



UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE DIREITO

DÉBORAH DA PAZ SOUZA

**PROTEÇÃO DE DADOS E O PROCESSO PENAL: DESAFIOS E PARÂMETROS  
DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL**

BRASÍLIA

2021

DÉBORAH DA PAZ SOUZA

**PROTEÇÃO DE DADOS E O PROCESSO PENAL: DESAFIOS E PARÂMETROS  
DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL**

Monografia apresentada como requisito parcial à  
obtenção do grau de Bacharel em Direito pela  
Faculdade de Direito da Universidade de Brasília

Orientador: Prof. Dr. Ney de Barros Bello Filho

BRASÍLIA

2021

DÉBORAH DA PAZ SOUZA

**PROTEÇÃO DE DADOS E O PROCESSO PENAL: DESAFIOS E PARÂMETROS  
DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL**

Monografia apresentada como requisito obrigatório para obtenção do título de Bacharela em  
Direito pela Universidade de Brasília – UnB

**Data da defesa: 21/05/2021**

**Resultado:**

**COMISSÃO AVALIADORA**

---

Dr. Ney de Barros Bello Filho  
Orientador

---

Ms. Guilherme Gomes Vieira  
(Membro)

---

Dr. Vallisney de Souza Oliveira  
(Membro)

## **AGRADECIMENTOS**

Agradeço a Deus por tudo e por tanto.

Aos meus pais, pelo amor e apoio incondicionais.

Às minhas irmãs, Laís e Gaby, por acreditarem em mim e serem minha fonte de inspiração. Também à minha cunhada Agatha, pela generosidade comigo.

Aos meus familiares, avós, tios e primas, pelo acolhimento e pela torcida que me permitiu seguir sempre em frente.

Aos meus amigos da Faculdade de Direito da Unb, especialmente ao Antonio, Amanda, Henrique, Joyce, Victor e Thayane. Nada faria sentido sem vocês.

Aos incríveis profissionais do Gabinete do 6.º Ofício Criminal da Defensoria Pública da União, por me mostrarem o motivo pelo qual devemos persistir sempre.

Ao meu orientador, Dr. Ney de Barros Bello Filho, por aceitar embarcar nessa pesquisa junto comigo, por toda compreensão e solicitude até aqui. Agradeço também aos professores Ms. Guilherme Vieira e Dr. Vallisney Oliveira, pela disponibilidade e gentileza.

À Universidade de Brasília, por ser o lar de mais um sonho.

*“Diz-se evidente o que dispensa a prova. Simulacro de auto-referencialidade, pretensão de uma justificação centrada em si mesmo, a evidência corresponde a uma satisfação demasiado rápida perante indicadores de mera plausibilidade. De alguma maneira, a evidência instaura um desamor do contraditório”.*

*(Rui Cunha Martins, O ponto cego do direito, 2011)*

## RESUMO

A sociedade de informação e a revolução tecnológica rompem com as referências tradicionais de todos os aspectos da experiência humana. Como um produto dessas transformações, a prova digital é um elemento cada vez mais presente nos processos penais, sendo a observação da sua cadeia de custódia um requisito essencial para sua admissibilidade. Por essa razão, busca-se, no presente estudo, suscitar as características distintivas da prova digital e suas implicações na construção de uma metodologia adequada e coerente a ser seguida na definição de um conjunto de procedimentos que sejam compatíveis com essa nova categoria probatória. Conclui-se que já existem parâmetros a serem seguidos para uma correta manipulação desses vestígios. Além disso, a elevação da confiabilidade e integridade dos sistemas informáticos como um novo direito fundamental, denotam a importância de um tratamento especial da cadeia de custódia na esfera digital. Para esse propósito são abordados, num primeiro momento, a própria contextualização da sociedade informacional e dos meios investigativos e probatórios, seu peso nas decisões judiciais e suas inflexões com a busca da “verdade real”. No segundo capítulo, trata-se especificamente das particularidades da prova digital e, em um segundo plano, discussões acerca da teoria das ilicitudes e a nova causa de impedimento por contaminação do juiz. Por fim, o terceiro capítulo discorre sobre os conceitos, importância e métodos da cadeia de custódia para garantir a fiabilidade de uma prova digital. Depreende-se, assim, que a segurança da informação nos sistemas informáticos, num cenário em que a proteção de dados ganha especial relevância, devem ser interpretados como um direito fundamental. Para isso, essa pesquisa utilizou-se de referenciais teóricos de países com doutrina e legislação mais avançada sobre o tema, artigos interdisciplinares da computação forense e ainda autores nacionais, conhecidos por promoverem o debate acerca do tema no país.

**Palavras-chave:** Cadeia de custódia; Prova digital; Direito fundamental a confiabilidade dos sistemas informáticos; Investigação criminal tecnológica.

## ABSTRACT

The information society and the technological revolution are breaking the traditional references of all aspects of human experience. As a product of these transformations, digital evidence is an increasingly present element in criminal proceedings, and the observation of its chain of custody is an essential requirement for its admissibility. For this reason, this study seeks to raise the distinctive characteristics of digital evidence, and its implications in the construction of an adequate and coherent methodology that are compatible with this new evidential category. It is concluded that there are already parameters to be followed for the correct handling of these traces. Moreover, the elevation of the reliability and integrity of computer systems as a new fundamental right denotes the importance of a special treatment of the chain of custody in the digital sphere. For this purpose, the very contextualization of the information society and the investigative and evidential means, their weight in judicial decisions, and their inflections with the search for the “real truth” are approached in a first moment. The second chapter deals specifically with the particularities of digital evidence and, in a second level, discussions about the theory of illicitness and the new cause of impediment due to contamination of the judge. Finally, the third chapter discusses the concepts, importance, and methods of the chain of custody to ensure the reliability of digital evidence. Thus, it is clear that information security in computer systems, in a scenario where data protection gains special relevance, must be interpreted as a fundamental right. To this end, this research used theoretical references from countries with more advanced doctrine and legislation on the subject, interdisciplinary articles on forensic computing, and also nationally known authors known for promoting the debate on the subject in the country.

**Keywords:** Chain of custody; Digital evidence; Fundamental right to the trustworthiness of information systems; Technological criminal investigation.

## **LISTA DE ABREVIATURAS**

ABNT - Associação Brasileira de Normas Técnicas

BSG - Bundessozialgericht

CNJ - Conselho Nacional de Justiça

COVID - Corona Virus Disease (Doença do coronavírus)

CP - Código Penal

CPP - Código Processo Penal

GPS -Global Positioning System (sistema de posicionamento global)

IEL - Companhia elétrica nacional

IP - Internet Protocol (protocolo de internet)

ISO - Organização Internacional de Padronização

TJSP - Tribunal de Justiça do Estado de São Paulo

REsp - Recurso Especial

SARS-Cov-2 - Severe Acute Respiratory Syndrome Coronavirus 2 (síndrome respiratória aguda grave do coronavírus 2)

## SUMÁRIO

<b>INTRODUÇÃO</b>	10
<b>1 NOVOS MEIOS PROBATÓRIOS ADVINDOS DA REVOLUÇÃO DIGITAL: O PANORAMA DO IMPACTO DAS NOVAS TECNOLOGIAS NO PROCESSO PENAL</b>	<b>13</b>
1.1 Sociedade informacional e o direito penal e seu impacto na legislação criminal brasileira	13
1.1.1 Os novos métodos investigativos e meios probatórios da era digital	18
1.1.2 As provas obtidas por métodos ocultos e infiltração por software	23
<b>2 A EXPERIÊNCIA PROBATÓRIA NO UNIVERSO DIGITAL</b>	<b>29</b>
2.1 A prova digital enquanto nova categoria: conceito e características singulares	29
2.2 A relação entre prova e verdade processual: a desmistificação da busca da verdade real e a necessidade de filtragem epistêmica da prova	34
2.2.1 A inadmissibilidade de provas ilícitas: A causa de impedimento por contaminação do juiz	39
<b>3 A CONFIABILIDADE DOS DADOS PROBATÓRIOS: A PRESERVAÇÃO CADEIA DE CUSTÓDIA NO CIBERESPAÇO E A SEGURANÇA DA INFORMAÇÃO</b>	<b>42</b>
3.1 A cadeia de custódia da prova digital: conceitos, fundamentos e riscos de sua quebra	
3.1.1 Parâmetros técnicos atuais de segurança da informação e fiabilidade dos vestígios no ambiente digital	47
3.2 O direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos: Segurança da informação e proteção de dados na persecução criminal	53
<b>CONSIDERAÇÕES FINAIS</b>	<b>58</b>
<b>REFERÊNCIAS</b>	<b>60</b>

## INTRODUÇÃO

*“A pós-verdade é uma forma de supremacia ideológica, por meio da qual seus praticantes tentam convencer alguém a acreditar em algo, independentemente da existência de evidências”<sup>1</sup>. (Lee McIntyre)*

A sociedade informacional promoveu profundas mudanças na forma como as instituições e os indivíduos se relacionam entre si. O advento da internet e das novas tecnologias de informação, particularmente, inserem-se tão intensamente na vida individual e coletiva que, muitas vezes, torna-se impensável valorar certos aspectos da vida social sem, necessariamente, considerar o arcabouço tecnológico como componente de análise.

Nesse cenário, em que há um aumento exponencial na quantidade de processamento de informações, encontramos-nos mergulhados em discussões em torno da veracidade, autenticidade e problemas das fontes dos conteúdos encontrados no ambiente virtual. O processo penal, a esse propósito, não se mantém à margem — é, aliás, especialmente sensível a essa realidade — seja pela postura de busca da “verdade real” adotada pelos seus magistrados e, mais ainda, pela característica de *ultima ratio* do direito penal, em razão do severo impacto nas liberdades individuais dos sujeitos condenados nessa esfera.

A cadeia de custódia da prova, nesse sentido, enquanto conjunto de procedimentos destinados justamente a resguardar a veracidade e integridade do meio probatório, só foi devidamente regulamentada em 2019, por meio do Pacote Anticrime (Lei 13.964), o qual já nasce pendente de atualização e complemento, por deixar de oferecer as condições de procedibilidade, confiabilidade e proteção das informações investigativas obtidas por meios cibernéticos.

Além disso, a discussão a respeito da proteção de dados no Brasil ganha novo fôlego após a vigência da Lei Geral de Proteção de Dados (Lei 13.709/18), em agosto de 2020, a qual estabeleceu um novo paradigma no âmbito do tratamento de dados pessoais. A partir desse marco, o Brasil passou a fazer parte de um rol composto por mais 100 países que se preocupam em delimitar a forma, condições de coleta, armazenamento e cuidados dos dados pessoais.

---

<sup>1</sup> Tradução livre. No original: “Post-truth amounts to a form of ideological supremacy, whereby it practitioners are trying to compel someone to believe in something whether there is good evidence for it or not” (McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018. p. 12).

É de se notar, no entanto, que houve expressa vedação no âmbito dessa lei no que diz respeito ao tratamento de dados sobre a segurança pública, defesa nacional, segurança do Estado ou atividades de investigação criminal e repressão de infrações penais por pessoas de direito privado (com exceção daqueles relativos a procedimentos de pessoas jurídicas de direito público). Por essa razão, iniciaram-se estudos e debates para a criação de uma lei específica para a proteção de dados que digam respeito à persecução penal e segurança pública (denominada “LGPD penal”), a qual já conta com um anteprojeto, inespecífico em relação ao tema da cadeia de custódia.

À vista disso, o estabelecimento de parâmetros transparentes e a reafirmação da importância de se estipular os aspectos técnicos que conferem a autenticidade e integridade que devem acompanhar uma prova obtida por meio digital (como exemplo, cito aquelas provenientes de smartphones, emails, dados em nuvens, etc.) mostra-se evidente. Com efeito, negligência metodológica deve implicar na nulidade e na impossibilidade de valorá-las prejudicialmente a um indivíduo numa persecução penal (nesse ponto, vale assinalar a imprescindibilidade da causa de impedimento imposta ao magistrado que tiver contato com provas ilícitas). No mesmo horizonte, além de uma correta preservação de vestígios, a definição procedimental é condição necessária ao respeito de diversos outros direitos fundamentais, como a privacidade, intimidade, identidade e domicílio digital, bem como a autodeterminação informacional.

Diante disso, observa-se a relevância da discussão, no contexto da emergência da temática na atividade dos diversos atores do sistema de justiça, na formação de peritos tecnicamente qualificados, perante o seu potencial violador de garantias e direitos tanto das vítimas, quanto dos acusados submetidos à esfera do direito penal. O descompasso legislativo e jurisprudencial reafirmam tal importância.

Além disso, o tema da proteção de dados, em observância às decisões do Tribunal Constitucional da Alemanha, requer um olhar aprimorado em relação à segurança da informação, de maneira que o direito à confiabilidade e integridade dos sistemas informáticos ganham o *status* de direito fundamental. Nesse ínterim, o debate recente no Supremo Tribunal Federal também reconheceu a proteção de dados como direito fundamental autônomo.

A esse propósito, realizo uma análise da literatura mais recente em relação a métodos e procedimentos probatórios no ambiente virtual, e de autores consagrados no âmbito da definição e estabelecimento da cadeia de custódia. Ademais, utilizam-se artigos interdisciplinares no âmbito da perícia computacional como uma base teórica importante nesse sentido.

Sendo assim, neste trabalho, intenta-se, primeiramente avaliar o contexto probatório na sociedade informacional e seus impactos na justiça criminal, com a sinalização dos meios probatórios advindos da revolução digital, a importância da cadeia de custódia no processo penal e os efeitos advindos de sua quebra, com a teoria da ilicitude das provas no paradigma da busca pela “verdade real”. A partir disso, debater-se-á o atual tratamento da cadeia de custódia com o apontamento das novidades legislativas e suas lacunas. Por fim, enfrenta-se o tratamento existente no tema, por influência das discussões travadas na Corte Constitucional da Alemanha, para a concretização do direito fundamental à confiabilidade e integridade de sistemas informáticos.

Dessa forma, no primeiro capítulo, localizaremos o contexto da sociedade informacional e seus reflexos no processo penal, perpassando pelos problemas do mito da verdade real e, nesse sentido, o surgimento da prova digital. Após, no segundo capítulo II, enfrenta-se a prova digital enquanto uma categoria de prova independente, destrinchando suas características, singularidades e novas problemáticas, além de afirmar um novo olhar a teoria das ilicitudes. No capítulo III, adentra-se no atual tratamento da cadeia de custódia, seus parâmetros técnicos no âmbito digital, seu atributo de direito fundamental, e a sua importância na construção de um processo penal legítimo e que respeite as garantias fundamentais dos indivíduos.

# 1 NOVOS MEIOS PROBATÓRIOS ADVINDOS DA REVOLUÇÃO DIGITAL: O PANORAMA DO IMPACTO DAS NOVAS TECNOLOGIAS NO PROCESSO PENAL

*"O uso seletivo de fatos que favorecem uma posição, e a completa rejeição de fatos que a contestam, parecem partes integrantes da realidade da pós-verdade".<sup>2</sup>(Lee McIntyre)*

## 1.1 Sociedade informacional e o direito penal e seu impacto na legislação criminal brasileira

O processo penal é o reflexo da sociedade na qual ele está inserido. A própria discussão em torno do modelo processual adotado, seja ele acusatório, inquisitório ou misto, está envolto nas características socioeconômicas, políticas e culturais de um determinado país. No mesmo sentido, se a sociedade passa a enfrentar uma eclosão de novas tecnologias de informação, é inafastável seu reverberio nos campos do direito e processo penal.

O impacto e o poder da informação atingem uma proporção de tal forma estrutural e paradigmática nas concepções, relações (econômicas e sociais) e vivências humanas, que Schwab<sup>3</sup> conclui que estamos diante de uma quarta revolução industrial, cujas transformações são incomparáveis a qualquer outra já experienciada. Em verdade, o autor traz à tona sua preocupação em como lidaremos com a revolução tecnológica se continuarmos com um modo de pensar linear tradicional e imediatista ou ainda se adotaremos uma postura incompatível com as dimensões das transformações que vivemos.<sup>4</sup>

Por essa razão, nasce a necessidade cabal de se romper com antigas metodologias para distinguir o momento vivido de qualquer outro momento histórico. Schwab<sup>5</sup> traça três características fundamentais dessa nova fase da vida em sociedade. A primeira delas refere-se à velocidade, porquanto desenvolve-se em um ritmo verdadeiramente exponencial, notadamente no seu potencial criador de novas ferramentas; em segundo lugar, pontua-se a

---

<sup>2</sup> Tradução livre. No original: "The selective use of facts that prop up one's position, and the complete rejection of facts that do not, seems part and parcel of creating the new post-truth" (McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018. p. 32).

<sup>3</sup> SHWAB, Klaus. **A quarta revolução industrial**. São Paulo. Edipro. 2016. p. 16.

<sup>4</sup> Ibidem.

<sup>5</sup> Ibidem. p. 15-16.

amplitude e profundidade, pois se insere em todas as camadas e esferas das relações econômicas e humanas; o terceiro e último aspecto, de forma mais geral, o impacto sistêmico, conclama seu espaço na medida em que ocorre “a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda sociedade”.<sup>6</sup>

Dentre as distinções necessárias das transformações ocorridas, Castells<sup>7</sup> pontua que o que torna a revolução tecnológica singular e disruptiva é também o modo lida com as informações que produz e coleta, não utilizando-se, portanto, de mecanismos que busquem centralizá-las, mas de maneira que inovações acabam por impulsionar a criação e o desenvolvimento de outras, num ciclo que se retroalimenta. Nesse sentido, é de se considerar o volume de informações fabricadas como fruto da própria dinâmica de criação e expansão desse novo momento histórico.

O processo e o direito penal, assim, passam a incorporar diversos elementos que decorrem das transformações tecnológicas da sociedade. Como exemplo, as discussões recentes da Suprema Corte em relação ao direito ao esquecimento,<sup>8</sup> que tiveram como palco este direito dentro espectro dos direitos de personalidade e, portanto, civilistas, mas cujo pano de fundo demonstra seus reflexos no âmbito da persecução e da sua relação criminal intrínseca entre o desenvolvimento das novas tecnologias de informação e seus reflexos no processo penal.

No âmbito legislativo penal, as primeiras inferências delineadas por esse paradigma foram nas leis nº 11.689/2008, 11.690/2008, 11.719/2008 e 11.900/2009, as quais introduziram a possibilidade do interrogatório do réu por videoconferência em casos específicos, bem como abriu também a possibilidade da utilização desse mecanismo para a oitiva de testemunhas. Pontua-se também a comunicação do ofendido por meios eletrônicos, além de diversos tipos de registro através do audiovisual, como os registros de depoimentos.<sup>9</sup>

<sup>6</sup> SHWAB, Klaus. **A quarta revolução industrial**. São Paulo. Edipro. 2016. p. 16.

<sup>7</sup> CASTELLS, Manuel. **A sociedade em rede**. 8. ed. rev. e ampl. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 2005. V. 1. p. 68-69.

<sup>8</sup> Refere-se especificamente aqui a tese de Repercussão Geral 786, firmada em fevereiro de 2021, tendo como *leading case* o caso “Aída Curi”. Na ocasião consignou-se : “É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social - analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível”. Em julgado anterior, o STJ proferiu entendimento, no REsp nº1.334.097, cujo caso era o da “Chacina da Candelária”, a considerar o esquecimento, mesmo em situações que comprovadamente ocorreram, como um direito do acusado.

<sup>9</sup> COSTA, Fabrício. O processo penal da sociedade da informação: As recentes reformas do Código de Processo Penal e o Direito fundamental à jurisdição criminal efetiva. **Revista brasileira de meio ambiente digital e sociedade da informação**. São Paulo, v. 1, n. 2, p. 73-223, jul./dez. 2014. p. 3. Disponível em: <https://revistaseletronicas.fmu.br/index.php/rbmad/article/view/617/737>. Acesso em: 23 de mar de 2021, p. 3.

A esse respeito, Fabrício Costa<sup>10</sup> assinala que essas alterações visam, em um primeiro quadro, o alinhamento com o princípio da celeridade processual conforme previsto no art. 5º, LXXVII da Constituição Federal, reduzindo assim custos processuais e tempo de trâmite, ao mesmo tempo, em que é uma resposta e uma correspondência às demandas dos novos tempos e de uma sociedade que necessita da assimilação de novas tecnologias. No mesmo sentido, faz parte de uma concretização dos anseios do Programa Sociedade da Informação, instituído pelo Decreto n. 3.294/1999.

No que se refere ao adentramento de métodos tecnológicos no Código Penal, cita-se a inserção dos parágrafos 4º e 5º ao art. 122, majorando o tipo penal que prevê a instigação, induzimento ou auxílio aos suicídios, quando esses se dão por meio do auxílio ou transmissão pela rede mundial de computadores, ou ainda quando o agente for o coordenador do grupo virtual. No ano de 2012, com a Lei nº 12.737, também conhecida “Lei Carolina Dieckmann”,<sup>11</sup> houve a tipificação de crimes informáticos, como a prática de *hackers*, de violação de computadores, roubo e exposição de senhas e conteúdos privados.

No campo processual penal, no entanto, seus impactos possuem menores dimensões. Vale-se aqui do exemplo relativo à interceptação das informações telemáticas e das implementações ocorridas com o Marco Civil da Internet e o uso de dados de servidores e provedores de conexão para fins probatórios, bem como a ampliação da figura do agente infiltrado virtual nos crimes contra a dignidade sexual da criança e adolescente, inserido pela Lei Anticrime na Lei federal 12.850/2013.<sup>12</sup>

No tocante às videoconferências, Cesari diz que as reverberações podem ser sentidas também nos registros audiovisuais, os quais permitem uma transcrição e replicação muito

---

As discussões em torno da incidência das novas tecnologias no processo penal também levam-nos a refletir sobre suas potencialidades, ou mesmo suas vantagens para o decorrer processual e investigativo, de modo que Fabrício Costa reflete sobre o Direito fundamental à uma jurisdição criminal efetiva nessas reformas, dado que essas transformações vão ao encontro com as mudanças decorrentes com a sociedade de informação e abrem o caminho para o debate dos limites da aplicação das tecnologias no processo penal. Por essa razão, parte da doutrina defende que essas alterações acabam por violar as garantias da ampla defesa e do contraditório do acusado, e representam, na verdade, uma maior fragilidade do sistema criminal. O autor intenta, nesse sentido, traçar a conformidade constitucional e a ponderação dos princípios em conflito, com foco nos institutos do interrogatório por videoconferência e a degravação do registro do interrogatório do acusado e das testemunhas. Por fim, conclui que os direitos dos indivíduos devem ser ponderados aos da coletividade, no que refere a uma prestação jurisdicional efetiva, de modo a permitir a assimilação das novas tecnologias no processo penal

<sup>10</sup> Ibidem.

<sup>11</sup> O nome dado à lei decorre como o nome da atriz Carolina Dieckmann, em razão da invasão de *hackers* ao seu email, com o conseqüente vazamento de suas fotos íntimas.

<sup>12</sup> FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 3. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 03 abr. 2021. Apontamentos sobre a cadeia de custódia da prova digital.

mais fidedigna de acontecimentos, a realização de audiências à distância, “impactando diretamente a maneira de entender a dialética procedimental e a própria noção de ‘ouvir’”.<sup>13</sup>

O contexto da pandemia de Covid-19, decretada no ano de 2020, colocou à prova sensivelmente essa nova metodologia dentro do Poder Judiciário, visto que tornou inevitável o seu uso em situações antes não consideradas, como o interrogatório do réu solto, como medida para evitar a disseminação do vírus da Sars-CoV-2. Na Resolução nº 329<sup>14</sup> do Conselho Nacional de Justiça (CNJ), ao discorrer sobre a necessidade das videoconferências para a continuidade da prestação jurisdicional, adiciona a restrição da sua utilização na audiência de custódia, porquanto incompatível com a própria essência do instituto<sup>15</sup>. Em abril de 2021, o Senado também derrubou o veto parágrafo primeiro do artigo 3-B da Lei 13.963/19, que previa somente a audiência de custódia de forma presencial.

A harmonização de soluções emergenciais necessárias ao enfrentamento ao quadro imposto pela pandemia, alude às controvérsias também presente no rito do Tribunal do Júri, uma vez que se trata de processo complexo e repleto de formalidades, muitas vezes incompatíveis com a virtualização de seu procedimento. Ficam deficientes, nessas circunstâncias, a garantia do sigilo das votações, a incolumidade dos jurados, além de prejudicar a argumentação e auto-defesa e a própria especialidade dada pela legislação vigente ao ritual especial do júri.

Esse universo de ineditismo possui desdobramentos também nas táticas policiais e na esfera investigativa. Atualmente, o grau de precisão, eficácia e quantidade de informações obtidas através das novas tecnologias ultrapassam qualquer possibilidade existente pré-internet e sistemas de geolocalização.<sup>16</sup> No âmbito das novas inteligências de controle, a

---

<sup>13</sup>CESARI, Claudia. Editoriale: L’impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite. **Rev. Bras. de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p. 1.170, set./dez. 2019.

<sup>14</sup>CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 329 de 30 de julho de 2020**. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3400>. Acesso em: 20 fev. 2021.

<sup>15</sup>A vedação da audiência de custódia por videoconferência é, na verdade, um tema de controvérsias, tendo sido o instituto de forma não presencial, mesmo durante a pandemia somente, por ocasião da derrubada do veto do pacote anticrime. O atual presidente do Supremo Tribunal Federal, ministro do Luiz Fux é um ferrenho crítico a decisão. Ocorreu que estudos apontam que é impossível garantir um adequado controle de atividade judicial de modo online, nem o evitamento de eventuais violações graves a direitos, como os casos de tortura. O Escritório das Nações Unidas para Drogas e Crimes (UNODC), inclusive também proíbe essa modalidade.

<sup>16</sup>Existe até mesmo a possibilidade de infiltração em um dispositivo através do uso de malwares, para assim criar uma, como aponta Claudia Cesari “interceptação onipresente e multifuncional, capaz de fornecer uma enorme quantidade de informações e dados, não comparáveis ao que poderia ser obtido da tradicional ‘interceptação telefônica’ (tradução livre do original “un’intercettazione ubiquitaria e polifunzionale, capace di offrire al processo un’enorme mole di informazioni e dati, non comparabile a quella che si poteva trarre dalla tradizionale ‘intercettazione telefonica’”). CESARI, Claudia. Editoriale: L’impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite. **Rev. Bras. de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p. 1172, set./dez. 2019.

“pulseira eletrônica” impõe-se com maior êxito como mecanismo de vigilância contínua e como meio de cumprimento de ordens de restrição e proteção às suas respectivas vítimas.<sup>17</sup>

Nesse contexto, faz-se forte o potencial da “justiça preditiva”, tanto da atuação policial como dos magistrados. No âmbito internacional, inclusive, várias cidades ao redor do mundo já adotam há alguns anos sistemas de cruzamentos de dados que possibilitam o policiamento preditivo, o qual consiste, em linhas gerais, no monitoramento tanto do ambiente físico, quanto do virtual, para então identificar padrões que possam indicar os indivíduos em que deve-se pairar a suspeita do cometimento de crimes.<sup>18</sup>

Em uma realidade não muito distante, conforme já se presencia no sistema norte-americano, concerne à utilização desses dados na forma de algoritmo na formação das decisões e convecção dos juízes, tanto no que se refere à perspectiva de uma eventual reincidência e fuga, como nos aspectos da dosimetria da pena. A proteção da propriedade intelectual do programa que fornece tais elementos, como muito bem mostrou a experiência dos Estados Unidos,<sup>19</sup> mostrou a relevância dessa problemática, enquanto tais informações podem se tornar inacessíveis à defesa e comprometer sua capacidade de responder a tais questionamentos, considerando ainda o peso psicológico que esses dados podem revelar-se numa sociedade altamente cientificista, ao mesmo tempo em que o direito à ampla defesa exige transparência e compreensão total das ferramentas utilizadas.

Vislumbra-se, portanto, um cenário cheio de riscos, possibilidades e, até mesmo, benefícios para o sistema de justiça criminal. O atual ambiente normativo, no entanto, embora não seja alheio em completo para essas mudanças, mostra-se em um descompasso significativo com as adições tecnológicas, o que resulta em possíveis inconformidades com direitos fundamentais e garantias dos indivíduos. Assim, busca-se resgatar os meios probatórios e investigativos já em utilização, no próximo tópico, e as problemáticas decorrentes no paradigma do Estado democrático de Direito.

---

<sup>17</sup> Ibidem.

<sup>18</sup> REIS, Brenda S.R. As adições tecnológicas ao processo penal: policiamento preditivo. Disponível em: <http://icp.org.br/Jovem/ComaPalavra/34>. Acesso em: 24 mar. 2021.

<sup>19</sup> Nos Estados Unidos o tema ganhou debate acalorado, com o caso *Estado vs Loomis*, oportunidade em que foi proferida “uma decisão conhecida e polêmica, que tem o uso de algoritmos seja permitido na sentença, desde que não exclusivamente, sendo de fato útil para garantir a aterrissagem de uma decisão individualizada, suficiente para garantir o direito de defesa que isso pode refutar sua confiabilidade, recorrendo ao manual do usuário da ferramenta”. CESARI, Claudia. Editoriale: L’impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite. **Rev. Bras. de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p.117, set./dez. 2019.

### 1.1.1 Os novos métodos investigativos e meios probatórios da era digital

A dinâmica de mudanças não lineares, sucessivas e constantes em que se depara a humanidade torna imprescindível que se pense o Direito em tempos de inigualáveis transformações. Essas modificações reverberam-se decididamente na criminalidade, na investigação criminal, na identificação de vestígios, e assim na racionalidade que as acompanham. Por essa razão, é importante que se enfrente o atual estado da arte desses aspectos da persecução penal, considerando ainda a tensão existente tanto em relação a seu alcance e efeito para o sistema, quanto ao indivíduo propriamente considerado.

Ressalta-se não pretender neste tópico destrinchar todos os atuais meios investigativos e probatórios originados das tecnologias de informação, visto que são muitos e em constante expansão, mas pontuar algumas problemáticas nos principais e mais usuais métodos que surgiram nesse sentido, descolados de previsões legais, além de indicar aqueles que estão envolvidos em discussões nos tribunais brasileiros. Dessa maneira, vemos no trabalho investigativo a adição de controles por geolocalização (GPS), para monitorar e encontrar suspeitos, a utilização de dados informáticos (senhas, fotos, IPs, dados em nuvem e e-mails, redes sociais) e por servidores de internet, mensagens enviadas e recebidas por aplicativos de mensagens instantâneas (o mais conhecido deles, *whatsapp*).

O Estado, nesse novo paradigma de tantas possibilidades de repressão penal, não raro ultrapassa os parâmetros constitucionais em relação à proteção da vida privada e legalidade penal, ao mesmo tempo em que caminha vagorosamente em estipular critérios e mecanismos que garantam a égide desse núcleo essencial de direitos.<sup>20</sup> Um exemplo, nesse sentido, seria a capacidade dos equipamentos tecnológicos de ultrapassarem os limites estabelecidos num sistema de garantias penais. No horizonte do controle por geolocalização, por exemplo, embora requeira-se uma delimitação de locais específicos, coleta-se, na realidade, uma série de informações, muito além do espectro do que seria considerado proporcional.<sup>21</sup>

---

<sup>20</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1 ed. São Paulo, Marcial Pons, 2014. p. 59.

<sup>21</sup> No ponto, cabe dizer que a proporcionalidade “é uma relação entre a ação do Estado e os efeitos sobre o indivíduo: de um lado está o tamanho da intervenção na esfera individual e, do outro, a finalidade, a idoneidade, a necessidade e a adequação da medida para a produção do resultado pretendido (relação finalidade-meio), ou seja, se a finalidade da intervenção está em uma relação equilibrada com os danos sofridos pelo titular do direito”, conforme o que explica Orlandino Gleizer, em análise sobre a busca estatal por informações digitais e a intervenção em direitos fundamentais, disponível em: <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-2-12082019>.

Um caso ilustrativo que esbarra nessa problemática se trata do assalto à Prosegur, ocorrido em Ribeirão Preto (São Paulo), em que o magistrado solicitou os dados das contas de celular ativas ao Google, Microsoft e Apple, de todos os que transitaram num raio de 500 metros, nas datas de 2 a 5 de julho de 2016 nos horários das 13 às 19 horas.<sup>22</sup> Na ocasião foram requisitadas

a relação dos locais salvos pelos usuários no Google Maps (aplicativo de mapa e GPS no celular), o histórico de localização e deslocamento nos últimos 30 dias, a atividade das respectivas contas nos últimos 30 dias, o Internet Protocol (IP) dos aparelhos telefônicos, data e hora dos acessos (logins), marca e modelo dos celulares, número telefônico do dispositivo, as fotos armazenadas nos últimos 30 dias no Google Fotos (plataforma de armazenamento de fotos), e todas as senhas armazenadas no serviço [passwords.google.com](https://passwords.google.com).<sup>23</sup>

Em segunda instância, a decisão foi parcialmente mantida, oportunidade em que a 4ª Câmara de Direito Criminal do Tribunal de Justiça de São Paulo (TJSP), indeferiu apenas a extensão em 500 metros das proximidades do imóvel e as senhas que poderiam ser acessadas. Esse não foi um caso isolado, embora muitas dessas decisões acabem por serem revistas pelos Tribunais, vê-se um aumento em fundamentações genéricas que não citam especificamente quais são os investigados ou os crimes a serem apurados com a medida interventiva.

Na mesma linha do posicionamento adotado no âmbito da geolocalização, Orlandino Gleize<sup>24</sup> verifica a compatibilidade de 4 julgamentos<sup>25</sup> que exploram a relação conflituosa existente entre medidas interventivas telemáticas e os direitos fundamentais que orbitam a questão. Cita-se, assim, o sucedido em Santa Fé do Sul (São Paulo), no qual ocorreram furtos de caminhões, o que levou o pedido ao Google, Apple e Waze de tais dados armazenados nos servidores da empresa. Na circunstância, também se envolvem informações de terceiros

<sup>22</sup> COURA, Kalleo; LEORATTI, Alexandre. Juízes ordenam quebra de sigilo de sigilo com base em localização. Disponível em: <https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao-27052019>. Acesso em: 03 mar. 2021.

<sup>23</sup> COURA, Kalleo; LEORATTI, Alexandre. Juízes ordenam quebra de sigilo de sigilo com base em localização. Disponível em: <https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao-27052019>. Acesso em: 03 mar. 2021.

<sup>24</sup> Cf. GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019> ( parte I) e <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-2-12082019> (parte II.)

<sup>25</sup> Os casos são aqui abordados aqui abordados de maneira ampassã, uma vez a complexidade e detalhamento deles fogem ao escopo do capítulo de assinalar um panorama geral, portanto para mais informações, recomenda-se a leitura da análise completa de feita por Orlandino Gleize, além da matéria jornalística completa do JOTA, confirme respectivos endereços apontados acima.

alheios à investigação. Em Catanduva (São Paulo), permitiu-se o acesso da localização em delitos de homicídios, de modo que, na medida que foi deferida, o juiz “também autoriza tais medidas interventivas sem individualização dos possíveis alvos, criando a possibilidade de afetação de inocentes não-suspeitos”.<sup>26</sup>

Nesse ponto, Gleize reforça o grande espaço criado para intervenções sem fundamento legal, tendo em vista que elas, em sua visão, significam uma representação da oposição dos fundamentos mais caros a um Estado de Direitos, ao mesmo tempo em que levanta o fato de haver terceiros inocentes não diretamente relacionados, o que representa uma clara arbitrariedade, pois não há menção a preocupação em justificar a necessidade da medida. Assim, ressalta que os Direitos Fundamentais já devem trabalhar como limitadores importantes de qualquer medida interventiva, sendo que quando se está diante de terceiros não-envolvidos, os motivos a uma ocorrência dessa natureza devem ser ainda mais evidentes.<sup>27</sup>

Por último, na investigação do caso Marielle Franco, foi possível ter acesso ao espaço digital dos dispositivos, conhecidos como nuvens, pertencentes a terceiros ou investigados, de forma que foi possível acessar uma enorme quantidade de informações como, por exemplo, um extenso conteúdo de ordem pessoal e histórico de buscas online. Dessa forma, Orlandino Gleize registra que

no caso Marielle Franco, a intervenção na esfera de terceiros atingiu números extraordinários (318 pessoas com fluxo de telecomunicação interceptado e 670 contas de usuários de internet analisadas), a indicar que não apenas a ideia de reserva legal mas também a de proporcionalidade parece ainda não ter sido verdadeiramente compreendida por nós.<sup>28</sup>

O que percebe, no que diz respeito à investigação criminal, é que sob o manto de combate à criminalidade,<sup>29</sup> adere-se cada vez mais a métodos invasivos, arbitrários e emergências, os quais constantemente ameaçam direitos fundamentais, além de ser o

---

<sup>26</sup> COURA, Kalleo; LEORATTI, op. cit.

<sup>27</sup> GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019>. Acesso em: 20 de abr de 2021.

<sup>28</sup> Idem. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal (parte II). Disponível em <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-2-12082019>.

<sup>29</sup> Inclusive, no caso citado do assalto à Prosegur, a juíza Ilona Cruz, da 5ª Vara Criminal de Ribeirão Preto, deferiu integralmente a medida que requiritava a quebra de sigilos, justificando que “A forma audaciosa na perpetração do crime denota complexa organização criminosa de modo que nesse momento não se mostram suficientes os meios tradicionais de obtenção de provas”.

principal propulsor de mudanças legislativas que ocorrem no processo penal.<sup>30</sup> A incidência de novas tecnologias, com o aperfeiçoamento de possibilidades investigativas e a proibição de produção de provas contra si, traz ainda, conforme será tratado mais detalhadamente no capítulo sobre métodos ocultos de investigação, o desmantelamento do princípio *nemo tenetur*; impedindo uma maior delimitação desse tipo de coação imposta ao indivíduo.<sup>31</sup>

Cabe dizer que a investigação criminal que se utiliza de procedimentos digitais informáticos não tem sua atuação limitada ao combate à criminalidade organizada, ou mesmo ao ambiente de crimes propriamente virtuais ou que necessitam desse ambiente para sua concretização, mas toda e qualquer infração delitativa. Isso ocorre porque em geral são ferramentas muito mais eficientes e não necessariamente mais efetivas, embora seja esse o argumento principal para justificar a metodologia adotada, de modo que atinge também a produção probatória, direta ou indiretamente, de ilícitos tradicionais.<sup>32</sup> A esse respeito, Juan Carlos Ortiz explica:

[...] A importância de aumentar a capacidade das autoridades no uso de quaisquer medidas de investigação tecnológica voltadas para a obtenção dessa informação em formato digital parece um pilar essencial em qualquer investigação criminal na atual sociedade informatizada em que vivemos. De facto, a principal vantagem da utilização destas novas medidas de investigação tecnológica reside na sua operacionalização (transversalidade) para a obtenção de provas de qualquer tipo de crime, sejam ou não os denominados "crimes informáticos", visto que são uma ferramenta eficaz no investigação de qualquer tipo de crime em que tais dispositivos eletrônicos constituam uma valiosa fonte de provas, devido às suas atuais capacidades de armazenamento de informações e ao seu uso para todos os tipos de comunicações [...].<sup>33</sup>

---

<sup>30</sup>MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, Salvador, 2020. p. 95.

<sup>31</sup> *Ibidem*, p. 103.

<sup>32</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, Salvador, 2020. p. 104-105.

<sup>33</sup> ORTIZ PRADILLO, Juan Carlos. **Informática y derechos fundamentales**: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos. 2013. p. 8. Disponível em: [http://www.fundacionalternativas.org/public/storage/estudios\\_documentos\\_archivos/b78e188fdcae153bcd14b71e5ca618e7.pdf](http://www.fundacionalternativas.org/public/storage/estudios_documentos_archivos/b78e188fdcae153bcd14b71e5ca618e7.pdf). Acesso em: 15 mar. 2021, (tradução livre). No original: “[...]La importancia de aumentar la capacidad de las autoridades de utilizar cualesquiera medidas tecnológicas de investigación destinadas a obtener esa información en formato digital se antoja un pilar esencial en cualquier investigación criminal en la actual sociedad informatizada en la que vivimos. De hecho, la principal ventaja del empleo de estas nuevas medidas tecnológicas de investigación reside en su operatividad (transversalidad) para la obtención de evidencias de cualquier clase de delito, sea o no de los denominados “delitos informáticos”, pues resultan una eficaz herramienta en la investigación de cualquier tipología delictiva en la que tales dispositivos electrónicos constituyan una valiosa fuente de prueba, debido a sus actuales capacidades de almacenamiento de información y a su empleo para todo tipo de comunicaciones[....]”

Em tempo, convém dizer sobre as provas obtidas através de aparelhos celulares, atualmente operados por sistemas altamente tecnológicos e uma imensa capacidade de armazenar informações e dados, boa parte pessoais e sigilosos, e compõem um dispositivo que representa uma parte integrante e fundamental na vida na da maioria das pessoas. Como o processo comunicativo também foi modificado e levando-se em consideração a garantia constitucional do sigilo das comunicações, para fins investigativos, mais recentemente pode-se dizer que os aplicativos de mensagens instantâneas passaram a compor um elemento-chave na obtenção de indícios e vestígios de práticas criminosas. Assim bem explicam Antonialli e Abreu:

Ao provocar uma transformação na forma como as pessoas se comunicam, possibilitando a substituição das chamadas telefônicas tradicionais por aplicações de mensagens instantâneas, e-mails e até chamadas de voz sobre IP habilitadas para web, os telefones celulares também se tornaram um tesouro de informações de comunicações, particularmente para autoridades de segurança pública. Além dos registros detalhados sobre quando, onde e por quanto tempo as comunicações ocorreram, essas novas formas de troca de informações também podem armazenar todo esse conteúdo e muito mais, como lista de contatos, fotos, notas, listas de leitura, histórico de páginas visitadas, dados de localização.<sup>34</sup>

O posicionamento do Superior Tribunal de Justiça em relação aos casos que demandaram seu entendimento foi do caráter ilícito de provas obtidas sem uma autorização judicial motivada, da devassa de dados de conversas de *whatsapp*, porquanto viola o direito à intimidade e privacidade.<sup>35</sup> A ponderação de direitos envolta na situação demanda o prestígio do direito individual e o resgate do princípio do *in dubio pro reo*, que deve prevalecer sobre o argumento *in dubio pro societate*.

Diante desse panorama, fica evidente que a incorporação tecnológica ao processo penal não acontece sem uma série de problematizações importantes que afetam, direta ou indiretamente, aspectos fundantes da persecução criminal e de direitos fundamentais de indivíduos, os quais exigem uma postura atenta e, acima de tudo, constitucional e legalmente amparada dos magistrados e, no âmbito legislativo, um olhar atento à compatibilidade e melhor maneira de realização de alterações.

---

<sup>34</sup>ANTONIALLI, Denny; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. São Paulo. InternetLab, 2019. V. 2. p. 62.

<sup>35</sup>BRASIL. Superior Tribunal de Justiça. HC. 509.345/SC. Rel. Min. Nefi Cordeiro, 6ª Turma. Julgado em: 06/08/2019. Dje em: 12/08/2019, p. 2-5. Disponível em: [https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1847245&num\\_registro=201901306316&data=20190812&formato=PDF](https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1847245&num_registro=201901306316&data=20190812&formato=PDF). Acesso em: 13 maio 2020.

### 1.1.2 As provas obtidas por métodos ocultos e infiltração por *software*

Os novos horizontes técnicos-científicos, colocam em xeque os meios usuais de obtenção de provas, ao passo que desafiam a ciência legislativa penal e a jurisprudência, com uma série de questões e problemáticas originárias de um mundo envolto na digitalidade. Ao mesmo tempo, o ambiente computacional oferece uma série de vantagens para uma prática delitiva bem sucedida, visto que proporciona o anonimato e maior dificuldade de identificação do ilícito praticado e do criminoso por trás dele<sup>36</sup>. Esse alcance não se restringe a uma modalidade de transgressão puramente virtual, mas estende-se como suporte à prática de crimes convencionais.

Os meios de obtenção de provas de uma atividade criminosa, pela mesma ótica e por decorrência lógica desse fenômeno, encontra-se em constante expansão, de modo que já sinalizam para a introdução de uma série de metodologias investigativas, na prática do sistema criminal, da qual se destacam as ações encobertas, gravação ou filmagem do lado externo, ou interno de residências, a vigilância eletrônica por vídeo, observação oculta e buscas *online*. Ainda nesse campo, a interceptação nas telecomunicações e a intromissão em conversas virtuais<sup>37</sup>, além da técnica de infiltração de um *software* de espionagem, sendo esse último objeto de uma análise mais aprofundada neste tópico, pelos seus riscos e implicações em princípios, como o da não auto-incriminação (*nemo tenetur se ipsum accusare*)

Nesse contexto, inserem-se os métodos ocultos como modalidade investigativa a qual obteve uma expressiva expansão em seu uso nas últimas duas décadas. Embora não se trate de um tema de completo ineditismo, pois é possível identificar esse tipo de prática na figura do agente infiltrado,<sup>38</sup> é certo que os avanços tecnológicos impulsionaram a sua disseminação e incorporação ao processo penal.

Essa tendência aparece paralelamente a atual conjuntura de constante tensão entre liberdade e segurança, amparada ainda pela retórica do risco, a qual orienta para um caminho em que direitos fundamentais são violados, em nome de uma ampliação dos recursos disponíveis ao Estado para uma maior repressão penal.<sup>39</sup> Além disso, Andrade explica duas

---

<sup>36</sup>Há ainda meio de encobrimento ou dificuldade de investigações criminais nas medidas antiforenses, como a ocultação e destruição de evidências, as quais, aliadas ao anonimato, somam as dificuldades da repressão criminal desse gênero.

<sup>37</sup> GOMES, Felismina. **A admissibilidade de métodos ocultos de investigação criminal em processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de Lisboa. Lisboa. p.37. 2019.

<sup>38</sup> No direito português, o assunto é objeto de debates desde a década de 60, com as figuras denominadas “agente encoberto e homens de confiança”, conforme aponta Felismina Gomes (Ibidem. p. 36).

<sup>39</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 59.

linhas causais como fatores determinantes para o emprego em massa dos métodos ocultos: o primeiro deles advém da influência estadunidense de guerra ao terrorismo; o segundo, das mudanças estruturais provocadas pelo domínio tecnológico.<sup>40</sup> Essa combinação de fatores implica numa atuação cada vez mais agressiva e implacável dos agentes investigativos, cenário em que os métodos de investigação ocultos passam a representar uma ameaça cada vez mais significativa a direitos fundamentais, principalmente aqueles concernentes ao âmbito da vida privada dos indivíduos.

Para mais propriamente conceituar em que consistem os métodos ocultos de investigação, utilizava-se a doutrina do português Manuel Andrade, como:

todos aqueles métodos que representam uma intromissão nos processos de ação, interação, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência ou disso sequer se apercebam.<sup>41</sup>

Pela própria definição e pelos aspectos levantados até então, é possível perceber as particularidades que demandam maior reflexão em uma investigação pautada na obtenção de provas por métodos ocultos: a primeira refere-se ao fato da pessoa atingida pela medida agir no escuro, sem conhecimento de estar sendo alvo de uma investigação, ou seja, isso possibilita que ao longo do percurso da medida, o indivíduo passe a agir de forma auto-incriminatória ou, conforme aponta Manuel Andrade, em síntese, “os meios ocultos” de investigação levam as pessoas atingidas – normalmente o suspeito – a ‘ditar’ inconscientemente para o processo ‘confissões’ não esclarecidas nem livres”.<sup>42</sup>

Geraldo Prado cita, nessa perspectiva, o fenômeno observado pelo alemão Schünemann denominado “efeito hidra”, em que métodos intrusivos de investigação atuam numa busca constante e incisiva, de modo a se deparar até com fatos desconhecidos que são descobertos ao “acaso”. Isso ocorre em razão da proliferação de medidas invasivas em um ambiente legalmente frágil.<sup>43</sup>

O direito ao silêncio, como corolário direto do princípio da não auto-incriminação, também sofre prejuízos, na medida em que fica inatingível para o indivíduo qualquer controle sobre as falas ou mensagens obtidas pelas entidades de investigação. Numa breve reunião do grupo de direitos fundamentais que são diretamente confrontados por esse meio de

---

<sup>40</sup> ANDRADE, Manuel da Costa. “**Bruscamente no Verão passado**”, a reforma do código de processo penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra, 2009. p. 109-111.

<sup>41</sup> Ibidem, p. 105.

<sup>42</sup> ANDRADE, Manuel da Costa. “**Bruscamente no Verão passado**”, a reforma do código de processo penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra, 2009. p. 105-106.

<sup>43</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 60.

investigação encontram-se aqueles relacionados, dentre outros, no âmbito material, à intimidade, bem como ao sigilo profissional, inviolabilidade de domicílio, sigilo profissional, além da integridade dos sistemas informacionais e autodeterminação informacional. Na ótica processual, além dos já citados diretos ao silêncio e não auto-incriminação, inclui-se também a recusa de prestar testemunho ou depoimento.<sup>44</sup>

É diante dessa conjuntura que alguns autores, como Carlos Mendes, posicionam-se pela inadmissibilidade desta medida investigativa, pois a danosidade acarretada pela aceitação dessa metodologia significa uma verdadeira deformidade na dinâmica processual, que passa a centrar-se não mais no julgamento, mas na conclusão obtida por meios ocultos. Nessa mesma lógica, desvirtua a finalidade investigativa e o caráter de *ultima ratio* de um processo criminal.<sup>45</sup> Deve-se ter mente ainda que os métodos tecnológicos devem, para fins investigativos, ser pensados mediante critérios de proporcionalidade e adequação, de forma que aponta o autor:

Por se tratar de graus de variabilidade da incidência tecnológica no âmbito do ilícito penal, poderia se pensar na equiparação entre o grau de lesividade do método de investigação tecnológica que incide nos direitos fundamentais do investigado, e o grau de ligação entre o cometimento do ilícito investigado e o meio tecnológico, ambos como critérios que sirvam para a determinação de quais tipos penais irão compor o rol. Isso porque a materialidade do delito a ser apurado pode não corresponder diretamente ou não possuir relação alguma com meios tecnológicos ou tecnologias de informação, seja na execução do ilícito ou no armazenamento de documentos em formato digital, necessários para a atividade probatória.<sup>46</sup>

Ressalta-se, contudo, que grande parte dos autores entende que a efetividade jurisdicional no combate aos crimes passará a tornar indispensável a investigação possibilitada pelos métodos ocultos, de modo que pensar sobre a melhor forma de adequação legal e restrita, torna-se o ponto central da discussão.

Acrescenta-se a isso, as constatações de Prado acerca do controle de legalidade praticado pelo juiz em relação aos métodos ocultos de investigação não poder se limitar àquele em torno da própria decisão, mas atingir também ao processo de execução das medidas que foram deferidas, pois, decisões judiciais, ainda que legítimas, podem mascarar cautelares evitadas por abusos e violações a direitos.<sup>47</sup> Nesse espectro, a distinção entre meios

---

<sup>44</sup> GOMES, Felismina. **A admissibilidade de métodos ocultos de investigação criminal em processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de Lisboa. Lisboa, 2019. p. 38.

<sup>45</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 102.

<sup>46</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 106.

<sup>47</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 68.

investigativos e de prova possuem especial relevância, conquanto ao serem encaradas como um mecanismo de auxílio à obtenção de informações úteis ao processo, diferem-se daquelas que são submetidas ao contraditório e, qualifica-se como componente de convencimento do juiz.

Observa-se que a tendência atual pelos responsáveis pela repressão criminal é de unificar os sentidos divergentes entre esses meios, especialmente por uma relação, da qual já pontuamos. Do peso os meios probatórios digitais exercem, além da ideia de que “o contraditório judicial seria motivo de contaminação da verdade”, enquanto os métodos ocultos surgem finalmente como capazes de alcançá-la.<sup>48</sup>

Com base nessas reflexões, é possível compreender que os métodos ocultos, enquadrados das novas tecnologias de informação e impulsionado por uma lógica repressiva que vai ao encontro do ideário da sociedade de risco e de maior confiança cognitiva em relação às provas a disposição, desafiam todo o nosso regime jurídico e uma interpretação constitucionalmente amparada do Código de Processo Penal. É nesses mesmos ares que a importância da fidedignidade da informação também entre em cena, conforme assevera Prado:

Assim, os métodos ocultos de investigação com a ancoragem nas inovações tecnológicas não configuram apenas novos suportes comunicacionais, mas instituem uma original subjetividade, desafia algo mais que os conhecidos cuidados com a autenticidade de informações registradas em suporte físico, para ficar na questão mais elementar da fiabilidade probatória.<sup>49</sup>

Passamos, então, a analisar uma espécie do gênero método oculto de investigação, intrinsecamente ligado ao advento da internet, conexões em rede e a ascensão dos computadores: a infiltração por *software*.<sup>50</sup> Em suma, eles consistem em “programas informáticos elaborados para fins de extração de dados contidos em um sistema informático

---

<sup>48</sup> Ibidem. p. 69.

<sup>49</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 73

<sup>50</sup> O termo *software* evita uma abordagem reducionista dessa técnica, muitas vezes resumida ao “Cavalo de tróia” ou *malware*, segundo explica Eduardo Riboli (A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. Galileu - Revista de Direito e Economia. Volume XIX. Fascículo II, p. 68. 2018.) “Preferimos adotar o termo software de espionagem para evitar a redução destes programas à determinadas modalidades de softwares espões, como é o caso dos autores que utilizam o termo “cavalo de Tróia”, o qual na verdade é apenas uma das espécies de software de espionagem identificação de uma modaldia de software de espionagem. Também afastamos o termo malware (contração de malicious software) a fim de evitar a interpretação de que todo o software de espionagem é necessariamente mal intencionado ou ilegal”.

ou aparelho eletrônico sem o conhecimento ou consentimento do seu utilizador”.<sup>51</sup> David Ramalho, de forma mais completa, o define como:

um programa simples ou auto-replicativo que directamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático.<sup>52</sup>

De acordo com a finalidade e com o dispositivo visado, esses programas podem aparecer mediante variadas formas, como através de *pen drives* ou *internet*. É certo que através dele é possível ter acesso a um número altamente expressivo de dados individuais, como a localização, senhas, câmara, microfone e mesmo alterar o conteúdo do interior do equipamento sob investigação. Conforme aponta Eduardo Riboli, “trata-se de um método de investigação mais intrusivo e potencialmente mais eficaz que uma mera interceptação de comunicações”.<sup>53</sup>

Nessa perspectiva reside a crítica de Gleize, pois a infiltração, de forma diferente da interceptação, atinge de modo muito profundo e intensamente a esfera íntima do indivíduo e sua autonomia. Impacta, na verdade, a “dimensão da *autodeterminação informacional*: o direito ao controle sobre o tratamento dos próprios dados”.<sup>54</sup> Através de uma infiltração, é possível traçar o acesso a um perfil completo e atemporal de vários aspectos da vida do investigado, inclusive de informações mantidas em sigilo por ele, à margem da intenção de ser compartilhado. Não se diferencia quais dados estão na esfera da vida privada.<sup>55</sup>

Essa discussão foi suscitada pela Corte Constitucional alemã no ano de 2008, ocasião em que também foi preconizado um novo direito fundamental, relativo à confidencialidade e integridade dos sistemas informáticos, como resposta à aderência que os sistemas de informação ganharam na vida das pessoas. Na ocasião, foi declarada inconstitucional a lei de um Estado que possibilitava aos órgãos de inteligência o monitoramento de suspeitos de práticas delitivas. A decisão não proibiu a prática do software espião, mas delimitou, de

<sup>51</sup> RIBOLI, Eduardo. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **Galileu – Revista de Direito e Economia**. Volume XIX. Fascículo II, 2018. p. 68.

<sup>52</sup> RAMALHO, David. **O uso de malware como meio de obtenção de prova**. Revista de Concorrência e Regulação n.º 16, 2013. p. 201-202.

<sup>53</sup> A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. Galileu - Revista de Direito e Economia. Volume XIX. Fascículo II, 2018. p. 69.

<sup>54</sup> GLEIZE, Orlandino. **Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-2-12082019>. Acesso em: 01 maio 2021.

<sup>55</sup> Ibidem.

forma bastante restrita seu alcance de uso, exigindo base legal específica e a indicação de um perigo concreto a um bem jurídico fundamental.<sup>56</sup>

Assim, Schertel conclui que esses mecanismos devem ser testemunhados a partir do “alto grau de interferência na vida das pessoas e da sensibilidade de informações que podem ser coletadas”, de forma que sem uma legislação anterior, em consonância com o artigo inciso XII, do art. 5º da Constituição Federal, que preveja seus limites e evite a ocorrência de abusos. Assim, é impossível pensar na licitude da utilização desses programas, notadamente por ausência de qualquer previsão legal.

---

<sup>56</sup> SCHERTEL, Laura. **Uso de softwares espiões pela polícia: prática legal?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 01 maio 2021.

## 2 A EXPERIÊNCIA PROBATÓRIA NO UNIVERSO DIGITAL

*“[...]Todos nós estamos em dívida com nossas fontes de informação. Mas ficamos especialmente vulneráveis quando elas nos dizem exatamente o que queremos ouvir:[...]”*.<sup>57</sup> (Lee McIntyre)

### 2.1 A prova digital enquanto nova categoria: *conceito e características singulares*

Como corolário de um processo penal desenvolvido no paradigma de um Estado democrático de Direito, uma decisão condenatória criminal precisa estar amparada em provas colhidas com respeito às garantias dos indivíduos e, defende-se ainda, que elas devem estar em sintonia com parâmetros objetivos mínimos, aptos a sustentar os fatos imputados.

É certo, conforme preleciona Aury Lopes Júnior, que o intento do processo penal, através da lógica utilizada pelo complexo maquinário judiciário, é a reconstrução, sempre aproximada, de fatos que já ocorreram. O juiz, nesse sentido, realiza uma atividade recognitiva com base no fato histórico exibido na peça acusatória e necessita, essencialmente, das provas para produzir o seu conhecimento que servirá de embasamento para a sentença proferida, de modo que “o processo penal e a prova nele admitida integram o que se poderia chamar de modos de construção do convencimento do julgador”.<sup>58</sup>

A sociedade de informação traz consigo a redefinição e ressignificação de categorias tradicionais. Em relação às provas, argumenta-se, no presente trabalho, inclusive, que ela inaugurou um tipo probatório. Isso decorre principalmente da sua especificidade e características que lhe são próprias.

No mesmo sentido, conforme explica Evandro Duarte, as novas tecnologias de comunicação foram muito além da facilitação de velhos afazeres dos juristas. Em verdade, faz o diagnóstico de cenários de profundas mudanças, especialmente em temáticas mais vulneráveis por sua natureza, como é o caso da prova e do sistema de garantias individuais do acusado.<sup>59</sup>

---

<sup>57</sup> Tradução livre. No original: “We are all beholden to our sources of information. But we are especially vulnerable when they tell us exactly what we want to hear” (McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018, p. 62).

<sup>58</sup> LOPES JUNIOR, Aury. **Direito Processual Penal**. São Paulo: Saraiva, p.153.2021.

<sup>59</sup> DUARTE, Evandro Charles Piza. A Máquina de Vidro: Sociedade de Informação e Processo Penal. **Cadernos da Escola de Direito e Relações Internacionais da UniBrasil**, Curitiba, v. 4, 2005. p. 40. Uma crítica pertinente do autor, a qual vale aqui pontuar, diz respeito ao real impacto das novas tecnologias de informação relativamente às trocas por elas proporcionadas. A esse respeito, destaca-se que a repercussão no âmbito de

Nesse âmbito das constatações realizadas pelo autor, ele identifica o “deslocamento definitivo da veracidade da informação do suporte para fonte”.<sup>60</sup> Em termos práticos, isso significou uma valoração e atenção não mais no aspecto material, físico, de um determinado conteúdo, mas sim de sua origem.

Desse modo, inicialmente, é importante alocar a prova digital enquanto espécie pertencente ao gênero prova científica. Isso significa dizer que, para uma bem sucedida coleta, manipulação e tratamento dos vestígios dessa natureza, a operação deve ser guiada por critérios e métodos científicos e, por consequência, requer que a pessoa responsável por esse procedimento seja dotada de qualificação e *expertise* para tanto.

Nesse ponto, salienta-se que mesmo a definição embasada e criteriosa de uma ciência valorativa das provas, não se confunde com uma conduta acrítica em relação a elementos probatórios dotados de um caráter científico. Mesmo nesses casos, prevalece o livre convencimento motivado, o que exige sua existência conjunta com outros meios de provas.<sup>61</sup>

Segundo Furlaneto e Santos,<sup>62</sup> a prova digital relevante ao processo penal é aquela que “contempla os arquivos informáticos que podem estar em poder do investigado ou de terceiros que contém informações úteis à busca da verdade”. Carvalho,<sup>63</sup> por outro lado, trabalha com a definição de que “as evidências no meio digital representam as informações armazenadas ou transmitidas eletronicamente na forma de *bits* que podem ser invocadas em juízo”. Guardia,<sup>64</sup> ao importar o conceito advindo da *common law*, sob a denominação de *digital evidence*, resgata a definição dada por Casey, como “qualquer dado armazenado ou transmitido por computador, que seja capaz de corroborar ou refutar uma tese sobre a prática de um crime, ou que esclareça elementos determinantes de um crime como a intenção do agente e álibi”.

---

intercâmbio de bens, pessoas e serviços, foi muito menor que a esperada, ao passo que em relação ao fluxo de informações, viu-se uma aceleração exponencial. Nesse mesmo raciocínio, conclui que “a globalização apresentou-se como fenômeno, predominantemente, ideológico”.

<sup>60</sup> DUARTE, Evandro Charles Piza. A Máquina de Vidro: Sociedade de Informação e Processo Penal. **Cadernos da Escola de Direito e Relações Internacionais da UniBrasil**, Curitiba, v. 4, 2005. p. 45.

<sup>61</sup> GUARDIA, Gregório. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 218.

<sup>62</sup> FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 5. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 30 de mai. 2021. Apontamentos sobre a cadeia de custódia da prova digital.

<sup>63</sup> CARVALHO, R.W.R.A Importância da Cadeia de Custódia na Computação Forense. **Rev. Bras. Crimin.**, v. 9, n. 2. 2020. p. 2.

<sup>64</sup> GUARDIA, Gregório. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 124.

A Convenção de Budapeste, enquanto documento internacional que visa combater cibercrime, tendo sido o Brasil convidado a aderir no ano de 2019, também apresenta uma definição em seu artigo 1.º, utilizando-se da expressão “dados informáticos”:

Art. 1o [...] b) ‘Dados informáticos’ significa qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função [...].<sup>65</sup>

Em sua tese, Denise Vaz<sup>66</sup> conceitua prova digital como sendo “dados em forma digital no ‘sistema binário’ constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contém a representação de fatos ou ideias”. Nessa acepção, todavia, as diferencia das evidências que apenas se utilizam de sistemas informáticos para fins analíticos, como é o caso, por exemplo, das reconstituições que se utilizam de programas de computador. Da mesma forma, a definição estabelecida não comporta os identificados como provas documentais, ainda que utilizem informação decorrentes de meio digitais, como as obtidas por entidades públicas ou terceiros, através de uma requisição. Por essa razão, a mera obtenção de informações por meios informáticos não adentra ao conceito de prova digital, de modo que não é o formato e sim o arquivo informático que determinará o enquadramento mais adequado.<sup>67</sup>

A autora, ao divergir de algumas classificações apontadas, não considera a não durabilidade como um elemento comum a toda prova do gênero, pois já se pode contar com técnicas que permitem a sua preservação, além da perenidade ser uma propriedade dos dados transmitidos em rede. Para ela, a disseminação de dados também não é atributo que possa ser elencado como uma qualidade que engloba esse tipo probatório, posto que o arquivo muitas vezes existirá em um único documento ou dispositivo. Essa possibilidade, no entanto, deve ser enfrentada durante a investigação de um delito.<sup>68</sup>

As características das provas digitais, conforme elenca Denise Vaz,<sup>69</sup> são: imaterialidade, com independência em relação ao suporte físico de origem, volatilidade, facilidade na clonagem e dispersão; e ainda a indispensabilidade de dispositivo acessório necessário à sua transmissão. Em relação ao mesmo tema, Dario Kist enumera quatro

---

<sup>65</sup> BUDAPESTE. Convenção de Budapeste sobre o Cibercrime. Budapeste. Publicado em 23 nov. 2011. Disponível em: [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 23 abr. 2021.

<sup>66</sup> VAZ, Denise. **Provas digitais no processo penal**: formulação de conceito, definição de características e sistematização do procedimento probatório. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 64.

<sup>67</sup> *Ibidem*, p. 65.

<sup>68</sup> *Ibidem*, p.68

<sup>69</sup> *Idem*.

propriedades que as singularizam: fragilidade, também a dispersabilidade e volatilidade, bem como a incorporeidade.<sup>70</sup>

Explica-se que a imaterialidade se refere a uma ausência de representação física, o que possibilita uma maior capacidade tanto de transmissão, como de armazenamento, dentro de um determinado dispositivo informático. Com efeito, afirma-se que elas são desvinculadas de seu suporte físico de origem.

Por outro lado, a volatilidade assume-se como a sua inconstância, em sua facilidade de transformação e suscetibilidade em sofrer modificações e transformações, sendo necessário para isso apenas a alteração de uma sequência numérica.<sup>71</sup> Quanto a esse aspecto, em virtude das consequências processuais significativas que possam decorrer de possíveis modificações do conteúdo das evidências, pontua-se a necessidade de comunicação prévia à defesa, para a designação de assistente técnico jurídico qualificado para acompanhar toda a produção probatória.<sup>72</sup>

A característica da imaterialidade acaba por provocar a facilitação do processo de clonagem, a qual viabiliza a produção de cópias fiéis aos originais, em quantidade infinita, sendo que pode ainda, conjuntamente, transmitir a outros dispositivos. O potencial de dispersão, conforme aponta Kist,<sup>73</sup> abrange a compreensão de duas dimensões: a primeira, enquanto sua viabilidade de coexistir em múltiplas localidades dentro do próprio sistema informático no qual ela está inserida; em segundo lugar, está a sua perspectiva geográfica, pois os servidores de rede podem estar localizados em qualquer lugar do mundo.

Quanto à necessidade de intermediação por um meio físico, ele é indispensável, pois é somente a partir dele que se traduzirá as informações codificadas para uma informação compreensível ao ser humano. Por assim ser, impescinde de um dispositivo para ser exteriorizada e acessada.<sup>74</sup> Cita-se que os meios pelos quais é possível a obtenção dessas provas são: requisição, busca e apreensão, interceptação dos fluxos de comunicação de informática e a perícia.

---

<sup>70</sup> KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019. p. 118.

<sup>71</sup> VAZ, Denise. **Provas digitais no processo penal: formulação de conceito, definição de características e sistematização do procedimento probatório**. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 68-69

<sup>72</sup> GUARDIA, Gregório. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 125-128.

<sup>73</sup> KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019. p. 120.

<sup>74</sup> VAZ, Denise. **Provas digitais no processo penal: formulação de conceito, definição de características e sistematização do procedimento probatório**. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 69-70.

Outrossim, a Norma ABNT NBR ISO/IEC 27037:2012 é defendida por alguns autores como o tratamento a ser dado a essas evidências, dada a ausência de regulação específica para defini-las. Existem uma série de razões que defendem essa posição: elas cumprem o padrão imposto pela Organização Internacional de Padronização (ISO), em atuação conjunta com a Companhia Eletrotécnica Internacional (IEL), além de comporem a ISO 27000 e, desse modo, integrem um conjunto de normas que servem como padrão e referência para a área de segurança da informação, sendo a usual da perícia forense digital.<sup>75</sup>

A norma em questão não é obrigatória, pois não tem explícita previsão legal, mas possui reconhecimento internacional e já é adotada por outros órgãos no Brasil para tais fins, como é o caso da Secretaria Nacional de Segurança Pública. O alcance em relação os dispositivos são consideráveis, conforme expõem Furlaneto e Santos:

A evidência digital considerada na norma ABNT NBR ISO/IEC 27037:2012 (ABNT,2013) pode ser produzida através de diferentes tipos de dispositivos digitais como HD, disquetes, CD/DVD, pen-drive, smartphones, tablets, assistentes digitais pessoais (PDA), dispositivos eletrônicos pessoais (PED), cartões de memória, sistemas de navegação móveis (GPS), sistemas embarcados, câmeras digitais de vídeo e fotografias (incluindo CFTV), desktops, notebooks, redes baseadas em TCP/IP e outros protocolos digitais, bem como dispositivos com funções semelhantes às descritas acima.<sup>76</sup>

No âmbito dessa normativa há, dentre outros pontos, a relação de três características fundamentais presentes em todas as evidências digitais: a primeira delas, trata-se de sua relevância, ou seja, a prova tem que servir como elemento de confirmação ou refutação do caso em discussão; outro aspecto é a confiabilidade, na medida em que deve manter correspondência com a original; assim, tem-se a suficiência como sua capacidade de responder com integridade e adequabilidade às questões que estão sendo levantadas. Ressalta-se outra divisão importante, quanto à volatilidade da prova (pode-se ser classificada como “volátil” ou “não volátil”), tendo em vista a sua possibilidade de ser armazenada ou não de forma duradoura.<sup>77</sup>

Classificam-se, ademais, as provas digitais como provas atípicas, porquanto enquadram-se na definição de Guilherme Dezem, como aquelas não previstas no

---

<sup>75</sup> FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 8. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 03 abr. 2021.

<sup>76</sup> Ibidem.

<sup>77</sup> ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=307273>. Acesso em: 06 abr. 2021.

ordenamento jurídico e “para a qual não há um procedimento probatório específico”.<sup>78</sup> Essa possibilidade só existe, conforme alerta Aury Lopes Júnior, mediante o respeito à base principiológica e legal compartilhadas com todos os outros meios de provas, por isso dispõe que

No tensionamento entre a epistemologia e o respeito às regras do jogo, é importante sempre destacar: há que se buscar um lugar comum, um equilíbrio, mas na falta ou impossibilidade disso, prevalecem sempre as regras do devido processo e as garantias constitucionais.<sup>79</sup>

Diante de todas as propriedades levantadas, somadas à evidente pertinência atual e expansiva dos vestígios digitais, deparamo-nos com uma negligência legislativa latente que, no melhor dos casos, volta-se a assuntos em torno da tramitação de processos, comunicação e atos via *internet*, como as previsões da Lei n.º 11.419/06.<sup>80</sup> Ignora, no entanto, toda a problemática no que diz respeito à prova digital, inclusive em alterações legislativas recentes.

Vislumbra-se, portanto, uma série de distinções e atributos específicos que estabelecem a prova digital como uma categoria inédita dentre as espécies probatórias tradicionais e que vão ainda refletir, numa relação causa-consequência, nos seus meios de obtenção, conforme será exposto no próximo tópico. Ademais, suas peculiaridades demandam procedimentos especiais e específicos para a realização dos procedimentos correspondentes à cadeia de custódia, os quais são objetos do capítulo seguinte.

## **2.2 A relação entre prova e verdade processual: a desmistificação da busca da verdade real e a necessidade de filtragem epistêmica da prova**

A questão probatória demanda o esclarecimento de diversos aspectos relativos ao tipo de sistema criminal que pretende se sustentar, O Estado democrático de direito, por exemplo, exige que se defina qual deve ser a postura das partes em relação às funções investigatórias e acusatórias, ou sobre quem recai o ônus das provas. Na mesma medida, toda a ciência da prova organiza-se por meio de critérios, regras e princípios bem definidos, na denominada teoria das provas.<sup>81</sup>

---

<sup>78</sup> DEZEM, Guilherme Madeira. **Da Prova Penal: Tipo Processual, Provas Típicas e Atípicas:** (atualizado de acordo com as Leis 11.689, 11.690/08 e 11.719/08). Campinas: Millennium, 2008. p. 149.

<sup>79</sup> LOPES JUNIOR, Aury. **Direito Processual Penal.** São Paulo: Saraiva, 2021. p. 169.

<sup>80</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal:** Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 115.

<sup>81</sup> A esse respeito utiliza-se o termo da mesma forma que Eugênio Pacelli: “Normalmente, a doutrina refere-se a uma teoria geral da prova para introduzir o tema relativo à prova no processo penal. A nosso juízo, uma teoria acerca de qualquer objeto de investigação científica haverá de ser sempre geral, no sentido de examinar integralmente o conteúdo e a essência daquele objeto. Por isso, o exame, se for rigoroso, há de ter a pretensão

A ambição desse tópico, no entanto, não é uma abordagem manualística de toda a teoria das provas, com o esgotamento dos principais e periféricos princípios atinentes, mas focalizar a correlação que existe entre a postura do magistrado enquanto perseguidor da “verdade” no processo penal e quais são as implicações disso. Indaga-se, no ponto, se realmente existe o princípio da verdade real e qual o papel do princípio da presunção de inocência nessa conjuntura.

Vê-se um intenso e permanente debate sobre o controle punitivo estatal, manifestado na forma de uma decisão judicial, e a sua dinâmica e correspondência com a prova produzida. Por essa razão, percebe-se a existência de “um tensionamento constante entre prova e decisão que culmina na necessidade de um controle epistêmico que permeia a admissão, produção, valoração e decisão”.<sup>82</sup>

Ocorre que nosso Código de Processo Penal é datado do ano de 1941 e contém diversos traços que denotam um caráter inquisitorial ao processo, como poderes acusatórios e ampla possibilidade de produção probatória ao juiz. Esses aspectos, no entanto, não foram recepcionados pela Constituição Federal de 1988 que prevê, em seu artigo 5º, um sistema de garantias individuais, além de ser incompatível com diversos tratados internacionais firmados pelo Brasil, como o Pacto de San José da Costa Rica.<sup>83</sup>

Assim sendo, percebe-se que a ‘verdade real’ está intimamente ligada com uma cultura inquisitiva, a qual utilizou-se do argumento de que no processo penal protege-se interesses mais relevantes e trataria de questões mais graves. Esse pensamento autorizou o uso de práticas probatórias das mais variadas espécies, ainda que ausente a previsão legal, pois estaria amparada pelo nobre propósito da busca da verdade.<sup>84</sup>

Nessa perspectiva, Aury Lopes Junior expõe que o mito da verdade real ganha seus contornos com a estrutura do sistema inquisitório com a justificativa de “interesse público”, a qual já serviu de base para a ocorrência de todo tipo de atrocidades ainda com o *modus operandis* de sistemas políticos autoritários, além de uma busca pela verdade que permitiria que os fins justificassem os meios.<sup>85</sup>

Desse modo, é importante esclarecer que com base nos atuais ditames constitucionais, não se busca exatamente a aferição da verdade, mas sim que o juiz forme o seu

---

de ser também geral. Daí a desnecessidade da referência ao aludido predicado, com o que ficaremos apenas com a expressão teoria da prova, para indicar o estudo dos princípios e regras aplicáveis ao tema, sem adentrar, ainda, a análise dos meios de prova”. PACELLI, Eugênio. **Curso de Processo Penal**. 24. ed. São Paulo: Atlas, 2020. p. 251).

<sup>82</sup> LOPES JUNIOR. Aury. **Direito Processual Penal**. São Paulo: Saraiva, 2021. p. 154.

<sup>83</sup> PACELLI, Eugênio. **Curso de Processo Penal**. 24. ed. São Paulo: Atlas, 2020. p. 251.

<sup>84</sup> *Ibidem*.

<sup>85</sup> LOPES JUNIOR. Aury. **Direito Processual Penal**. São Paulo: Saraiva, 2021.

convencimento, o qual deve ser arquitetado nos estreitos limites do contraditório e do devido processo penal.<sup>86</sup> Embora Aury Lopes Junior não seja adepto à expressão “verdade processual”,<sup>87</sup> Eugênio Pacelli utiliza-se da denominação para dizer que “toda verdade judicial é sempre uma “verdade processual”, e isso decorre principalmente, não apenas pelo seu cunho no processo, mas porque se está diante de uma verdade de significado tão e exclusivamente jurídica.<sup>88</sup> Acrescenta-se, entretanto, conforme Aury Lopes Junior defende, que “desconstruir o mito da verdade real não é suficiente, é necessário questionar também a “verdade processual” e, principalmente, a “ambição de verdade”.<sup>89</sup>

Dessa forma, o objetivo de um processo penal, que implicará em sua incorporação em um tipo de decisão ou sentença, não deverá se basear tão somente na verdade como elemento fundante. Ao mesmo tempo, Prado alerta que “a existência de uma liga entre verdade, prova e processo penal configura condição de possibilidade de um processo penal conformado aos mandamentos do estado de direito”.<sup>90</sup> Vale ressaltar que, ao contrário do processo civil no qual a ausência de impugnação de uma demanda acarreta em sua aceitação como incontestável, é imprescindível que haja, no processo penal, a materialização da prova ou ainda, na verdade em seu sentido material.

Superado, portanto, o alocamento da verdade e seus contornos dentro do quadro processual penal, há ainda que se ter em mente o papel do princípio da presunção de inocência que distribui a carga do interesse em demonstrar a existência do delito para a acusação.<sup>91</sup> A partir disso, tem-se o dimensionamento da carga da prova no processo penal, enquanto ponto central para o desenvolvimento de um direito penal que não se pronuncia sobre a gravidade do crime ou a situação do criminoso e sim a sua vinculação às proeminentes regras norteadoras, os *standards* probatórios, aptos a ensejar a punição de um ilícito.<sup>92</sup>

---

<sup>86</sup> op. cit, p. 156.

<sup>87</sup> Explica-se que o autor não exclui a verdade do processo penal, apenas dá a ela um tratamento contingencial, conforme se depreende “[...]O que propomos não é negar a verdade, mas sim um deslocamento da discussão para outra dimensão, em que a verdade é contingencial e não estruturante do processo. Dessa forma, não se nega a verdade, mas tampouco a idolatramos (evitando assim incidir no erro de dar ao processo a missão de revelar a verdade na sentença, o que conduziria à matriz inquisitorial). A verdade, assim, é contingencial e a legitimação da decisão se dá por meio da estrita observância do contraditório e das regras do devido processo. São essas regras que, estruturando o ritual judiciário, devem proteger do decisionismo e também do outro extremo, em que se situa o processo inquisitório e sua verdade real” (op. cit., p. 156)

<sup>88</sup> PACELLI, Eugênio. **Curso de Processo Penal**. 24. ed. São Paulo: Atlas, 2020. p. 251.

<sup>89</sup> LOPES JUNIOR, Aury. **Direito Processual Penal**. São Paulo: Saraiva, 2021. p.155.

<sup>90</sup> PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2019, p. 31.

<sup>91</sup> op. cit.

<sup>92</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. São Paulo: Marcial Pons, 2014.

Sob esse ponto de vista, a temática probatória no processo é realmente desafiadora, porquanto reivindica para si o enfrentamento de questões que extrapolam o ambiente processual e o mundo jurídico, como a lógica, a epistemologia e a psicologia. Por um lado, do ponto de vista epistemológico, a proposta recai sobre a possibilidade de se obter a verdade; enquanto no campo processual, requer-se o estabelecimento de *standards* que permitam verificar qual a medida para que se possa afirmar a (in)suficiência das provas existentes no autos para a comprovação determinado fato. É nesse sentido que o ônus da prova passa a trabalhar substituindo a verdade, como um itinerário que o juiz deve seguir diante da incerteza que o assola, sendo que a verdade e a certeza devem revestir-se de um caráter negativo no âmbito do ônus da prova.<sup>93</sup>

É nesse sentido que se tem que a verdade deve agir como um termômetro aferidor da conformação epistemológica, consoante o que se depreende das lições de Geraldo Prado, o qual atesta que “a verdade cumpre a função de indicador epistêmico em um tipo de processo baseado na pesquisa e demonstração dos fatos penalmente relevantes”.<sup>94</sup> A epistemologia da prova corresponde à noção de uma aquisição de conhecimento firmada em critérios que realmente viabilizem a produção de uma prova transparente, fundamentada e justificada.

Não se ignora, no entanto, que embora a prova possua a função precípua de uma adequada reconstrução dos fatos da causa no processo penal, elas nem sempre serão suficientes para aclarar de forma adequada as questões envoltas no processo. Nesse cenário em questão, os *standards* probatórios e a construção de uma teoria adequada a esse respeito cumprem um papel ainda mais proeminente.

Além disso, uma filtragem epistêmica, do ponto de vista de quais provas são admissíveis com base nas garantias individuais por atuarem assim como limitadores do exercício e material probatório com a consequente exclusão dos elementos violadores de direitos fundamentais, diminui o espectro de informações atingíveis e o alcance do projeto epistêmico da prova judicial. Ao mesmo tempo, o método epistêmico serve como base da atuação racional do juiz, valorada em parâmetros objetivos em sua decisão sobre os fatos, e não puramente orientado pela experiência pessoal do julgador.<sup>95</sup>

Por assim ser, Márcio Widál Filho coloca:

---

<sup>93</sup> BADARÓ, Gustavo. Ônus da prova no processo penal. *Revista dos Tribunais*, São Paulo, 2003. p. 9-10.

<sup>94</sup> PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos*. São Paulo: Marcial Pons, 2014. p. 18.

<sup>95</sup> FILHO WIDAL, Márcio. *A conformação epistêmica do processo penal democrático e os estándares de prova*. 2017. p. 7. Disponível em: <https://marciowidal.files.wordpress.com/2017/09/a-conformac3a7c3a3o-episte3aamica-do-processo-penal-de-mocrc3a1tico-e-os-este3a2ndares-de-prova.pdf>. Acesso em: 01 abr. 2021. p. 7.

A partir de um ponto de vista epistemológico, a racionalidade das decisões sobre os fatos passa pela formulação de estândares de prova no processo penal, que podem definir critérios que dimensionam o grau de comprovação necessário para que se considere como provada uma hipótese acusatória (fato imputado).<sup>96</sup>

Desse modo, percebe-se que ainda que a demarcação de estândares probatórios seja um aspecto intrínseco na cultura jurídica anglo-saxã, cujos juízes leigos atuam sem a necessidade de motivar suas decisões, o intercâmbio desses saberes dentro da cultura romano-germânica “permite espaço reservado à livre valoração das provas pelos julgadores, definindo critérios que permitam uma decisão racional sobre os fatos”.<sup>97</sup>

A premissa o estabelecimento de um *standard* probatório não se confunde com o já superado sistema da prova tarifada, porquanto no sistema valorativo de provas legais existe a postulação legal e prévia de quais elementos e as espécies probatórias que devem estar presentes para que haja a condenação de alguém. Diferentemente ocorre no sistema racional de valoração, que não define uma correlação da quantidade e qualidade das provas que devem estar presentes; mas critérios, que em consonância da totalidade do rastro probatório produzido, devem estar presentes, tornando, o que se pretende se sustentar, provado além da considerada dúvida razoável.<sup>98</sup>

Diante disso, Vasconcellos define dois momentos em que devem ser considerados para a proposição de um *standard*<sup>99</sup> probatório que ultrapasse a linha de “prova além da dúvida razoável”: o primeiro, diz respeito à comprovação, que deve ser consistente e amparada em provas lícitas e norteadas pelo princípio do contraditório. Ressalta-se que a incriminação deve explicar coerentemente a todos a ocorrência do delito imputado, de modo individual e específico. Posteriormente, e essa é a principal distinção da noção civilista de

<sup>96</sup> Ibidem, p. 9.

<sup>97</sup> FILHO WIDAL, Márcio. **A conformação epistêmica do processo penal democrático e os estândares de prova.** 2017. p. 7. Disponível em: <https://marciowidal.files.wordpress.com/2017/09/a-conformac3a7c3a3o-epistc3aamica-do-processo-penal-de-mocrc3a1tico-e-os-estc3a2ndares-de-prova.pdf>. Acesso em: 01 abr. 2021. p.10.

<sup>98</sup> VASCONCELLOS, Vinicius Gomes de. **Standard probatório para condenação e dúvida razoável no processo penal:** análise das possíveis contribuições ao ordenamento brasileiro. Rev. direito GV, São Paulo, v. 16, n. 2, e1961, 2020. Disponível em: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1808-24322020000200203&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322020000200203&lng=en&nrm=iso). Acesso em: 5 abr. 2021. O ator também explica que “A ‘prova além da dúvida razoável’ determina que, para ser considerada provada, a hipótese precisa ter uma probabilidade bastante elevada de ocorrência e, além disso, as demais hipóteses alternativas não podem ser aceitáveis. Veda-se que exista qualquer dúvida razoável em relação à versão que se pretende afirmar como provada”.

<sup>99</sup> Conforme adverte Aury Lopes Junior “é sempre importante advertir que a adoção de um standard probatório como o BARD não é a solução para todos os males do decisionismo, senão mais uma medida de redução de danos e de ampliação de garantias, bem como de aumento do nível de exigência de qualidade da própria decisão penal que, cravada na racionalidade probatória, precisa demonstrar racionalmente a valoração da prova e dos fatos em julgamento”. LOPES JUNIOR, Aury. **Direito Processual Penal.** São Paulo: Saraiva, 2021. p. 158.

“preponderância de provas”, não deve existir qualquer outra explicação alternativa aplicada aos fatos que foram provados.<sup>100</sup>

Portanto, a discussão epistemológica em torno da prova realça o valor de uma metodologia que permita assentar balizas norteadoras e aplicáveis ao processo de recolhimento de vestígios, visto que sua verificação é necessária para uma correta e melhor compreensão dos fatos e da dinâmica que reivindica a sua elucidação. É também a partir dessa perspectiva que esse trabalho procura enfrentar a elaboração de uma cadeia de custódia. Não se ignora, no entanto, que embora a prova possua a função precípua de uma adequada reconstrução dos fatos da causa no processo penal, elas nem sempre serão suficientes para aclarar de forma adequada as questões envoltas no processo. Nesse cenário em questão, os *standards* probatórios e a construção de uma teoria adequada a esse respeito cumprem um papel ainda mais proeminente.

### **2.2.1 A inadmissibilidade de provas ilícitas: A causa de impedimento por contaminação do juiz**

Ao longo dos últimos tópicos foi possível perceber que o cenário aponta para uma assincronia entre a ebulição de tipos probatórios e de meios investigativos, os quais ultrapassam qualquer parâmetro legislativo vigente. Na mesma medida, abre-se o leque de ilicitudes que devem ser arguidas por uma defesa criminal na proteção do indivíduo acusado que teve os seus direitos violados. Aparece, com especial importância, nesse sentido, a discussão sobre a dissonância cognitiva do juiz e a necessidade de seu afastamento ao ter contato com provas ilícitas, conforme o parágrafo quinto, acrescido ao artigo 157 do Código de Processo Penal, pela Lei nº 13.964/2019.

O referido artigo já foi objeto de veto pela Presidência da República por duas vezes: em 2008, na forma do §4º do art. 157, na ocasião da Lei n.º 11.690/2008 e após, em 2019, nos acréscimos ao Código de Processo Penal, ocasionados pela Lei n.º 13.964/2019, §5º do art. 157. Nesse último momento, sua permanência só foi possível após a derrubada dos vetos pelo Congresso Nacional no dia 19 de abril de 2021, conjuntamente com mais alterações que foram promulgadas.

A vedação de provas ilícitas tem sobretudo uma função política, pois considera desproporcional que se sacrifique direitos fundamentais dos indivíduos na busca de uma

---

<sup>100</sup> op. cit.

verdade processual. É na esfera criminal que esse raciocínio é ainda mais evidenciado, tendo em vista que “seria absurdo que o Estado, para impor a pena ao autor de um crime, permitisse a prática de métodos criminosos para apurar a verdade sobre o fato”.<sup>101</sup>

Dessa forma, entende-se que os objetivos perseguidos em relação à apuração da verdade dos fatos, dentro de um processo judicial, devem harmonizar-se com o conjunto de interesses também valorizados e presentes em uma ordem jurídica.<sup>102</sup> Dentro desse universo, pode-se distinguir essas provas em dois grupos: ilícitas e ilegítimas. As primeiras, respectivamente, são aquelas obtidas por meio da violação de normas de direito material, enquanto as outras significam uma ofensa a algum preceito processual. Há também a diferença entre o momento da transgressão e os seus efeitos: nas ilícitas, a ilegalidade é configurada já na sua obtenção, como resultado, elas não podem adentrar ao processo e, caso isso ocorra, devem ser desentranhadas. Por outro lado, nas ilegítimas, a mácula ocorre na etapa de produção de prova, e o ato eivado do vício deve ser renovado.<sup>103</sup> A exceção que comporta a teoria das ilicitudes são as provas utilizadas a favor do réu, ou cuja fonte de prova é independente da imaculada, ainda aquelas provindas de encontro fortuito ou descoberta inevitável.

É em decorrência dessa divisão que, na visão crítica de Antônio Gomes, o conceito definido no art. 15 do CPP de provas ilícitas como “as obtidas em violação a normas constitucionais ou legais”, enfrenta problemáticas, pois além de não satisfazer o intento de clarificar a previsão constitucional, provocou o resultado oposto de confundir as características das duas, levando a compreensão equivocada de, por exemplo, o descumprimento de previsões de ordem processual levaria a ilicitude da prova e seu desentranhamento quando, na verdade, acarreta sua nulidade e a renovação do ato.<sup>104</sup>

Por esse ângulo, surge a problemática que orbita a relação do magistrado que teve contato com as provas ilícitas e o peso psicológico que elas emanam em sua decisão. No campo das provas digitais, equaciona-se também a maior credibilidade, muitas vezes dotadas de imagem e som, que as provas digitais exercem na construção subjetiva, causando assim um duplo fator que pode estampar o decisionismo em suas sentenças. A partir dessas premissas, posiciona-se Aury Lopes Júnior:

A desconsideração de que se opera uma grave contaminação psicológica (consciente ou inconsciente) do julgador faz com que a discussão seja ainda

---

<sup>101</sup> GOMES FILHO, Antonio. **A inadmissibilidade das provas ilícitas no direito brasileiro**. 2014. p. 6. Disponível em: [http://www.cidp.pt/revistas/rjlb/2015/1/2015\\_01\\_0005\\_0019.pdf](http://www.cidp.pt/revistas/rjlb/2015/1/2015_01_0005_0019.pdf). Acesso em: 01 maio 2021.

<sup>102</sup> Ibidem.

<sup>103</sup> Ibidem, p.13.

<sup>104</sup> Ibidem.

mais reducionista. Esse conjunto de fatores psicológicos que afetam o ato de julgar deveria merecer atenção muito maior por parte dos juristas, especialmente dos tribunais, cuja postura até agora tem se pautado por uma visão positivista, cartesiana até, na medida em que separa emoção e razão, o que se revela absolutamente equivocado no atual nível de evolução do processo.<sup>105</sup>

Ainda que a decisão proferida não seja diretamente fundamentada com base em provas ilícitas, mostra-se impossível a tarefa de verificar se houve ou não a contaminação do consciente, ou inconsciente do julgador por esses meios probatórios.<sup>106</sup> É incabível que se avalie em que graus de vestígio obtidos por violações a direitos entrarão na esfera *psique* do juiz; mas, é certo que elas possuem seu grau de participação, uma vez avistadas, nos rumos de uma decisão.

É por essa razão que se considera acertada a inclusão, renascendo o com a Lei nº 13.964/2019, do §5º ao art. 157 do Código de Processo Penal. Dispõe-se no referido artigo que “o juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão”. O desentranhamento somente em relação às provas ilícitas e a manutenção do juiz não cumpre adequadamente o manejo de sua contaminação no processo, uma vez que “a garantia do impedimento da utilização e valoração das provas ilícitas deve refletir também no campo psíquico, ou seja, nas convicções subjetivas do magistrado”.<sup>107</sup>

Segundo as considerações de Miguel Reale:

Na realidade, sabemos que o juiz, antes de ser juiz, é homem partícipe de todas as reservas afetivas, das inclinações e das tendências do meio social, e que nós não podemos prescindir do exame dessas circunstâncias, numa visão concreta da experiência jurídica, por maior que deva ser necessariamente a nossa aspiração de certeza e objetividade.<sup>108</sup>

Em face do exposto, é imprescindível que se considere, na amplitude das outras questões já expostas, conforme direciona Prado, os arquivos digitais “tende(m) a ser colocado(s) acima(s) do debate, em uma espécie de consenso irreal acerca de sua infalibilidade e correção”,<sup>109</sup> o que conseqüentemente implica numa necessidade ainda maior de afastar magistrado que se depara no contexto de ilicitude probatória.

<sup>105</sup> LOPES JUNIOR, Aury. **Direito Processual Penal**. São Paulo: Saraiva, p. 180. 2021.

<sup>106</sup> SALGRETI, Maria. A inconveniência jurídica na admissibilidade das provas ilícitas pelo seu mero desentranhamento físico dos autos e pela continuidade do juiz que dela tivera conhecimento à frente do processo na persecução dos crimes de natureza. **Revista Brasileira de Ciências Criminais**, v. 117, 2015. p. 8.

<sup>107</sup> KELLEN, Soares. A quebra da cadeia de custódia resultante na contaminação da prova e do magistrado. Disponível em: <https://canalcienciascriminais.com.br/a-quebra-da-cadeia-de-custodia-resultante-na-contaminacao-da-prova/>. Acesso em: 02 maio 2021.

<sup>108</sup> REALE, Miguel. **Filosofia do direito**. 17. ed. São Paulo: Saraiva, 1996. p. 114.

<sup>109</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. São Paulo: Marcial Pons, 2014. p. 73.

### 3 A CONFIABILIDADE DOS DADOS PROBATÓRIOS: A PRESERVAÇÃO CADEIA DE CUSTÓDIA NO CIBERESPAÇO E A SEGURANÇA DA INFORMAÇÃO

*‘Quer chamemos isso de pós-verdade ou pré-verdade, é perigoso ignorar a realidade. E é disso que estamos falando aqui. O perigo da pós-verdade não é apenas permitir que nossas opiniões e sentimentos desempenhem um papel na formação do que pensamos acerca dos fatos e da verdade, mas, ao fazê-lo, correr o risco de se distanciar da própria realidade’.*<sup>110</sup> (Lee McIntyre)

#### 3.1 A cadeia de custódia da prova digital: conceitos, fundamentos e riscos de sua quebra

Os primeiros capítulos possibilitaram demarcar os desafios diversos dos direitos penal e processual penal quando confrontados com as transformações paradigmáticas ocorridas com o processo de informatização da sociedade. A investigação, a criminalidade e os meios probatórios certamente acompanharam tais mudanças ao ponto de inserirem novas questões à persecução criminal de modo que é possível perceber que há a intersecção com o próprio debate acerca da proteção de dados, sendo perceptível que em numerosos momentos a discussão colide com uma questão proeminente: como garantir a confiabilidade dos dados coletados na forma de prova digital?

É em torno dessa perspectiva que surge a *digital forensic*, como o ramo da perícia forense dos elementos dos vestígios deixados no âmbito informático-digital. Por meio desta ciência, é possível realizar a análise dos arquivos eletrônicos e computadorizados, bem como a recuperação e descoberta desses dados para comporem o universo probatório.<sup>111</sup>

Conforme Gomes aponta, ao referir-se aos estudos de Benjamin Rodrigues, essa perícia envolve “a recolha, preservação, análise, e apresentação da prova eletrónico-digital”, e para se ter acesso a esses elementos é necessária a execução de uma série de requisitos e protocolos que permitam que essas provas sejam admissíveis em juízo.<sup>112</sup> Assim, se apresenta a “cadeia de custódia” da prova ou *chain of custody*, como correspondente a esse conjunto de

<sup>110</sup> Texto original (tradução livre): “Whether we call it post-truth or pre-truth, it is dangerous to ignore reality. And that is what we are talking about here. The danger of post-truth is not just that we allow our opinions and feelings to play a role in shaping what we think of as facts and truth, but that by doing so we take the risk of being estranged from reality itself” (McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018, p. 172).

<sup>111</sup> MARTINEZ, Thiago Hartmann. **Os direitos fundamentais X segurança pública**: a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. Dissertação (Mestrado em Direito). Faculdade de direito da Universidade de Lisboa. Lisboa, 2019. p. 16.

<sup>112</sup> MARTINEZ, Thiago Hartmann. **Os direitos fundamentais X segurança pública**: a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. Dissertação (Mestrado em Direito). Faculdade de direito da Universidade de Lisboa. Lisboa, 2019. p. 17.

procedimentos a serem observados e adotados em uma prova judicial, seja ela física ou digital.

A cadeia de custódia, portanto, identifica-se como uma espécie de história cronológica da prova, conforme se depreende da definição de Gustavo Badaró:

um procedimento de documentação ininterrupta, desde o encontro da fonte de prova, até a sua juntada no processo, certificando onde, como e sob a custódia de pessoas e órgãos foram mantidos tais traços, vestígios ou coisas, que interessam à reconstrução histórica dos fatos no processo, com a finalidade de garantir sua identidade, integridade e autenticidade.<sup>113</sup>

Geraldo Prado, autor de obra exclusiva sobre o assunto, a conceitua como “dispositivo dirigido a assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória”.<sup>114</sup> Além das definições doutrinárias, é possível trazer à baila duas acepções sobre o instituto, uma delas referente à Portaria nº 82 de 2014, do Ministério da Justiça, e a outra decorrente da sua regulamentação pela Lei 13.964/19 (Pacote anticrime), que inseriu no CPP o art. 158-A. Dessa forma, apresentam-se, respectivamente, cada uma:

Denomina-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.<sup>115</sup>

158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.<sup>116</sup>

Com base nisso, é possível perceber que, no Brasil, antes mesmo de sua previsão em lei, a cadeia de custódia da prova física já se guiava por um conceito e obtinha ainda o seu conteúdo procedimental pelas diretrizes estabelecidas pela Portaria nº 82 de 2014.<sup>117</sup> Em muitos momentos, o próprio CPP já continha diversas disposições no mesmo sentido, distribuídas entre seus artigos, como é o caso, por exemplo, do art. 6.º que prevê etapa

<sup>113</sup> BADARÓ, Gustavo. **A cadeia de custódia e sua relevância para a prova penal**. In: SIDI, Ricardo; LOPES, Anderson B. (org.). *Temas atuais da investigação preliminar no processo penal*. Belo Horizonte: D’Plácido, 2018. p. 523.

<sup>114</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014. p. 86.

<sup>115</sup> BRASIL. Secretaria Nacional de Segurança Pública. **Portaria n. 82 de 18 de julho de 2014**. Estabelece as Diretrizes Sobre os Procedimentos a Serem Observados no Tocante à Cadeia de Custódia de Vestígios. Disponível em: [http://www.lex.com.br/legis\\_25740023\\_portaria\\_n\\_82\\_de\\_16\\_de\\_julho\\_de\\_2014](http://www.lex.com.br/legis_25740023_portaria_n_82_de_16_de_julho_de_2014). Acesso em: 05 maio 2021.

<sup>116</sup> BRASIL. **Lei nº 13.964**, de 24 de dezembro de 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13964.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm). Acesso em: 06 maio 2021.

<sup>117</sup> Cf. SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA DO MINISTÉRIO DA JUSTIÇA. **Portaria SENASP nº 82 de 16 de julho de 2014**. Disponível em: <https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm>. Acesso em: 06 maio 2021.

semelhante ao descrito agora como o isolamento dos vestígios, com a atitude do policial de conservação do estado das coisas até a chegada do perito.<sup>118</sup>

Antes dessas disposições, o tema só era tratado intuitivamente entre os peritos como um debate estritamente técnico. Ocorre que toda a discussão remete diretamente ao tema de provas ilícitas, ou seja, de uma garantia elencada constitucionalmente. Assim sendo, a “cadeia de custódia das provas digitais é uma garantia de natureza constitucional e não mera consequência lógica do sistema de preservação do corpo de delito digital”.<sup>119</sup> O seu alcance é ainda mais relevante quando os vestígios são de natureza digital, em que há um elevado risco de manipulação.<sup>120</sup>

Prado refere-se à experiência norte-americana para ilustrar e contribuir ao debate legislativo brasileiro relativamente ao papel da cadeia de custódia em relação às provas ilícitas, tendo em vista que o sistema do país é pensado de modo a dirimir a complexidade que orbita o cosmos da vedação dessas ilicitudes, incorporando a relação procedimento no processo de valoração da prova. Nesse sentido é que aponta que a interrupção da cadeia de custódia é atributo apto a inviabilizar a admissibilidade de uma evidência.<sup>121</sup>

Alberi Espindula explica que a cadeia de custódia deve abranger desde a etapa recolha do objeto até o trânsito em julgado do processo. Isso significa que sua compreensão não envolve somente a perícia criminal, mas implica sua observância desde da entrada do objeto na delegacia, ou ainda o primeiro contato do policial o material potencialmente ligado a uma persecução penal. Nesse cenário, conclui que “o valor probatório de uma evidência ou documento

---

<sup>118</sup> MAGNO, Levy; COMPLOIER, Mylene. **Cadeia de custódia da prova penal**. p. 4. Disponível em: [https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj\\_n57\\_10\\_cadeia%20de%20cust%C3%B3dia.pdf?d=637437206976264894](https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj_n57_10_cadeia%20de%20cust%C3%B3dia.pdf?d=637437206976264894). Acesso em: 06 maio 2021. O artigo elenca as disposições que apontavam para a necessidade e o procedimento cabível para a preservação da prova: Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: I – dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; II – apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; III – colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; (...) VII — determinar, se for caso que se proceda a exame de corpo de delito e a quaisquer outras perícias (art. 6.º, CPP); art. 11 (acompanhamento dos objetos que interessam à prova aos autos do inquérito), art. 159 e §1º (realização do exame de corpo de delito), indicação de assistentes técnicos (art. 159, 3.º, e §4º, CPP), art. 159 §6º, art. 161 (momento de feitura do exame de corpo de delito), art. 162 (autópsia), arts. 163 a 166 (procedimento de exumação), art. 168 (complemento do exame pericial), art. 169 (exame de local do crime), art. 170 (guarda de material para eventual nova perícia), art. 171 (crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa ou por meio de escalada), art. 172 (avaliação de coisas), art. 173 (crime de incêndio), art. 174 (exame para reconhecimento de escritos), art. 177 (exame por precatória) e art. 180 (divergência entre peritos). (Ibidem).

<sup>119</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 10. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

<sup>120</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 82.

<sup>121</sup> Ibidem, p. 81.

será válido se não tiver sua origem e tramitação questionada. Assim, qualquer questionamento acarretará prejuízo para o processo como um todo”.<sup>122</sup>

Percebe-se, portanto, que o procedimento relativo ao manuseio e documentação das suas etapas em ordem, denotam um *status* verdadeiramente fundamental para o adentramento das fontes de prova ao processo judicial. Deve-se perquirir, portanto, “onde”, “como”, “por que” e ainda “quem” no universo de questões a serem expostas no registro da cadeia de custódia do material probatório.<sup>123</sup> Carlos Mendes, dessa forma, estabelece que não só o conteúdo das evidências tecnológicas deve ser questionado, mas também o próprio método de recolha digital do qual elas advêm.<sup>124</sup> A esse respeito, o autor, utilizando-se dos ensinamentos de Torres, acentua que

[...] existem dois requisitos fundamentais para prosseguir uma investigação informática. O primeiro é a ‘confiabilidade do método de tratamento dos dados’, o segundo, refere-se à ‘verificabilidade da idoneidade do método’. Isso porque a confiabilidade da prova digital no processo penal depende de uma complexa garantia que abarque tanto a originalidade do dado, em termos de conservação, como a cópia deste ao ponto de sua ‘genuinidade’ e ‘não modificação’. Tais resultados podem ser alcançados através de um protocolo procedimental metodologicamente guiado, cujo objetivo é a preservação do risco de comprometer o resultado final.<sup>125</sup>

Por efeito dessas considerações, compreende-se que o procedimento para garantir a fiabilidade e integridade de uma prova é permeado pelo questionamento em volta do mecanismo organizador da prova, eis que o dispositivo informático é alvo de maior inquietação acerca da sua manipulação. Nessas circunstâncias, Geraldo Prado assinala dois princípios que surgem às vistas da proteção das provas no processo penal: a “mesmidade” e a “desconfiança”. O primeiro diz respeito à garantia de que a prova colhida corresponde a uma cópia fiel da original, em todos os seus aspectos, de modo que apenas parte da evidência não é suficiente para responder ao critério de “mesma prova”.<sup>126</sup> Por outro lado, a “desconfiança”

<sup>122</sup> ESPINDULA, Alberi. **Perícia criminal e cível: uma visão geral para peritos e usuários da perícia**. 3. ed. Campinas: Millenium, 2013. p. 165.

<sup>123</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal: Entre a proteção de dados e a infiltração por software**. Salvador: Juspodivim, 2020. p.147.

<sup>124</sup> *Ibidem*. p. 147

<sup>125</sup> *Ibidem*, p.112

<sup>126</sup> Acerca do debate, Aury Lopes Júnior e Rosa (In: **A importância da cadeia de custódia para preservar a prova penal**. Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>. Acesso em: 06 maio 2021). estabelecem ser essa “Questão recorrente nas interceptações telefônicas está na violação da “mesmidade” e, por via de consequência, do direito da defesa de ter acesso a integralidade da prova na sua originalidade (manifestação do contraditório=direito a informação e paridade de armas), na medida em que a prova é ‘filtrada’ pela autoridade policial ou órgão acusador, que traz para o processo (e submete ao contraditório diferido) apenas o que lhe interessa. Não é ‘a mesma’ prova colhida, mas apenas aquela que interessa ao acusador, subtraindo o acesso da defesa. A manipulação (e aqui se emprega no sentido físico do vocábulo, sem juízo de desvalor ou atribuição de má-fé ao ‘manipulador’) é feita durante a custódia e viola exatamente as regras de preservação da idoneidade.

consiste em submeter os vestígios a um rito com parâmetros objetivos que assegurem sua credibilidade, que é realmente aquilo que a parte alegar ser.<sup>127</sup>

Com base nisso, ressalta-se a necessidade de se desconstruir a “presunção de fidedignidade” em relação aos sistemas informáticos, dado que carece de uma justificativa para tanto. Uma atuação com base nesse pressuposto, de uma fonte de prova que está a salvo de qualquer confrontação, ignora o fator humano, seja ele realizado de forma proposital ou não, como passível de ser responsável pela contaminação da prova, bem como objeto de questionamento, sendo certo que uma perspectiva que assuma uma autenticidade irrefutável, notadamente é prejudicial ao direito ao contraditório.<sup>128</sup> De modo semelhante, assevera Aury Lopes Junior, ao constatar a existência de provas “acabam por sedar os sentidos e anular o contraditório”,<sup>129</sup> de modo que

A discussão acerca da quebra da cadeia de custódia adquire especial relevância nas provas que têm pretensão de ‘evidência’, verdadeiros atalhos para obtenção da tão almejada (e ilusória) ‘verdade’, que sedam os sentidos e têm a pretensão de bastar-se por si sós, de serem autorreferenciadas[...]. Nestas situações, por serem obtidas ‘fora do processo’, é crucial que se demonstre de forma documentada a cadeia de custódia e toda a trajetória feita, da coleta até a inserção no processo e valoração judicial.<sup>130</sup>

Falar em quebra da cadeia de custódia não é indagar sobre a postura dos agentes estatais enquanto dotada de má-fé. O seu significado não possui uma associação com tais critérios subjetivos. O que se pretende é “objetivamente definir um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente”.<sup>131</sup> De certo que, conforme preleciona Prado, “no caso de quebra da cadeia de custódia não se cogita perquirir sobre a boa ou má-fé dos agentes policiais que manusearam o produto da atividade de investigação dos meios de prova”.<sup>132</sup>

Quando há uma violação, uma quebra, da cadeia de custódia, não se questiona seu valor probatório ou mesmo a sua relevância, ou seja, simplesmente não se pode valorar uma prova obtida nessas circunstâncias. Não de outra maneira, deve ocorrer com o material probatório digital. Dessa forma, determina Prado que “violada a cadeia de custódia do elemento probatório, não é mais possível assegurar a autenticidade da prova e sua

<sup>127</sup> PRADO, Geraldo. Ainda sobre a quebra da cadeia de custódia das provas. **Boletim do IBCCrim**, São Paulo, n. 262, setembro de 2014a. p.16-17.

<sup>128</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 148.

<sup>129</sup> LOPES JUNIOR, Aury. **Direito Processual Penal**. São Paulo: Saraiva, 2021. p. 182.

<sup>130</sup> Idem.

<sup>131</sup> Ibidem.

<sup>132</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 83.

integridade, sendo a prova inadmissível, pois, insuscetível de exame de peso ou força probatória”.<sup>133</sup> Excepcionalmente, essa proibição será relativizada quando seu intento for em favor da defesa ou liberdade de um inocente.<sup>134</sup>

A cadeia de custódia, portanto, cumpre um inestimável valor epistêmico, afastando do campo gravitacional valorativo das provas, aquelas cuja origem é temerária ou não se pode ser realmente acessada. Essa acepção é bem ilustrada por Prado:

Evitar a zona de contágio da evidência é a tarefa epistêmica do processo, que se arma de instrumentos para filtrar a maior parte das pulsões devoradoras das provas, porque é disso que se trata a evidência: algo que, ao dispensar, a prova, devora os procedimentos probatórios, que são substituídos inconscientemente pelas crenças, em aparência imunes às tentativas das partes influenciarem na formação da convicção do juiz.<sup>135</sup>

Assim, a cadeia de custódia serve com o propósito de ser mais um dispositivo probatório que funciona como escudo ao contágio das crenças do juiz na fundamentação de suas decisões, sem uma correspondente comprovação empírica, eis que se adiciona mais um elemento essencial para a garantia de sua fiabilidade, bem como medidas que visam a sua proteção em relação a possíveis falsificações.<sup>136</sup> Por conseguinte, urge a necessidade de definir procedimentos específicos como referência a cadeia de custódia da prova digital.

Em que se pese as dificuldades inerentes em se estabelecer critérios para a prática computacional forense, dada a velocidade das mudanças das tecnologias de informação, o que acaba por gerar um comportamento mais reativo dos peritos defrontados com a exigência de uma metodologia, já existem documentos com reconhecimento internacional que servem ao menos como ponto de partida.<sup>137</sup> Na maioria dos casos, portanto, existem procedimentos já vigentes que fornecem uma base concreta para as diligências a serem satisfeitas.

### **3.1.1 Parâmetros técnicos atuais de segurança da informação e fiabilidade dos vestígios no ambiente digital**

---

<sup>133</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 5. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

<sup>134</sup> Ibidem, p. 2-26.

<sup>135</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 85.

<sup>136</sup> Ibidem, p. 86.

<sup>137</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 7. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

A partir do exposto no último tópico, foi possível compreender o papel ocupado pela cadeia de custódia, num primeiro plano para a paridade de armas e garantia do contraditório e direito de defesa,<sup>138</sup> notadamente quando referenciadas no ambiente digital. Ocorre que o tratamento dado pela alteração legislativa decorrente da Lei nº 13.964/2019 não trouxe a inclusão de provas que não sejam físicas. Além disso, é inaceitável que se pense em ser usada alguma espécie de analogia a equiparar essas espécies probatórias, eis que essencialmente distintas, o que traria uma solução quase sempre inadequadas.

Nessas circunstâncias, revela-se o valor da cadeia de custódia ainda mais evidentes nas provas de natureza digital, de forma que

se manuais, guias de procedimento, atos normativos de toda espécie, estatais e supra estatais, enfatizam em geral o papel que a cadeia de custódia desempenha para assegurar integridade e autenticidade à prova digital, fato é que a jurisprudência firmada por cortes constitucionais e tribunais de direitos humanos assinala à cadeia de custódia da prova digital funções ainda mais relevantes.<sup>139</sup>

Por essa razão, destacamos aqui alguns passos importantes que fazem parte da cultura forense em relação à integridade dos sistemas informáticos e vestígios digitais, com atenção às características singulares que elas exprimem. Há que dizer que um relatório detalhado cumpre uma função primordial no objetivo de se preservar a cadeia de custódia, informações como: 1) código *hash*; 2) a devida localização da fonte; 3) a assinatura eletrônica; 4) identificação dos indivíduos que a contactaram; 5) bem como o momento de acesso à prova, indicam um primeiro panorama de sua análise.<sup>140</sup>

Explica-se que a função de *hash* é um algoritmo capaz de transformar uma enorme quantidade de informações numa muito menor, e é alterado toda vez que apenas um *bit* é de qualquer forma modificado.<sup>141</sup> Em maiores detalhes.

A função hash produz um resumo matemático: ela recebe uma entrada de dados de qualquer comprimento e cria uma saída de comprimento fixo. Por exemplo: ao submetermos o arquivo da Constituição Federal disponível no site do planalto à função digestora (MD5) reduzimos seus volumosos

<sup>138</sup> PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1. ed. São Paulo: Marcial Pons, 2014. p. 59.

<sup>139</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 10. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

<sup>140</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 149) “Para uma um mais aprimorado relato de data/hora de acesso ao material probatório digital tem o *Time Stamp*, como “ferramentas utilizadas para marcar o exato horário referente a um log (data/hora). Em sistemas de arquivos, a data e a hora podem se referir às datas e relacionadas à criação do arquivo ou a modificação do arquivo”. MENDES, Carlos, p. 159 In COSIC, Jasmin. BACA, Miroslav. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp, p. 3).

<sup>141</sup> R.W.R. Carvalho. A Importância da Cadeia de Custódia na Computação Forense. **Rev. Bras. Crimin.** 9(2), p.136, 2020.

669.114 caracteres para apenas 32: 'b846221c1f44390f4c6ece0ebac941db'. É uma via de mão única. Não há como recuperar o texto constitucional a partir do seu resumo matemático. Originalmente concebida para comprimir dados e otimizar recursos nos processos de indexação e busca de informações, a função digestora produz um segundo benefício: um identificador único. Qualquer alteração no arquivo da Constituição Federal, para continuarmos com o mesmo exemplo, gerará um resumo diferente. Duas mensagens nunca devem retornar o mesmo hash.<sup>142</sup>

Vale dizer que além da contaminação digital, eis que a alterabilidade é um atributo marco desse gênero probatório, a incorreta manipulação física também acarreta consequências danosas. Nesse sentido, mesmo os procedimentos próprios das provas tradicionais contribuem para verificar a forma de contágio, como a partir de impressões digitais ou marcas de um determinado componente do maquinário, a exemplo do disco rígido.<sup>143</sup>

Diante disso, Mendes, com o amparo dos estudos de Marshal, elenca quatro princípios que podem servir como modelo orientador: o primeiro é endereçado aos agentes estatais que não devem realizar nenhuma alteração no material colhido e que será posteriormente levado ao Tribunal; em segundo lugar, deve-se ter pessoas capacitadas e especializadas para ter acesso aos dados ou armazenamento do dispositivo; um terceiro princípio dispõe que através dos registros fornecidos referentes ao processo de recolha da fonte de prova, deve ser de tal forma preciso que um terceiro à parte conseguia obter os mesmos resultados; por fim, estabelece que para que esses princípios sejam devidamente seguidos, requer-se que a pessoa responsável pela investigação seja encarregada de fazer valer toda a metodologia pertinente, inclusive dos preceitos em questão.<sup>144</sup>

A ABNT NBR ISO/IEC 27037:2012, além de possuir o conceito de vestígio digital e suas características, possui em seu escopo um conjunto de procedimentos destinados a garantir a segurança da informação. Assim, assinalam-se outros conceitos definidores relevantes acerca dos dispositivos digitais necessários a compreensão dos momentos da cadeia de custódia da prova: sua auditabilidade, justificabilidade e reprodutibilidade. Dessa maneira, respectivamente, a auditabilidade analisa se houve a correta aplicação da técnica

---

<sup>142</sup> VIEIRA, Thiago. **O que é a função digestora HASH e qual é sua relevância para a computação forense?**. Disponível em: <https://medium.com/contrarraz%C3%B5es/o-que-%C3%A9-a-fun%C3%A7%C3%A3o-digestora-hash-e-qual-%C3%A9-sua-relev%C3%A2ncia-para-a-computa%C3%A7%C3%A3o-forense-2351a2d81fec>. Acesso em: 05 maio 2021.

<sup>143</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p. 149.

<sup>144</sup> *Ibidem*, p. 153.

compatível com o sistema, a atividade ou a informação comunica-se, portanto, com o que já delineamos como o princípio da “desconfiança”.

No que tange a justificabilidade, indica a adequação entre os resultados pretendidos e a metodologia adotada na evidência digital. A repetibilidade é a capacidade de se obter os mesmos resultados, sob as mesmas condições, daqueles originalmente vistos, correspondente ao que seria a “mesmidade”. A reprodutibilidade, por outro lado, exige que em distintos dispositivos e condições, resista-se a verossimilhança obtida pela fonte original.<sup>145</sup>

A obtenção da prova digital, no que lhe concerne, deve seguir as seguintes etapas: identificação, coleta, aquisição e preservação. Mendes, por outro lado, define como um procedimento minimamente adequado aquele composto pela “recolha, autenticação, exame, análise e relatório”.<sup>146</sup> A recolha ou identificação é etapa por meio da qual os investigadores forenses sinalizam para as fontes de provas relevantes. A fase compatível ao exame representa o processo de seleção, dentre as fontes de prova identificadas, as quais assumem especial relevância no processo. Após, segue-se para a verificação, é nessa etapa que é possível atestar adequadamente a autenticidade e integridade de uma prova. É nesse momento, por exemplo, que entra em cena a função *hash*.<sup>147</sup>

O armazenamento é o próximo estágio do itinerário protocolar. Nesse ponto, ganha importância a adoção de uma unicidade procedimental e a padronização de métodos dos dados colhidos e armazenados. O relatório, por sua vez, é o documento que conecta as alegações defensivas e acusatórios em torno da prova no processo judicial.<sup>148</sup>

Nesse sentido, deve-se considerar tanto sua representação física quanto lógica. A física diz respeito à representação tangível no aparelho, enquanto a lógica refere-se a virtual. A técnica a ser utilizada deve valer-se da pesquisa, reconhecimento de toda a documentação da evidência digital, contexto que demonstra a necessidade de, num momento inicial, identificar a natureza do dispositivo quanto a sua volatilidade, para garantir assim sua integridade; e frisa-se aqui também a indispensabilidade de serem feitas, nesse momento, buscas relativas à adulteração e apagamento de dados.<sup>149</sup>

---

<sup>145</sup> FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 8. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 03 abr. 2021. p. 9.

<sup>146</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal: Entre a proteção de dados e a infiltração por software**. Salvador: Juspodivim, 2020. p. 155-156.

<sup>147</sup> Ibidem, p. 154-155.

<sup>148</sup> Ibidem, p. 160.

<sup>149</sup> FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 8. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 03 abr. 2021. p. 10.

É por essa característica específica, a volatilidade, bem como em alguns casos a fragilidade, que uma maior agilidade na preservação de dados é especialmente interessante, senão indispensável, seja no tocante aos dados de informação ou aqueles em tráfego de comunicação.<sup>150</sup>

Na perspectiva das considerações acima, depreende-se que a preservação dos vestígios depende de uma correta coleta, registro, acondicionamento e transporte, os quais são elementos da cadeia de custódia, que visa exatamente corresponder a história cronológica de uma prova. Importa-se dizer que “as evidências no meio digital representam as informações armazenadas ou transmitidas eletronicamente na forma de bits que podem ser invocadas em juízo”. Conforme exposto anteriormente, a alteração ou exclusão em apenas um único desses bits pode provar sua alteração, de modo que deve ser calculado o algoritmo da mídia e o da coleta para fins comparativos.<sup>151</sup>

Pequenas observações procedimentais ou mesmo falhas podem significar sua impossibilidade de ser considerada pelo magistrado. Assim sendo, um número de *hash* diferente ou a paralisação da documentação da custódia em algum momento pode gerar a inadmissibilidade da prova. Há duas formas de gerar um questionamento dessa natureza: quando não houve de fato a realização da cadeia de custódia, e ainda quando há a ilicitude da evidência, uma vez que não houve a correta preservação do seu conteúdo. Cita aqui como exemplo a operação Ouro Verde, na qual a polícia, antes mesmo de gerar o código *hash* acessou o disco rígido do notebook apreendido, embora tenha dito em depoimento que não realizou nenhuma modificação. A sentença, no entanto, foi mantida pelo Tribunal Regional Federal da 4ª Região.<sup>152</sup>

Salienta-se que nunca se deve utilizar a evidência original para a realização desses procedimentos. Isso se dá em razão da necessidade de preservação do vestígio original e manutenção da sua integridade. O melhor parâmetro atual que permitiria uma garantia de intocabilidade da evidência original, é a *image*, como a “operacionalização de uma fotografia digital, uma cópia mestra protegida, que evita o manuseio das fontes probatórias originais e assim conserva sua integralidade”.<sup>153</sup>

---

<sup>150</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p.139.

<sup>151</sup> R.W.R. Carvalho. A Importância da Cadeia de Custódia na Computação Forense. **Rev. Bras. Crimin.** 9(2), p.135, 2020.

<sup>152</sup> Ibidem. p. 136. Cf. BRASIL. Tribunal Regional Federal (4. Região). Apelação Criminal Nº 5012492-10.2012.4.04.7100. Apelante: Marylin Preto Kulkes.. Apelado: Ministério Público Federal. Relator: Leandro Paulsen.

<sup>153</sup> MENDES, Carlos Hélder C. F. **Tecnoinvestigação criminal**: Entre a proteção de dados e a infiltração por software. Salvador: Juspodivim, 2020. p.156.

Ademais, ressalta-se a importância de as mídias de coletas estarem limpas, ou sejam, completamente livres de qualquer outra informação, ou um *bit* sequer, sob pena de se produzir resultados inverídicos e inconsistentes. Vale dizer que conforme determina o Código de Processo Penal, em seu art. 159, §6º, é direito da defesa que a evidência esteja à disposição para ser examinada, quesitada ou consultada.<sup>154</sup>

Trabalha-se, a partir do horizonte de questões apresentadas, o modelo que consiste numa base comum de padrões normalmente seguidos para a realização da cadeia de custódia. O requisito número um é a identificação do equipamento com o número do caso, o item e sua descrição, fabricante, modelo e número de série. Posteriormente, preparam-se os detalhes sobre a imagem dos dados com a data e hora da captura da imagem, a identificação do perito e método utilizado, o nome da imagem e quantidade de partes que foi dividida, e o drive e sua correspondência algorítmica (*hash*). O formulário de cadeia de custódia também deve abordar seus motivos e itinerário, de modo a demarcar o destino da evidência, horário e local de saída, a respectiva identificação do responsável pela sua guarda e a fundamentação de eventuais mudanças.<sup>155</sup>

Como se exige a perícia como regra para os crimes que deixam vestígios, é necessário a expedição de mandado de busca e apreensão, e que o perito seja acompanhado preferencialmente do delegado de polícia e policiais civis na cena do crime. Assim determina ainda que

a equipe computacional forense deve estar munida de equipamento fotográfico, case externo de leitura e escrita, case externo protegido contra escrita, mídias de inicialização contendo softwares forenses, equipamento computacional portátil equipado com softwares forenses, assim como hardwares para armazenamento dos vestígios digitais a serem coletados.<sup>156</sup>

A cadeia de custódia é de suma importância na rastreabilidade das provas e a comprovação da sua integridade e atributo indispensável à atividade probatória. A especificidade das provas digitais e o aumento dos crimes realizados no ambiente tecnológico, juntamente com a necessidade de sua preservação para o uso em uma persecução criminal, exigem a definição da cadeia de custódia dessa espécie probatória, bem como a especialização de agentes públicos responsáveis pela investigação criminal para garantir sua preservação e correto tratamento. Para isso, já existem normativos que servem de base, como

---

<sup>154</sup> CARVALHO, Romullo Wheryko de. A Importância da Cadeia de Custódia na Computação Forense. **Bras. Crimin.**, v. 9, n. 2, p. 134-138, 2020. p. 136.

<sup>155</sup> Idem.

<sup>156</sup> FURLANETO NETO, Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. 2020, p. 11. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130/940>. Acesso em: 03 abr. 2021.

a ABNT NBR ISO/IEC 27037:2012 e o próprio procedimento operacional veiculado pela SENASP que devem ser incorporados, além de se encontrar fontes na literatura especializada nacional e especialmente internacional, para a formação de peritos computacionais forenses.

### **3.2 O direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos: Segurança da informação e proteção de dados na persecução criminal**

O quadro delineado pelo escopo desse estudo aponta para uma ruptura profunda da forma como lidamos com a informação, inclusive daquelas que dizem ao nosso privado, do “intocável”. Os dados, e conseqüentemente a proteção deles, mais do que nunca importam e recrudescem em relevância enquanto surgem formas cada vez mais invasivas da atuação dos agentes de investigação. Está certo que se estabelece, pois, uma relação intrínseca entre a investigação criminal atual e também em uma visão prospectiva dela, com o direito à intimidade e privacidade.

Nessas circunstâncias, em que se proclama uma atuação do Estado no sentido de criar condições que garantam o respeito aos direitos fundamentais em face de um exponencial volume de dados gerados pelas novas tecnologias de informação, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) surge como resposta a essas demandas ocasionadas pela sociedade de informação. Dentre a base principiológica utilizada como fundamento para a referida legislação, insurge-se o princípio da autodeterminação informativa. Como vimos, trata-se de um princípio que visa dar aos indivíduos o controle do gerenciamento de seus dados, sendo “a capacidade do indivíduo para determinar, em princípio, a divulgação e o uso de seus dados pessoais”.<sup>157</sup>

A origem desse instituto encontra-se numa decisão de 1983 do Tribunal Constitucional da Alemanha (*Bundesgerichtshof*), passando a oferecer assim uma visão objetiva à intimidade, que não estaria tão somente atrelada a questões privadas. Sua interpretação foi construída a partir do direito ao livre desenvolvimento da personalidade, fortemente afetado pelo desenvolvimento tecnológico. O propósito do presente estudo, no entanto, possui uma abrangência mais específica, embora correlacionado as outras questões e princípios também atinentes ao tema: o direito fundamental à garantia da confidencialidade e

---

<sup>157</sup> PEREIRA, Alexandre Libório Dias. O direito à autodeterminação informativa» na jurisprudência portuguesa: breve apontamento. *Ars Iuris Salmanticensis*, v. 5, dez. 2017, p. 27. Disponível em: <http://revistas.usal.es/index.php/ais/article/view/18011/18411>. Acesso em: 06 maio 2021.

da integridade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

A gênese do referido direito também ocorre com uma decisão do Tribunal alemão, que decorre igualmente da extensão do direito geral à personalidade. O contexto do julgamento deu origem a essa proteção, que ultrapassou a já cunhada autodeterminação informativa. Cabe, nesse sentido, mostrar que em 2007, o assunto já havia entrado em pauta no BSG, na discussão a respeito da infiltração de métodos ocultos na investigação criminal, por meio da utilização de sistemas informáticos, o qual era aplicado com base na analogia de três normas existente no direito alemão: a permissão de apreensão de objetos que tenham finalidade investigativa, a busca domiciliar e ainda o monitoramento das telecomunicações.<sup>158</sup>

Foi somente no ano de 2008, no entanto, na análise de constitucionalidade da lei do Estado de *Nordrhein-Westfalen*, no âmbito do uso das autoridades policiais de medidas de infiltração em computadores que se firmou o entendimento e criação de um novo direito fundamental à garantia da confiabilidade e integridade de sistemas informáticos, o Art. 2, I, c/c Art. 1, I, da Lei Fundamental alemã. Faz-se pertinente a explicação de Schertel sobre um dos fundamentos da decisão:

Na sua fundamentação, a Corte constitucional argumentou que o enorme desenvolvimento das tecnologias da informação nos últimos anos alterou os comportamentos e os hábitos dos indivíduos, ampliando especialmente a relação de dependência entre o homem e a tecnologia.<sup>159</sup>

A Corte alemã consignou, portanto, que as concepções até então prestigiadas e alcançadas pela expressão do direito da personalidade não atenderia de modo adequado as

---

<sup>158</sup> GRECO, Luís; GLEIZE, Orlandino. Infiltração online no processo penal : Notícia sobre a experiência alemã. *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1488, set.-dez. 2019. Pertinente dizer que na decisão do Tribunal alemão houve a necessidade de se desconstruir tais argumentos, que no fim foram tidos como insuficientes e inadequados para a proteção do direito em debate. Assim explicam os autores: [...]os direitos fundamentais dos Arts. 10 e 13 GG – que garantem proteção ao sigilo das telecomunicações e ao domicílio, respectivamente – não seriam aptos a proteger o indivíduo suficientemente contra o acesso a seus sistemas informáticos [...]A Corte entendeu, no entanto, que nem o acesso às informações nas mídias de armazenamento, nem o monitoramento da utilização de um sistema informático seriam intervenções à garantia de confiabilidade da telecomunicação do Art. 10 GG. E isso mesmo que a transferência dos dados obtidos nos dispositivos infiltrados até a central do investigador ocorresse por meio de sistemas de telecomunicação, como acontece com o acesso online em mídias de armazenamento de um computador alheio[...] b) O Art. 13 GG, protetor da inviolabilidade do domicílio, garante ao indivíduo, com vistas à dignidade humana e ao interesse no desenvolvimento da personalidade, um espaço físico elementar de vida. O bem protegido desse direito fundamental é a esfera espacial na qual a vida privada se desenvolve.<sup>31</sup> Na visão do BVerfG, esse direito fundamental não seria pertinente, pois seu objeto de proteção seria uma componente espacial do âmbito privado, que não seria tangenciada, caso uma intervenção ocorresse fora do domicílio ou o local do dispositivo em questão (um laptop ou um smartphone) não fosse reconhecível durante a investigação. A utilização de uma conexão do dispositivo com a internet ou com um outro computador também não interferiria na esfera espacial da vida privada (Ibidem).

<sup>159</sup> SCHERTEL, Laura. **Uso de softwares espões pela polícia: prática legal?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espies-pela-policia-pratica-legal-04062015>. Acesso em: 01 maio 2021.

novas demandas da sociedade. Nesse ponto, inovou-se ao entender que, em particular, a autodeterminação informacional não corresponderia as dimensões dos direitos tratados, pois se dirige à proteção de dados privados. A infiltração não teria essa limitação, eis que

A classificação de dados como privados depende ainda, muitas vezes, do contexto nos quais os dados são descobertos e da relação que tenham com outros dados. Frequentemente, a infiltração do sistema, que nem sempre possibilita a coleta apenas de dados privados e atinge indiscriminadamente todos aqueles armazenados no dispositivo, não permite, de antemão, verificar o significado dos dados para o afetado e quais outras informações podem ser construídas ao relacionar esses dados entre si.<sup>160</sup>

Conforme foi visto, a decisão não foi de banir o método da prática policial, mas, considerando o seu potencial altamente lesivo a direitos fundamentais, estipular rígidas exigências para haver sua realização, como a suspeita do fato, gravidade no caso concreto, subsidiariedade, proporcionalidade, entre outros aspectos.<sup>161</sup> As cautelas técnicas necessárias, ao definir protocolos de procedimentos garantem, nesse sentido, o que corresponderia ao controle da cadeia de custódia do procedimento da medida.<sup>162</sup>

Sendo assim, as questões levantadas no arcabouço da decisão trazem consigo um desdobramento que atinge diretamente uma sociedade completamente imersa na digitalização: a necessidade de um direito que “proteja não apenas contra invasões à privacidade, mas também contra manipulações em sistemas informáticos privados”.<sup>163</sup> Dessa maneira, “o funcionamento adequado desses sistemas pressupõe que quem os utiliza pode confiar que as informações produzidas não sofrem interferência, interceptação, nem manipulação de qualquer tipo”.<sup>164</sup>

Apreende-se, em vista desses esclarecimentos, que a elevação da tutela da integridade e confidencialidade dos sistemas de comunicação, posta na categoria de direito fundamental, é uma função proeminentemente percebida através da cadeia de custódia da prova digital, ao permitir a verificação da autenticidade de elemento probatório dessa natureza.<sup>165</sup> Assim, por meio do instituto da cadeia de custódia da prova digital:

são tutelados os direitos fundamentais à confidencialidade e garantia da integridade dos sistemas de tecnologia da informação, à proteção do entorno

<sup>160</sup> GRECO, Luís; GLEIZE, Orlandino. Infiltração online no processo penal: Notícia sobre a experiência alemã. **Rev. Bras. de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p.1494.

<sup>161</sup> Ibidem.

<sup>162</sup> Ibidem, p. 1504-1505.

<sup>163</sup> Ibidem, p. 1511

<sup>164</sup> SCHERTEL, Laura. **Uso de softwares espões pela polícia: prática legal?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espoes-pela-policia-pratica-legal-04062015>. Acesso em: 01 maio 2021.

<sup>165</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 7. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

digital, da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente a essa esfera da vida.<sup>166</sup>

Ainda cabe dizer, nesse ângulo, mais uma vez, que o universo digital não distingue a categoria de informações, entre privada e pública, o que denota um caráter ainda mais urgente e relevante da separação e distinção específica em relação a uma cadeia de custódia tradicional, tanto em complexidade, bem como, nesse aspecto, sua relevância. É por essa razão que a etapa de armazenamento bem como a identificação, segundo o discorrido no capítulo anterior, são valorosas no conjunto de procedimentos a serem adotados.

A Lei de Proteção de Dados (Lei nº. 13.709, de 14 de agosto de 2018), nessas circunstâncias, surge com o intuito de suprir essa demanda de proteção de dados. No entanto, veda em seus artigos 3º e 4º sua utilização no âmbito da segurança pública, defesa nacional, segurança do Estado, bem como as atividades de investigação e repressão das infrações penais, somente autorizados quando sob a tutela jurídica de pessoa de direito público.<sup>167</sup> Em razão dessa exceção, os dados do âmbito criminal não são regidos por essa mesma norma, devendo ser regulados a partir de uma lei específica.

É nesse quadro que entra em cena o Anteprojeto da “LGPD penal”, ou a “Lei de Dados para segurança pública e persecução penal”, a qual foi elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019. Pela análise de seu conteúdo, contudo, foram elencadas determinações essenciais para a proteção da intimidade como, apenas a título exemplificativo em face dos seus 68 artigos, o previsto em seu art. 14 e parágrafo 1º:

Art. 14. O tratamento de dados pessoais sigilosos por autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal. §1º O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável.<sup>168</sup>

Percebe-se na exposição dos motivos uma das justificativas de sua existência:

há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para

---

<sup>166</sup> Ibidem. p. 10.

<sup>167</sup> BRASIL. Lei 13.709 de 14 de agosto de 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 07 maio 2021.

<sup>168</sup> Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>. Acesso em: 07 maio 2021.

utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos.<sup>169</sup>

Pelo trecho, é visível que a segurança e tratamento de dados é um dos objetivos a ser perseguido pelo anteprojeto. Ocorre que não foi incluída no documento elementos específicos que padronizariam e forneceriam a base da formação de uma cadeia de custódia da prova digital, ainda que ela seja um elemento central do processo penal, com o advento de novas tecnologias, sendo certo a necessidade de “condições concretas de efetivação de um contraditório digital”.<sup>170</sup>

É imprescindível a atual posição de direito fundamental integridade e confiabilidade dos sistemas informáticos, cuja decisão do Tribunal alemão devem permear as discussões brasileiras, haja o alcance de seus vieses também no âmbito de uma cadeia de custódia que seja associada a parâmetros de discussões em torno da prova digital.

Traz-se, dessa forma, um conceito fundante para se compreender o processo de dependência do homem com a tecnologia: a ubiquidade. A ubiquidade é justamente o “fenômeno segundo o qual a tecnologia da informação e o processamento de dados perpassam todas as áreas da vida de um indivíduo”, sendo que sua principal consequência é “o desequilíbrio de poderes entre o indivíduo e os organismos que processam os dados pessoais e a conseqüente perda de controle individual sobre o fluxo de seus dados”.<sup>171</sup> Certamente, a cadeia de custódia seria mais um passo no sentido de equilibrar essa balança.

---

<sup>169</sup> Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-ju-ristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>. Acesso em: 11 nov. 2020.

<sup>170</sup> PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 15. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em: 07 maio 2021.

<sup>171</sup> SCHERTEL, Laura. **Uso de softwares espiões pela polícia: prática legal?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 07 maio 2021.

## CONSIDERAÇÕES FINAIS

*“Não somos pós-verdade, tal como não somos pré-verdade, a menos que nós permitamos. A pós-verdade não tem a ver com realidade; mas sim da forma como os seres humanos reagem à realidade”<sup>172</sup>. (Lee McIntyre)*

O debate em torno da aderência tecnológica à justiça criminal é uma demanda de uma sociedade que já não é mais a mesma. O impacto do paradigma da sociedade informacional, da “quarta revolução industrial”, indicam um caminho sem volta nas mudanças estruturais ocasionados pelos avanços tecno-científicos no âmbito das investigações criminais e em seus meios probatórios.

Nesse contexto, entram em cena, o uso cada vez mais frequentes de métodos ocultos de investigação, como uma resposta dos agentes estatais responsáveis pela repressão de crimes em relação às interações com o ambiente digital. Essas medidas, muitas vezes, altamente intrusivas no âmbito da vida privada, são realizadas sem um respaldo legal e sem parâmetros de proporcionalidade. Da mesma forma ocorre com a tática de infiltração por *software*, cujo alcance a dados pessoais é ainda maior.

Assim sendo, se a lógica da repressão à criminalidade muda, suas correspondentes formas de prova, enquanto elementos centrais de um processo penal, não permanecem imunes. As provas digitais são essencialmente distintas das tradicionais: são voláteis, facilmente manipuláveis e dispersas, além de serem imateriais. O arcabouço normativo que contempla meios não digitais, conseqüentemente, não é suficiente para sustentar as suas singularidades. No mesmo sentido, dado o seu peso psicológico no processo decisório, por sua presunção de fidedignidade, é ainda mais necessário que, caso ela seja proveniente de meios ilícitos, o juiz contaminado seja considerado impedido para atuar na causa.

Nesse mesmo horizonte, desmistificar a prova digital e as evidências dessa natureza enquanto infalíveis é uma importante missão ao se aprofundar no estudo de suas características, tendo em vista que as provas digitais são altamente suscetíveis a manipulação. E é nesse sentido que a cadeia de custódia, específica, singular e bem regulamentada é um ponto essencial para sua utilização em juízo. Com esse fim, a norma ABNT NBR ISO/IEC

---

<sup>172</sup> Tradução livre. No original: We are not post-truth any more than we are pre-truth, unless we allow ourselves to be. Post-truth is not about reality; it is about the way that humans react to reality”(McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018. p. 172).

27037:2012, além de estudos da perícia computacional forense de outros países já possuem um roteiro consolidado, que será flexibilizado a depender dos processos de inovações que surgirem. Sua identificação, coleta, análise e a elaboração de relatórios detalhados constituem atributos fundamentais para garantir a confiabilidade de um meio probatório levado a juízo, além de permitirem o contraditório e o acesso integral das fontes de prova pela defesa.

As preocupações atuais acerca da proteção de dados também é abarcada pelo instituto da cadeia de custódia, notadamente nas discussões a respeito da segurança da informação. Confiabilidade e integridade de dados dos sistemas informáticos são aspectos indissociáveis da nova vida em sociedade, de tal forma que devem ser elevados à categoria de direito fundamental. Diante disso, uma Lei de Proteção de Dados para segurança pública e persecução penal não pode ser inerte a essa discussão, cenário em que a cadeia de custódia da prova digital deve ser abrangida como uma garantia de fundamento constitucional.

## REFERÊNCIAS

ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=307273>. Acesso em: 06 abr. 2021.

ANDRADE, Manuel da Costa. **“Bruscamente no Verão passado”**, a reforma do código de processo penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra, 2009.

Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>. Acesso em 07 de mai de 2021.

ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. São Paulo. InternetLab, 2019. V. 2.

BADARÓ, Gustavo. **A cadeia de custódia e sua relevância para a prova penal**. In: SIDI, Ricardo; LOPES, Anderson B. (org.). Temas atuais da investigação preliminar no processo penal. Belo Horizonte: D'Plácido, 2018.

BRASIL. **Lei nº 13.964**, de 24 de dezembro de 2019. Disponível em <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13964.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm)> Acesso em 06 de mai de 2021.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Disponível em <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)> Acesso em 07 de mai de 2021.

BUDAPESTE. **Convenção de Budapeste sobre o Cibercrime**. Budapeste. Publicado em 23 nov. 2011. Disponível em: [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 23 abr. 2021.

CARVALHO, R.W.R.A **Importância da Cadeia de Custódia na Computação Forense**. Rev. Bras. Crimin. 9(2), 134-138, 2020.

CASTELLS, Manuel. **A sociedade em rede**. Vol. 1. 8ª ed. rev.ampl. Tradução? Roneide Venâncio Majer. Editora: Paz e Terra. São Paulo, 2005.

CESARI, Claudia. Editoriale: **L’impatto delle nuove tecnologie sulla giustizia penale** – un orizzonte denso di incognite. Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1167-1188, set.-dez. 2019.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 329 de 30 de julho de 2020.** Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3400>. Acesso em: 20 fev. 2021

COSTA, Fabrício. **O processo penal da sociedade da informação:** As recentes reformas do Código de Processo Penal e o Direito fundamental à jurisdição criminal efetiva. Revista brasileira de meio ambiente digital e sociedade da informação. São Paulo, volume 1, número 2, p. 73-223, Jul./Dez. 2014, p. 3. Disponível em <<https://revistaseletronicas.fmu.br/index.php/rbmad/article/view/617/737>>.

COURA, Kalleo; LEORATTI, Alexandre. **Juizes ordenam quebra de sigilo de sigilo com base em localização.** Disponível em: <https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao-27052019>. Acesso em: 03 mar. 2021.

DEZEM, Guilherme Madeira. **Da Prova Penal:** Tipo Processual, Provas Típicas e Atípicas: (atualizado de acordo com as Leis 11.689, 11.690/08 e 11.719/08). Campinas: Millennium, 2008.

DUARTE, Evandro Charles Piza. A Máquina de Vidro: Sociedade de Informação e Processo Penal. **Cadernos da Escola de Direito e Relações Internacionais da UniBrasil**, Curitiba, v. 4, 2005.

ESPINDULA, Alberi. **Perícia criminal e cível: uma visão geral para peritos e usuários da perícia.** 3.ed. Campinas. Editora Millenium.

FILHO WIDAL, Márcio. **A conformação epistêmica do processo penal democrático e os padrões de prova.** 2017. Disponível em: <https://marciowidal.files.wordpress.com/2017/09/a-conformac3a7c3a3o-epist3aamica-do-processo-penal-democr3a1tico-e-os-estc3a2ndares-de-prova.pdf>. Acesso em: 01 abr. 2021.

FURLANETO, Neto Mário; SANTOS, José. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil.** Disponível em <<https://revista.univem.edu.br/emtempo/article/view/3130/940>>. Acesso em 03/04/2021.

GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019>. Acesso em 01 de abr de 2021.

\_\_\_\_\_. Busca estatal pro informações digitais e intervenções em direitos fundamentais (parte II). Disponível em <<https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-2-12082019>> Acesso em 01 de abr de 2021.

GOMES, Felismina. **A admissibilidade de métodos ocultos de investigação criminal em processo penal.** Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de Lisboa. Lisboa, 2019.

GOMES FILHO, Antônio Magalhães, **Direito à prova no processo penal**. Editora RT, São Paulo, 1997.

GRECO, Luís; GLEIZE, Orlandino. **Infiltração online no processo penal** : Notícia sobre a experiência alemã. Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3.

GUARDIA, Gregório. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012. p. 218.

KELLEN, Soares. **A quebra da cadeia de custódia resultante na contaminação da prova e do magistrado**. Disponível em: <https://canalcienciascriminais.com.br/a-quebra-da-cadeia-de-custodia-resultante-na-contaminacao-da-prova/>.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019.

LOPES JUNIOR, Aury. **Direito Processual Penal**. São Paulo, Editora Saraiva, 2021. 9786555590005. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555590005/>. Acesso em: 01 de fev de 2021.

MAGNO, Levy; COMPLOIER, Mylene. **Cadeia de custódia da prova penal**. p. 4. Disponível em: [https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj\\_n57\\_10\\_cadeia%20de%20cust%C3%B3dia.pdf?d=637437206976264894](https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj_n57_10_cadeia%20de%20cust%C3%B3dia.pdf?d=637437206976264894) Acesso em 06 de mai de 2021.

MARTINEZ, Thiago Hartmann. **Os direitos fundamentais X segurança pública** : a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. Dissertação (Mestrado em Direito). Faculdade de direito da Universidade de Lisboa. Lisboa, 2019.

McINTYRE, Lee. **Post-truth**. Cambridge: The MIT Press, 2018.

MENDES, Carlos Hélder C. F. “ **Tecnoinvestigação criminal: Entre a proteção de dados e a infiltração por software**”. Editora Juspodivim, Salvador, 2020.

ORTIZ PRADILLO, Juan Carlos. **Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos**. 2013. Disponível em: [http://www.fundacionalternativas.org/public/storage/estudios\\_documentos\\_archivos/b78e188fdcae153bcd14b71e5ca618e7.pdf](http://www.fundacionalternativas.org/public/storage/estudios_documentos_archivos/b78e188fdcae153bcd14b71e5ca618e7.pdf). Acesso em: 15 mar. 2021.

PACELLI, Eugênio. **Curso de Processo Penal**. – 24. ed. – São Paulo: Atlas, 2020

\_\_\_\_\_. **Direito Penal e Processual Contemporâneos**. São Paulo. Grupo GEN, 2018. 9788597019407. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597019407/>. Acesso em: 29 Mar 2021

PRADO, Geraldo. PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021, p. 15..Disponível em <<https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>> Acesso em 07 de mai de 2021.

\_\_\_\_\_. Ainda sobre a quebra da cadeia de custódia das provas. Boletim do IBCCrim, São Paulo, n. 262, setembro de 2014a.p.16-17.

\_\_\_\_\_. **Prova penal e sistema de controles epistêmicos**. São Paulo: Marcial Pons, 2014b.

PEREIRA, Alexandre Libório Dias. **O «direito à autodeterminação informativa» na jurisprudência portuguesa**: breve apontamento. *Ars Iuris Salmanticensis*, v. 5, dez. 2017, p. 27. Disponível em: <http://revistas.usal.es/index.php/ais/article/view/18011/18411>. Acesso em: 06 de mai de 2021.

REIS, Brenda S.R. **As adições tecnológicas ao processo penal**: policiamento preditivo. Disponível em: <http://icp.org.br/Jovem/ComaPalavra/34>. Acesso em: 24 mar. 2021.

RAMALHO, David. **O uso de malware como meio de obtenção de prova**. *Revista de Concorrência e Regulação* n.º 16, 2013.

REALE, Miguel. **Filosofia do direito**. 17. ed. São Paulo: Saraiva, 1996.

RIBOLI, Eduardo. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **Galileu – Revista de Direito e Economia**. Volume XIX. Fascículo II, 2018.

SALGRETI, Maria. A inconveniência jurídica na admissibilidade das provas ilícitas pelo seu mero desentranhamento físico dos autos e pela continuidade do juiz que dela tivera conhecimento à frente do processo na persecução dos crimes de natureza. **Revista Brasileira de Ciências Criminas**, v. 117, 2015.

SCHERTEL, Laura. **Uso de softwares espões pela polícia: prática legal?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espiones-pela-policia-pratica-legal-04062015>. Acesso em: 01 maio 2021.

SECRETÁRIA NACIONAL DE SEGURANÇA PÚBLICA DO MINISTÉRIO DA JUSTIÇA. **Portaria SENASP nº 82 de 16 de julho de 2014**.Disponível em <<https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm>> Acesso em 06 de mai de 2021

SHWAB, Klaus. **A quarta revolução industrial**. São Paulo. Editora Edipro. 2016.

VASCONCELLOS, Vinicius Gomes de. **Standard probatório para condenação e dúvida razoável no processo penal**: análise das possíveis contribuições ao ordenamento brasileiro. *Rev. direito GV*, São Paulo, v. 16, n. 2, e1961, 2020. Disponível em: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1808-24322020000200203&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322020000200203&lng=en&nrm=iso). Acesso em: 5 abr. 2021.

VAZ, Denise. **Provas digitais no processo penal**: formulação de conceito, definição de características e sistematização do procedimento probatório. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012.

VIEIRA, Thiago. **“O que é a função digestora HASH e qual é sua relevância para a computação forense?”**. Disponível em <https://medium.com/contrarraz%C3%B5es/o-que-%C3%A9-a-fun%C3%A7%C3%A3o-digestora-hash-e-qual-%C3%A9-sua-relev%C3%A2ncia-para-a-computa%C3%A7%C3%A3o-forense-2351a2d81fec> . Acesso em 05/05/2021.