Coleta e tratamento de dados na transformação tecnológica da investigação criminal

Data collection and processing in the technological transformation of criminal investigation

NEREU JOSÉ GIACOMOLLI[1]
nereu@giacomolli.com

DANIELA DORA EILBERG[2]
danielaeilberg@gmail.com

GALILEU – REVISTA DE DIREITO E ECONOMIA · e-ISSN 2184-1845
Volume XXIV · 1st January Janeiro – 31ST December Dezembro 2023 · pp. 123-140
DOI: https://doi.org/10.26619/2184-1845.XXIV.1/2.7
Submitted on October 29th, 2023 · Accepted on December 31st, 2023
Submetido em 29 de Outubro, 2023 · Aceite a 31 de Dezembro, 2023

SUMÁRIO I. Introdução, II. O ciclo de vida dos dados da prova digital, III. Acesso a dados e a prova digital no ordenamento jurídico brasileiro, IV. Tratamento de dados no processo penal, Considerações Finais.

RESUMO O processo penal é permeado, contemporaneamente, pela relação das autoridades do sistema de justiça criminal com os dados, de modo que o novo paradigma fundado no elemento digital demanda uma responsável gestão do ciclo de vida dos dados obtidos e tratados em nome da justiça. A autoridade judicial imparcial deve atentar às novas formas de processamento de dados que sejam auditáveis e confiáveis, vez que os conflitos judicializados se embasam em análise da informação à disposição da autoridade judicial, cuja coleta foi possível no contexto da transformação tecnológica. Este artigo analisa as formas de acesso aos dados para finalidade probatória, as consequências que o art. 4.º , III da Lei n.º 13.709/2018 possui no tratamento de dados para a finalidade de investigação

1 Doutor em Direito pela *Universidad Complutense de Madrid*, Professor na Pontifícia Universidade Católica do Rio Grande do Sul, Brasil (PUCRS), vinculado ao Mestrado e Doutorado em Ciências Criminais, onde leciona a disciplina de processo penal e sistemas jurídico-criminais comparados, respectivamente. Líder do projeto de pesquisa "Processo Penal na Era Digital" e do Grupo de Estudos Processo Penal Contemporâneo: fundamentos, perspectivas e problemas atuais. Pesquisador Integrado do *Ratio Legis* – Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa, Portugal, no Projeto *Corpus Delicti*, Estudos de Criminalidade Organizada Transnacional. Desembargador jubilado do Tribunal e Justiça do Rio Grande do Sul, Brasil, Advogado e consultor jurídico. E-mail: nereu@giacomolli.com. Orcid: https://orcid.org/0000-0003-1753-0334.

2 Doutoranda e Mestra em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) com período sanduíche na Corte Interamericana de Direitos Humanos. Bolsista CAPES. Bacharela em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS) com período sanduíche na Université Paris I Panthéon Sorbonne. Advogada criminalista. Orcid: 0000-0002-3240-6318.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

criminal no Brasil e as adequações legais que a intencionada reforma do Código de Processo Penal se ateve – ou deveria se ater – quanto ao capítulo da prova digital.
PALAVRAS-CHAVE Processo penal. Investigação Criminal. Proteção de Dados. Prova Digital.
ABSTRACT The criminal procedure is contemporaneously infused by the relationship between the authorities of the criminal justice system and data. The digital element inherent in the new established paradigm demands responsible management of the life cycle of the data obtained and processed in the name of justice. The independent judicial authority must be aware of the new forms of data processing that are auditable and reliable, since judicialized conflicts are based on analysis of data available to the judicial authority whose collection was possible due to technological transformation context. This article analyzes the data collection, the consequences of art. 4.º , III, Act n.º 13.709/2018 for data processing to criminal investigations in Brazil, as well as highlight the cautions to amend the Code of Criminal Procedure on digital evidence.
KEYWORDS Criminal procedure. Criminal Investigation. Data Protection. Electronic Evidence.

I. Introdução

A natureza do elemento digital é fundante e balizadora do novo paradigma instaurado à realidade processual. O processo passa a ser percebido, contemporaneamente, a partir da reformulação da relação com os dados. Delgado Martins[3] é certeiro ao evidenciar como a uma autoridade judicial imparcial depende de novas formas de processamento de dados, vez que o conflito judicializado possui resolução, cuja análise se dá em um conjunto de dados à disposição da autoridade judicial.

Tal coleta foi possível em razão das transformações tecnológicas, e a aplicação das tecnologias não apenas nas relações cotidianas, mas ao sistema de justiça criminal, demanda responsável pela gestão do ciclo de vida dos dados obtidos e tratados em nome de e perante o Estado. A matéria tecnológica exige um mínimo de literacia e alfabetização digital, para evitar a opacidade, como bem apontam Bolzan e Flaviane com base em Jenna Burrell[4], quando debatem sobre a "opacidade de modelos computacionais de mineração de dados e desafio da transparência e integridade dos modelos de aplicação"[5]. Exige-se

3 DELGADO, Joaquin. Judicial-Tech, el proceso digital y la transofrmación de la justicia. Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020, p. 13.

4 BURREL, Jena. How the machines thinks: Understanding opacity in machine learning algorithms. In Big data & Society, Jan-jun, 2016.

5 BARROS, Flaviane de Magalhães; MORAIS, José Bolzan. Era digital e o processo penal brasileiro: busca de uma nova gramática, em VALENTE, Manuel Monteiro Guedes et all. (coord.) Direito e Liberdade, estudos em

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

que todos os atores da justiça criminal se atualizem quanto ao básico que o conhecimento digital deve propiciar, mas com a consciência suficiente da necessidade de assistência de *experts* que a matéria tecnológica exige, como uma realidade constante. Juízes e juízas, promotores e promotoras não estudaram para ser peritos forenses digitais. Mas entender as características do dado digital (principalmente a sua volatilidade) e o básico sobre o que se exige da tecnologia é preciso para que se identifique se houve a preservação da cadeia de custódia é o começo ao diálogo com este conhecimento técnico.

Quando se diz prova digital, portanto, refere-se primordialmente a dados. É nesse sentido que os fundamentos principiológicos de um processo penal democrático são atraídos ainda mais fortemente pelo campo magnético da dogmática constitucional da proteção de dados. A exceção do art. 4.º , III, da Lei Geral de Proteção de Dados no Brasil não foi simplesmente uma escusa do legislador para deixar de proteger os dados tratados para as finalidades dispostas no inciso III.

Pelo contrário, o dispositivo não deixou de reforçar que os princípios gerais e os direitos dos titulares previstos na LGPD devem também ser observados pelas exceções (§1.º , art. 4.º , LGPD), e inclusive depositou na figura da Autoridade Nacional de Proteção de Dados (ANPD) a responsabilidade por emitir opiniões técnicas ou recomendações referentes às exceções, a ela devendo ser submetidos os relatórios de impacto de ferramentas tecnológicas para as finalidades das exceções do III do art. 4.º da LGPD. Vale ressaltar que a regulação separada para o tratamento de dados no processo penal é tendência internacional.

Os desafios inerentes às transformações que a investigação digital ou a investigação sobre dados digitais proporciona é realidade nos mais variados países. A reformulação e seus impactos nos sistemas de justiça dos países europeus, por exemplo, se vê refletida no corpo jurisprudencial do Tribunal Europeu de Direitos Humanos. Autores[6] exploram os casos de bancos de dados e dados pessoais, busca e apreensão digital, rastreamento de localização, dados de tráfego e interceptação em massa de comunicações para retratar os caminhos adotados pelos países europeus na jornada da incorporação das tecnologias na investigação criminal.

homenagem ao prof. Nereu José Giacomolli. Coimbra: Almedina, 2022, p. 624 e ss.

6 HIRSCH BALLIN, M.; GALIČ, M. Digital investigation powers and privacy: Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure. Boom Strafblad, 2021, 2(4), p. 148-159. https://doi.org/10.5553/BSb/266669012021002004007. Acesso em 04/09/2023.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

II. O ciclo de vida dos dados da prova digital

O terreno globalizado expõe visceralmente a crise das normas e princípios tradicionais, de modo a exigir inovações em todos os ramos. O anacronismo do Direito evidencia-se nas suas legislações (ou na falta delas). Justamente da ausência da regulação no processo penal, em sua dinamicidade, é que se vê o desenho da "sociedade da transparência"[7] expressa na possibilidade extrema de personificação de cada dizer. A possibilidade de reconstrução do passado de uma pessoa por meio de dados digitais por ela produzidos é a grande chave investigadora. As tecnologias não apenas passaram a ser uma espécie de extensão da capacidade de memória humana, como também alteraram as instituições políticas, o exercício de cidadania na chamada ciberdemocracia[8], razão pela qual a maneira com a qual o governo difunde a livre adesão a pautas de agenda criminais populistas no denominado ciberespaço[9] é bruta.

Inexiste, atualmente, previsão legal de meio de prova digital no ordenamento jurídico brasileiro[10]. No entanto, dentre as diversas tentativas de reforma processuais, tem-se o Projeto de Lei n.º 4939/2020, que retrata uma das tentativas de regulamentar novos meios de obtenção de prova digital mais adequados à realidade atual que aqueles previstos na era analógica pelo Código de Processo Penal datado de 1941.

Contudo, por mais que não haja a previsão legal, a realidade da investigação brasileira é de expansão do uso de meios de investigação a partir das ferramentas tecnológicas. Uma série de técnicas são adotadas pela polícia para investigar e muitas vezes aparecem transmutados como se buscas fossem[11]. Cada um dos meios de prova digital gera diferentes meios de obtenção de prova, e na realidade das plataformas e empresas prestadoras de serviços, tem-se a realidade das normas processuais refletindo as regras da cooperação internacional[12].

Frente aos câmbios nessa configurada sociedade de informação[13], os avanços tecnológicos passaram a permitir a utilização de mecanismos poderosos de investigação

7 HAN, Byung-Chul. Sociedade da transparência. Petrópolis: Rio de Janeiro, Vozes, 2017.
8 LEVY, Pierre. Ciberdemocracia. Lisboa: Editions Odile Jacob, 2002.
9 BECK, Ulrich. Sociedade do risco: rumo a uma outra modernidade. São Paulo: ED34, 2010.
10 Vid. ILLUMINATI, Giulio. Prova digitale e ammisibilità, em VALENTE, Manuel Monteiro Guedes (coord.). Direito e Liberdade, estudos em homenagem ao prof. Nereu José Giacomolli, p. 945 e ss., a delimitação da prova digital.
11 EILBERG, Daniela Dora; GLOECKNER, Ricardo Jacobsen. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. In Revista Brasileira de Ciências Criminais, vol. 156/2019, p. 353 a 393.
12 SALT, Marcos. Nuevos desafíos de la evidencia digital: acceso transfornterizo y técnicas de acesso remoto a datos informáticos. 1.ª ed. Buenos Aires: Ad-hoc, 2017, p. 11.
13 O termo *sociedade da informação* passou a ser utilizado para se referir aos últimos anos do presente século, uma vez identificada a alteração da dinâmica econômica da sociedade "pós-industrial" ou "informacional" – nas palavras de Castells – a partir da introdução das novas tecnologias.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

na obtenção de informações relevantes para processos penais, conforme explorado por Salt[14]. Essas inovações técnicas e tecnológicas de investigação, contudo, demandam conhecimentos específicos, tendo em vista que de suas investigações é possível recolher fontes cuja função é proporcionar o conhecimento de informações cada vez mais fidedignas e relevantes ao processo penal.

Ao abordarmos as fases do ciclo de vida dos dados no processo penal, a primeira diz respeito à coleta de dados, momento sobre o qual se deve analisar a legitimidade da obtenção dos dados para serem utilizadas como prova no processo[15]. Nesse momento em que estarão não apenas os meios de obtenção e meios de prova tradicionais, como também novos meios de investigação.

Ou seja, a quantidade de dados nas redes sociais, nos dispositivos eletrônicos, nas nuvens, ou de posse dos provedores de serviços são o enfoque dos novos desafios à compreensão da licitude da prova obtida e os limites legais para tanto na primeira fase. E nesse campo, os conflitos de jurisdição assumem protagonismo pelo caráter transfronteiriço inerente à comunicação tecnológica, que faz uso de plataformas cujas prestadoras de serviço estão em jurisdições no exterior e com tendência de armazenamento em servidores em jurisdição terceira, rompendo com a lógica da territorialidade do lugar físico do dispositivo[16].

A segunda fase diz respeito à classificação e armazenamento dos dados e a terceira, sobre o uso e tratamento de tais dados. Os problemas relacionados aos tratamentos de dados pessoais no processo penal, bem como a segurança de tais dados armazenados nas atuais plataformas e softwares do sistema de justiça e/ou das empresas privadas prestadoras de serviço para a justiça são os principais desafios desta fase. Justamente, em uma era de *data breaches*, questionamentos sobre a segurança digital dos dados da Justiça é uma das pavorosas face da moeda, sendo a outra relacionada à interoperabilidade de tais dados com outras autoridades estatais ou com o setor privado. O avanço tecnológico também trará importantes avanços aplicados a tais dados, como são os casos da inteligência artificial e do *blockchain*.

Por último, a fase de transmissão ou compartilhamento de dados também está fadada à problemática dos dados coletados sobre terceiros e o tratamento de dados pelo setor privado. A grande crítica trazida ao acesso de dados de terceiros para a finalidade de

14 SALT, Marcos. Nuevos desafíos de la evidencia digital: acceso transfornterizo y técnicas de acesso remoto a datos informáticos. 1.ª ed. Buenos Aires: Ad-hoc, 2017, p. 20.

15 DELGADO, Joaquin. Judicial-Tech, el proceso digital y la transofrmación de la justicia. Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020, p. 16.

16 SALT, Marcos. Obtención de pruebas informáticas en extraña jurisdicción: Los "conflictos" del principio de territorialidad en un mundo virtual sin fronteras", 2016, p. 518.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

investigação criminal diz respeito ao fato de que em sua maioria essas pessoas sequer são alvo de investigação e duvidoso, portanto, a coleta de dados seus sem qualquer base legal. Sempre tão esquecida, porém imprescindível, é a eliminação dos dados. Precisamos falar a respeito do limite de prazo de armazenamento e do regime de finalização de dados pessoais no processo penal, de modo a se determinar quando serão completamente deletados dos registros os dados que foram armazenados pelo tempo legal necessário.

III. Acesso a dados e a prova digital no ordenamento jurídico brasileiro

A possibilidade de que as autoridades encarregadas da persecução penal de um Estado acessem à prova digital em servidores ou dispositivos informáticos é uma questão de variadas controvérsias jurídicas geradas na atualidade, tanto em nível doméstico como da cooperação jurídica internacional em matéria penal.

As formas de acessar dados para a finalidade probatória no processo penal dentro do contexto da *e-evidence* envolvem busca de dispositivos, busca de dados na nuvem, a busca remota, a obtenção de dados sob custódia de provedores de serviço, a busca de dados preservados por provedores, além da cooperação internacional (formal ou informal) que gera compartilhamento de dados e da investigação de dados em redes abertas ou do agente infiltrado virtual.

Como bem evidencia Salt[17], a polêmica tende a se aprofundar com o uso massivo de dispositivos capazes de armazenar dados computacionais, com o aumento vertiginoso das opções de serviços de computação em nuvem (*cloud computing*) e com a realidade crescente de hospedagem de informações em servidores externos aos dispositivos nos quais as informações são geradas (ou seja, provocando consequente perda da localização física das informações).

No que diz respeito à realidade sob um ordenamento jurídico em específico, na esfera da produção probatória, a exploração de vulnerabilidades de segurança na tecnologia pelas autoridades policiais para obtenção de dados ocorre, muitas vezes, de forma oculta e remota. Algumas outras práticas já são comumente aplicadas, de *web scraping* ou de *web crawling* para fins de investigação criminal, muitas vezes com o uso de ferramentas de *Open Source Intelligence (OSINT)* para se analisar e indexar metodicamente o conteúdo da *web*, em específico utilizadas nos buscadores, geram questionamentos e exigência de adequação legal.

17 SALT, Marcos. Nuevos desafíos de la evidencia digital: acceso transfornterizo y técnicas de acesso remoto a datos informáticos. 1.ª ed. Buenos Aires: Ad-hoc, 2017.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

A primeira questão imprescindível para todos os meios de prova digitais é a observação sobre os tipos de dados que estão envolvidos. Uma conceituação clássica é a de i) dados cadastrais (por exemplo, saber a quem pertencia o IP determinado, ou um número telefônico e dados de faturação de um telefone. Ou seja, tudo que pode ter registrado um provedor de serviço; ii) metadados (das comunicações) ou dados de conteúdo (precisamente o conteúdo da comunicação, por exemplo, o que diz o e-mail).

Para a obtenção dos dados pelas autoridades estatais, a categorização clássica representaria um grau escalonado de intrusividade, porque não seria a mesma coisa saber a quem pertence um IP quando comparado a quem se comunicou, ou sobre o próprio conteúdo da comunicação. A primeira diferenciação é: quem pode pedir o tipo de dado? Isso será verificado na questão da busca e apreensão. É sempre necessário ter uma autorização judicial ou alguns dados podem ser coletados pela polícia ou MP diretamente? Como Jacqueline Abreu e Dennys Antonialli já identificaram em trabalho primoroso sobre as comunicações no Brasil[18], algumas previsões legais no ordenamento jurídico são interpretadas nesse sentido, como a Lei das Organizações Criminosas e o acesso aos registros telefônicos sem autorização judicial, a Lei de Lavagem de Dinheiro e o acesso ao MP de dados cadastrais sem autorização, ou o acesso a dados cadastrais e geolocalização para os casos dos arts. 13-A e 13-B do CPP[19].

Ainda sobre os pedidos de autorização e, no caso, a no Superior Tribunal de Justiça, por exemplo, houve o precedente relacionado ao caso de Marielle Franco em que o Judiciário manteve a obrigação do Google de ceder os dados privados de milhões de pessoas que sequer eram alvo de investigação para a investigação do homicídio da vereadora, configurando verdadeira prática de *fishing expedition*. Além de não haver autorização nos termos da reserva de lei para tanto, há proibição quanto aos pedidos genéricos ou inespecíficos no Decreto n.º 8.771/2016 e por isso autores como Heloisa Estellita e Gleizer direcionaram críticas às coletas de dados pessoais de pessoas insuspeitas.

No que diz respeito à categorização clássica dos dados, percebemos como as mudanças tecnológicas também provocaram crises do ponto de vista jurídico. Basicamente, existem dados modernos que são difíceis de enquadrar nessa classificação, bem como outros dados como o IP dinâmico, por exemplo, passam a questionar a divisão do que seria um dado cadastral e um metadado. O *caso Benefiz vs. Slovenia*, do Tribunal Europeu de Direitos

18 ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wpcontent/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso em: 05/2020, p. 27 e 35.

19 Quanto aos três cenários, temos as ADI 5063/DF, ADI 4906 e ADI 5642.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

Humanos, abordou essa questão – gerando diferentes respostas nos países quanto à regulação do IP dinâmico nos ordenamentos jurídicos. Isso é importante porque os sistemas jurídicos dispõem de diferentes questões para a coleta desses tipos de dados.

Como premissa, este trabalho entende que ao elemento probatório digital não devermos transpor o raciocínio dos elementos probatórios físicos. A doutrina do *plain view*, por exemplo, não se configura da mesma forma no mundo digital. No mundo digital, não há encontro fortuito com as características justificantes de aproveitamento probatório do encontro fortuito de prova que tenha uma corporeidade no mundo digital, vez que no mundo digital tudo é direcionado, calculado, premeditado com algoritmos.

O desenvolvimento de um regime uniforme de garantias no acesso a provas digitais é essencial. Em algumas das tentativas de reformas, utilizaram a distinção "dados em repouso" e "dados em transmissão" para determinar os critérios da coleta, como o caso da proposta de reforma Código de Processo Penal pelo PL n.º 845/2010. A doutrina de proteção de dados pessoais levanta problemáticas quanto à suscetibilidade de abusos que tal distinção pode levar, uma vez que abre mão de salvaguardas já assentadas no Supremo Tribunal Federal quando discutida a Lei de Interceptação telemática[20], e poderia recair a arbitrariedades devido ao volume de dados em repouso ser muito maior.

A configuração de uma sociedade contemporânea cuja dinâmica foi completamente reestruturada é o primeiro ponto que deve ser destacado para se compreender as mudanças em escala macro e micro das relações sociais. Não apenas a lógica de relacionamentos intrapessoais se modificou, como também a relação do Estado com os indivíduos. O delineamento de um contexto completamente renovado é evidenciado, na medida em que são incorporados, constante e exponencialmente, novos meios de tecnologias de informação e comunicação (TIC) – a ponto de catalisar o chamado processo da obsolescência em todas as esferas.

Diante do cenário global criado a partir do domínio das TICs, algumas mudanças são imperativas para que se adapte as ciências jurídicas à realidade. Isso porque, o desenho desse terreno expôs visceralmente a crise das normas e princípios tradicionais, de modo a exigir inovações em todos os ramos do direito[21]. Sob essa perspectiva, com o Direito Processual Penal não poderia ter sido diferente.

As inovações técnicas e tecnológicas de investigação explicitadas na expansão dos métodos ocultos de investigação demandam conhecimentos específicos, tendo em vista a coleta de *fontes* cuja função é proporcionar o conhecimento de informações cada vez mais

20 Data Privacy. Tabela de análise de reforma do Código de Processo Penal, 2021.
21 SALT, Marcos. Nuevos desafíos de la evidencia digital: acceso transfornterizo y técnicas de acesso remoto a datos informáticos. 1.ª ed. Buenos Aires: Ad-hoc, 2017, p. 11.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

fidedignas e relevantes ao processo penal. Interessante o apontamento de Guimarães que ressalta a catalização da inteligência artificial a partir do acesso à rede[22]. Tais fontes de prova, quando colhidas em ambiente digital ou informático, e em virtude da complexidade metodológica e científica, também ostentam a característica do que se denomina prova científica.

Em contrapartida ao quadro configurado, as transformações do modelo processual penal tradicional não foram devidamente refletidas nos campos da dogmática e do legislativo – os quais, inclusive, corriqueiramente simplificam a temática[23]. Os perigos, por exemplo, se evidenciam nos projetos de lei sobre provas digitais para o processo penal. A diferenciação de "fonte de prova digital" para "prova digital" é imprescindível para a dogmática processual penal e o aprofundamento teórico de uma adequada cadeia de custódia da prova digital.

A partir do crescimento vertiginoso de ferramentas e o aprimoramento das tecnologias, a denominada "prova digital" (*e-evidence* ou prova eletrônica) tem sua quantidade decorrente do *boom* das plataformas e *softwares* em que o cotidiano passou a ser socializado e é denominada como "classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos"[24].

Dentre as principais características das provas digitais, destacam-se a imaterialidade e, por consequência, a sua volatilidade e fragilidade, a complexidade e a pulverização. Referente à imaterialidade, observa-se que a prova digital se apresenta como uma sequência de *bits* que independe de suporte físico – salvo para sua perceptibilidade –, de modo a exigir apenas um transportador. A intangibilidade dos dados digitais é apontada por Walden[25] como decorrente justamente da complexidade inerente à investigação informática.

Os requisitos para a aquisição da prova digital são passíveis de controle judicial, visto que o processo penal como entidade epistêmica[26] de controle tem como objetivo o uso

22 GUIMARÃES, Rodrigo R. C. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal. In Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp 1555-1588.

23 RAMALHO, David Silva. Métodos ocultos de investigação criminal em ambiente digital. Coimbra: Almedina, 2017, p. 93.

24 DELGADO MARTIN, Joaquin. Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020, p. 55.

25 WALDEN, Ian. Computer crimes and digital investigations. Oxford: Oxford University Press, 2007, p. 205 *apud* VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de doutorado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012, p. 68.

26 PRADO, Geraldo. Prova penal e sistemas de controles epistêmicos. 1.ª ed. São Paulo: Marcial Pons, 2014, p. 45.

de informações relevantes e confiáveis[27]. Contudo, pela cientificidade metodológica empregada e a pulverização em potencial de fontes de provas relevantes, questiona-se como proceder com o controle judicial quanto à metodologia de recolha da prova para uma maior qualidade e consequente valoração racional da prova digital[28]

Dentre requisitos formais dos meios de obtenção de prova digital, por exemplo, estão a fidedignidade da coleta e a cadeia de custódia da prova digital[29]. É importante reiterar as críticas quanto à inexistência de valor probatório no material colhido pelos meios de obtenção de prova, devendo ser descartado junto ao inquérito policial.

O incremento ao valor da cadeia de custódia se dá com a natureza digital do elemento probatório. As características específicas da prova digital chamam atenção para questões como a suscetibilidade de manipulação que afeta a compreensão tradicional da natureza das fontes de prova e elementos de prova, qual seja, a de "materialidade" – diferente de 'fisicalidade'[30] – já que estamos falando em dados digitais que não são corpóreos – conhecidos como verdadeiras "sequências de eletricidade 0 e 1"[31] –, e que são voláteis e frágeis, vez que podem ser copiados e clonados.

Segundo as diretrizes do *National Institute for Standard and Technology (NIST)*, as fases da computação forense envolvem a coleta de dados, seu posterior exame, a análise o relatório. Da mesma forma, o *Electronic Evidence Guide do Conselho da Europa* dispõe acerca da documentação da coleta da prova digital, e o *Internet Engineering Task Force* (IETF) e a *Association of Chief Police Officers* (ACPO).

O laudo pericial deverá conter a introdução, descrição da fonte de prova digital, o resumo do exame realizado, a individualização do sistema de arquivos examinados, a análise e os resultados da perícia, bem como a conclusão[32]. A diferenciação da cadeia de custódia com relação ao equipamento apreendido e aos dados coletados é outro ponto essencial, destacado pelo *Mobile Forensic Investigations.*

É justamente através da cadeia de custódia que serão preservados, dentre outros, os direitos fundamentais à confidencialidade e garantia da integridade de sistemas de

27 VAZQUEZ-ROJAS, Carmen. Sobre la cientificidad de la prueba científica en el proceso judicial. Anuário de Psicologia jurídica, vol. 24. enero-diciembre, 2014, pp 65-73. Colégio Oficial de Psicólogos de Madrid, Madri. Espanha, p. 68.

28 MENDES, Carlos Helder. Tecnoinvestigação criminal: entre a proteção de dados e a infiltração por software. Salvador: JusPodivm, 2020.

29 RAMALHO, David Silva. Métodos ocultos de investigação criminal em ambiente digital. Coimbra: Almedina, 2017.

30 DANIELE, Marcelo. La prova digitale nel processo penale. In Rivista di Diritto Processuale, Anno LXVI (Seconda Serie) – n. 2. Marzo – Aprile, 2011, p. 283.

31 KERR, Orin. S. Digital evidence and the new criminal procedure. 105 Columbia Law review, 2005, p. 284.

32 CASEY, Eoghan. Digital evidence and computer crime. 3.ª. Ed. London: Elsevier, 2011, p. 76.

tecnologia da informação. A complexidade inerente à multifuncionalidade dos dispositivos e aos direitos fundamentais e de personalidade, contudo, é contraposta por argumentos acerca da inexistência de direitos fundamentais absolutos[33]. Geraldo Prado destaca como o caráter constitucional da preservação da cadeia de custódia da prova digital exige que a perícia seja oficial, independente, imparcial e indelegável para entes privados[34]. Por se tratar de matéria reativa, não há possibilidade de pré-determinação de melhores diretrizes forenses, pois cada tipo de ferramenta requer uma adaptação metodológica para que haja uma perícia forense igualmente competente, e o faz a partir dos autores Ahmed e Roussev[35].

No entanto, por se tratar de matéria constitucional que exige grandes cuidados, é possível buscar melhores metodologias internacionalmente convencionadas como mais adequadas para a preservação da prova digital, tais como ISO/IEC 27037:2012 e, no Brasil, ABNT NBR ISO/IEC 27037:2013 e ISO/IEC 27037:2012.

Ainda Prado[36], com base nos ensinamentos de Heilik[37] e Taruffo[38], desenvolve sobre como a cadeia de custódia da prova digital oferece desenlaces aos pontos relacionados à integralidade, à espoliação e à volatidade do dado digital, diferenciando os dados digitais e os documentos armazenados em computadores dos tradicionais, assim como determinando formas de coleta, apresentação e valoração da como prova judicial. É por tal razão que existem técnicas específicas de perícia forense digital que permite analisar a integralidade de uma prova digital por meio dos códigos *hash* – como Prado ao afirmar que o objeto eletrônico fica vulnerável quando "não lacrado eletronicamente (hash)"[39].

Por fim, no que diz respeito à temática de encontro fortuito e, principalmente, aos perigos da prática de *fishing expedition* no acesso de dados não-abertos por meio de ferramentas de raspagem automática, reitera-se a necessidade de atentar aos requisitos de

33 EILBERG, Daniela Dora; GLOECKNER, Ricardo Jacobsen. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais / vol. 156/2019 / p. 353 – 393 / Jun/2019, p. 360.

34 PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. 2021, p. 12.

35 AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). Security, Privacy, and Digital Forensics in the Cloud. Hoboken, Singapura: John Wiley & Sons, 2019, p. 302.

36 PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. 2021, p. 18.

37 HEILIK, Jacob. *Chain of Custody for Digital Data*: A Practitioner's Guide. Canadá: Independently published, 2019, p. 15.

38 TARUFFO, Michele. *A prova*. São Paulo: Marcial Pons, 2014. p. 83-84.

39 PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. 2021, p. 23.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

continência e conexão de dados relacionados à infração penal que ensejou a investigação, sob pena de ser contrário à justa causa[40].

Isso porque, principalmente quando diz respeito à coleta da prova digital judicialmente autorizada, há possibilidade de direcionamento técnico para não coletar certos dados. Em havendo, ainda, a coleta de dados continentes e conexos, concebe-se como *fonte* de prova digital – jamais como prova digital – e, portanto, deve ser remetido como *notitia criminis* ao órgão de investigação.

IV. Tratamento de dados no processo penal

A escolha de política legislativa do Estado brasileiro de excetuar o tratamento de dados para finalidades de segurança pública, investigação criminal, defesa nacional e segurança nacional na Lei n.º 13.709 seguiu a tendência internacional[41] e possui a sua razão de ser. Ou seja, o fundamento da exceção do dispositivo 4.º da LGPD está no fato de que o levantamento de dados para o campo penal e de segurança pública possui premissa completamente diferente das demais áreas, ou seja, trata-se de coleta coercitiva[42], razão pela qual falar em consentimento não é suficiente e depende de base legal.

A proteção dos dados pessoais hoje já garantida como constitucional, inclui a garantia ao livre desenvolvimento da personalidade, qual seja, o direito à autodeterminação informacional, à confiabilidade e integridade de sistemas informáticos, ao sigilo das comunicações e inviolabilidade ao domicílio. Ou seja, a regra é de que o Estado tem o direito de abstenção com relação aos direitos de aplicação imediata (art. 5.º , §1.º , CF), razão pela qual o direito da proteção de dados é configurado como "proteção (constitucional) dos dados e não como proteção aos dados[43]. Sendo assim, por mais que os direitos fundamentais não sejam absolutos e tampouco impedem a ingerência do Estado, ao Estado de Direito exige-se a previsão de normas autorizativas (art. 5.º , II, CF) sobre as

40 SILVA, Viviani GHIZONI; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. Fishing Expedition e Encontro Fortuito na Busca e Apreensão. Florianópolis: EMais, 2019.

41 A mesma direção do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e sua diferenciação da Diretiva 2016/680– a qual regula a utilização de dados para fins de prevenção e investigação. No Brasil, uma comissão de juristas foi instituída em 2020 e elaborou o Anteprojeto da Lei Geral de Proteção de Dados. Apesar da extrema qualificação dos componentes da composição da comissão de juristas e do aprofundamento teórico e principiológico adotado na escrita de tal anteprojeto, houve a proposição de um projeto de lei n.º 1515/2021 que não contemplou todas as salvaguardas previstas no anteprojeto.

42 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. Dossiê – Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Pena. In RDP, Brasília, v.18, n. 100, p. 608.

43 GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons, 2021, p. 6.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

intervenções dos direitos fundamentais que são justamente diferenciadas daquelas que são as denominadas normas de competência[44].

Nesse sentido, compreende-se que, das normas de competência não estão derivadas as de autorização, ou seja, é preciso haver clara e importante diferenciação para que possamos compreender que o fato de uma agência ter a competência de coletar um dado não significa, em si, pode coletá-lo a qualquer custo, havendo condições para tal autorização. Nesse sentido, seriam a forma e a proporcionalidade a limitação ao poder legislativo[45].

Portanto, estamos falando em reserva de lei (legalidade) e reserva judicial (autorização judicial). Um direito que é reconhecido constitucionalmente como "inviolável" não significa "intocável" (absoluto), mas dependente de previsão legal para justificar a sua tangibilidade, como abordado por Greco ao introduzir o trabalho de Wolter[46].

O reconhecimento da autodeterminação informacional para além da abstenção do dever do Estado em relação aos dados dos cidadãos, também significa que, ao ser somada com direitos que protejam o livre desenvolvimento da personalidade representam importante contenção à vigilância, além de a reserva de lei e parlamentar serem imprescindíveis para pensarmos o tratamento dos dados no campo penal. Em sendo dessa forma, a transparência e o *accountability* são importantes princípios para o controle da gestão pública que seja transparente e que a justeza procedimental com relação às atividades de *law enforcement* e compliance sejam garantidos[47].

Após adentrarmos na coleta de dados e sua licitude, precisamos também determinar quais são as técnicas que serão utilizadas para tratar tais dados uma vez considerados lícitos. São tempos de automatização, em que a regulamentação do uso de inteligência artificial, por exemplo, é urgente. Inúmeras iniciativas internacionais, como a proposta de regulação do Parlamento Europeu e do Conselho Europeu para harmonizar as regras do uso de inteligência artificial a partir do *Artificial Intelligence Act* que emenda outras previsões legais.

44 GRECO, Luís. Introdução – o inviolável e o intocável no direito processual penal. In: WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (org.). 1.ª ed. São Paulo: Marcial Pons, 2018, p. 199.

45 GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons, 2021, p. 9.

46 GRECO, Luís. Introdução – o inviolável e o intocável no direito processual penal. In: WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (org.). 1a ed. São Paulo: Marcial Pons, 2018, p. 32.

47 BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020, pp 3-4.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

Ao mesmo tempo em que práticas automatizadas podem gerar mais eficiência à investigação, traz também maior riscos aos direitos dos titulares dos dados pessoais[48]. A era do *Big Data* permite análise massiva de dados de velocidade sem precedentes ocorre a partir das etapas de coleta de dados (de múltiplas fontes), da categorização desses (dados a partir da técnica de mineração, *data mining,* a qual busca correlação e padrões nos dados) e da interpretação (inferência de valor)[49]. Tal contexto gera questionamentos sobre a veracidade e fiabilidade dos dados, cuja afetação na análise de tais dados será consequente, bem como a suscetibilidade à volatilidade desses dados que poderão ser destruídos antecipadamente, razão pela qual se fala em preservação. No caso do Brasil, a previsão normativa da Lei Geral de Proteção de Dados dispõe sobre os princípios fundantes da proteção de dados. Precisamos essencialmente tratar os dados primando pelos princípios da finalidade, necessidade, transparência e *accountability.*

O princípio da finalidade exige que o dado coletado para um fim especifico deve ser tratado apenas para tal finalidade, razão pela qual uma autorização judicial para compartilhar um dado para um caso específico não justifica automaticamente a extensão do uso desse dado para outro caso, devendo ocorrer nova autorização judicial para respeitar a reserva jurisdicional, como bem retrataram Flaviane e Bolzan[50] e Heloisa Estellita[51] quanto à decisão do STF sobre o compartilhamento de dados bancários e fiscais.

O princípio da necessidade deve conduzir as investigações, pois a conformação da democracia está fundada em um Estado tem limites quanto ao acesso de dados da vida privada das pessoas ao tratamento do mínimo necessário, apenas para o necessário e proporcional. O impacto que tal coleta poderá acarretar riscos, principalmente se estivermos falando de dados sensíveis (como os dados biométricos) exige uma redobrada de esforços quanto à metodologia para mitigação de riscos[52], ainda mais se tais dados estiverem associados à inteligência artificial, devido à desigualdade dos poderes informacionais.

48 BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

49 DELGADO, Joaquin. Judicial-Tech, el proceso digital y la transofrmación de la justicia. Obtención, tratamiento y protección de datos en la justicia. MadridÇ Wolters Kluwer, 2020, p. 214.

50 BARROS, Flaviane de Magalhães; MORAIS, José Bolzan. Compartilhamento de Dados e Devido Processo: Como o uso da inteligência artificial pode implicar em uma verdadeira aleteica. 1.ª ed.. Salvador: Editora JusPodivim.

51 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. Dossiê – Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Pena. IN RDP, Brasília, v.18, n. 100, p. 608.

52 AMBA KAK (ed.). Regulating Biometrics: Global Approaches and Urgent Questions AI Now Institute, September 2020, Disponivel em: https://ainowinstitute.org/regulatingbiometrics.html. Acesso em: 12/2020.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

O princípio da transparência porque necessitamos combater as opacidades inerentes aos modelos computacionais para se evitar "a verdade aleteica"[53], com a necessidade de conhecer detalhadamente o *input* e o método de mineração de dados[54] para que possamos também compreender o uso do *output* para finalidade probatória, por exemplo.

O princípio da *accountability*, porque a prestação de contas responsável centra-se, na seara regulatória, neste princípio – como bem desenvolve Bioni, determina-se a responsabilização (*accountable*) da prestação de contas quanto aos riscos relacionado para se reduzir as assimetrias de poderes informacionais e para "prescrever critérios normativos"[55].

V. Considerações Finais

As ferramentas tecnológicas podem trazer inovações, mas também podem significar apenas a sofisticação dos mesmos processos e respostas. Portanto, não idializar a inovação, mas compreendê-la enquanto delineadora dos novos desafios que demandam novas respostas ou adequação de tradicionais respostas será o primeiro passo.

As bases fundantes do processo penal estão na compreensão de uma disputa acusatória que envolve paridade de armas, cujo fundamento se dá no direito à ampla defesa e ao contraditório. Portanto, as bases principiológicas quanto à licitude da prova estão constitucionalmente estabelecidas desde 1988, não havendo discussão quanto ao "regime de antijuricidade da prova".

As dificuldades da temática de aquisição probatória, quando se tratam de provas digitais, estão concebidas desde a etapa inicial de conceituação dos seus termos, uma vez que a matéria se faz extremamente novel perante às produções normativas e os seus avanços contínuos e exponenciais expõe violentamente a configuração da constante lógica da obsolescência até mesmo da temática – haja vista a incapacidade de se acompanhar as consequências da produção tecnológica a partir de uma teoria científica séria sem que se esteja referindo a algo que não mais se apresenta como de última geração tecnológica.

As transformações do modelo processual penal tradicional não foram devidamente refletidas nos campos da dogmática e do legislativo – os quais, inclusive, corriqueiramente

53 BARROS, Flaviane de Magalhães; MORAIS, José Bolzan. Compartilhamento de Dados e Devido Processo: Como o uso da inteligência artificial pode implicar em uma verdadeira aleteica. 1.ª ed. Salvador: Editora JusPodivim, p. 284.

54 BARROS, Flaviane de Magalhães; MORAIS, José Bolzan. Compartilhamento de Dados e Devido Processo: Como o uso da inteligência artificial pode implicar em uma verdadeira aleteica. 1.ª ed.. Salvador: Editora JusPodivim, p. 284.

55 BIONI, Bruno. Regulação e proteção de dados pessoais – o princípio da *accountability*. São Paulo: Forense, 2022.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

simplificam a temática[56]. Os requisitos para a recolha da prova digital devem ser passíveis de controle judicial, visto que o processo penal como entidade epistêmica[57] de controle tem como objetivo o uso de informações relevantes e confiáveis[58].

Contudo, pela cientificidade metodológica empregada e a pulverização em potencial de fontes de provas relevantes, a pergunta que se faz é: como se procederá o controle judicial quanto à metodologia de recolha da prova para uma maior qualidade e consequente valoração racional da prova informática? A resposta parece beirar alguns caminhos: i) o repúdio ao uso análogo de procedimentos propostos à prova físicas[59]; ii) a reinterpretação como uma relação tricotômica: busca-apreensão-custódia[60]; iii) a consignação de normas procedimentais específicas a essas provas, calcadas na tipicidade processual.

A questão de direitos e garantias fundamentais e sua ingerência com as novas tecnologias, que catalisam o processo de redução do seu núcleo de proteção, desperta debates quanto aos meios de investigação, as medidas cautelares probatórias, o que se configura como busca e o princípio do *nemo tenetur se detegere*. Observa-se, inclusive, o princípio da liberdade probatória em tensão constante com a *nulla coactio sine lege* e a interpretação dela feita[61].

A ausência de previsão legal de certas medidas intrusivas acaba por desaguar em um fenômeno de eufemização de institutos, com a crescente criação de categorias apartadas da sua natureza jurídica parece se tornar regra que se evidencia como desenvolvimento exponencial da tecnologia. Exigem-se renovações das concepções de antigos institutos processuais penais, de diretrizes específicas aos métodos de obtenção de fonte de prova ou, até mesmo, da compreensão de seu tratamento enquanto busca e não meio investigativo. Há que se pensar, inclusive, em uma nova concepção teórica da prova que seja capaz de abarcar essas inovações conformativas das naturezas jurídicas em jogo.

A importância do entrecruzamento das áreas salta aos olhos ao confrontarmos a legalidade penal com a fidedignidade dos meios probatórios, na compreensão de que a tipicidade processual está completamente ligada à legalidade processual (constitucional) penal.

56 RAMALHO, David Silva. Métodos ocultos de investigação criminal em ambiente digital. Coimbra: Almedina, 2017, p. 93.

57 PRADO, Geraldo. Prova penal e sistemas de controles epistêmicos. 1.ª ed. São Paulo: Marcial Pons, 2014, p. 45.

58 VAZQUEZ-ROJAS, Carmen. Sobre la cientificidad de la prueba científica en el proceso judicial. Anuário de Psicologia jurídica, vol. 24. enero-diciembre, 2014, pp. 65-73. Colégio Oficial de Psicólogos de Madrid, Madri. Espanha, p. 68.

59 MENDES, Carlos Helder Furtado. Dado informático como fonte de prova penal confiável (?) apontamentos procedimentais sobre a cadeia de custódia digital. In Revista Brasileira de Ciências Criminais, v. 161, 2019, p. 131-161.

60 GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora . Busca e apreensão de dados em telefones celulares: novos desafios frente aos avanços tecnológicos. In *Revista Brasileira de Ciências Criminais*, v. 156, 2019, p. 355.

61 SALT, Marcos. Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal. *Jornada de Trabajo*, 2017.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 123-140

Buscamos trazer os desafios relacionados ao acesso aos dados para finalidade de investigação criminal, o que exige conhecimentos básicos sobre diferenciação da metodologia e dos requisitos para a coleta de dados disponíveis em dispositivos eletrônicos, em fontes abertas, ou sob custódia de provedores de serviço. Após compreender tais desafios, buscou-se entender como serão tratados os dados, primando-se pelo embasamento principiológico da dogmática constitucional da proteção de dados.

REFERÊNCIAS

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wpcontent/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Consultado em maio de 2020.

AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). Security, Privacy, and Digital Forensics in the Cloud. Hoboken, Singapura: John Wiley & Sons, 2019.

AMBA KAK (ed.). Regulating Biometrics: Global Approaches and Urgent Questions AI Now Institute, September 2020, Disponivel em: https://ainowinstitute.org/regulatingbiometrics.html. Consultado em 15/09/2023.

BECK, Ulrich. Sociedade do risco: rumo a uma outra modernidade. São Paulo: Ed. 34, 2010.

BARROS, Flaviane de Magalhães; MORAIS, José Bolzan. Era digital e processo penal brasileiro: busca de uma nova gramática, em VALENTE, Manuel Monteiro Guedes et all (coord.). Direito e liberdade, estudos em homenagem ao prof. Nereu José Giacomolli. Coimbra: Almedina, 2022, p. 613-630.

BIONI, Bruno. Regulação e proteção de dados pessoais – o princípio da *accountability*. São Paulo: Forense, 2022.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BURREL, Jena. How the machines thinks: Understanding opacity in machine learning algorithms. Big data & society. Jan-jun 2016.

CASEY, Eoghan. Digital evidence and computer crime. 3. Ed. London: Elsevier, 2011.

DANIELE, Marcelo. La prova digitale nel processo penale. Rivista di Diritto Processuale Anno LXVI (Seconda Serie) – n. 2. Marzo – Aprile, 2011.

DELGADO, Joaquin. Judicial-Tech, el proceso digital y la transofrmación de la justicia. Obtención, tratamiento y protección de datos en la justicia. MadridÇ Wolters Kluwer, 2020.

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. Dossiê – Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Pena. In RDP, Brasília, v.18, n. 100, 606-636, out./dez. 2021.

ESTELLITA, Heloisa; GLEIZER, Orlandino. A investigação penal de insuspeitos. STJ fere direitos ao exigir coleta massiva de dados. Disponível em: 12/09/2020.

EILBERG, Daniela Dora; GLOECKNER, Ricardo Jacobsen. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais / vol. 156/2019 / p. 353 – 393 / Jun/2019.

GRECO, Luis. Introdução – o inviolável e o intocável no direito processual penal. In: WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (org.). 1a ed. São Paulo: Marcial Pons, 2018.

GUIMARÃES, Rodrigo R. C. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, set./dez. 2019, p. 1555-1588. https://doi.org/10.22197/rbdpp.v5i3.260.

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

HAN, Byung-Chul. Sociedade da transparência. Petrópolis: Rio de Janeiro, Vozes, 2017.

HIRSCH BALLIN, M.; GALIČ, M. Digital investigation powers and privacy: Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure. Boom Strafblad, 2(4), 148-159, 2021. https://doi.org/10.5553/BSb/266669012021002004007.

HEILIK, Jacob. *Chain of Custody for Digital Data*: A Practitioner's Guide. Canada: Independently published, 2019.

ILLUMINATI, Giulio. Prova digitale e ammisibilità, em VALENTE, Manuel Monteiro Guedes et all (coord.). Direito e Liberdade, estudos em homenagem ao prof. Nereu José Giacomolli. Coimbra, 2022, p. 945 a 959.

KERR, Orin. S. Digital evidence and the new criminal procedure. 105 Columbia Law review, 2005.

LEVY, Pierre. Ciberdemocracia. Lisboa: Editions Odile Jacob, 2002.

MENDES, Carlos Helder Furtado. Dado informático como fonte de prova penal confiável (?) apontamentos procedimentais sobre a cadeia de custódia digital. In Revista Brasileira de Ciências Criminais. v. 161, 2019, p. 131-161.

OLIVERIA, Arlindo. Inteligência Artificial. Lisboa: Fundação Francisco Manuel dos Santos, 2019.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital, 2021.

RAMALHO, David Silva. Métodos ocultos de investigação criminal em ambiente digital. Coimbra: Almedina, 2017.

SALT, Marcos. Obtención de pruebas informáticas en extraña jurisdicción: Los "conflictos" del principio de territorialidad en un mundo virtual sin fronteras", 2016.

SALT, Marcos. Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos. 1.ª ed. Buenos Aires: Ad-hoc, 2017.

SALT, Marcos. Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal. Jornada de Trabajo, 2017.

TARUFFO, Michele. A prova. São Paulo: Marcial Pons, 2014.

VALENTE, Manuel Monteiro Guedes, WUNDERLICH, Alexandre; EBERHARDT, Marcos; GIACOMOLLI, Felipe; SAIBRO, Henrique; STEIN, Ana Carolina (coord.). *Direito e liberdade, estudos em homenagem ao prof. Nereu José Giacomolli*. Coimbra: Almedina, 2022.

VAZQUEZ-ROJAS, Carmen. Sobre la cientificidad de la prueba científica en el proceso judicial. Anuário de Psicologia jurídica, vol. 24. enero-diciembre, 2014, pp. 65-73. Colégio Oficial de Psicólogos de Madrid, Madri. Espanha, p. 68.

WALDEN, Ian. *Computer crimes and digital investigations*. Oxford: Oxford University Press, 2007, p. 205 *apud* VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de doutorado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012, p. 68.