XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

ZULMAR ANTONIO FACHIN

FABIANO HARTMANN PEIXOTO

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Fabiano Hartmann Peixoto; Zulmar Antonio Fachin – Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-567-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Direitos Sociais, Constituição e Democracia na América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governança. 3. Novas tecnologias. XI Encontro Internacional do CONPEDI Chile - Santiago (2: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O XI ENCONTRO INTERNACIONAL DO CONPEDI, com temática "Direitos sociais, Constituição e Democracia na América Latina", ocorrido entre os dias 13 e 30 de outubro de 2022, reuniu centenas de pesquisadores de diversos países. Com submissão extremamente substantiva, a linha de pesquisa Direito, Governança e Novas Tecnologias necessitou de subdivisão. A presente apresentação, então, refere-se aos trabalhos submetidos, selecionados e efetivamente apresentados e discutidos no GT Direito, Governança e Novas Tecnologias II.

Foi traço marcante a discussão sobre os impactos e as interfaces da tecnologia com temas tradicionais do Direito. Percebeu-se nela um papel extremamente relevante para o desenvolvimento do conhecimento e ensino jurídicos.

Fenômeno intensificado na última década, a tecnologia vem provocando análises e/ou avaliações no campo constitucional, processo e especialidades jurídicas. O cenário digital e cibernético teve abordagens multidisciplinares em trabalhos aprofundados. Assim, destacam-se as grande temáticas do GT:

• Inteligência Artificial

• Algoritmos

• Metaverso

• Lei Geral de Proteção de Dados

• Economia disruptiva

• Autodeterminação informacional

• Provas digitais

• Regulação internacional de dados

• Regulação de ciberespaço

• Compliance

• Inclusão digital

Centralmente, os trabalhos sobre Inteligência Artificial buscaram demonstrar a íntima relação entre compromissos éticos no uso ou desenvolvimento de sistemas com referenciais de direitos fundamentais. Discutiu-se, da mesma forma, os impactos dos novos sistemas de IA nos conceitos e alcances de institutos tradicionais do Direito, tais como a responsabilidade civil.

Igualmente presente, as análises de estratégias regulatórias também ocuparam relevante espaço no GT, especialmente no sentido dos desafios internacionais sobre a temática. Manifestações mais recentes da tecnologia no campo jurídico também foram apresentadas, destacando-se a interface dos direitos da personalidade no metaverso e a ampliação dos chamados "cookies" como ferramentas de potenciais fragilizações no sistema de proteção de dados.

Apresentado por pesquisadores do país anfitrião (Chile), aspectos da economia disruptiva em interface com a tecnologia promoveram debates sobre possíveis leituras chilenas das influências econômicas sobre o Direito e uma comparação com o panorama brasileiro.

Como não poderia ser diferente, os desafios da gestão e proteção de dados e os desdobramentos da Lei Geral brasileira também foram objeto de apresentação de pesquisas e demonstraram quantos novos desafios são postos à comunidade jurídica internacional.

Destacam-se, nesta breve apresentação, a análise e discussões sobre o incremento dos sistemas de certificação digital - tão intensificados em tempos de pandemia -, notadamente pelas inevitáveis dúvidas em razão do debate público-privado e das necessárias cautelas impostas pelos riscos de aumento na desigualdade entre cidadãos.

De uma maneira geral, as discussões do GT se encaminharam para a percepção de profundas alterações no modo tradicional de se observar o fenômeno jurídico, das inúmeras oportunidades apresentadas pela tecnologia e da proporcional necessidade de se observar riscos que as acompanham, especialmente sob a ótica de direitos fundamentais.

Dentro desta variedade interessante de relatos de pesquisa, os coordenadores desse grupo de trabalho convidam a todas e todos para a leitura na íntegra dos artigos.

Zulmar Antonio Fachin - Unicesumar e Faculdades Londrina - zulmarfachin@uol.com.br

Fabiano Hartmann Peixoto - Universidade de Brasília - fabiano_unb@unb.br

PERSECUÇÃO PENAL E PROVAS DIGITAIS OBTIDAS A PARTIR DE DISPOSITIVOS MÓVEIS: ENTRE A COLETA E PRESERVAÇÃO DA PROVA E A ILICITUDE PROBATÓRIA

CRIMINAL PROSECUTION AND DIGITAL EVIDENCE OBTAINED FROM MOBILE DEVICES: BETWEEN THE COLLECTION AND PRESERVATION OF EVIDENCE AND EVIDENCE ILLEGALITY

João Paulo Machado Piratelli [1]
Cinthia Obladen de Almendra Freitas [2]

Resumo

O presente artigo tem como temática a persecução penal e desenvolve-se na relação entre provas digitais, cadeia de custódia, provas ilícitas e Computação Forense. Descreve-se o entendimento do Superior Tribunal de Justiça (STJ) a respeito da licitude ou ilicitude de provas digitais obtidas a partir de dispositivos móveis com base em julgados paradigmáticos divulgados por meio dos Informativos de Jurisprudência da Corte Superior. Do mesmo modo, são descritas técnicas de Computação Forense destinadas à obtenção, autenticação e análise de provas digitais extraídas de dispositivos móveis. Para tanto, utilizou-se do método hipotético-dedutivo e da técnica de pesquisa bibliográfica associada à análise crítica de teorias da prova e de técnicas de Computação Forense em comparação com o que foi decidido nos referidos julgados. Pretendeu-se, com isso, avaliar a hipótese de que o STJ anula casos criminais indevidamente em razão da falta de conhecimentos técnicos básicos de Computação Forense. Alfim, concluiu-se que a hipótese é verdadeira.

Palavras-chave: Computação forense, Dispositivos móveis, Provas digitais, Provas ilícitas, Superior tribunal de justiça

Abstract/Resumen/Résumé

This article has as its theme the criminal prosecution and is developed in the relationship between digital evidence, chain of custody, illicit evidence, and Computer Forensic. The understanding of the Superior Court of Justice of Brazil regarding the legality or illegality of digital evidence obtained from mobile devices based on paradigmatic judgments published through the Superior Court Jurisprudence Reports is described. Likewise, Computer Forensic techniques aimed at obtaining, authenticating, and analyzing digital evidence extracted from mobile devices are described. We used the hypothetical-deductive method and the technique of bibliographic research associated with the critical analysis of theories of evidence and of

[1] Mestrando em Direito Socioambiental e Sustentabilidade. Pontifícia Universidade Católica do Paraná – PUCPR. jpmpiratelli@gmail.com.

[2] Doutora em Informática Aplicada. Coordenadora do Programa de Pós-Graduação em Direito da PUCPR. Pontifícia Universidade Católica do Paraná – PUCPR. cinthia.freitas@pucpr.br.

Computer Forensic techniques in comparison with what was decided in the judgments. It was intended, with this, to evaluate the hypothesis that the Superior Court unduly annuls criminal cases due to the lack of basic technical knowledge of Computer Forensic. Finally, it was concluded that the hypothesis is true.

Keywords/Palabras-claves/Mots-clés: Computer forensic, Mobile devices, Digital evidence, Illicit evidence, Superior court of justice

1 Introdução

O Superior Tribunal de Justiça (STJ) tem, dentre suas competências constitucionais, a função de pacificar e uniformizar a jurisprudência nacional relacionada à aplicação da legislação federal, conforme art. 105, inciso III, Constituição Federal (BRASIL, 1988). Por sua vez, a persecução penal é regida integralmente por leis federais, haja vista que é de competência privativa da União legislar sobre Direito Penal e Direito Processual, conforme dispõe o art. 22, inciso I, Constituição Federal (BRASIL, 1988). Tanto é assim que os principais diplomas legais que regem a persecução penal – Código Penal (BRASIL, 1940) e Código de Processo Penal (BRASIL, 1941) – são federais.

Desse modo, considerando-se que o avanço tecnológico também fez com que crimes passassem a ser cometidos ou, ao menos, dependessem de algum modo do mundo digital, é imprescindível o estudo da jurisprudência do STJ, notadamente, para compreender a aplicação da legislação em vigor aos casos criminais que dependem de provas digitais, em especial, as que são obtidas a partir de dispositivos móveis, tais como *smartphones*. Todavia, a utilização de provas digitais na persecução penal nem sempre é devidamente compreendida pelos ministros do STJ, o que pode resultar em erros judiciários gravíssimos, como a decretação de nulidade de um caso penal com base num equívoco de interpretação sobre determinadas características técnicas de Computação Forense.

Com base nesse contexto, o problema aqui investigado pode ser sintetizado na seguinte pergunta: o STJ anula casos criminais indevidamente em razão da falta de conhecimentos técnicos básicos de Computação Forense? Para responder a essa pergunta é necessário demonstrar que a mera extração de dados de dispositivos móveis tem como objetivo a preservação da prova e da cadeia de custódia, dispensando autorização judicial específica, a qual somente é necessária para a análise desses dados.

Desse modo, a presente pesquisa tem como objetivo geral descrever o entendimento do STJ a respeito da licitude ou ilicitude de provas digitais obtidas a partir de dispositivos móveis em 3 (três) cenários distintos: (i) busca e apreensão de dispositivos móveis em razão de mandado judicial; (ii) apreensão de dispositivos móveis a partir de prisão em flagrante; e (iii) entrega espontânea de dispositivos móveis. Já os objetivos específicos visam descrever técnicas de Computação Forense destinadas a aquisição, autenticação e análise de provas digitais obtidas a partir de dispositivos móveis, para, posteriormente, correlacioná-las à cadeia de custódia, às provas ilícitas e ao direito fundamental à prova.

Para tanto, utilizou-se do método hipotético-dedutivo e da técnica de pesquisa bibliográfica associada à análise crítica de teorias da prova e de técnicas de Computação

Forense em correlação a 3 (três) julgados paradigmáticos do STJ no campo do Direito Processual Penal, os quais foram publicados pela Corte Superior em compilados periódicos oficiais denominados “Informativos de Jurisprudência”, cujo desiderato é divulgar as principais teses firmadas pelo Tribunal e com significativa repercussão no meio jurídico. Como resultado desse estudo, pretende-se confirmar ou falsear a hipótese de que o STJ anula casos criminais indevidamente em razão da falta de conhecimentos técnicos básicos de Computação Forense.

2 Provas digitais a partir de dispositivos móveis e o entendimento do STJ

Inicialmente, é importante ressaltar que a investigação criminal consiste no conjunto de diligências, inferências e hipóteses destinado à elucidação ou à comprovação de um fato delituoso. Por sua vez, dispositivo móvel é qualquer aparelho portátil com conexão à Internet que oferece diferentes recursos para serem usados no dia a dia. Tais dispositivos contam com recursos de computação, executando funções e processos, tais como: reprodução de mídia (vídeo, som), navegação na Internet, acesso a e-mail e mensagens instantâneas, localização GPS, calculadora, calendário, agenda e os mais variados aplicativos.

2.1 Busca e Apreensão de Dispositivos Móveis

O ordenamento jurídico brasileiro trata da busca e apreensão no Código de Processo Penal (CPP), mais especificamente no seu Livro I (“Do Processo em Geral”), Título VII, (“Da Prova”), Capítulo XI (“Da Busca e da Apreensão”), compreendendo, portanto, os artigos 240 a 250 do referido diploma legal (BRASIL, 1941). Entretanto, em que pese a busca seja tratada juntamente à apreensão, tais verbetes possuem diferentes significados no contexto jurídico. A busca diz respeito à diligência realizada para encontrar pessoas ou objetos. Por sua vez, a apreensão é uma medida de constrição que coloca a pessoa ou objeto sob a custódia dos órgãos de persecução penal (LOPES JÚNIOR, 2022). Com isso, caso algum objeto seja entregue de modo voluntário, há apreensão sem busca. O contrário também é verdadeiro, pois é possível que sejam feitas diligências de busca sem sucesso, ou seja, sem que seja encontrada a pessoa ou o objeto visado, inexistindo, com isso, apreensão (LIMA, 2020, p. 793). Nesse sentido, Lima (2020, p. 793) afirma que a busca e apreensão não é meio de prova, mas meio de obtenção de prova e, portanto, de natureza procedimental, o que permite, inclusive, a sua realização por outras pessoas que não o magistrado, a exemplo dos policiais.

Além disso, a leitura do art. 240 do CPP (BRASIL, 1941) demonstra, claramente e de modo exemplificativo, que uma das principais funções da busca é descobrir elementos necessários à prova de infração penal e à elucidação do fato investigado. Por sua vez, o art. 242

do CPP (BRASIL, 1941) prevê que a busca poderá ser realizada de ofício ou a requerimento de qualquer das partes. Quanto a isso, Lima (2020, p. 794) afirma que é necessário fazer distinção entre a busca pessoal e a busca domiciliar. Para o citado autor, segundo o art. 6º, inciso II, do CPP (BRASIL, 1941), "tendo a autoridade policial conhecimento da infração, deverá apreender os objetos que tiverem relação com a infração, após liberados pelos peritos. Nesse caso, a autoridade policial age de ofício, sendo dispensável prévia autorização judicial." (LIMA, 2020, p. 794). Tal circunstância guarda relação com a busca pessoal, pois durante uma prisão em flagrante, por exemplo, o agente policial faz busca pessoal para verificar e, se for o caso, apreender o que está em posse do autor da infração e que seja de interesse para a persecução penal. Por outro lado, considerando-se a inviolabilidade do domicílio do indivíduo – garantia constitucional prevista no art. 5º, inciso, XI, da Constituição Federal (BRASIL, 1988)[1] –, a busca domiciliar somente é possível com mandado expedido por autoridade judiciária competente, observadas as regras do juiz natural (LIMA, 2020, p. 794).

O art. 240 do CPP (BRASIL, 1941) traz rol exemplificativo de pessoas e coisas que podem ser objeto de busca e apreensão (LIMA, 2020, p. 795). Nesse sentido, merecem destaque o previsto nas alíneas "f" e "h" do §1º do citado dispositivo; respectivamente: "apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato", e "colher qualquer elemento de convicção". Portanto, considerando-se que a redação original do CPP é da década de 1940 e que naquela época muitas das tecnologias atuais eram inexistentes, conclui-se como acertada a decisão do legislador em dar caráter exemplificativo[2] ao referido rol, pois isso permite inferir que a busca e apreensão também se aplica às provas digitais[3], que podem ser obtidas a partir de dispositivos móveis. Tanto é assim que é notório que o próprio Poder Judiciário reconhece a prova digital como meio hábil à comprovação e à elucidação de fatos.

Assim, cabe destacar tal qual Jansen & Ayers (2007), que os Princípios de Probatória consideram a prova digital em 02 (dois) aspectos, a saber: a) os componentes físicos, periféricos e mídia, que podem conter dados; b) os dados extraídos a partir dessas fontes originárias. Na verdade, os autores caracterizam os tipos de evidências a serem produzidas a partir dos dispositivos apreendidos, a saber (FREITAS, 2009): a) Físicas: computadores (servidor,

[1] O art. 5º, inciso XI, da CF (BRASIL, 1988) dispõe que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial."

[2] Em sentido contrário, Aury Lopes Júnior (2022) entende que o rol é taxativo, pois traz extenso leque de possibilidades e diz respeito à restrição de direitos fundamentais.

[3] O conceito de "provas digitais" será aprofundado posteriormente.

desktops, laptops), HD externos, pen-drives (mp3-player), CDs, DVDs, celulares, câmeras digitais, jogos e outros e b) Lógicas ou demonstrativas: dados, informações, arquivos, textos, imagens, vídeos, músicas, e-mails, entre outros que se encontram armazenados em suportes físico, seja este eletrônico, ótico ou magnético.

Jansen & Ayers (2007) sugerem que sejam respeitados 04 (quatro) princípios ao se trabalhar com evidências digitais, que podem ser resumidos como a seguir:

a) ações realizadas por investigadores/peritos não devem alterar dados contidos em dispositivos digitais ou em mídias de armazenamento que podem posteriormente ser solicitados perante o Juiz;

b) indivíduos que acessam dados originais devem ser competentes para fazê-lo e ter a capacidade de explicar suas ações, visto que tais procedimentos são questionáveis pelas partes ou em juízo;

c) uma cadeia de custódia deve ser estabelecida, bem como o registro de todos os procedimentos realizados deve ser mantido, de maneira que se possa garantir a replicação dos resultados por um terceiro independente, sendo que toda documentação deve ser criada e preservada, documentando-se cada passo investigativo/pericial;

d) a pessoa encarregada das análises tem a responsabilidade geral de assegurar os procedimentos já mencionados e se os mesmos serão ou foram seguidos em conformidade com os métodos científicos e as leis vigentes.

No que diz respeito aos dispositivos móveis, a exemplo dos *smartphones*, a jurisprudência do STJ entende que é lícito que os órgãos de persecução penal, após o cumprimento de mandados judiciais de busca e apreensão, acessem os dados armazenados nos dispositivos apreendidos, sob o argumento de que esse meio de obtenção de prova não se submete à Lei nº. 9.296/1996 (BRASIL, 1996)[4], nem viola o disposto no art. 5º, inciso XII, da Constituição Federal (BRASIL, 1988)[5], conforme decidido no Recurso em *Habeas Corpus* nº. 75.800-PR (CAVALCANTE, 2022a, p. 1). Isso, porque, segundo o STJ, a Constituição (BRASIL, 1988) e a Lei nº. 9.296/1996 (BRASIL, 1996) consideram que existe interceptação somente quando há comunicação em andamento, e não quando a comunicação já foi finalizada e os seus dados estão armazenados no dispositivo móvel. Até porque o acesso a esses dados somente é possível em razão da liberalidade do interlocutor, o qual optou por não os excluir do

[4] Conhecida como a "Lei das Interceptações Telefônicas".

[5] O art. 5º, inciso XII, da CF (BRASIL, 1988) dispõe 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."

dispositivo (CAVALCANTE, 2022a, p. 3). Por outro lado, mesmo que se invoque o art. 7º da Lei nº. 12.965/2014, conhecida como Marco Civil da Internet (BRASIL, 2014), que assegura a inviolabilidade e o sigilo de comunicações privadas e armazenadas, ainda assim não haverá ilicitude probatória, visto que o acesso aos dados do dispositivo móvel decorre justamente do cumprimento de ordem judicial de busca e apreensão (CAVALCANTE, 2022a, p. 4). Portanto, em síntese, para o STJ, o acesso aos dados de dispositivos móveis é lícito quando decorrente do cumprimento de ordem judicial de busca e apreensão. Todavia, importante salientar que o STJ não faz distinção técnica, do ponto de vista da Computação Forense, sobre o que vem a ser o termo "acesso", tratando-o em sentido genérico, o que pode mudar significativamente o rumo do caso penal.

2.2 Dispositivos móveis apreendidos em decorrência de prisão em flagrante delito

A prisão em flagrante é instituto de direito processual e consiste em meio de defesa da própria sociedade diante do cometimento de uma infração penal (crime ou contravenção), seja de modo concomitante ou logo após à sua ocorrência, e "se divide em quatro momentos distintos: captura, condução coercitiva, lavratura do auto de prisão em flagrante e recolhimento à prisão" (LIMA, 2020, p. 1028). Com isso, o nível de certeza da prática delitiva justifica a prisão do indivíduo sem autorização da autoridade judiciária competente, respeitando-se a garantia fundamental prevista no art. 5º, inciso LXI, da Constituição Federal (BRASIL, 1988)[6] (LIMA, 2020, p. 1027). Além disso, tal medida também repreende a infração penal contemporânea e otimiza as investigações, pois permite que os órgãos de persecução tenham maior contato com os vestígios deixados pela dinâmica delituosa, tornando, assim, o procedimento investigatório mais eficiente e célere (LIMA, 2020, p. 1028).

As hipóteses taxativas de cabimento da prisão em flagrante estão previstas nos incisos I a IV do art. 302 do CPP (LOPES JÚNIOR, 2022). Com base nesses dispositivos, a doutrina classifica o flagrante em várias espécies: (i) flagrante próprio, perfeito, real ou verdadeiro; (ii) flagrante impróprio, imperfeito, irreal ou quase-flagrante; (iii) flagrante presumido, ficto ou assimilado; (iv) flagrante preparado, provocado, crime de ensaio, delito de experiência ou delito putativo por obra do agente provocador; (v) flagrante esperado; (vi) flagrante prorrogado, protelado, retardado ou diferido: ação controlada e entrega vigiada; e (vii) flagrante forjado, fabricado, maquinado ou urdido (LIMA, 2020, p. 1032-1039).

[6] O art. 5º, inciso LXI, da CF (BRASIL, 1988) dispõe que "ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, salvo nos casos de transgressão militar ou crime propriamente militar, definidos em lei."

O flagrante próprio, perfeito, real ou verdadeiro é o que está previsto no art. 302, incisos I e II, do CPP (BRASIL, 1941), e consiste na prisão do indivíduo no momento em que ele comete o delito ou imediatamente após seu cometimento. Por sua vez, o flagrante impróprio, imperfeito, irreal ou quase-flagrante ocorre quando o indivíduo comete o crime e é imediatamente perseguido e preso em razão das circunstâncias do caso concreto que indicam ser ele o autor do delito, conforme art. 302, inciso III, do CPP (BRASIL, 1941). Já o flagrante presumido, ficto ou assimilado difere do flagrante impróprio, porque inexiste o requisito da perseguição, bastando que indivíduo seja encontrado logo após a ocorrência da infração penal com instrumentos, armas, objetos ou papéis que façam presumir ser ele autor do fato (art. 302, inciso IV, CPP) (LIMA, 2020, p. 1033-1034).

No que diz respeito às espécies de flagrante preparado (provocado, crime de ensaio, delito de experiência ou delito putativo por obra do agente provocador) e de flagrante esperado, a sua distinção é imprescindível, pois repercute na licitude da medida. O flagrante preparado é medida processual ilícita, pois os órgãos de persecução instigam o agente a praticar o delito, tratando-se, portanto, de crime impossível. Inclusive, o Supremo Tribunal Federal (STF) editou Súmula nº. 145 (BRASIL, 1963) consolidando esse entendimento: "Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação." Situação com ilicitude mais grave é a do flagrante forjado, fabricado, maquinado ou urdido, uma vez que o flagrante é "totalmente artificial, policiais ou particulares criam provas de um crime inexistente, a fim de 'legitimar' (falsamente) uma prisão em flagrante" (LIMA, 2020, p. 1039).

Já o flagrante esperado é lícito, porque o Estado não instiga a prática do crime, o qual ocorre espontaneamente. Apenas aguarda-se o cometimento do crime para se efetuar a prisão em flagrante (LIMA, 2020, p. 1035-1036). Semelhante a essa figura, existe o flagrante prorrogado, protelado, retardado, diferido, ação controlada ou entrega vigiada. Nesta última espécie, há o retardamento da intervenção policial, que deve ocorrer no momento mais oportuno do ponto de vista da investigação criminal ou da colheita de provas (LIMA, 2020, p. 1039). Importante destacar que a ação controlada exige a prévia comunicação ao juízo competente, conforme determina o art. 8º, §1º, da Lei nº 12.850/2013, que dispõe sobre Organizações Criminosas (BRASIL, 2013).

No que se refere às provas obtidas a partir de dispositivos móveis apreendidos por ocasião de prisão em flagrante, o STJ considera como ilícito o seu acesso sem que haja autorização da autoridade judiciária competente, conforme consta no julgamento do Recurso em *Habeas Corpus* (RHC) nº. 51.531-RO (BRASIL, 2016h). Por exemplo, a polícia não pode acessar conversas armazenadas em *smartphone* apreendido com o autuado em flagrante delito

sem que um magistrado autorize expressamente esse acesso. Segundo o STJ, isso decorre do art. 5º, incisos X[7] e XII[8], da Constituição Federal (BRASIL, 1988), que dispõem sobre as garantias constitucionais de inviolabilidade da intimidade, do sigilo de correspondência, de dados e de comunicações telefônicas. Portanto, nesses casos, cabe à autoridade policial apreender o celular e somente acessar o seu conteúdo após obter autorização judicial para tanto (CAVALCANTE, 2016b, p. 26). Vale ressaltar, entretanto, que a leitura do inteiro teor do julgado RHC nº. 51.531-RO (BRASIL, 2016h) demonstra que termos como, por exemplo, acesso, extração, obtenção e perícia são utilizados como sinônimos. O que por vez não é adequadamente aplicável do ponto de vista da Computação Forense.

2.3 Dispositivos móveis pertencentes à vítima do delito e entregues espontaneamente aos órgãos de persecução penal

No ano de 2017, o STJ julgou Recurso em *Habeas Corpus* (RHC) nº. 86.076-MT (BRASIL, 2017) e a decisão foi de grande repercussão nos casos de análise de provas obtidas a partir de dispositivos móveis. Como visto anteriormente, o STJ entende que, em regra, o acesso aos dados de dispositivos móveis só é possível mediante autorização judicial, seja no caso de apreensão de dispositivo em flagrante delito, seja de modo derivado com o cumprimento de mandados judiciais de busca e apreensão. Entretanto, a decisão proferida no referido RHC (BRASIL, 2017) considerou que "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." (CAVALCANTE, 2017, p. 1).

Aqui a distinção diz respeito ao proprietário do dispositivo móvel: se investigado ou vítima. Se, por exemplo, o celular pertence ao investigado, a autorização judicial é imprescindível em qualquer hipótese. A única diferença é nos casos de ordem judicial de busca e apreensão cujo alcance do poder jurisdicional também abarca os dados dos dispositivos móveis visados. Portanto, de qualquer modo, a reserva se jurisdição está presente. Por outro lado, quando o proprietário do celular é a vítima, presume-se que é de seu interesse solucionar o crime cometido. Nas palavras de Cavalcante (2017, p. 4), essa interpretação em relação à vítima decorre da ausência da "violação à intimidade do investigado, titular de garantias no

[7] O art. 5º, inciso X, da CF (BRASIL, 1988) dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."
[8] O art. 5º, inciso XII, da CF (BRASIL, 1988) dispõe 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."

processo penal.” Ou seja: o Direito Processual Penal, por um lado, destina-se a resguardar os direitos e garantias fundamentais do suspeito, investigado, indiciado, acusado ou réu; por outro, visa punir o delito e proteger os interesses da vítima e, secundariamente, os interesses da sociedade como um todo (decorrente da função de pacificação social do Direito).

Em regra, para o STJ é dispensada autorização judicial para acessar os dados de dispositivo móvel pertencente à vítima do delito. Todavia, em que pese isso, entende-se que tal entendimento deve ser aplicado com cautela no caso concreto. O caso paradigmático que foi analisado pela Corte Superior diz respeito a crime de homicídio consumado, isto é, a vítima já não estava mais viva e um familiar, interessado em solucionar o crime, forneceu espontaneamente o dispositivo móvel (celular) do falecido para que a polícia pudesse utilizar os seus dados nas investigações. Por outro lado, nos casos de homicídio tentado ou em outras infrações penais em que a vítima está viva e em sã consciência, entende-se que ainda assim se faz necessária ordem judicial para acesso ao conteúdo de seus dispositivos móveis, salvo entrega espontânea à autoridade policial; ou seja, quando a vítima espontaneamente renuncia, mesmo que de forma tácita, ao seu próprio sigilo de dados. Por fim, saliente-se que, mais uma vez, o STJ tratou termos como extração e acesso com imprecisão técnica do ponto de vista da Ciência da Computação e da Computação Forense.

3 Prova em sentido amplo e provas digitais

Segundo Dallagnol (2018), prova consiste na inferência racional que correlaciona evidências e hipóteses. O autor ensina que aquilo que é popularmente conhecido como “prova” é tecnicamente chamado, do ponto de vista epistemológico, de “evidência” (DALLAGNOL, 2018). O caminho percorrido pelo raciocínio humano entre a evidência e a hipótese é a inferência racional, em outras palavras, a prova (BADARÓ, 2019). Em síntese: a evidência é o vestígio materialmente deixado na realidade; a hipótese é a possibilidade causal que originou determinado vestígio; e a inferência é o raciocínio que liga, por meio de uma explicação, a evidência à hipótese e que, portanto, prova algo (BADARÓ, 2019). Quanto a isso, importante destacar que a hipótese é, em regra, indissociável da inferência, pois uma pressupõe e é a razão de ser da outra. Afinal, não se pode falar em raciocínio abstrato sem hipóteses, nem se falar em hipóteses sem inferências (isto é, sem “caminhos” racionais).

É nesse contexto que surge a denominada “dúvida razoável” ou o adágio latino “*in dubio pro reo*”. Tais expressões condensam o princípio de Direito Processual Penal que determina a absolvição do réu em caso de existência de dúvida razoável sobre seu envolvimento ou mesmo sobre a existência do crime julgado. De acordo com Dallagnol (2018), com base na

tríade "evidência, hipótese e inferência", os casos penais devem ser guiados por um *standard* probatório mínimo pautado na denominada "inferência para a melhor explicação" (IME). A IME consiste na adoção do raciocínio que melhor explica, a partir da experiência humana (*background* de crenças empíricas[9]), determinado conjunto de provas (DALLAGNOL, 2018, p. 25).

Tome-se como exemplo a apreensão de *smartphone* em cuja memória estão mensagens de texto que demonstram a comercialização de "pneus" – primeira evidência. Todavia, a apreensão desse dispositivo móvel se deu em investigação de tráfico de drogas. Portanto, qual seria a relação de pneus com drogas? A primeira hipótese é a de que os traficantes também aproveitam a logística das drogas para descaminhar pneus. Por outro lado, caso venha a se descobrir – por meio de uma segunda evidência – que "pneu" é código para "cocaína", surge a hipótese de que todos os pneus negociados nessas mensagens de texto são, na verdade, drogas. Desse modo, considerando o contexto das investigações e das mensagens trocadas, deve-se adotar a hipótese que, acima de uma dúvida razoável, melhor explica o caso concreto por meio de inferências racionais (DALLAGNOL, 2018). Portanto, a IME resulta na criação do conhecimento utilizado para a tomada de decisão por parte dos atores do Sistema de Justiça Criminal. Afinal, é com base na IME que o magistrado decidirá se absolve ou não réu.

Desse modo, transmutando esses ensinamentos sobre prova para o mundo digital, é possível falar que as evidências correspondem aos dados, as hipóteses às informações e as inferências, ao conhecimento. Para se entender essa assertiva, é necessário que antes se saiba o que é, do ponto de vista técnico da Ciência da Computação, o significado dos termos dado, informação e conhecimento. De acordo com Boff, Fortes e Freitas (2018), os dados nada mais são do que símbolos ou signos brutos e sem significado relacional que representam determinada parcela da realidade, seja passada ou presente. Por exemplo, "azul" é um dado que remete a uma cor, mas não se relaciona a algo ou alguém. Por sua vez, informação é significado objetivo a partir da correlação de dados com semântica (BOFF; FORTES; FREITAS, 2018). Nesse sentido, se houver correlação entre três dados isolados como, por exemplo, "azul", "mar" e "água", é possível obter a informação de que "a água do mar é da cor azul". Por fim, o conhecimento é o fruto da sintetização obtida a partir de reflexões mentais destinadas à tomada de decisão.

Com base no citado exemplo, é possível que determinado indivíduo tome a decisão de mergulhar no mar por entender que ele não está poluído em razão da sua água ser da cor azul.

[9] Badaró (2019) chama isso de "máximas de experiência".

Ou seja, a partir da informação extraída da realidade de que "o mar é da cor azul" conjugada com a informação de *background* (extraída de crenças empíricas) de que "mar azul significa que ele não está poluído", o indivíduo toma a decisão de mergulhar no mar. Com isso, verifica-se que há equivalência de conceitos técnicos entre as tríades "evidência, hipótese e inferência" do Direito Processual, e "dado, informação e conhecimento" da Ciência da Computação. Assim, em última análise, é possível afirmar que o dado é a base de toda análise probatória das provas digitais.

Pode-se assim conceituar prova digital, mas para tal é necessário compreender a área denominada de Computação Forense ou Forense Computacional (*Computer Forensic*), a qual envolve a extração, identificação, preservação e documentação de evidências digitais a partir de dados e informações armazenadas em mídias: magnéticas, ópticas ou eletrônicas (CRAIGER, 2007). A Computação Forense pode ser definida como uma peça do quebra-cabeça da investigação. Provas digitais são, portanto, evidências digitais que podem ser coletadas e analisadas por métodos e técnicas de Computação Forense, visando a partir de hipóteses obter inferências válidas. De acordo com Kruse & Heiser (2002), os métodos e técnicas da Computação Forense aplicáveis às provas digitais podem ser resumidos por meio do mnemônico "3A's", a saber: 1) Adquirir as evidências sem alterar ou danificar o original; 2) Autenticar que as evidências recuperadas são idênticas aos originais; 3) Analisar os dados sem que estes sofram modificações.

Na Publicação Especial 800-101 do NIST (*National Institute of Standards and Technology*) Jansen & Ayres (2007) sugerem que a chave para o sucesso na análise forense de dispositivos móveis é a compreensão das características de hardware e software dos referidos equipamentos. Os dados dos assinantes e suas atividades por meio de celulares são muitas vezes uma fonte valiosa de provas em uma investigação. Portanto, para que a produção de provas digitais possa ser realizada, conta-se com um conjunto básico de características, obtido a partir da maioria dos celulares, sendo este conjunto comparável entre diferentes aparelhos. Como exemplos de características que são comuns na maioria dos dispositivos móveis atuais podem ser citados: microprocessador, memória ROM (*Read Only Memory*), memória RAM (*Random Access Memory*), módulo de rádio, processador de sinal digital, alto falante, tela, sistema operacional, bateria, PDAs (*Personal Digital Assistants*), GPS (*Global Positioning System*), câmera, entre outros recursos.

De um modo um pouco diferente, Eleutério & Machado (2010, p. 94-99) apresentam as fases dos exames periciais em dispositivos móveis, que geralmente podem ser assim definidas:

1) preservação: visa preservar tanto o equipamento de origem quanto as evidências contidas no dispositivo móvel;

2) extração: permite a coleta efetiva das evidências digitais, extraindo-se todos os dados armazenados (chamadas efetuadas e recebidas, registros contidos na agenda, mensagens de texto, imagens, áudios, vídeos, entre outros) e metadados (dados sobre os dados). Nessa fase procede-se, inicialmente, uma cópia eletrônica (bit a bit) por meio de procedimento denominado de "imagem" (KRUSE; HEISER, 2002) ou "espelhamento" (ELEUTÉRIO; MACHADO, 2010, p. 55). Novamente, ressalta-se a importância da integridade e autenticidade das provas extraídas, sendo que as mesmas servirão para a instrução do processo judicial. A realização do procedimento de "imagem" necessita da utilização de ferramentas forenses, hardware e software, de modo a permitir que as cópias sejam duplamente garantidas. Isto significa que devem ser utilizados equipamentos denominados de *writer blocker*, ou seja, equipamentos que bloqueiam a escrita no equipamento origem durante o referido procedimento. Tais equipamentos podem ser auxiliados por programas que efetuam propriamente dita as cópias bit a bit, existindo diversos hardware e software que permitem aos peritos realizarem tais cópias;

3) análise: consiste no exame pericial propriamente dito, com o objetivo de identificar evidências digitais que apresentem relação com o delito investigado ((ELEUTÉRIO; MACHADO, 2010, p. 65);

4) formalização: é a fase de elaboração do laudo pericial, apontando o resultado (conclusão) e respondendo aos quesitos. O laudo deve apresentar uma descrição detalhada dos procedimentos aplicados, incluindo as técnicas de preservação, extração e análise do conteúdo das provas digitais (ELEUTÉRIO; MACHADO, 2010, p. 70).

É importante trabalhar na extração e análise de evidências digitais tal qual o usuário vê ou utiliza o seu dispositivo móvel ou outros equipamentos. Deve-se ter em mente que as evidências lógicas ou demonstrativas provêm de evidências físicas e que as provas digitais necessitam de suporte físico para existir. Deste modo, a ligação entre evidências físicas e lógicas é relevante para sustentar judicialmente a correta relação entre os suportes materiais e digitais (FREITAS, 2009).

4 Cadeia de custódia, provas ilícitas e direito fundamental à prova

Lima (2020, p. 718) define cadeia de custódia como um "mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração." Em outras palavras, a cadeia de custódia é um procedimento que permite rastrear a prova desde sua origem até a sua chegada

no processo judicial correspondente, inclusive, de modo cronológico e concatenado. Tal medida permite que acusação, defesa e órgão julgador verifiquem se o acervo que compõe o processo é autêntico ou se existem "provas plantadas", isto é, provas forjadas, seja para condenar, seja para absolver. Para Lopes Júnior (2022, p. 1036), "cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico." Eventual quebra na cadeia de custódia pode gerar a nulidade de todo um caso criminal (LOPES JÚNIOR, 2022, p. 1043), haja vista a possibilidade de contaminação das demais provas por derivação. Há ainda que se considerar que as provas digitais podem sofrer danos acidentais ou intencionais, especificamente quanto à (FERREIRA, 1963): a) ocultação: não deixar ver, não mostrar, não revelar, disfarçar, dissimular, encobrir, esconder; b) obliteração: eliminar, suprimir, destruir por completo sem deixar vestígios; e c) adulteração: falsificar, corromper.

Para melhor compreender a cadeia de custódia, se faz necessário discorrer sobre as provas ilícitas. O art. 5º, inciso LVI, da Constituição Federal (BRASIL, 1988), positiva o direito fundamental à prova ao dispor que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos". No âmbito do Direito Processual Penal, Lima (2020, p. 685) afirma que "a vedação das provas ilícitas também funciona como uma forma de controle da regularidade da persecução penal, atuando como fator de inibição e dissuasão à adoção de práticas probatórias ilegais." Nesse sentido, prioriza-se a eficiência processual mesmo que isso resulte em absolvição indevida, haja vista que o contrário poderia resultar numa condenação injusta e, portanto, mais grave. Ditados populares como "os fins não justificam os meios" e "melhor absolver um culpado do que condenar um inocente" podem ser didaticamente tomados como base para a compreensão do raciocínio por trás das provas ilícitas.

Lima (2020) ensina que prova ilegal é gênero do qual são espécies a prova ilícita e a prova ilegítima. A primeira – prova ilícita –, é fruto da violação do direito material como a confissão obtida mediante crime de tortura. Já a segunda é resultado da inobservância do direito processual como ocorre em Plenário do Tribunal do Júri quando uma das partes exibe uma prova aos jurados sem que ela tivesse sido juntada ao processo com antecedência mínima de 3 (três) dias da sessão, conforme determina o art. 479 do CPP (LIMA, 2020).

O citado autor também afirma ser possível a existência de prova ilegal com origem em violações de direito material e de direito processual (LIMA, 2020). Nesse último caso, tendo como base provas digitais em dispositivos móveis, pode-se dizer que há prova digital ilegal, ilícita e ilegítima quando ela é obtida mediante a invasão da residência do investigado no período noturno por policial que apreende celular e usa suas conversas em inquérito policial.

Aqui, há violação das normas processuais que regem a busca e apreensão, porque ela foi efetuada sem mandado judicial. Do mesmo modo, há violação de direito material em razão do cometimento do crime de abuso de autoridade tipificado no art. 22, §1º, inciso III, da Lei nº. 13.869/2019 (BRASIL, 2019), que trata da busca e apreensão domiciliar após as 21h00min (vinte e uma horas) ou antes das 5h00min (cinco horas) (LIMA, 2020).

Uma vez apresentados os conceitos de cadeia de custódia e de prova ilegal (ilícitas e ilegítimas), cumpre agora correlacioná-los entre si a fim de que, posteriormente, seja compreendida a ligação desses institutos com a obtenção de provas digitais em dispositivos móveis. Nesse contexto, indispensável discorrer sobre a prova ilícita por derivação, que está positivada expressamente no art. 157 do CPP[10] e tem origem na teoria dos frutos da árvore envenenada, em língua inglesa "*fruit of the poisonous tree doctrine*", haja vista sua origem estadunidense no caso *Silverthorne Lumber Company, Inc., et al. v. United States*, julgado pela Suprema Corte do Estados Unidos, em 1920 (CARVALHO, 2014).

O referido caso avaliava, do ponto de vista constitucional, a possibilidade de o Estado utilizar cópias de livros contábeis apreendidos ilegalmente para processar empresas por sonegação fiscal. Em suma, a Suprema Corte americana decidiu que isso não era possível, porque essas cópias derivavam de outras evidências obtidas ilicitamente. Ou seja, a árvore de provas do processo foi envenenada pela apreensão ilegal de livros contábeis e causou a contaminação das suas cópias, tornando-as imprestáveis para o processo. Portanto, se uma prova é ilegal, tudo que dela derivar também o será, razão pela qual deve ser determinado seu desentranhamento dos autos (ESTADOS UNIDOS DA AMÉRICA, 1920).

Todavia, há exceções a esse postulado. O art. 157, §1º, do CPP (BRASIL, 1941) ressalva que é possível utilizar provas que, num primeiro momento, pareçam ser derivadas de provas ilícitas quando não restar evidenciado nexo de causalidade entre elas, ou quando as provas derivadas puderem ser obtidas de modo independente das provas ilícitas originárias (CARVALHO, 2014). Para o diploma processual penal (BRASIL, 1941), as fontes independentes de prova são aquelas que "seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova." (art. 157, §2º, CPP). Quando determinada prova possui um vício que a torne ilegal, ela, por si só, não poderá ser utilizada no processo, assim como tudo que dela derivar. Então, verifica-se que a

[10] O CPP (BRASIL, 1941) e a CF (BRASIL, 1988) usam genericamente a expressão "provas ilícitas". Contudo, ressalta-se a precisão técnica anteriormente mencionada a respeito do gênero provas ilícitas e suas espécies: provas ilícitas e ilegítimas. De qualquer modo, o presente artigo utilizará, como regra, a expressão adotada pelo ordenamento jurídico, isto é, a de provas ilícitas *lato sensu*.

cadeia de custódia permite o rastreamento da prova, tornando-a auditável do ponto de vista jurídico e possibilitando a aferição sobre sua ilegalidade, ilicitude ou ilegitimidade. Dada a sua importância, o legislador detalhou o instituto da cadeia de custódia nos artigos 158-A a 158-F do CPP (BRASIL, 1941). Todavia, esse incremento legislativo deixou de lado os vestígios deixados no mundo digital. Para suprir essa lacuna, lança-se mão de procedimentos tecnológicos que permitem tanto tornar a prova digital auditável quanto conferem à mesma as seguintes propriedades: integridade, rastreabilidade, autenticidade, veracidade, confiabilidade, legalidade, transparência e idoneidade; de modo a torná-la lícita e legítima. Na Computação Forense, integridade de dados está relacionada com a garantia de que os dados não foram adulterados, destruídos ou modificados durante as fases de preservação e extração, ou mesmo durante as análises forenses. Também de acordo com o site Significados.com.br "A integridade de dados é uma das características essenciais da Segurança da Informação, e garante que as informações não sofreram alterações que não foram autorizadas ou que são impróprias. A integridade de dados também assegura que um documento não é alterado depois de ter sido assinado". Portanto, os peritos registrarão, no laudo pericial, as alterações do estado das coisas e discutirão, no relatório, as consequências dessas alterações na dinâmica dos fatos, conforme art. 169, parágrafo único, do CPP (BRASIL, 1941). Os peritos e demais profissionais devem garantir e preservar a integridade das evidências de um modo geral, digitais ou não. Se não for garantida a integridade, as evidências poderão ser invalidadas como provas legítimas. A garantia da integridade das evidências digitais consiste na utilização de ferramentas que aplicam procedimentos de criptografia com geração do respectivo código *hash*.

Explica Freitas (2008) que a função *hash* tem por objetivo identificar univocamente cada conjunto de informações, ou seja, para cada documento criptografado gera-se uma cadeia alfanumérica única, sendo que o procedimento (ou algoritmo) de geração usa o conteúdo do documento para gerar tal cadeia. Assim, se um documento for modificado e novamente criptografado, nunca conterá o mesmo *hash*, pois o conteúdo do documento foi alterado e, assim, será o *hash.* Portanto, a simples comparação dos valores dos *hashs* de dois documentos, permite a validação da autenticidade dos mesmos. Visto que, somente para *hashs* iguais têm-se documentos iguais. Portanto, garante-se as propriedades técnicas de evidências digitais, destacando-se a integridade dos arquivos extraídos e analisados.

Assim sendo, verifica-se que a cadeia de custódia associada à criptografia com geração de *hash* constitui procedimento adequado para resguardar o direito fundamental à prova ao preservar sua autenticidade e integridade, bem como demais propriedades tecnológicas e jurídico-legais, evitando-se que qualquer ilicitude macule as evidências digitais. É com base

nisso que a seguir realiza-se a avaliação da hipótese de que o STJ anula casos criminais indevidamente em razão da falta de conhecimentos técnicos básicos de Computação Forense. Ou seja, avalia-se se a jurisprudência atual do STJ tem levado em conta as nuances técnicas do manuseio de provas digitais, e se as decisões que vem sendo tomadas têm sido ou não equivocadas em razão disso. Afinal, como mencionado, a legislação atual não trata expressamente da cadeia de custódia relacionada ao mundo digital.

5 Conclusão

O STJ não faz distinção de termos técnicos da área de Computação Forense. É com frequência que, por exemplo, se considera a mera extração de dados como sinônimo de análise de dados, o que leva a anulação indevida de casos penais. Todavia, com base no mnemônico "3A's" (aquisição, autenticação e análise de evidências), verifica-se que há nulidade probatória somente quando os órgãos de persecução penal analisam dados colhidos em dispositivos móveis sem autorização do poder jurisdicional. Por outro lado, a aquisição e a autenticação de provas digitais não só podem, como devem ser feitas de ofício pelos agentes persecutórios. Tais medidas visam justamente, por meio de criptografia, garantir a incolumidade da prova, assim como a higidez da sua cadeia de custódia. Sem isso, o próprio direito de defesa resta prejudicado. Afinal, toda e qualquer atitude persecutória, notadamente relacionada à provas digitais, precisa ser auditável.

De modo didático, é possível afirmar que a mera extração de dados de dispositivos móveis é equivalente, por exemplo, à apreensão de projéteis encontrados no local em que ocorreu um homicídio por arma de fogo. Por sua vez, a análise dos dados extraídos consiste no acesso direto ao elemento de prova capaz de construir inferências e hipóteses necessárias à prova do fato ou à sua elucidação. No exemplo dos projéteis apreendidos, a análise de dados é equivalente à sua análise em comparação com a arma de fogo encontrada com o suspeito de ser o autor do homicídio. Destarte, em síntese, a extração de dados – isto é, aquisição e autenticação de evidências –, não se confunde com sua análise de evidência, haja vista que se destina tão somente a preservar a prova digital e sua respectiva cadeia de custódia. Desse modo, a ausência de conhecimento técnico a respeito da Computação Forense, faz com que se interpretem indevidamente como sinônimos termos como, por exemplo, extração, análise e perícia, dentre outros, o que gera a anulação indevida de casos criminais. Portanto, resta comprovada a hipótese de que o STJ pode anular casos criminais indevidamente, em razão da falta de conhecimentos técnicos básicos de Computação Forense.

6 Referências

BADARÓ, Gustavo Henrique. **Epistemologia jurídica e prova penal.** São Paulo: Thomson Reuters Brasil, 2019. 6 Mb. ePUB.

BRASIL. Constituição da República Federativa do Brasil, 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em: 21 ago. 2022.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 31 ago. 2022.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, 3 out. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 31 ago. 2022.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências, 2 ago. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 31 ago. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 ago. 2022.

BRASIL. **Lei nº 13.869, de 5 de setembro de 2019**. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), 5 set. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm. Acesso em: 31 ago. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, 24 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 31 ago. 2022.

BRASIL. Superior Tribunal de Justiça. Recurso em *Habeas Corpus* nº 51.531/RO – Rondônia. Relator: Ministro Néfi Cordeiro, Sexta Turma, julgado em 19/4/2016, DJe de 9/5/2016. **Jurisprudência do STJ.** Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 31 ago. 2022.

BRASIL. Superior Tribunal de Justiça. Recurso em *Habeas Corpus* nº 86.076/MT – Mato Grosso. Relator: Ministro Sebastião Reis Júnior, relator para acórdão Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 19/10/2017, DJe de 12/12/2017. **Jurisprudência do STJ.** Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2786076%27)+ou+(%27RHC%27+adj+%2786076%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 31 ago. 2022.

BRASIL. Superior Tribunal de Justiça. Recurso em *Habeas Corpus* nº 75.800/PR – Paraná. Relator: Ministro Felix Fischer, Quinta Turma, julgado em 15/9/2016, DJe de 26/9/2016. **Jurisprudência do STJ.** Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2775800%27)+ou+(%27RHC%27+adj+%2775800%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 31 ago. 2022.

BRASIL. Supremo Tribunal Federal. Súmula nº 145. *In:* **_____. Aplicação das Súmulas no STF**. Brasília, 1963. Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2119#:~:text=N%C3%A3o%20h%C3%A1%20crime%2C%20quando%20a,torna%20imposs%C3%ADvel%20a%20sua%20consuma%C3%A7%C3%A3o. Acesso em: 31 ago. 2022.

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Processo Penal e Constituição: princípios constitucionais do processo penal**. São Paulo: Editora Saraiva, 2014. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502224308/. Acesso em: 16 ago. 2022.

CAVALCANTE, Márcio André Lopes. **É lícito o acesso aos dados armazenados em celular apreendido com base em autorização judicial**. Buscador Dizer o Direito, 2016, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/5c3b99e8f92532e5ad1556e53ceea00c>. Acesso em: 08 ago. 2022.

CAVALCANTE, Márcio André Lopes. **Informativo esquematizado:** Informativo 583-STJ. Dizer o Direito, 2016, Manaus. Disponível em: <https://dizerodireitodotnet.files.wordpress.com/2016/07/info-583-stj1.pdf>. Acesso em: 10 ago. 2022.

CAVALCANTE, Márcio André Lopes. **Mesmo sem autorização judicial, polícia pode acessar conversas do Whatsapp da vítima morta, cujo celular foi entregue pela sua esposa**. Buscador Dizer o Direito, 2017, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/211b39255232ab59ce78f2e28cd0292b>Acesso em: 08 ago. 2022.

CRAIGER, John Philip. Computer forensics procedures and methods. To appear in H. Bigdoli (Ed.), Handbook of Information Security. John Wiley & Sons, 2007.

DALLAGNOL, Deltan Martinazzo. **As lógicas das provas no processo**: prova direta, indícios e presunções. Porto Alegre: Livraria do Advogado, 2018. 362 p.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a computação forense. São Paulo: Novatec Editora, 2010.

ESTADOS UNIDOS DA AMÉRICA. *Supreme Court of the United States*. *Silverthorne Lumber Company, Inc., et al. v. United States*. Relator: *Judge* Oliver Wendell Holmes Jr. Washington, D.C., 26 de janeiro de 1920. **HeinOnline.** Disponível em: < https://heinonline.org/HOL/P?h=hein.usreports/usrep251&i=425 > Acesso em 18 ago. 2022.

FERREIRA, Aurélio Buarque de Hollanda. Pequeno Dicionário Brasileiro da Língua Portuguesa, 10ª Edição, Editora Civilização Brasileira S.A., Rio de Janeiro, 1963.

FREITAS, Cinthia Obladen de Almendra. Assinatura Digital: necessidade ou obrigação? In EFING, Antônio Carlos; FREITAS, Cinthia Obladen de Almendra (Orgs.). Direito e questões tecnológicas: aplicados no desenvolvimento social. Curitiba, PR: Juruá, 2008.

FREITAS, Cinthia Obladen de Almendra. Procedimentos Técnicos e Jurídicos para a Produção Antecipada de Provas Digitais. In: I Congresso de Computação Forense, 2009, São Paulo. Anais do I Congresso de Computação Forense. São Paulo: Univ. Presbiteriana Mackenzie, 2009. v. 1. p. 1-10.

JANSEN, Wayne; AYERS, Rick. Computer Security - guidelines on cell phone forensics, NIST - Special Publication 800-101. 2007.

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Indianapolis: Addison-Wesley, 2002.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: Volume Único. 8. ed. rev. atual. e aum. Salvador: Juspodivm, 2020. 1952 p.

LOPES JÚNIOR, Aury. **Direito processual penal**. 19. Ed. São Paulo: Saraiva, 2022. *E-book*.

MICHAUD, D.J. Adventures in computer science. SANS Institute, 2001.