REPENSANDO O ENCONTRO FORTUITO DE PROVAS NA ERA DIGITAL

RETHINKING THE FORTUITOUS DISCOVERY OF EVIDENCE IN THE DIGITAL AGE

Pedro Ivo Rodrigues Velloso Cordeiro[1]
Universidade de São Paulo, USP, Brasil
pedroivo@fv.com.br

Francisco Felippe Lebrão Agosti[2]
Universidade Presbiteriana Mackenzie, Brasil
francisco@fv.com.br

Pedro Luís de Almeida Camargo[3]
Universidade de São Paulo, USP, Brasil
pedro.camargo@fv.com.br

DOI: https://doi.org/10.5281/zenodo.13834573

Resumo: O presente trabalho analisa os impactos trazidos pela transformação digital em um instituto do processo penal: o encontro fortuito de provas. Tendo em vista os impactos que o uso generalizado de dispositivos eletrônicos na sociedade causa na prática da obtenção das provas, a ampla aceitação do encontro fortuito de provas e do "princípio da serendipidade", na forma como hoje concebidos, apresenta riscos significativos aos direitos fundamentais. Dessa forma, busca-se a criação de critérios limitadores para a autorização judicial e para a execução de buscas e apreensões de provas digitais, para melhor preservar tais direitos fundamentais e evitar abusos na atividade persecutória.

Palavras-chave: prova digital; serendipidade; proporcionalidade; busca e apreensão.

Abstract: This paper analyzes impacts brought upon the fortuitous discovery of evidence by the digital transformation. Due to the impact caused on the collection of evidence by the widespread use of electronic devices in society, the current broad acceptance of accidentally discovered evidence and the "serendipity principle" pose significant threats to fundamental rights. Therefore, this paper aims to create a test about the issuance and execution of search warrants on digital evidence to better preserve such fundamental rights and prevent abuses on law enforcement activities.

Keywords: digital evidence; serendipity; proportionality; search and seizure.

1. Introdução

A revolução digital transformou profundamente a experiência humana. A repercussão dessa nova realidade no processo penal vem ensejando o debate sobre diversos dos institutos tradicionais da doutrina processual, com a sua adaptação — ou até criação de novos parâmetros dogmáticos — para o mundo digitalizado.

A doutrina e a jurisprudência que foram construídas em um mundo analógico precisam, no mínimo, serem repensadas nessa nova realidade. E, se por um lado, os impactos das transformações digitais na busca e a apreensão de dispositivos informáticos vêm recebendo grande atenção da doutrina brasileira, alguns de seus desdobramentos precisam ser mais bem explorados.

Dentre eles, situa-se o chamado encontro fortuito de provas, ou princípio da serendipidade, o qual dita que os elementos casualmente descobertos no curso de diligências investigativas, referentes a fatos independentes da hipótese criminal original,

[1] Doutor em Direito Processual Penal pela Universidade de São Paulo e Mestre em Direito, Estado e Constituição pela Universidade de Brasília. Professor de Direito Penal da Escola de Direito de Brasília do Instituto de Direito Público. Advogado. Link Lattes: http://lattes.cnpq.br/7389277522042037. ORCID: https://orcid.org/0000-0002-3854-9651. LinkedIn: linkedin.com/in/pedro-ivo-velloso-cordeiro-49235b26/.

[2] Bacharel em Direito pela Universidade Presbiteriana Mackenzie. Associado ao Instituto de Garantias Penais e Associado Fundador do Innocence Project Brasil. Advogado. Link Lattes: http://lattes.cnpq.br/1855378661817244. ORCID: https://orcid.org/0009-0005-8750-8695. LinkedIn: linkedin.com/in/francisco-felippe-lebrão-agosti-147687138/.

[3] Mestrando em Direito Processual Penal pela Universidade de São Paulo. Especialista lato sensu em Obtenção, Interpretação e Valoração da Prova pela Universidade de Salamanca. Bacharel em Direito pela Universidade de São Paulo. Advogado. Link Lattes: http://lattes.cnpq.br/8451429372152340. ORCID: https://orcid.org/0000-0003-1330-0929. LinkedIn: linkedin.com/in/pedro-luís-de-almeida-camargo-489a63144/.

são válidos e podem ser aproveitados para a apuração do crime recém-descoberto. Esse é o tema a ser trabalhado no presente artigo, que examinará se a aceitação pacífica da serendipidade deve se manter na nova realidade da persecução penal.

2. A transformação da persecução penal na era digital

Os *smartphones* e a *internet* passaram a ser os mediadores universais da vida pessoal, social e profissional de grande parte da população mundial. E, com isso, cada indivíduo carrega em seu bolso dados digitais que registram todas as facetas de seu cotidiano: transações financeiras, anos de mensagens escritas, documentos pessoais e profissionais, dados de geolocalização, histórico de navegação na *internet*, dados de redes sociais, entre muitos outros[1].

Essa realidade transformou profundamente a investigação criminal, que teve de se adaptar à realidade digital. Justamente por serem grande fonte de informações e registros, a busca e apreensão dos dispositivos informáticos é, comumente, a primeira medida ostensiva de investigação e/ou a mais importante para comprovar a materialidade e a autoria de uma ampla gama de delitos — tanto aqueles próprios da realidade digital, como os novos tipos de fraudes e invasões *hacker*, quanto crimes "tradicionais", como tráfico de drogas e delitos econômicos. A isso, soma-se o fato de que provedores de aplicações como *e-mails* e servidores em nuvem são comumente demandados pelas autoridades para o fornecimento de dados que armazenam em função da prestação de seus serviços[2]. As chamadas provas digitais ganharam proeminência ímpar na persecução penal.

Essas provas digitais[3] possuem algumas características próprias. São dotadas de imaterialidade, porque são dados que, ainda que estejam armazenadas em um dispositivo físico, são dele independentes[4]. Possuem elevado risco de dispersão e manipulabilidade por serem voláteis e frágeis[5], porque podem ser rapidamente transmitidas ou alteradas, com poucos rastros. E, ainda, possuem a característica da "promiscuidade": os dados são facilmente agregáveis e misturáveis, fazendo com que dispositivos de armazenamento físicos ou em nuvem possuam diversos tipos de dados, muitas vezes não relacionados entre si, e em grande volume[6].

Dessas características, surgem desafios para a compreensão doutrinária dos institutos processuais penais. Alguns que já vêm sendo intensamente debatidos incluem: a cadeia de custódia dos elementos de prova digital[7]; o tratamento da proteção de dados no compartilhamento de dados digitais[8]; a gradação da proteção ao sigilo dos dados eletrônicos[9]; a necessidade de autorização judicial para visualização de dados em celulares no curso de uma prisão em flagrante (**Zilli**, 2018).

Uma das características mencionadas possui um impacto particular para o tema ora trabalhado. A chamada "promiscuidade" da prova digital faz com que buscas e apreensões de dispositivos informáticos frequentemente encontrem mais do que aquilo que estavam originalmente buscando, especialmente quando há ampla autorização judicial para vasculhar os dados armazenados. E é nesse ponto que reside a importância de debater o impacto da realidade digital para o encontro fortuito de provas, não sem antes entender como ele é atualmente compreendido na jurisprudência.

3. O encontro fortuito de provas

O chamado "encontro fortuito de provas" descreve a situação, tão comum na persecução penal, em que

> [...] no cumprimento de uma diligência relativa a um delito, a autoridade policial casualmente encontra provas pertinentes à outra infração penal (crime achado), que não estavam na linha de desdobramento normal da investigação (**Lima**, 2020, p. 699).

Esse encontro pode acontecer em qualquer medida tomada no curso de investigação, mas é especialmente comum em buscas e apreensões domiciliares, em interceptações telefônicas, bem como em quebras de sigilo telemático. Como tais meios de obtenção de prova exigem autorização judicial e são extremamente invasivos, a jurisprudência cotidianamente enfrenta questionamentos a respeito da legalidade do encontro fortuito nesses casos.

A jurisprudência dos Tribunais Superiores não costuma ver ilegalidade nesse expediente. Afinal, se a autorização para um determinado meio de obtenção de provas foi hígida e obedeceu aos requisitos legais, e o cumprimento da autorização se deu dentro dos parâmetros fixados, não haveria qualquer mácula à validade dos elementos casualmente obtidos. É o chamado princípio da serendipidade, termo que designa a ocorrência de algo positivo de maneira inesperada e não provocada. Os precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça nesse sentido são múltiplos e incluem julgados recentes[10].

Esse parâmetro, no entanto, não é absoluto. Os próprios julgados excetuam situações de claro desvio de finalidade na execução da medida dessa regra geral de admissibilidade, ocasião em que se configura o chamado *fishing expedition* ou pescaria probatória[11]. Isso já foi reconhecido, por exemplo, em casos envolvendo a busca indeterminada de provas quando do cumprimento de mandado de prisão em residência (**Brasil**, 2024a) ou busca pessoal sem fundada suspeita (**Brasil**, 2023a).

Apesar dessa salutar limitação, não parece ser o suficiente para lidar com a realidade digital. A prática forense demonstra que, no mais das vezes, não há qualquer limitação em um mandado judicial expedido para autorizar o acesso aos dados salvos em um *smartphone* ou um computador, bem como não há limitação significativa aos dados requisitados a provedores de aplicação[12]. O objeto amplo do mandado e a variedade e o volume de dados presentes em dispositivos informáticos ou dados armazenados em nuvem podem dar azo a significativas extrapolações do objeto da medida, tornando-a desproporcional na afetação a direitos fundamentais como a privacidade (art. 5º, X, CF) e o sigilo das comunicações (art. 5º, XII, CF)[13]. Dessa forma, é necessário ir além da mera análise do desvio de finalidade para que se coíba o abuso no acesso indiscriminado a dados — ainda que ele não ocorra de maneira intencional.

4. O tratamento do encontro fortuito de provas na era digital

Dentre os diversos princípios constitucionais que devem pautar a busca e a apreensão no processo penal, o presente estudo discorrerá inicialmente sobre os princípios da proporcionalidade, inadmissibilidade da prova ilícita, inviolabilidade da vida privada e da intimidade, do sigilo das comunicações e da proteção de dados, como forma de demonstrar — que sua não aplicação — podem ocasionar apreensões ilegais, no que diz respeito aos elementos encontrados fortuitamente.

Na sequência, será levantada a discussão sobre como a apreensão de dados na era digital — à míngua de balizas legais — deu um "*bypass*" nos outros meios de obtenção de prova previstos no ordenamento jurídico brasileiro.

Os princípios são verdadeiras linhas-mestras no Direito e estabelecem os limites de atuação do Estado, impondo parâmetros para o exercício do *jus puniendi* estatal frente ao *jus libertatis* dos seus cidadãos (**Antunes**, 2016. p. 32).

O princípio da proporcionalidade (*lato sensu*), admitido no sistema constitucional brasileiro, pretende instituir a relação entre o meio e o fim; isto é, tem o condão de limitar o exercício do poder do Estado. Em seu sentido estrito, engloba os seguintes requisitos (subprincípios): adequação, necessidade e proporcionalidade.

Extrai-se, em síntese, que o subprincípio da adequação (também conhecido como idoneidade ou conformidade) prevê que uma medida é adequada caso seja minimamente eficaz para fomentar a concretização de sua finalidade. O requisito da necessidade, por sua vez, tem como por objetivo garantir que a medida adotada seja indispensável — ou a menos gravosa — para atender ao fim visado

e tem como pressuposto "a verificação da inexistência de meio menos gravosos para atingir os fins visados" (**Fernandes**, 2010, p. 53) para a conservação de determinado direito fundamental. Por fim, a proporcionalidade em sentido estrito visa a ponderação entre o ônus imposto e o benefício obtido, para constatar se é justificável a interferência na esfera dos direitos fundamentais do cidadão (**Barroso**, 1999, p. 220).

Em resumo, pode se dizer que

> [...] uma medida é adequada se atinge o fim almejado, exigível, por causar o menor prejuízo possível e finalmente, proporcional em sentido estrito, se as vantagens que trará superarem as desvantagens (**Guerra Filho**, 1989, p. 75).

A inadmissibilidade da prova ilícita analisada neste artigo, por sua vez, tem como ponto principal a prova ilegal que, segundo a doutrina clássica, é gênero da qual são espécies a prova ilícita e a prova ilegítima[14]. Essa conceituação, todavia, parece não ter sido adotada na reforma do Código de Processo Penal (CPP) em 2008, que passou a prever no art. 157 a inadmissibilidade das provas ilícitas assim entendidas como aquelas obtidas em violação a normas constitucionais ou legais. Ou seja, para a caracterização da prova ilícita, não foi feita nenhuma distinção entre a natureza da norma violada, se material ou processual.

Sobre esse tema, deve ser levado em conta a proposta trazida por **Gustavo Badaró** (2022, p. 466), que pretender ampliar os efeitos da inadmissibilidade da prova ilícita no processo para considerar que tanto provas obtidas mediante a violação de normas de direito material quanto aquelas obtidas mediante violações a normas processuais são igualmente inadmissíveis no processo, sendo que para ambas cabe a sanção do desentranhamento.

Essa conceituação sobre inadmissibilidade da prova ilícita é importante para o presente estudo, posto que, muitas vezes, as medidas que demarcam a distinção entre prova ilícita e prova ilegítima se revelam insuficientes. É o caso, por exemplo, quando há violações de dispositivos constitucionais ou legais que possuem um duplo aspecto, podendo ser lidos, de um lado, como uma garantia constitucional de proteção das liberdades públicas e, de outro, como regramento processual delimitando os mecanismos para a realização de um meio ou obtenção de prova (**Badaró**, 2022, p. 466).

Já o princípio da inviolabilidade da vida privada e da intimidade foi previsto na Carta Constitucional de 1988, art. 5, inciso X. Com isso, o Constituinte assegurou ao cidadão que o estado ou terceiros não tenham acesso aos seus dados a não ser em decorrência das hipóteses previstas em lei. Isso ocorre, pois

> todas as esferas da privada, em maior ou menor grau, são merecedoras de proteção na sociedade moderna, porque o respeito à privacidade surge como reação ao absolutismo e em decorrência do desenvolvimento dos direitos de personalidade (**Almeida**, 2008, p. 720).

A ele se soma o sigilo das comunicações, previsto no art. 5º, XII, que traz proteção especial e autônoma às comunicações privadas — inclusive por meio telemático.

O direito constitucional à proteção de dados traz consigo também compreensões absolutamente relevantes, que devem ser consideradas sempre que órgãos públicos e privados estiverem diante de dados pessoais. Nesse particular, destacam-se os princípios enunciados ao teor do art. 6º, da Lei Geral de Proteção de Dados, que dispõe que o tratamento de dados está condicionado à adequação e à necessidade dessa atividade, que deve guardar estrita observância com a finalidade que ensejou a coleta dessas informações.

É dizer, a coleta dos dados deve buscar o mínimo de informações pessoais necessárias para a consecução de um objetivo previamente determinado, sendo que a utilização desses dados para fins diversos daqueles originalmente previstos torna o tratamento de dados uma atividade ilegal. O tratamento de dados somente é legítimo quando estritamente vinculado à finalidade que o justificou, sendo restrita sua transferência a terceiros, bem como a utilização abusiva para fins diversos (**Doneda**, 2011, p. 100). Esse arcabouço principiológico não apenas garante a privacidade (**Mendes, L.**, 2019), como também se relaciona à separação informacional dos poderes e à vedação ao tratamento indiscriminado e injustificado de dados pessoais[15].

Não obstante a Lei Geral de Proteção de Dados não se aplique em sua totalidade às atividades de persecução penal, matéria que será regulamentada por lei específica (art. 4º, III, "d"), a própria Lei ressalva que seus princípios gerais, os direitos de titulares e o princípio da proporcionalidade devem ser levados em consideração em quaisquer atividades estatais nessa seara (art. 4º, §1º). Esse dispositivo, aliado à introdução da garantia fundamental à proteção dos dados pessoais, inclusive em meios digitais, no art. 5º, LXXIX, da Constituição pela Emenda Constitucional 115/2022 demonstram a aplicabilidade imediata das normas protetivas na seara da persecução penal[16].

Feitas essas breves considerações, eis que surge o ponto fulcral de discussão deste estudo: os riscos da aplicação irrestrita da serendipidade na apreensão de dados digitais.

O debate é muito mais amplo do que os tradicionais exemplos da doutrina sobre a apreensão fortuita de drogas, documentos ou armas que foram localizadas no curso de mandados de busca e apreensão. Nesses casos, de fato, não parece haver dúvidas sobre a legalidade da apreensão do objeto encontrado de forma fortuita, desde que não haja desvio de finalidade na execução.

Por outro lado, no que diz respeito aos elementos de informação (dados) encontrados de forma fortuita em aparelhos celulares e computadores, a resposta não deve ser a mesma.

Essa conclusão decorre, essencialmente, de uma análise constitucional da busca e apreensão no ordenamento jurídico brasileiro.

Explica-se: a previsão legal da busca e apreensão tem redação datada de 1940, quando esse tipo de documento e os dados pessoais eram inimagináveis. Portanto, é preciso assimilar o rito previsto em lei com as balizas e princípios constitucionais.

Como mencionado, a grande maioria dos dados — pessoais, bancários, fiscais, de comunicações, entre outros — de uma pessoa é produzida e armazenada em um único *smartphone*. O Estado, ao ter acesso a essas informações, ainda que mediante autorização judicial, não pode agir livremente e devassar a vida de um particular, sobretudo diante do direito constitucional à inviolabilidade da vida privada, ao sigilo das comunicações e à proteção de dados.

Ocorre que não é isso o que se verifica na praxe forense. Em muitos casos, observam-se as autoridades persecutórias representarem pela busca e apreensão em face de investigados com expressa autorização para acesso aos dados armazenados em celulares, HDs, *pendrives*, *desktops* e *notebooks*, de modo a viabilizar a exploração de dados, análise e eventual realização de exame — sem fazer qualquer limitação temporal, de quais dados são analisados ou sobre qual o assunto que é objeto da investigação.

Ora, se há um pedido dessa magnitude, é certo que a autoridade judicial não deve deferir o pedido com base apenas nas regras esculpidas no art. 240 do CPP, mas sim conjugá-las com outros princípios constitucionais.

Afinal, a alínea "e", do parágrafo primeiro do art. 240 do CPP — descobrir objetos necessários à prova da infração — não pode ser um cheque em branco para as autoridades vasculharem a vida privada do investigado e de terceiros.

O deferimento da medida deve passar, assim, por um crivo; isto é, pela análise da pertinência do meio de obtenção de provas com outros princípios constitucionais. Nesse sentido, o princípio da proporcionalidade acima elencado deve ser levado em consideração quando da análise da representação.

A autoridade incumbida de decidir sobre determinado pedido deve analisar se a medida solicitada (o acesso à integralidade dos dados apreendidos) é adequada, indispensável, ou proporcional sob o ponto de vista de interferência na esfera dos direitos fundamentais do cidadão.

Também deve ser levado em consideração o direito constitucional à proteção de dados, isto é, a coleta dos dados deve buscar o mínimo de informações pessoais necessárias para a consecução de um objetivo previamente determinado, bem como o princípio da inviolabilidade da vida privada e da intimidade.

A desconsideração dessas garantias constitucionais deve, sem dúvida, ocasionar a inadmissibilidade da prova (encontrada fortuitamente) nos autos por violação direta dos dispositivos constitucionais anteriormente elencados.

Mas não é só. Como decorrência desse tema, verifica-se uma segunda possível teratologia na forma como são obtidos os dados apreendidos de forma fortuita na investigação.

No caso, verifica-se que a medida cautelar de busca e apreensão se tornou um indevido atalho para execução de outras medidas probatórias sem passar pelo respectivo crivo legal.

Tal situação se verifica, por exemplo, após a apreensão do aparelho eletrônico, momento em que a autoridade passa a ter acesso a dados e ao fluxo de comunicações de informática e telemática, apesar de não haver a respectiva autorização nos moldes específico, como é o caso da Lei 9.296/1995 e o Marco Civil da Internet[17], que possuem regramento próprio e que acabam, todavia, sendo substituídos (indevidamente) pelo deferimento de acesso aos dados apreendidos na busca e apreensão.

Diante desse cenário de riscos aos direitos fundamentais e potencial desproporcionalidade, aliado à falta de tratamento específico da matéria, é imperiosa a necessidade de impor limites à validade das provas encontradas fortuitamente em diligências relacionadas à obtenção de provas digitais, como buscas e apreensões de dispositivos informáticos, ou requisições de dados a provedores de aplicações.

Para além da análise constitucional acima exposta, uma série de limitações (temporal/temática) podem constar da decisão judicial autorizadora da obtenção dos dados, devendo ser empregadas quando da execução da medida como parâmetros de proporcionalidade.

Uma primeira possível medida é a limitação dos tipos de dados que podem ser acessados, garantindo que sejam apenas aqueles adequados à finalidade da medida e necessários para a sua consecução. Se os dispositivos informáticos contêm uma multiplicidade de tipos de dados — arquivos de vídeo, texto, áudio, comunicações escritas, geolocalização, dados de aplicações, entre outras —, não há motivo para que não sejam indicados quais tipos de arquivos podem ser acessados e quais estão fora do alcance da medida investigativa. Por exemplo: não há, em princípio, justificativa legítima para acesso irrestrito a dados de geolocalização ou ao histórico de navegação na *internet* se o delito investigado é de sonegação fiscal e a medida de busca e apreensão foi justificada com base na possibilidade de localizar notas fiscais fraudulentas.

Outra possível limitação é a indicação estrita do lapso temporal, igualmente regrada pela adequação e necessidade. Pensando no exemplo da interceptação telefônica, há uma limitação legal a quinze dias de prazo, nos termos do art. 5º da Lei 9.296/1995. Ainda que essa limitação se relacione à natureza "de tempo real" da medida, há um claro indicativo de que seu fundamento é possibilitar a proporcionalidade em sua execução, evitando interceptações infindáveis ou sem objeto definido. Dessa maneira, não há óbices para que alguma espécie de limitação temporal ocorra para investigações relacionadas à obtenção de provas digitais. O exemplo paradigmático que pode ser dado é o de dados de comunicação armazenados — como em aplicativos de mensagens ou *e-mails*. Nesses casos, é fácil que a limitação temporal se dê de maneira apriorística, para que somente sejam acessadas comunicações próximas à data do suposto ilícito investigado, de maneira que o agente responsável pela execução da medida sequer possa acessar comunicações de datas que extrapolem a indicada. Mesmo no caso de arquivos diversos, o acesso a metadados como data de criação e modificação de arquivos, ou *logs* de aplicativos, também indicam que há como estabelecer tecnicamente uma limitação temporal para a medida. No caso de uma investigação a respeito de um suposto crime licitatório que teria ocorrido em 2020, não há justificativa legítima e proporcional para franquear o acesso das autoridades de persecução penal a mensagens ou *e-mails* desde o ano de 2012.

Na execução da medida, há meios adicionais de limitação que podem ser empregados. Na maior parte das vezes, a apreensão tem como objeto os dispositivos informáticos, suportes físicos nos quais os dados estão armazenados, para somente então realizar a busca de elementos específicos relacionados à hipótese criminal investigada. No próprio ato de execução da medida, podem ser utilizadas palavras-chave relacionadas ao fato imputado ou seus indícios, com a realização da cópia de segurança somente dos arquivos indicados, sem a apreensão do restante dos dados para evitar abusos ou desproporcionalidade.

Essa medida é de fácil emprego por meio da utilização de *softwares* forenses. Quando não for materialmente possível realizar a filtragem no próprio ato de apreensão, deve ser feita uma cópia integral do disco rígido para, no posterior ato de análise, ser realizada a busca daquilo que for relevante ao objeto da investigação, com o descarte imediato do restante dos dados. O uso de inteligência artificial nessa filtragem — permitindo a busca de arquivos de imagem ou vídeo, correlações com palavras-chave ou temas de interesse e outras ferramentas de seleção — pode ser especialmente relevante[18].

Por fim, é relevante mencionar a chamada *plain view doctrine* como um possível critério de validade de provas encontradas fortuitamente em âmbito digital, conforme desenvolvida no Direito norte-americano. Traduzida como "visibilidade imediata", essa doutrina reputa como válidos aqueles elementos de prova que, embora desconectados do delito apurado pela investigação, sejam encontrados fortuitamente, desde que: i) o elemento esteja imediatamente à vista; ii) haja justificativa legítima para que o agente esteja no local onde visualizou o elemento; e iii) o elemento, por conta própria ou juntamente com outros fatos conhecidos, fornece uma probabilidade razoável de dizer respeito a uma atividade criminosa (**Mendes, P.**, 2021, p. 241).

Por ter sido elaborada para o mundo físico, a jurisprudência norte-americana enfrentou casos práticos que forçaram a adaptação da doutrina ao mundo digital[19]. No caso *United States v. Carey*, a localização de arquivos de pornografia infantil que extrapolavam as palavras-chave de uma busca e apreensão de computadores foi considerada ilícita e não abrangida pela *plain view doctrine* por ter sido fruto de uma busca indiscriminada e geral nos arquivos, conforme decidido pelo Tribunal de Apelação competente (**Estados Unidos da América**, 1999a). Já no caso *State v. Schroeder*, o investigador, ao realizar uma pesquisa de arquivos digitais em um computador apreendido, visualizou uma imagem de pornografia infantil que não possuía relação com o delito originalmente investigado. Diante dessa constatação, imediatamente interrompeu a pesquisa e buscou um mandado judicial adicional, o que foi considerado válido pelo Tribunal em questão (**Estados Unidos da América**, 1999b). Ou seja, pelos parâmetros fixados na jurisprudência, a *plain view doctrine* não justifica a busca irrestrita de elementos desconectados com o objeto do mandado judicial, mas pode tornar válidas aquelas provas que sejam verdadeiramente fruto de um encontro fortuito, desde que o agente tome as medidas adequadas para realizar a investigação do delito aparentemente descoberto — como o início de uma nova investigação ou a obtenção de um mandado judicial adicional.

Dessa forma, uma aplicação da *plain view doctrine* é plenamente possível no âmbito brasileiro como uma limitação adicional para a validade do encontro fortuito de provas no âmbito digital.

Caso um elemento visivelmente indicativo de prática criminosa diversa daquela que ensejou a diligência seja avistado pelo agente no cumprimento regular do mandado, esse elemento é considerado válido para ensejar uma nova investigação e até a expedição de outro mandado por juiz competente. Inválidos seriam aqueles elementos de prova oriundos de buscas adicionais sem autorização realizadas após essa visualização, ou a localização de elementos de prova por um vasculhamento geral e irrestrito dos dados apreendidos.

Ainda que não exista um regramento legal específico para o encontro fortuito de provas, essas limitações podem ser empregadas pela jurisprudência como parâmetros adicionais de proporcionalidade e proteção dos direitos fundamentais que estejam sob risco significativo no cenário das apreensões de dados. Essa adoção de limites e parâmetros é instrumental para evitar potenciais abusos que possam ser praticados sob o manto da atual aplicação — quase irrestrita — do princípio da serendipidade.

5. Conclusão

O presente trabalho buscou reavaliar o chamado encontro fortuito de provas diante da nova realidade da persecução penal — profundamente influenciada pelo fenômeno da digitalização.

Como visto, a aceitação irrestrita de elementos de prova encontrados fortuitamente nesse cenário se revela desproporcional e potencialmente violadora das garantias constitucionais enumeradas, com particular atenção à proteção da intimidade e da vida privada e à proteção de dados pessoais, além da inadmissibilidade das provas ilícitas.

Seria importante que o legislador fixasse um regramento legal específico para a apreensão de dados, incorporando limitações que possam compatibilizar a necessidade investigativa com a proteção aos direitos e garantias fundamentais, em respeito ao princípio da proporcionalidade. A legalidade estrita que impera no processo penal e a restrição aos direitos fundamentais imposta pelos meios de obtenção de prova torna inafastável que cada um tenha um regramento específico, com procedimento previsto em lei e um tratamento adequado sob o prisma da proporcionalidade. Apenas dessa forma, pode-se ter a segurança jurídica necessária e a conjugação do interesse persecutório com a proteção aos direitos fundamentais.

No entanto, enquanto não haja disciplina legal da apreensão de dados, nada impede que a jurisprudência faça os filtros apropriados a partir de uma interpretação sistemática da legislação e da Constituição, declarando inválidas as provas que extrapolem as limitações fixadas. As principais limitações tratadas foram as de natureza temática e temporal, facilmente implementáveis pela própria autoridade judicial na decisão autorizadora dos meios de obtenção de prova. Outras limitações sugeridas incidem na própria execução da medida, limitando os dados que serão adquiridos e analisados. Por fim, sugeriu-se uma adaptação da *plain view doctrine* para tratar dos casos limítrofes de encontro fortuito — separando as verdadeiras casualidades, juridicamente válidas, das expedições de pescaria probatória que são ilegítimas e desproporcionais.

Com a implementação prática desses limites e parâmetros, busca-se minimizar o risco de violação de direitos fundamentais, criando claros incentivos para que as autoridades públicas zelem pela proporcionalidade e pelo respeito aos direitos fundamentais no desenvolvimento da investigação. Ou seja, previne-se tanto o abuso intencional e o *bypass* investigativo sob o falso manto da serendipidade, quanto o excesso de agentes públicos que, embora bem-intencionados, desviem-se da autocontenção necessária para o empreendimento da atividade persecutória.

Informações adicionais e declarações dos autores (integridade científica)

Declaração de conflito de interesses: os autores confirmam que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** todos e somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listados como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade. **Declaração de originalidade:** os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; eles também atestam que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

CORDEIRO, Pedro Ivo Rodrigues Velloso; AGOSTI, Francisco Felippe Lebrão; CAMARGO, Pedro Luís de Almeida. Repensando o encontro fortuito de provas na era digital. **Boletim IBCCRIM**, São Paulo, v. 32, n. 384, p. 21-26, 2024. DOI: https://doi.org/10.5281/zenodo.13834573. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1658. Acesso em: 1 nov. 2024.

Notas

1 Sobre a variedade de dados presentes nos *smartphones* e sua importância para a investigação criminal contemporânea, ver Antonialli, Cruz e Abreu (2018).

2 Para examinar as peculiaridades na apreensão de dados localizados em servidores remotos, ver, por todos, Costa e Leonardi (2011).

3 Carlos Hélder Carvalho Furtado Mendes (2023) utiliza a definição de Eoghan Casey para a prova digital, como sendo "qualquer dado armazenado ou transmitido através de um computador que apoie ou refute uma hipótese de como um delito ocorreu, ou que aborda elementos críticos do ilícito, como a intenção ou álibi", sendo os dados uma combinação numérica que representa informações de variados tipos, incluindo textos, imagens, áudios ou vídeos.

4 Apesar de os *bits* sequenciais que formam as informações de dados serem independentes de um suporte físico, eles dependem desse suporte para que se tornem percebíveis, ainda que isso não retire a autonomia dos dados desmaterializados (Mendes, C., 2023, p. 271).

5 Volatilidade e fragilidade se relacionam, respectivamente, com a facilidade de desaparecimento e com a possibilidade de contaminação (Mendes, C., 2023, p. 271-272).

6 A nomenclatura da "promiscuidade" das provas digitais ora utilizada é uma tradução livre daquela empregada por Marcello Daniele (2011).

7 Ver, por todos: Badaró (2021, p. 7-9) e Prado (2021, p. 173-214).

8 Para uma introdução ao tema da proteção de dados no processo penal e na segurança pública, ainda que não exclusivamente sobre o prisma dos dados digitais: Gleizer, Montenegro e Viana (2021).

9 Maria Thereza Rocha de Assis Moura e Daniel Marchionatti Barbosa (2020) explicam como os ordenamentos costumam proteger, em ordem do mais ao menos protegido: o fluxo telemático, os dados armazenados, os dados pessoais e, dentre esses, os dados cadastrais como sendo aqueles com o menor nível de proteção.

10 Alguns julgados recentes ilustrativos, a título de exemplo: Brasil (2023b, 2024b, c, d).

11 *Fishing expedition* ou pescaria probatória é "a procura especulativa, no ambiente físico ou digital, sem 'causa provável', alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém" (Rosa, 2021).

[12] Carina Quito (2020, p. 170-171) aborda a problemática do acesso irrestrito a comunicações armazenadas e a grave situação de desproporcionalidade dele decorrente.

[13] Carina Quito (2020, p. 171-173) também aborda a incongruência e os riscos na utilização dos dispositivos legais de busca e apreensão, formulados para a apreensão de coisas físicas, para dados digitais armazenados em dispositivos móveis, computadores e servidores, criando a situação de acesso irrestrito e potencial violação à privacidade por falta de disciplina legal específica.

[14] A primeira ocorre quando há violação de direito material ou constitucional no âmbito de sua coleta, admissão ou produção no curso do processo; já a segunda viola regra de Direito Processual Penal no momento de sua produção. De forma geral, a doutrina clássica entende que, enquanto as provas ilícitas são inadmissíveis no processo, devendo ser desentranhadas, as ilegítimas são nulas e sua produção — a depender do caso — pode ser renovada. Essa distinção é encontrada, por exemplo, em Grinover (1982, p. 98-99).

[15] Heloisa Estellita (2021, p. 613) destaca que qualquer cada forma ou fase do tratamento de dados — como a obtenção, o armazenamento, a utilização, a transferência etc. — é uma intervenção autônoma à autodeterminação informacional. A própria alteração de finalidade de um dado previamente coletado pode ser considerada, portanto, uma intervenção na esfera do titular.

[16] Heloisa Estellita (2021, p. 615) destaca que a aplicação de todo o instrumental normativo vinculado à proteção de dados pessoais independe de uma lei federal de proteção de dados para o âmbito penal, ainda que uma lei nesse sentido seja desejável.

[17] A quebra de dados telemáticos constitui modalidade de intervenção no sigilo de dados telemáticos protegido pelo art. 5º, X, da Constituição Federal, consistente na apreensão das conversas de e-mail já efetivadas e armazenadas, e é regulada pela Lei 12.965/2014 (Marco Civil da Internet) (Sidi, 2016).

[18] Paulo de Sousa Mendes (2021, p. 238-240), com base nas *Federal Guidelines for Searching and Seizing Computers* dos Estados Unidos da América, destaca a importância de utilização desses métodos de filtragem para mitigar os danos à privacidade digital.

[19] Essa evolução da jurisprudência norte-americana é trabalhada por Paulo de Sousa Mendes (2021, p. 242-247).

Referências

ALMEIDA, José Raul Gavião. Anotações acerca do direito à privacidade. *In*: MIRANDA, Jorge; SILVA, Marco Antônio Marques da (Coords.). *Tratado luso-brasileiro da dignidade humana*. São Paulo: Quartier Latin, 2008. p. 719-726.

ANTONIALLI, Dennys; CRUZ, Francisco Brito; ABREU, Jacqueline de Souza. Smartphones: baús do tesouro da Lava Jato. *In*: ANTONIALLI, Dennys; ABREU, Jacueline de Souza (Eds.). *Direitos fundamentais e processo penal na era digital*. v. 1. São Paulo: Internet Lab, 2018. p. 56-63.

ANTUNES, Leonardo Leal Peret. *(Re)pensando a busca e apreensão no processo penal*: uma análise constitucional dos seus limites. Rio de Janeiro: Lumen Juris, 2016.

BADARÓ, Gustavo Henrique. Os *standards* metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7-9, 2021.

BADARÓ, Gustavo Henrique. *Processo Penal*. 10. ed. São Paulo: Thomson Reuters, 2022.

BARROSO, Luís Roberto. *Interpretação e aplicação da Constituição*: fundamentos de uma dogmática constitucional transformadora. 3. ed. São Paulo: Saraiva, 1999.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. AgRg no *HC* 909.611/RS, relator Ministro Reynaldo Soares da Fonseca, julgado em 12 ago. 2024, DJe de 15 ago. 2024c.

BRASIL. Superior Tribunal de Justiça. Sexta Turma. AgRg no *RHC* 198.226/PR, relator Ministro Sebastião Reis Júnior, julgado em 1 jul. 2024, DJe de 3 jul. 2024d.

BRASIL. Superior Tribunal de Justiça. Sexta Turma. *HC* 834.675/RS, relator Ministro Jesuíno Rissato (Desembargador Convocado do TJDFT), julgado em 12 set. 2023, DJe de 15 set. 2023a.

BRASIL. Superior Tribunal de Justiça. Sexta Turma. *HC* 868.155/SP, relator Ministro Jesuíno Rissato, Desembargador Convocado do TJDFT, julgado em 16 abr. 2024, DJe de 19 abr. 2024a.

BRASIL. Supremo Tribunal Federal. Primeira Turma. *HC* 223.478 ED, relator Ministro Alexandre de Moraes, julgado em 25 abr. 2023, DJe de 26 abr. 2023b.

BRASIL. Supremo Tribunal Federal. Primeira Turma. *RHC* 239.805 AgR, relator Ministro Cristiano Zanin, julgado em 7 maio 2024, DJe de 9 maio 2024b.

COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 19, n. 88, p. 203-223, 2011.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Pádua, v. 46, n. 2, p. 283-298, 2011.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, Chapecó, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 18 set. 2024.

ESTADOS UNIDOS DA AMÉRICA. The United States Court of Appeals (10th Circuit). United States v. Carey, 172 F:3d 1268. Denver, CO, 14 abr. 1999a. Disponível em: https://casetext.com/case/us-v-carey-9. Acesso em: 27 ago. 2024.

ESTADOS UNIDOS DA AMÉRICA. Wisconsin Court of Appeals. State v. Schroeder, 613M.W.2d911. Milwaukee, WI, 4 fev. 1999b. Disponível em: https://casetext.com/case/state-v-schroeder-40. Acesso em: 27 ago. 2024.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. *Revista de Direito Público*, Brasília, v. 18, n. 100, p. 606-636, 2021. https://doi.org/10.11117/rdp.v18i100.5991

FERNANDES, Antonio Scarance. *Processo Penal Constitucional*. 6. ed. São Paulo: Revista dos Tribunais, 2010.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. São Paulo: Marcial Pons, 2021.

GRINOVER, Ada Pellegrini. *Liberdades públicas e processo penal*: as interceptações telefônicas. 2. ed. São Paulo: Revista dos Tribunais, 1982.

GUERRA FILHO, Willis Santiago. *Ensaios de teoria constitucional*. Fortaleza: Universidade Federal do Ceará, 1989.

LIMA, Renato Brasileiro de. *Manual de Processo Penal*. 8. ed. Salvador: Juspodivm, 2020.

MENDES, Carlos Hélder Carvalho Furtado. *Prova penal digital*: direito à não autoincriminação e contraditório na extração de dados armazenados em sistemas informáticos. Tese (Doutorado em Ciências Criminais) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, 2023. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/10650. Acesso em: 17 set. 2024.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coords.). *Caderno Especial*: Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019. p. 35-56.

MENDES, Paulo de Sousa. A privacidade digital posta à prova no processo penal. *Quaestio facti: Revista Internacional sobre Razonamiento Probatorio*, Girona, v. 2, p. 225-250, 2021. https://doi.org/10.33115/udg_bib/qf.i2.22487

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. *In*: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (Coords.). *Direito, Processo e Tecnologia*. São Paulo: Revista dos Tribunais, 2020. p. 477-502.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 2. ed. São Paulo: Marcial Pons, 2021.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. *In*: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. (Org.). *Direito, Processo e Tecnologia*. São Paulo: Revista dos Tribunais, 2020. p. 161-186.

ROSA, Alexandre Morais da. A prática de *fishing expedition* no processo penal. *Consultor Jurídico*, 2 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishing-expedition-processo-penal/ Acesso em: 26 ago. 2024.

SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: D'Plácido, 2016.

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. *In*: ANTONIALLI, Dennys; ABREU, Jacueline de Souza (Eds.). *Direitos fundamentais e processo penal na era digital*. v. 1. São Paulo: Internet Lab, 2018. p. 64-99.