam partir da mesma fonte, de forma ampla (SOUZA, 2020).

Essa exceção se explica, pois uma vez concebida a ilicitude da prova (v.g. conteúdo de mensagens armazenadas em aplicativo de *whatsApp*; registro de conversas por meio de e-mail, etc.), por ter sido obtida com afronta a regra de direito material (inseridas na Constituição Federal, em Normas Internacionais internalizadas pelo Brasil e Leis), não pode aquela própria prova ser aproveitada ou refeita, mas tendo o equipamento tecnológico (celular, *smartphone*, etc.) sido apreendido regularmente, como na situação aqui analisada ele se constitui em fonte de provas e não em elemento de prova (prova = resultado extraído da fonte de provas), desde que tenham sido obedecidas as regras de

cujos produtos devem ser desentranhados dos autos (RHC 51.531/RO–Rel. Min. Nefi Cordeiro–DJe 09.05.2016).

TRE-AC: Perícia resultante de acesso a registros telefônicos, a mensagens e a conversas WhatsApp de aparelho celular obtido por meio de medida cautelar de busca e apreensão previamente autorizada por ordem judicial não constitui prova ilícita, tendo em vista que não se confundem comunicação telefônica e registros telefônicos e, além disso, a proteção constitucional é da comunicação de dados e não dos dados. Precedentes do STJ e do STF. (TRE-AP-RP: 224081-AP, Rel.: Décio José dos Santos Rufino–DJE–Diário da Justiça Eletrônico–TRE/AP, Tomo 199–Data 07.10.2016, Página 8).

integridade da cadeia de custódia na preservação do aparelho e de seus dados armazenados e aplicativos periciados, conforme recentes alterações introduzidas no CPP pela Lei 13.964/2019, encontra-se autorizado o novo acesso ao conteúdo daquelas fontes, para a produção de provas judicialmente autorizadas⁵.

5 CONCLUSÃO

De fato, os modernos dispositivos tecnológicos, a exemplo dos *smartphones*, *tablets*, *smartwatches*, *notebooks*, etc., e os crescentes aplicativos de redes sociais, fazem parte do cotidiano da atual sociedade da informação. Essa nova realidade, ao passo que contribui para o inegável progresso da humanidade ao facilitar o acesso à informação e ao conhecimento, também impõe novos desafios sobretudo à segurança dos dados que circulam no ambiente digital, deixando mais vulneráveis a privacidade e a intimidade dos cidadãos.

Sabe-se que os métodos tradicionais de investigação criminal se mostram insuficientes para ultrapassar as dificuldades impostas à persecução criminal nesse complexo ambiente da atual sociedade em rede e em risco. É inevitável, portanto, que haja uma reação do sistema jurídico no sentido de permitir que o Estado persecutor utilize-se dos avanços tecnológicos que impliquem investigações mais invasivas e insidiosas aos direitos fundamentais, para fazer frente à paralela evolução de práticas criminosas mais graves.

Nesse contexto, os dados obtidos pelo Delegado a partir do acesso ao celular do acusado apresentam-se como um dos meios de investigação ou de obtenção de prova dos mais insidiosos, principalmente pelo seu multiforme potencial técnico que o habilita a uma ampla capacidade investigativa, com repercussão limitativa de diferentes direitos fundamentais.

⁵ STJ: por ocasião da própria prisão em flagrante – sem, portanto, a prévia e necessária autorização judicial –, o policial atendeu o telefone do réu e afirmou que a ligação tratava de um pedido de venda de substância entorpecente. Na delegacia o celular do réu foi apreendido, desbloqueado e nele verificada a existência de mensagens de texto que indicavam prévia negociação da venda de entorpecentes, sem, portanto, anterior autorização judicial. 3. A denúncia se apoiou em elementos obtidos a partir da apreensão do celular pela autoridade policial, os quais estão reconhecidamente contaminados pela forma ilícita de sua colheita. [...] (STJ–HC: 542293 SP 2019/0322281-7–Rel.: Min.Rogério Schietti Cruz–DJe 19.12.2019). TJRS: Insurge-se a defesa considerando a mídia acostado aos autos e na qual registrados, pela autoridade policial e seus agentes, áudios extraídos de aplicativo de mensagens (*WhatsApp*). Atividade policial que se pautou em prévia autorização judicial, não se verificando qualquer falta de zelo no manejo da prova a gerar a afirmada quebra da cadeia de custódia.

Por outro lado, a recusa absoluta da possibilidade do emprego de técnicas investigativas inominadas ou insatisfatoriamente regulamentadas poderá resultar na total incapacitação do Estado de cumprir a sua importante missão de apurar condutas criminosas de alta complexidade. Desse modo, a exclusão apriorística da possibilidade do emprego de todo e qualquer método investigativo inovador oriundo da evolução tecnológica não parece se coadunar com o desejável equilíbrio entre a necessidade de eficiência das investigações criminais e a garantia de proteção dos direitos fundamentais.

Ademais, a ordem constitucional e legal brasileira não impõe um sistema rígido de taxatividade dos meios de obtenção de prova, admitindo-se o recurso a meios de investigação ou de obtenção de prova não disciplinados expressamente em lei, desde que respeitada a estrita observância dos limites constitucionais e processuais da prova, atendidas, ainda, a excepcionalidade e a proporcionalidade da medida⁶, para garantia do núcleo essencial dos direitos fundamentais atingidos

REFERÊNCIAS

BRASIL, Lei 2.848 de 7 dezembro de 1940. **Código Penal Brasileiro**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 3 abr. 2021.

BRASIL. **Decreto-Lei nº 3689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 3 abr. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

Brasil. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19296.htm. Acesso em: 3 abr. 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código

6 Em Voto-vista, o Min. Rogério Schietti Cruz, no julgamento do Habeas Corpus nº 315.220/RS do Superior Tribunal de Justiça (HC 315.220/RS, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 15/09/2015, DJe 09/10/2015), entendeu que o acesso à conta de correio eletrônico não se trata de interceptação, porque a sua captação não era atual, mas se cuida de quebra de sigilo de comunicações telemáticas (sem previsão legal). Desse modo, sustentou que a medida implementada judicialmente aproxima-se, em sua essência, da busca e apreensão de documentos virtualmente armazenados em provedor de internet, devendo, pois, regular-se pelo disposto no art. 240 [§1º, f] do Código de Processo Penal, que regulamenta a busca domiciliar ou pessoal.

Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 3 abr. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 3 abr. 2021.

CAMBI, Eduardo. **Curso de Direito Probatório**. Curitiba: Juruá Editora, 2014.

DIAS, J.F. **Direito Processual Penal**. Coimbra: Coimbra Editora, 2004.

GRECO FILHO, Vicente. **Interceptação Telefônica**. 3. ed.. São Paulo: Saraiva, 2015.

GRINOVER, A.P.; FERNANDES, A.S.; GOMES FILHO, A.M. **As nulidades no processo penal**. 12. ed.. São Paulo: Revista dos Tribunais, 2011.

HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic sproblem, *Digital Investigation - The international Journal of Digital Forensics & Incident Response*, V. 03 – Suplemento, 2006.

HENRIQUE, W.G. **Anti Forensics**: dificultando análises forenses computacionais. 2006. Disponível em: <http://ws.hackaholic.org/artigos/AntiForensics.ppt>. Acesso em: 3 abr. 2021.

LOPES JR., A. **Direito Processual Penal**. 13. ed. São Paulo: Saraiva, 2016.

MIRABETE, Julio Fabbrini. **Código de Processo Penal interpretado**. 9. ed. São Paulo: Atlas, 2015.

NETHER, N.A.B. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018.

RAMALHO, D.S. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Almedina, 2016.

RODRIGUES, B.S. **Refers to the idea of digital domicile for the purpose of online searches – Da Prova Penal – Bruscamente...** A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal. Lisboa: Rei dos Livros, 2010, v. 2.

SILVA, G.M. **Curso de Processo Penal**. Tomo I, Verbo, 2010

TOURINHO FILHO, Fernando da Costa. **Processo penal**. 17. ed. São Paulo: Saraiva, 2017.

ZANELLA, Everton Luiz. **Infiltração de Agentes e o Combate ao Crime Organizado**. 2 ed. Curitiba: Juruá Editora, 2020.