



Pró-Reitoria Acadêmica

Escola de Direito

Curso de Combate à Corrupção e à Lavagem de Dinheiro

Cadeia de Custódia de Provas Digitais nos Processos do  
Direito Administrativo Sancionador com a adoção da  
tecnologia Blockchain

Autores:

Alexandro Mariano Pastore

Manoel Augusto Cardoso da Fonseca

Orientador:

Prof. Dr. Maurin Almeida Falcão

Brasília – DF

2022

**ALEXANDRO MARIANO PASTORE  
MANOEL AUGUSTO CARDOSO DA FONSECA**

**CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS NOS PROCESSOS DO DIREITO  
ADMINISTRATIVO SANCIONADOR COM A ADOÇÃO DA TECNOLOGIA  
BLOCKCHAIN.**

**Artigo apresentado ao curso de  
especialização em Combate à Corrupção e à  
Lavagem de Dinheiro da Universidade  
Católica de Brasília, como requisito parcial  
para obtenção do título de Especialista em  
Direito.**

**Orientador:  
Prof. Dr. Maurin Almeida Falcão**

**Brasília  
2022**

Artigo de autoria dos alunos Alexandro Mariano Pastore e Manoel Augusto Cardoso da Fonseca, intitulado **CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS DE PROCESSOS DO DIREITO ADMINISTRATIVO SANCIONADOR COM A ADOÇÃO DA TECNOLOGIA BLOCKCHAIN** para a obtenção do grau de Especialista do curso de Direito da Universidade Católica de Brasília em \_\_\_/\_\_\_/\_\_\_\_\_ defendido e aprovado pela banca examinadora abaixo assinada

Brasília  
2022

## **Dedicatória de ALEXANDRO**

A DEUS – Pai, Filho e Espírito Santo – pelo dom da Vida e todas as graças recebidas.

À Santíssima Virgem Maria, Mãe de Deus e nossa Mãe, Auxílio dos Cristãos.

Aos meus pais e minha irmã, cujo amor sempre me motiva a seguir adiante.

A Alessandra Valle Lafetá, Carmen Regina da Silva, Lúcia Guimarães Joffre, Pedro Antunes Alexandre e Simei Susã Spada – pessoas iluminadas que tive a honra de conhecer na CGU, em reconhecimento pelo exemplo profissional e gratidão pelo apoio ofertado nos momentos difíceis.

## Dedicatória de MANOEL

Aos meus pais Leonardo e Maria (*in memoriam*) e meus irmãos Mercedes e Leonardo pelo exemplo e amor fundamentais na formação de meu caráter.

À minha querida esposa Raquel pela parceria e amor incondicional nesta jornada que seguimos juntos.

Aos meus filhos: Gabriela, Roberto e Manoela, cujo amor e carinho sempre me motiva a seguir adiante.

Aos meus amados netinhos: Antônio, Bento, Olívia e Helena que me inspiram na luta por um mundo melhor.

**ABSTRACT:** This article deals about chain of custody of digital evidence in the processes of Sanctioning Administrative Law. Digital evidence is the means of demonstrating a fact that occurred in digital media, or that has in the digital environment an instrument to demonstrate a certain fact of its content (TAMMAY e MAURICIO, 2020, p. 33). Considering the advances in digital technology, where hacker attacks can compromise the integrity of information, it is essential to establish mechanisms that ensure adequate custody of this data by presenting a proposal from a theoretical-practical point of view. In the second section, we discuss all legal aspects that involve the validity of digital evidence. Chain of custody is precisely the sequence of procedures that will occur while the material collected is under the protection of the State. It happens that in the Sanctioning Administrative Process, the occurrence of digital evidences has increased, whether recorded statements, information and digital native documents from computerized systems or Big Data. The third section presents an approach to Blockchain Technology as multi-purpose technology, which – with its characteristics of auditability, encryption and immutability of data stored in a blockchain – is suitable to be adopted in a chain of custody model of digital evidence. The fourth section presents the proposed model. Finally, in the final considerations, we establish perspectives on the theme and the possibility of applying the model to a real use case within the Brazilian Federal Internal Affairs System.

**Keywords:** chain of custody, digital evidence, evidence, process, Sanctioning Administrative Law, Blockchain

**RESUMO:** Este artigo versa sobre o tema cadeia de custódia de provas digitais nos processos do Direito Administrativo Sancionador. A prova digital é o meio de demonstrar um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo (TAMMAY e MAURICIO, 2020, p. 33). Considerando os avanços da tecnologia digital, onde os ataques de hackers podem comprometer a integridade das informações, é fundamental estabelecer mecanismos que assegurem uma adequada custódia desses dados, apresentando uma proposta do ponto de vista teórico-prático. Na segunda seção, abordam-se todos os aspectos jurídicos que envolvem a validade da prova digital. Cadeia de custódia é justamente a sequência de procedimentos que ocorrerão enquanto o material coletado estiver sobre tutela do Estado. Ocorre que, no Processo Administrativo Sancionador, tem crescido a ocorrência das provas digitais, sejam depoimentos gravados, informações e documentos digitalizados ou natos digitais, provenientes de sistemas informatizados ou do Big Data. A terceira seção apresenta uma abordagem sobre a Tecnologia Blockchain como tecnologia de múltiplo propósito, que, com suas características de auditabilidade, criptografia e imutabilidade dos dados armazenados numa cadeia de blocos - é adequada para ser adotada num modelo de cadeia de custódia de provas digitais. Na quarta seção apresenta-se o modelo proposto. Por fim, nas considerações finais, estabelecemos perspectivas sobre o tema e a possibilidade de aplicação do modelo a um caso de uso real no âmbito do Sistema de Corregedorias.

**Palavras-chave:** cadeia de custódia, provas digitais, provas, processo, Direito Administrativo Sancionador, Blockchain

## Sumário

<b>1. INTRODUÇÃO.....</b>	<b>7</b>
<b>2. A CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS NO DIREITO ADMINISTRATIVO SANCIONADOR.....</b>	<b>8</b>
2.1 A PROVA DIGITAL .....	8
2.2 A CADEIA DE CUSTÓDIA.....	9
2.3 FUNDAMENTAÇÃO.....	10
2.4 APLICABILIDADE DA CADEIA DE CUSTÓDIA. FONTES DE PROVAS REAIS, FUNGÍVEIS, MATERIAIS OU IMATERIAIS. ....	10
2.5 O PACOTE ANTICRIME.....	11
2.6 CONSEQUÊNCIAS DA VIOLAÇÃO OU QUEBRA DA CADEIA DE CUSTÓDIA .....	12
2.7 CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS .....	12
2.8 CADEIA DE CUSTÓDIA: DIREITO PENAL E DIREITO ADMINISTRATIVO SANCIONADOR .....	13
<b>3. A APLICAÇÃO DE TECNOLOGIAS DISRUPTIVAS COMO FORMA DE GARANTIR A GUARDA E INTEGRIDADE DA CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS .....</b>	<b>15</b>
3.1 A TECNOLOGIA BLOCKCHAIN .....	16
3.1.1 CONCEITOS .....	16
3.1.2 ANÁLISE DE DILEMA ( <i>TRADE-OFF</i> ).....	17
3.1.3 PADRÕES DE DESIGN MOTIVADORES NO DESENHO DE NOSSO MODELO .....	18
<b>4. MODELO PROPOSTO DE CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS.....</b>	<b>19</b>
<b>5. CONCLUSÃO.....</b>	<b>21</b>
<b>REFERÊNCIAS .....</b>	<b>23</b>

## 1. Introdução

A Lei n.º 13.964 de 2019, também conhecida como Pacote Anticrime, estabelece que a cadeia de custódia dos vestígios compreende diversas etapas (reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte).

Ao analisar esse diploma legal, fica evidente a preocupação do legislador em descrever detalhadamente a cadeia de custódia de provas físicas e materiais, não tratando dos procedimentos quanto à custódia de provas digitais, cada vez mais frequentes em casos de corrupção, lavagem de dinheiro e crimes econômicos em geral. Uma lacuna que deve ser suprimida, em razão do possível prejuízo processual (inadmissibilidade e exclusão dos autos ou minoração da sua força probatória, a depender do entendimento esposado).

O objetivo deste artigo é propor um modelo, baseado em normas vigentes e tecnologias disruptivas, que assegure a guarda adequada das provas digitais numa cadeia de custódia.

As hipóteses consideradas nos indicam a produção, em nosso trabalho, de conhecimento sistêmico, uma vez que, no modelo proposto, se estabelece a conexão de informação produzida mediante conhecimentos distintos, especificamente no universo do Direito Administrativo, Direito Penal, Direito Comparado, Tecnologia da Informação, Teoria Geral dos Sistemas, Blockchain, Criptografia, Internet etc.

Adotou-se o método qualitativo para que, a respeito dos temas estudados, seja proposto um modelo com aplicações específicas e relacionado com um caso de uso.

A metodologia adotada para a produção do trabalho foi uma extensa pesquisa bibliográfica, documental, sobre o estado da questão relativo ao tema objeto do estudo e a possível aplicação de tecnologias disruptivas nos problemas a serem enfrentados pelas hipóteses propostas.

Este trabalho está estruturado em quatro seções: 1. Introdução; 2. A cadeia de custódia de provas digitais no Direito Administrativo Sancionador; 3. A aplicação de tecnologias disruptivas como forma de garantir a guarda e integridade da cadeia de custódia de provas digitais; 4. Modelo proposto; e 5. Conclusão.

Na seção 1 apresentamos a metodologia, objetivos e justificativa para elaboração deste artigo.

Na seção 2 abordamos conceitualmente, sob a ótica do Direito, o conceito de prova digital, a importância da preservação da cadeia de custódia de provas, com destaque para as digitais. São analisados aspectos do Direito Internacional e Comparado, com ênfase nos impactos da lacuna detectada no ordenamento jurídico nacional em relação ao tema.

Na seção 3 abordamos conceitos de Tecnologia da Informação, especificamente da tecnologia Blockchain, cujos atributos e componentes podem ser integrados para a solução das questões e das hipóteses do trabalho.

Na seção 4 apresentamos uma proposta de modelo a ser adotado no controle da cadeia de custódia de provas digitais.

Na conclusão apresentamos as premissas correspondentes ao atingimento dos objetivos e comprovação das hipóteses apresentadas. Neste tópico também se estabelecem comentários a respeito de novas linhas de pesquisa derivadas do tema.



## 2. A cadeia de custódia de provas digitais no Direito Administrativo Sancionador

### 2.1 A prova digital

Na processualística moderna, o julgamento baseia-se nos elementos de convicção coligidos, os quais, regularmente admitidos no processo e submetidos ao crivo do contraditório e da ampla defesa, erigem-se em provas ou evidências<sup>1</sup>, com as quais se busca reconstituir historicamente determinado conjunto de fatos, com vistas a alcançar a verdade dita “processual”<sup>2</sup>.

O vocábulo “prova” admite múltiplos significados, dentre os quais interessa mais diretamente ao presente trabalho a prova na acepção de “elemento de prova”, isto é, o fato probante (*factum probans*), o fato utilizado para provar algo – em oposição ao “objeto de prova”, que corresponde ao fato provado (*factum probandum*)<sup>3</sup>.

Na realidade, o resultado probatório decorre de juízos probabilísticos submetidos aos *standards* probatórios.<sup>4</sup>

A prova digital (também chamada eletrônica, tecnológica ou *e-evidence*) pode ser definida como “qualquer classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos”, como informa Geraldo Prado.<sup>5</sup>

Gustavo Badaró traz, como exemplos de provas digitais, “o conteúdo de conversas telefônicas, ou de transmissão de e-mails, mensagens de voz, fotografias digitais, filmes armazenados na internet etc.”<sup>6</sup>, com o que abarca duas acepções conceituais, as quais serão abordadas mais adiante.

<sup>1</sup> Recebe críticas o emprego de “evidência” como sinônimo de “prova”, por se tratar de anglicismo semântico (“evidence”); no presente trabalho, o termo será evitado, apesar do uso quase que generalizado na literatura jurídica.

<sup>2</sup> A expressão “verdade processual” pretende superar a tradicional dicotomia entre a “verdade real” (Processo Penal) e a “verdade formal” (Processo Civil): “Por outro lado, mesmo com os poderes conferidos ao Juiz, na justiça penal, a procura e o encontro da verdade real se fazem com as naturais reservas oriundas da limitação e falibilidade humanas, e, por isso, melhor seria falar de ‘verdade processual’ ou ‘verdade forense’, até porque, por mais que o Juiz procure fazer a reconstrução histórica do fato objeto do processo, muitas e muitas vezes o material de que ele se vale (ah! as testemunhas...) poderá conduzi-lo a uma ‘falsa verdade real’, e por isso mesmo Ada P. Grinover já anotava que ‘verdade e certeza são conceitos absolutos, dificilmente atingíveis, no processo ou fora dele’ (A iniciativa instrutória do juiz no processo penal acusatório, RF, 347/6).” (TOURINHO FILHO, F. D. C. **Manual de processo penal**. 15. ed. São Paulo: Saraiva, 2012, p. 58-59).

<sup>3</sup> “*Factum probans* e *factum probandum* se conectam na medida em que o primeiro prova o segundo.” (DALLAGNOL, D. M. **As lógicas das provas no processo: prova indireta, indícios e presunções**. 1. ed. Porto Alegre: Livraria do Advogado, 2018, p. 16).

<sup>4</sup> “De fato, a justiça humana se constrói sobre juízos probabilísticos<sup>2</sup>, alcançados pela atividade probatória, e sobre *standards* probatórios, os quais minimizam os riscos probabilísticos mediante a definição de que grau de convicção se exige para cada decisão” (DALLAGNOL, D. M.; CÂMARA, J. D. A. S. R. A cadeia de custódia da prova. *In*: SALGADO, D. D. R.; QUEIROZ, R. P. D. (Org.). **A prova no enfrentamento à macrocriminalidade**. 3. ed. Salvador: Jus Podivm, 2019. p. 529-530).

<sup>5</sup> DELGADO MARTÍN *apud* PRADO, G. L. M. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital, 2021. Disponível em: <<https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/>>. Acesso em: 15 Abril 2022.

<sup>6</sup> BADARÓ, G. H. R. I. A Cadeia de Custódia e sua Relevância para a Prova Penal. *In*: SIDI, R.; LOPES, A. B. (Org.). **Temas Atuais da Investigação Preliminar no Processo Penal**. Belo Horizonte: Editora D'Plácido, 2017. p. 522.

## 2.2 A cadeia de custódia

A cadeia de custódia da prova corresponde, na linguagem jurídica, ao conjunto de procedimentos exigidos à preservação e rastreabilidade desses elementos de convencimento, caracterizando requisito de validade do resultado da atividade probatória primária, após a sua admissibilidade e valoração.

A expressão remete metaforicamente a uma corrente<sup>7</sup>, formada por elos, que seriam os agentes que interagem com determinado vestígio material, desde o momento da sua localização até o término da sua utilização processual.

Geraldo Prado<sup>8</sup>, apoiando-se na doutrina norte-americana (na qual a figura foi engendrada):

"Conforme Robert A. Doran leciona 'a cadeia de custódia é um processo usado para manter e documentar a história cronológica da evidência. Este processo deve resultar num produto: a documentação formal do processo'."

Gustavo Badaró apresenta definição mais detalhada<sup>9</sup>, segundo a qual a cadeia de custódia é “a história cronológica escrita, ininterrupta e testemunhada, de quem teve a evidência desde o momento da coleta até que ela seja apresentada como prova no tribunal”.<sup>10</sup>

Para Deltan Dallagnol e Juliana Câmara, “a cadeia de custódia da prova é a corrente histórica ou seqüência da posse de uma dada prova.”<sup>11</sup>

Renato Brasileiro de Lima conceitua-a como “um mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração. Funciona, pois, como a documentação formal de um procedimento destinado a manter e documentar a história cronológica de uma evidência, evitando-se, assim, eventuais interferências internas e externas capazes de colocar em dúvida o resultado da atividade probatória, assegurando, assim, o rastreamento da evidência desde o local do crime até o Tribunal.”<sup>12</sup>

Como bem destacado por Gustavo Badaró, a expressão “cadeia de custódia” deve ser compreendida como elipse de “documentação da cadeia de custódia” e nessa acepção será empregada ao longo do presente.

Isso porque a “cadeia de custódia” em si equivale diretamente ao conjunto de *pessoas* que sucessivamente tiveram contato com a fonte de prova real, ao passo que a “documentação da cadeia de custódia” refere-se ao *registro* formal dessas pessoas (quem) e dos momentos em que mantiveram o contato (quando).

<sup>7</sup> Em outros idiomas fica mais evidenciada a acepção de “cadeia” como “corrente”: chain of custody (Inglês), Beweismittelkette (Alemão), catena di custodia (Italiano) e cadena de custodia (Espanhol).

<sup>8</sup> PRADO, G. L. M. **Prova penal e sistema de controles epistêmicos: A quebra da cadeia de custódia das provas obtidas por métodos ocultos**. São Paulo: Marcial Pons, 2014.

<sup>9</sup> “The witnessed, unbroken, written chronological record of everyone who had an item of evidence, and when each person had it; also accounts for any changes in the evidence. (SWANSON Charles R., CHAMELIN, Neil C., TERRITO, Leonard).

<sup>10</sup> BADARÓ, *op. cit.*, p. 561.

<sup>11</sup> DALLAGNOL e CÂMARA, *op. cit.*, p. 530.

<sup>12</sup> BRASILEIRO DE LIMA, R. **Manual de Processo Penal**. 8. ed. Salvador: Jus Podivm, 2020.

Pode-se afirmar que a cadeia de custódia corresponde à atividade probatória secundária, ou seja, a “prova sobre a coleta da prova”<sup>13</sup>, ou, mais sinteticamente, “a prova da prova”<sup>14</sup>. Ou, ainda, “uma prova de segundo grau ou meta prova”<sup>15</sup>.

Exemplificativamente, pode-se mencionar a documentação relativa à pistola com a qual foi cometido um homicídio, desde o momento em que é encontrada pelos peritos criminais, acondicionada, transportada, examinada, depositada judicialmente e eventualmente encaminhada para destruição, doação ou restituição à corporação policial.<sup>16</sup>

Como adiantado, a temática despontou no Direito estadunidense (“chain of custody”), no campo do Direito Penal e Processual Penal, irradiando para o Direito Europeu Continental, sobretudo na área pericial.

### 2.3 Fundamentação

A questão diz respeito à demonstração da *autenticidade e integridade* de cada fonte de prova. A autenticidade reporta-se à origem da fonte; a integridade, à sua conservação até que apresentada em Juízo<sup>17</sup>, atendendo ao que, na doutrina espanhola, foi designado “mismidad de la prueba”<sup>18</sup>.

Nessa esteira, Geraldo Prado (2014, p. 300) alicerça a cadeia de custódia nos princípios da “mesmidade” e da “desconfiança”, este último contraposto, por Deltan Dallagnol e Juliana Câmara, aos princípios da presunção de regularidade da evidência e de boa-fé dos agentes<sup>19</sup>, que parece encontrar convergência, em se tratando de Direito Administrativo Sancionador, na presunção de legitimidade de provas acusatórias, abordada por Fábio Osório (2020, p. 432).

### 2.4 Aplicabilidade da cadeia de custódia. Fontes de provas reais. Fungíveis. Materiais ou imateriais.

As provas podem provir de pessoas ou de coisas, daí a tradicional classificação doutrinária: fontes de prova pessoais ou reais.

A cadeia de custódia tem relação com as *fontes de prova reais* (“real evidences”), como informa Gustavo Badaró.<sup>20</sup>

<sup>13</sup> MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. NOTA TÉCNICA Nº 04/2021-PGJ - CAOCrim. Documentação da Cadeia de Custódia. São Paulo, 22 jan.2021. Disponível em: <[http://www.mpsp.mp.br/portal/page/portal/Criminal/notas\\_tecnicas/Nota%20T%C3%A9cnica%20004-21.pdf](http://www.mpsp.mp.br/portal/page/portal/Criminal/notas_tecnicas/Nota%20T%C3%A9cnica%20004-21.pdf)> Acesso em: 25 Janeiro 2022.

<sup>14</sup> LIMA, P. G. C.; ROMANELLI, L. L. A cadeia de custódia a partir da reforma do CPP: atividade probatória de segundo grau. **Revista do Ministério Público Militar**, Brasília, 2021, p. 99.

<sup>15</sup> DALLAGNOL e CÂMARA, *op. cit.*, p. 530.

<sup>16</sup> V. Conselho Nacional de Justiça (CNJ). Resolução n.º 134/2011.

<sup>17</sup> “A autenticidade significa que a fonte de prova é genuína, autêntica quanto a sua origem. A partir de um conjunto de dados individualizadores, garante-se que a coisa objeto de perícia ou simplesmente apresentada em juiz [sic] é a mesma que foi colhida e guardada e examinada. Por outro lado, a integridade é a condição de a fonte de prova que se apresenta íntegra [sic] ou inteira, não tendo sido adulterada, sofrendo diminuição ou alteração de suas características, que se mantêm as mesmas desde a sua colheita.” (BADARÓ, *op. cit.*, p. 525).

<sup>18</sup> *Ibid.*, p. 525.

<sup>19</sup> “Não discordamos que devam existir indicações de que a prova é o que o proponente afirma que ela é e de que seu conteúdo foi preservado. Contudo, a avaliação dessas indicações pode e deve tomar em consideração, inclusive, a própria presunção de regularidade da evidência e de boa-fé dos agentes. Não há, como aponta PRADO, princípio da ‘desconfiança’, salvo se pretendermos subverter os princípios básicos que guiam as relações humanas.” (DALLAGNOL e CÂMARA, *op. cit.*, p. 543)

<sup>20</sup> “Embora a cadeia de custódia esteja normalmente ligada à prova científica e, mais especificamente, à perícia de laboratório, sua aplicação é mais ampla, estando relacionada com qualquer fonte de prova real” (BADARÓ, *op. cit.*, p. 522).

Mais ainda, conforme anotam Deltan Dallagnol e Juliana Câmara<sup>21</sup>, relacionam-se com as *provas reais fungíveis*, isto é, que podem ser substituídas por outra de mesma espécie, qualidade e quantidade.<sup>22</sup>

Com efeito, em se tratando de provas reais infungíveis, a individualização que as caracteriza dispensa a comprovação da cadeia de custódia.

O detalhe digno de nota é que há uma situação particular, na qual a cadeia de custódia, em caráter excepcional, será aplicável a provas reais infungíveis: no caso das provas imateriais, ou seja, as digitais<sup>23</sup>, precisamente o objeto do presente.

Como será abordado mais adiante, o modelo tecnológico proposto neste trabalho implica que todos os elementos de convicção, mesmo que não originalmente digitais (como o caso dos documentos impressos), ao serem digitalizados para inserção no sistema de gestão documental dos processos administrativos sancionadores, recebam individualização tecnológica que assegure a sua autenticidade e integridade.

Ou seja, independentemente da sua natureza originária, todos os elementos de convencimento serão alçados à condição de digitais, como etapa necessária à sua inserção no sistema de gestão documental (tokenização).

A preocupação com a cadeia de custódia e sua disciplina, no que diz respeito às chamadas provas digitais, tem – como marco legal – a Convenção de Budapeste sobre o Crime Cibernético (2001)<sup>24</sup>, o que, como bem salienta Geraldo Prado, "é bem ilustrativo da interseção entre conceitos consagrados há séculos no direito processual penal de matriz continental europeia e novos conceitos e noções que resultam da vida biodigital do nosso tempo".<sup>25</sup>

## 2.5 O Pacote Anticrime

A legislação brasileira não previa expressamente o regramento concernente à cadeia de custódia, embora possam ser apontados dispositivos do Código de Processo Penal (art. 6º, arts. 169 e 170) que indiretamente já continham regras voltadas à preservação da integridade probatória.<sup>26</sup>

No curso da tramitação do PL n.º 8.045/2010<sup>27</sup>, mais especificamente com a redação do Parecer do Relatório Parcial na Comissão Especial, de 04/07/2017, foi inserida a proposta de inclusão de um título para disciplinar a cadeia de custódia da prova, sob a inspiração dos códigos processuais do Chile e, especialmente, da Colômbia.

Posteriormente, com o PL n.º 10.372/2018<sup>28</sup>, nos termos do Parecer do Relatório, de 02/07/2019, foi novamente incluída a previsão atinente à cadeia de custódia.

Finalmente, a Lei n.º 13.964/2019, conhecida como Pacote Anticrime, aproveitou o trabalho precedente, vindo a modificar substancialmente os Códigos Penal e de Processo Penal, tendo introduzido – no ordenamento jurídico pátrio – a menção expressa a cadeia de custódia, com a sua respectiva disciplina.

Assim, o art. 158-A do Código de Processo Penal considera, como cadeia de custódia, “o conjunto de todos os procedimentos utilizados para manter e documentar a história

<sup>21</sup> DALLAGNOL e CÂMARA, *op. cit.*, p. 534.

<sup>22</sup> V. Código Civil, art. 85.

<sup>23</sup> DALLAGNOL e CÂMARA, *op. cit.*, p. 538-539.

<sup>24</sup> Aprovado pelo Brasil mediante Decreto Legislativo n.º 37/2021, ainda aguardando a Ratificação.

<sup>25</sup> PRADO, 2021.

<sup>26</sup> BADARÓ, *op. cit.*, p. 526.

<sup>27</sup> Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263>>

Acesso em: 02 Fevereiro 2022

<sup>28</sup> Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2178170>>

Acesso em: 02 Fevereiro 2022

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”, cujas etapas – desde o reconhecimento até o descarte – são detalhadas no art. 158-B.

## 2.6 Consequências da violação ou quebra da cadeia de custódia

Convém anotar que a Lei n.º 13.964/2019 não previu expressamente a consequência jurídica para a inobservância de qualquer das etapas da cadeia de custódia ("break on the chain of custody").

Há, pois, significativo dissenso doutrinário, podendo-se reconhecer, basicamente, duas vertentes: por uma, a violação da cadeia de custódia implicaria a sua ilicitude, acarretando a inadmissibilidade ou exclusão dos autos, assim como das provas decorrentes (Renato Brasileiro de Lima, Geraldo Prado, e Aury Lopes Júnior); por outra, o rompimento da cadeia de custódia não afetaria a admissibilidade e validade processual, mas a sua valoração probatória, isto é, o seu peso na formação de convencimento do julgador (Deltan Dallagnol e Juliana Câmara, e Gustavo Badaró).

Deltan Dallagnol e Juliana Câmara<sup>29</sup> alertam para o risco de mera transposição do instituto do direito norte-americano para o brasileiro, sem atentar para as particularidades de cada um dos sistemas jurídicos.

Isso porque, nos Estados Unidos, a prova da cadeia de custódia é uma das formas de autenticação da prova (o que não impede que o fim seja atingido por outro meio de autenticação), no momento da sua admissibilidade pelo magistrado, para posterior julgamento pelo júri, ao passo que, no Brasil, o juiz de direito é também o julgador (com exceção dos crimes dolosos contra a vida), razão pela qual eventual deficiência da cadeia de custódia repercutiria no peso valorativo a ser atribuído à prova.

No plano jurisprudencial pátrio, é importante mencionar a modificação de entendimento do Superior Tribunal de Justiça (STJ), no âmbito da 6ª Turma, que se posicionou no HC n.º 160.662/RJ<sup>30</sup> em 2014 num sentido (ilicitude), tendo-o revisto por ocasião do HC n.º 653.515/RJ<sup>31</sup> e do AgRg no RHC n.º 147.885/SP<sup>32</sup>, em 2021 (valoração probatória).

De todo modo, ressaí bastante clara a necessidade de prevenir a ocorrência de situações que prejudiquem a higidez da cadeia de custódia da prova<sup>33</sup>, afinal, ainda que não acarrete o seu descarte, a minoração da força probatória já é consequência claramente indesejável para a sociedade.

## 2.7 Cadeia de custódia das provas digitais

Não obstante a sua recentidade, é certo que a Lei n.º 13.964/2019 não trouxe qualquer especificação no que diz respeito à cadeia de custódia referente às provas digitais.

Argumenta-se que não caberia ao legislador exaurir o regramento desses elementos eletrônicos, tendo em vista o constante avanço científico-tecnológico que os caracteriza.

No plano infralegal, são duas as principais fontes normativas que se propõem ao estabelecimento de padrões aplicáveis às provas digitais: a ABNT ISO/IEC 27027:2013, da Associação Brasileira de Normas Técnicas – ABNT/Organização Internacional de Normatização – ISO, e a RFC 3227/2002, da International Engineering Task Force – IETF.

<sup>29</sup> DALLAGNOL e CÂMARA, *op. cit.*, p. 564-565.

<sup>30</sup> 6ª Turma, j. 18/02/2014.

<sup>31</sup> 6ª Turma, j. 23/11/2021.

<sup>32</sup> 6ª Turma, j. 07/12/2021.

<sup>33</sup> STJ HC n.º 653515 / RJ (2021/0083108-7).

## 2.8 Cadeia de custódia: Direito Penal e Direito Administrativo Sancionador

É verdade que muito ainda se discute a conceituação do Direito Administrativo Sancionador, e a sua relação com o Administrativo e o Penal.

Fábio Medina Osório<sup>34</sup> advoga a autonomia do Direito Administrativo Sancionador em relação a esses ramos jurídicos:

A consolidação do Direito Administrativo Sancionador – seu regime jurídico – passa por uma visão jurisprudencialista, na medida em que resulta da jurisprudência dos Tribunais Superiores, à luz da segurança jurídica, o conjunto de balizamentos e contornos dos direitos fundamentais tutelados por esse ramo jurídico.

"Pode-se sustentar, também, que o Direito Administrativo Sancionador, conquanto tenha raízes mais diretas no Direito Administrativo, ostenta profunda interface com o Direito Penal e o Direito Constitucional, além de impactar sobremaneira o Direito Processual Público, vale dizer, o novo Direito Processual Punitivo. Desse modo, inegavelmente estamos diante de um novo ramo jurídico no Brasil, cuja autonomia científica há de ser reconhecida, como forma de assegurar-lhe evolução crítica e constante, e cuja absorção pelas Universidades é medida que se impõe de forma urgente."

Nessa linha, o autor<sup>35</sup> vislumbra, no Direito Administrativo Sancionador, a confluência do Direito Administrativo com o Direito Penal, em razão do caráter punitivo dos respectivos ilícitos:

Em nossa ótica, no lugar de conectar a sanção à atividade da Administração Pública, com exclusividade, é necessário conjugar tal instituto com o Direito Administrativo em sua vertente disciplinadora do poder punitivo estatal, o que implica as já mencionadas interfaces com o Direito Penal. Assim, à ideia de ilícito, disciplinado pelo Direito Administrativo, associa-se a sanção.<sup>14</sup>

Justen Filho<sup>36</sup>, perfilhando a visão de Odete Medauaur e Vitor Schirato, preleciona acerca do regime jurídico das sanções administrativas:

“As sanções administrativas representam configuração próxima às sanções de natureza penal, sujeitando-se a regime jurídico senão idêntico, ao menos semelhante.<sup>14</sup> Os princípios fundamentais de direito penal vêm sendo aplicados no âmbito do direito administrativo repressivo. Lúcia Valle Figueiredo afirmava que os procedimentos sancionatórios caracterizam-se precisamente pela aplicação dos princípios do processo penal.<sup>15</sup> Isso propicia inúmeras decorrências.”

A discussão não tem feição meramente epistemológica. Antes, tem importância fundamental para determinar o cabimento e a extensão da aplicabilidade de normas penais

<sup>34</sup> OSÓRIO, F. M. **Direito administrativo sancionador**. 7. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 27.

<sup>35</sup> *Ibid.*, p. 89.

<sup>36</sup> JUSTEN FILHO, M. **Curso de Direito Administrativo**. 11. ed. São Paulo: Revista dos Tribunais, 2015, p. 591.

materiais e processuais (princípios e regras, incluídos os relativos às garantias) aos processos administrativos (com destaque para o Processo Administrativo Disciplinar e o Processo de Apuração de Responsabilidade).

Ainda Justen Filho<sup>37</sup>, a respeito das garantias na aplicação das sanções administrativas:

“A incidência do regime penalístico produz necessariamente a extensão dos princípios processuais pertinentes no tocante à aplicação das sanções administrativas. O sancionamento tem de ser produzido segundo rigoroso processo administrativo, no qual se adotarão garantias de extrema relevância em prol do acusado.”

As divergências de posicionamento concentram-se majoritariamente na definição do alcance da aplicabilidade, podendo-se afirmar que é consensual o reconhecimento da similitude entre ambas as áreas jurídicas.

A questão seria, pois, *em qual medida* os ditames do Direito Penal podem ser integralmente transpostos ao Direito Administrativo Sancionador, sob pena de extrapolar a semelhança para a equivalência, desnaturando este último.

Em outras palavras, reconhecendo que são numerosos os pontos de convergência entre essas instâncias jurídicas, caberia, pois, investigar quais seriam as especificidades de um e de outro, as divergências – o que extrapolaria o foco deste estudo.

Ora, se a observância da cadeia de custódia dimana dos princípios da Ampla Defesa e do Contraditório, e uma vez que tais princípios de natureza penal, *em maior ou menor extensão*, são aplicáveis ao Direito Administrativo Sancionador, erige-se a necessidade de observância dos procedimentos que assegurem a autenticidade e integridade das provas – incluídas as digitais.

Com efeito, estabelecida, *quando menos*, a semelhança entre a atividade probatória administrativa e a penal, interessa mais propriamente passar à importância da adoção de uma cadeia de custódia das provas digitais para uso no Direito Administrativo Sancionador, como fator assegurador da higidez da prova.

Enfatize-se que, no tocante à cadeia de custódia das provas digitais, a exigência de assegurar, no Direito Administrativo, a incolumidade da prova não difere em nada do cabível ao Direito Penal ou a qualquer outro ramo jurídico, pois os requisitos não advêm de normas jurídicas, mas da própria matriz tecnológica que condiciona a documentação da cadeia de custódia.

Urge, pois, desenvolver e adotar um sistema tecnológico que proporcione rastrear, com segurança, a identificação dos agentes que tiveram contato com determinada prova digital, assegurando a sua autenticidade e integridade ao longo de todas as etapas. Como exemplo, pense-se no conteúdo de um disco rígido, um *pendrive*, um *smartphone*.

Ora, nesses casos, como bem ilustra Geraldo Prado<sup>38</sup>, a preservação da cadeia de custódia demandará ir além do procedimento para as provas convencionais, exigindo adicionalmente a adoção de cuidados e procedimentos tecnológicos:

"Com isso, por exemplo, a apreensão de computadores por si só não garante integridade da informação e autenticidade da fonte de prova, estas sujeitas a adoção de métodos que consideram algoritmos criptografados destinados a reter e preservar os dados (cópias espelho e lógica e cálculo da função HASH).<sup>23</sup> Adiante estas técnicas serão mencionadas.

---

<sup>37</sup> *Ibid.*, p. 597.

<sup>38</sup> PRADO, 2021.



Acrescentem-se ao arsenal investigativo as tecnologias de acesso remoto e o domínio ou não, pelas autoridades de investigação, das chaves de acesso aos repositórios de dados e se compreenderá a imperatividade atribuída à adoção de métodos de preservação da cadeia de custódia da prova digital em guias e roteiros de investigação digital."<sup>39</sup>

### 3. A aplicação de tecnologias disruptivas como forma de garantir a guarda e integridade da cadeia de custódia de provas digitais

No século XXI, não se pode imaginar a troca de dados e informações sem a utilização de fontes eletrônicas, por consequência, tal aspecto reverberou nos meios utilizados para a prática de delitos e, por óbvio, nas formas de obtenção das provas (SOBRINHA, 2021, p. 7)

A problemática ganha forma quando se questionam os procedimentos utilizados durante a cadeia de custódia da prova digital, a fim de verificar a idoneidade do material coletado ou gerado.

A tecnologia Blockchain é apontada por muitos especialistas como a protagonista da próxima revolução nos negócios digitais pelo seu grande potencial disruptivo. Tal como aconteceu na emergência da Internet nos anos 90, que transformou de forma profunda e definitiva a sociedade, existem grandes expectativas de que a Blockchain seja a inovação tecnológica que mais estimulará mudanças nos ambientes de negócio e em serviços prestados em diversos setores da economia (CERNEV e DINIZ, 2019, p. 1)

Esta tecnologia, é considerada uma tecnologia de propósito geral (*General Purpose Technology*), e como tal, tende a transformar diversos modelos de negócio, inclusive a Internet.

A Internet que usamos hoje é apátrida, o que significa que os usuários não podem manter seu estado e transferi-lo nativamente. Quando o *Bitcoin* foi lançado, ele trouxe a Blockchain, permitindo-nos manter o estado digital e nativamente. Aqueles que usam o ecossistema Blockchain começaram a se referir a essa capacidade como *Web3* e, embora ainda seja relativamente novo, já estamos começando a ver como ele pode nos beneficiar.

Como nos diz Anderson<sup>40</sup>, a camada de estado é responsável por preservar o estado de tudo o que acontece abaixo dela. Somente a infraestrutura Blockchain fornece esta camada e todos os usuários podem participar desde que cumpram as regras. Isto a torna uma rede de sucesso que fornece uma infraestrutura padrão, confiável e muito assemelhada aos DNS de hoje.

Feita a introdução quanto à solidez da infraestrutura Blockchain, cabe-nos agora apresentar suas principais propriedades que evidenciam sua aplicabilidade ao desenho de nosso modelo proposto:

- Armazenamento distribuído baseado em blocos (*Distributed Ledger Technology*);
- Identidade digital única, através de criptografia de cada bloco, o *hash*. O *hash* tem algumas propriedades fundamentais: capacidade de ocultar o conteúdo original, resistência às colisões (o que torna inviável a geração de *hashes* idênticos a partir de diferentes conteúdos de entrada) e garantia de imutabilidade

<sup>39</sup> *Ibid.*

<sup>40</sup> ANDERSON, A. **WEB3: Decentralized web the complet guide.** (p. 13). Edição do Kindle.



dos dados de um bloco a partir de seu registro. Ele cria uma identidade digital única;

- Protocolo de consenso que assegura a confiança do *ledger*<sup>41</sup> distribuído da rede sem a necessidade de uma autoridade central. Nas modalidades permissionada e híbrida pode haver autoridade central, o que traz benefícios em termos de desempenho e flexibilidade.

Em se tratando de um estudo sistêmico cujo principal foco está na segurança jurídica do tratamento de provas digitais, vamos nos abster de detalhes muito específicos de tecnologia, apenas apresentando seus principais conceitos, que deverão ser aprofundados, desde que aplicáveis, por ocasião da apresentação das opções a serem adotadas.

### 3.1 A tecnologia Blockchain

Entre a euforia inicial de qualquer tecnologia emergente, como Blockchain, e sua maturação, com o sucesso de aplicação em diversos casos de uso, temos um gap normal de 15 anos.

Se considerarmos que o *White Paper* do *Bitcoin* foi publicado em 2008 por Satoshi Nakamoto, podemos considerar a tecnologia Blockchain tendo atingindo somente agora o nível de maturidade como tecnologia de núcleo.

Ao focarmos no conjunto de padrões oferecidos e que asseguram rastreabilidade, armazenamento distribuído, integridade, não-repúdio, confiança, escalabilidade e a possibilidade de integração com sistemas maiores, entende-se o porquê deste protocolo ser considerado o núcleo da *Web3*.

#### 3.1.1 Conceitos

Os conceitos da tecnologia, relacionados aos propósitos de nosso trabalho, são:

Conceito 1 (*Blockchain*): uma blockchain é um livro-razão distribuído que está estruturado em uma lista de blocos vinculados. Cada bloco contém um conjunto ordenado de transações. Soluções típicas usam *hashes* criptográficos para proteger o link de um bloco em relação ao seu antecessor, de forma que, se um bloco for alterado, como o seu *hash* original é utilizado no bloco sucessor, fica caracterizada uma quebra de integridade (XU, WEBER e STAPLES, 2019, p. 5)

Conceito 2 (*Blockchain Platform*): uma plataforma blockchain é a combinação de todos estes fatores: maneira distribuída e transparente de registrar dados, construção de confiança, interação direta (em tempo real) (REVOREDO, 2019, p. 34), característica de tecnologia de núcleo que potencializa sua integração com as demais tecnologias.

Conceito 3 (Registro e Guarda de Dados Direitos Digitais e Gerenciamento de IP). Uma blockchain pode fornecer um registro confiável de ativos de mídia ou outra propriedade intelectual e pode fornecer a capacidade de gerenciar, delegar ou transferir informações de acesso e direitos para diversos tipos de ativos. Observe-se que as mídias não são necessariamente armazenadas na blockchain em si. Em vez disso, *hashes* criptográficos,

---

<sup>41</sup> *Ledger* é o conceito de livro-razão, onde um conjunto de contas tem suas transações gravadas. Na tecnologia Blockchain temos um conjunto de transações gravadas em blocos e o protocolo de consenso assegura a fidedignidade das informações.

metadados e outros identificadores armazenados na blockchain podem ser integrados com tecnologias de armazenamento e comunicação fora da cadeia em massa.

Conceito 4 (*Consensus Protocol*): a escolha do protocolo de consenso impacta a segurança e a escalabilidade. Uma vez que um novo bloco é gerado por um minerador, o minerador propaga o bloco para seus pares conectados na rede blockchain. No entanto, os mineradores podem encontrar diferentes blocos concorrentes e resolver isso usando os mecanismos de consenso da blockchain. Normalmente, a abordagem é fixada para uma blockchain específica; mas o Hyperledger Fabric<sup>42</sup> desvia-se dessa norma, como uma estrutura com uma arquitetura modular que atende a implementações plugáveis de vários protocolos de consenso. Nas blockchains privadas ou permissionadas isto pode ser resolvido mais facilmente.

Conceito 5 (*Hash*): um *hash* é uma função que atende às demandas criptografadas necessárias para resolver uma computação blockchain. Os *hashes* têm um comprimento fixo, pois torna quase impossível adivinhar o comprimento do *hash* se alguém estiver tentando quebrar a blockchain. Os mesmos dados sempre produzirão o mesmo valor de *hash*. Uma função *hash* é um algoritmo matemático que pode usar qualquer tipo de entrada, como uma *string*, um arquivo de texto, ou um arquivo de imagem, e traduzi-lo para uma *string* de saída de tamanho fixo chamado *hash*. É uma função unidirecional, o que significa que a única maneira de recriar os dados de entrada originais (mensagem) do *hash* é tentar todas as variações possíveis para ver se elas produzem uma correspondência. O que só é possível utilizando-se os dados originais.

### 3.1.2 Análise de Dilema (*Trade-off*<sup>43</sup>)

Como em qualquer software, existem *trade-offs* entre os requisitos não funcionais nos sistemas baseados em uma tecnologia específica, como é o caso da tecnologia Blockchain. Algumas decisões afetam principalmente a escalabilidade (como tamanho de bloco e frequência), segurança (como o protocolo de consenso), eficiência/custo (como o tipo de blockchain), ou performance (como estrutura de dados) (XU, WEBER e STAPLES, 2019, p. 105). Segundo esses autores, as decisões de design que melhoram a performance de um atributo de qualidade podem ter impacto em outros.

São exemplos disso:

- a) Criptografar os dados antes de armazená-los numa blockchain podem aumentar a confidencialidade, porém vão reduzir a performance, e podem comprometer a transparência ou auditabilidade;
- b) Armazenar somente um *hash* dos dados *on-chain* e guardando o conteúdo *off-chain* pode melhorar a confidencialidade e a performance, porém, em parte minam os benefícios de confiança distribuída da blockchain. Isto pode criar um “single point” de falha reduzindo a disponibilidade e autenticidade;
- c) Utilizar uma blockchain permissionada em vez de uma blockchain pública pode permitir um grande controle na admissão dos nodos de processamento e transações no sistema, mas podem aumentar as barreiras de entrada para novos

<sup>42</sup> O Hyperledger Fabric, um projeto de software livre da Linux Foundation, é a estrutura de blockchain modular e o padrão dominante para plataformas de blockchain empresariais.

<sup>43</sup> *Trade-off* é uma situação em que você decide entre duas situações opostas. O *trade-off* é o nome que se dá a uma decisão que consiste na escolha de uma opção em detrimento de outra. Para se tratar de um *trade-off*, o indivíduo deve, necessariamente, deixar de lado alguma opção em sua escolha.

participantes e com isso reduzir os benefícios da blockchain como instrumento de consenso entre partes não confiáveis.

- d) Uma prática comum é armazenar dados *hashed*, metadados e alguns dados públicos de pequeno porte na cadeia e manter dados grandes ou privados fora da cadeia. Devido ao tamanho limitado da capacidade dos blocos de dados, fornecida pela blockchain, um armazenamento de dados fora da cadeia é necessário para alguns aplicativos, como é o caso das provas de vídeo, normalmente de grande tamanho. A seguir, a partir da adoção desta tecnologia de núcleo passa-se a estabelecer os padrões de design a serem aplicados. Mais uma vez temos um dilema, pois resolvido o problema do tamanho do arquivo deve-se preocupar com a segurança do conteúdo *off-chain*.

Para a solução dessas questões, além de um profundo conhecimento da solução e seus requisitos, podemos nos socorrer dos Padrões de Design da tecnologia em questão. Esta análise faremos no próximo tópico.

### 3.1.3 Padrões de Design motivadores no desenho de nosso modelo

Em engenharia de software, um padrão de design é uma solução reusável para um problema que comumente ocorre dentro de um dado contexto durante o design do software.

Um padrão de design define restrições que estabelecem limites aos papéis de elementos arquitetônicos (processamento, conectores e dados) e a interação entre estes elementos.

Em relação à tecnologia Blockchain, podemos ter coleções de padrões relativas a: interações com o mundo externo, gerenciamento de dados, segurança e estrutura de *Smart Contracts*.

Vamos abordar somente os padrões destes domínios que possam impactar, se utilizados, a integração da tecnologia Blockchain como interface da cadeia de custódia de provas digitais a uma solução monolítica existente.

No caso de combinarmos armazenamento *on-chain* e *off-chain*, as funções *hash*, identidades digitais dos blocos, são funções unidirecionais fáceis de calcular, mas difíceis de inverter. Mesmo uma pequena alteração de dados no arquivo original mudaria radicalmente o valor de *hash* do bloco correspondente. O *hash* é uma maneira de verificação garantidora da integridade dos dados brutos armazenados fora da cadeia (XU, WEBER e STAPLES, 2019, p. 127). O valor de *hash* registrado imutavelmente em um bloco garante a integridade das transações registradas nesse bloco, bem como dos metadados e informações relativas aos dados brutos originais dos quais o *hash* foi derivado. Isto é importante em relação ao objeto de nosso estudo.

É necessário, portanto, quanto ao armazenamento *off-chain*, adotar mecanismos de segurança em relação a guarda dos dados, uma vez que os dados brutos podem sofrer alteração, apesar de que essa alteração será detectada via *hash* do bloco que armazena sua identidade.

Uma das opções estudadas em nosso modelo é o armazenamento das provas (dados brutos) na camada de dados do sistema existente, havendo a integração com a adoção de uma blockchain privada integrada na camada de aplicação, que armazenará os *hashes* das provas digitais, assegurando-lhes a fidedignidade e imutabilidade e estando integrado ao sistema existente.

Quanto à guarda compartilhada de dados, deve-se analisar soluções específicas que estabeleçam, para o processo de armazenamento *off-chain*, mecanismos de segurança e replicação em rede para prevenir os acessos não autorizados, mesmo que a imutabilidade do *hash* assegure a segurança da cadeia de custódia quanto às violações, através da identidade digital única. Em se tratando de uma solução de blockchain privada a utilização de servidores

autorizados pelo órgão central ou até armazenamento em nuvem e Blockchain *as a service* podem ser opções seguras.

Quando falamos de provas digitais, estamos falando de ativos, quer sejam eles documentos ou dispositivos eletrônicos. Deve-se também considerar toda a movimentação dos dispositivos digitais, registrando-a em transação específica.

A seguir, detalha-se o modelo conceitual de utilização da tecnologia Blockchain integrada a sistemas de guarda de evidências digitais como forma de garantir a cadeia de custódia dessas evidências.

Uma proposta a ser considerada, e que abordaremos na conclusão deste artigo, é a integração de soluções inovadoras ao sistema existente, num processo de inovação aberta.

#### 4. Modelo proposto de cadeia de custódia de provas digitais

Inicialmente cabe aqui a distinção entre potencial prova digital adquirida e dispositivo digital coletado.

Em nosso artigo, trabalhamos com o conceito de prova digital coletada no âmbito do Direito Administrativo Sancionador e cujo armazenamento se dá na Matriz de Responsabilização do Sistema ePAD, desenvolvido pela Corregedoria-Geral da União (CRG), da Controladoria-Geral da União (CGU), cujo uso é obrigatório para o gerenciamento da atividade correccional dos órgãos e entidades do Poder Executivo Federal (PEF)<sup>44</sup>.

No caso de dispositivos digitais - como computadores e *smartphones* - o acondicionamento em meio físico é importante, e, apesar de fugir do escopo original de nosso trabalho, que é centrado em arquivos digitais, a garantia de preservação da cadeia de custódia pode ser assegurada através da rastreabilidade de seu ciclo de vida desde a coleta.

A espoliação de dispositivos digitais pode resultar de uma degradação magnética, degradação elétrica, temperatura elevada, exposição à alta ou baixa umidade, bem como choques e vibrações.

Se controlarmos através de transação específica com registro na blockchain todas as movimentações dos dispositivos digitais requeridos como prova, ao estabelecer o rastreamento de suas movimentações e utilização, podemos determinar os possíveis pontos de espoliação.

Em relação aos requisitos de negócio, a abordagem de prova digital nos parece a mais adequada, principalmente ao se analisar a própria semântica do termo digital agregado, o que – como já exposto - induz a duas acepções de compreensão.

Uma primeira, segundo a qual a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é, um fato que tenha como suporte a utilização de um meio digital. E, uma segunda, em que, embora o fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais (TAMMAY e MAURICIO, 2020, p. 32).

A seguir, deve-se considerar o tratamento de provas digitais desde o momento em que elas são coletadas até o momento em que sejam apresentadas como tais em processos jurídicos.

Durante o ciclo de vida de uma prova digital, várias pessoas lidam com elas e, dadas as novas tecnologias de edição, há a possibilidade de que possam ser adulteradas, perdendo a fidedignidade como prova.

Assim, para garantir a resistência à adulteração, é importante que a integridade, a imutabilidade, a autenticidade e a segurança sejam mantidas.

---

<sup>44</sup> V. Portaria CGU/CRG nº 2.463/2020.

Nesse caso, a segurança conferida pelas características da tecnologia Blockchain integrada à camada de aplicação do sistema é a mais adequada.

Uma solução de arquitetura de software sempre consistiu em três camadas: 1) a camada de interface do usuário, apresentação ou ainda *frontend*; 2) a camada de aplicação (onde os dados são processados); e 3) a camada de dados, onde os dados são armazenados.

O modelo que apresentamos a seguir segue a linha de arquitetura em camadas; no entanto, em se tratando de um modelo que busca integração de componentes e oferecimento de escalabilidade, considera-se a adoção de microsserviços com a adoção de APIs<sup>45</sup> na camada de aplicação, micro *frontends* na camada de interface do usuário e armazenamento distribuído (P2P) ou em nuvem na camada de dados, flexibilizando esta integração com qualquer tipo de arquitetura.

Do ponto de vista comercial, como estamos baseando nosso modelo em um caso de uso onde haverá a integração com um sistema existente de gestão do fluxo de trabalho dos procedimentos do Direito Administrativo Sancionador, com componentes de tecnologia já consolidados - como é o caso da tecnologia Blockchain – vamos apresentar conceitualmente a estrutura de nosso *framework*, citando a opção que entendemos mais adequada à flexibilização da guarda de dados e confiabilidade quanto à imutabilidade da prova, considerando opções disponíveis no mercado:

1. Camada de Interface do Usuário. Vai estabelecer o acesso e operação dos ambientes integrados das camadas de aplicação e de dados. A arquitetura de micro *frontends* pode ser adotada como modelo. Ela é, basicamente, uma extensão do estilo de arquitetura de *microservices* e visa a aplicar os mesmos princípios desta arquitetura à camada de interface do usuário, para obter as vantagens de interoperabilidade (AJAY, 2020, p. 39). Como a estrutura atual é monolítica, é importante considerarmos soluções de fácil integração. Até porque a integração proposta vai agregar componentes às demais camadas (camadas de aplicação e de dados). No caso específico das transações de registro e movimentação das provas digitais pode-se adotar este conceito objetivando facilitar a implementação.
2. Camada de Aplicação. Baseada na *Web*, no caso, tem como núcleo a já existente camada de aplicação do sistema de gestão do fluxo de trabalho do processo eletrônico (sistema ePAD da CGU), a evidência digital cujo upload foi realizado para a camada de dados do sistema (off chain) terá a transação registrada na rede blockchain permissionada. O registro da transação na blockchain (on chain) vai cumprir todos os requisitos de garantia da imutabilidade e integridade da prova armazenada. Além disso a auditabilidade e rastreabilidade são asseguradas pela própria característica de *ledger* da blockchain. A implementação desta solução pode se dar através de um API (Interface de Programação de Aplicações) que é a implementação do conceito de microsserviço, garantindo a escalabilidade no sentido de permitir a integração com a camada de dados em nuvem ou *on-premises*<sup>46</sup>. A solução permite também a criação de transações registradas na blockchain do dispositivo eletrônico, cuja custódia também deve ser preservada, a fim de manter a sua idoneidade contra o espoliamento.

---

<sup>45</sup> API - Interface de Programação de Aplicação - cuja sigla API provém do Inglês *Application Programming Interface*, é um conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por aplicativos que não pretendem envolver-se em detalhes da implementação do software, mas apenas usar seus serviços.

<sup>46</sup> Um servidor **on-premise** é aquele em que a própria empresa tem a responsabilidade de processar suas aplicações de hardware e software. Em outras palavras, toda a infraestrutura, customização, configuração e atualização é feita internamente.

3. Camada de dados (*off-chain*). Suporta o meio de armazenamento confiável dos dados do sistema e das provas digitais, podendo utilizar tecnologia de nuvem ou *on-premise*, como já comentamos, pois são aderentes ao sistema existente. Toda evidência gravada nesta camada vai ter sua identidade digital única assegurada através da incorporação de código *hash* gravado na camada de aplicação garantindo o requisito de imutabilidade.

A implementação do modelo proposto considera a possibilidade de aproveitamento de componentes blockchain e outros recursos tecnológicos já implementados em casos de uso específicos, inclusive relacionados com Cadeia de Custódia, integrando-os ao sistema existente. Neste contexto, a Blockchain vai executar a etapa de preservação (integridade depois da coleta). A flexibilidade de utilização de multiplataformas no armazenamento permite, se desejável, o compartilhamento da guarda dos dados, uma vez feita a associação do local de guarda por ocasião do cadastro da corregedoria, isto no caso do ePAD.

O Sistema ePAD é um sistema de gestão do fluxo de trabalho dos procedimentos disciplinares. A sua concepção é revolucionária, pois caminha para a criação de uma inteligência processual no Direito Administrativo Sancionador. O sistema é oferecido sem ônus a todos os órgãos e entidades federais que atuam diretamente com Direito Disciplinar - o que, além de promover uma economia gigantesca, evitando desenvolvimentos redundantes, vem criando uma linguagem comum entre as diversas esferas do Poder. Ao mesmo tempo é importante pilar como ferramenta no combate à corrupção.

Verifica-se, no entanto, que a incorporação de funcionalidades suportadas por tecnologias de ponta vai oferecer um *upgrade* enorme aos operadores do Direito Administrativo, além de proporcionar mais segurança jurídica. Um dos objetivos desta evolução é permitir sua transformação em Processo Eletrônico Correcional, com total autonomia à solução. Neste contexto nosso modelo foi concebido.

Em se tratando de um artigo acadêmico, procuramos focar nos aspectos mais conceituais, tanto do Direito como da Tecnologia.

A gama de produtos já existentes é profícua em diversos tipos de soluções, que, através de integração, podem resolver de forma definitiva algumas carências do sistema. Um exemplo disso é a incorporação da assinatura eletrônica.

## 5. Conclusão

No que diz respeito à primeira das hipóteses formuladas, consideramos que a adoção da Norma ISO/IEC 27027:2013 como guia foi adequada. Além de se tratar de um normativo consolidado internacionalmente, aborda todo o ciclo de vida de uma prova digital, até mesmo estabelecendo os princípios relativos.

Os principais componentes de identificação, coleta e aquisição da prova digital segundo a norma são: cadeia de custódia, precauções no local do incidente, papéis e responsabilidades, competência, utilização de cuidado razoável, documentação, instruções, priorização da coleta e aquisição e preservação da potencial evidência digital.

Do ponto de vista do modelo proposto, os componentes que estão relacionados com a solução tecnológica proposta (cadeia de custódia, papéis e responsabilidades, competência, utilização de cuidado razoável e preservação da potencial evidência digital) estão plenamente atendidos.

Quanto à segunda hipótese, relativa ao modelo tecnológico, também se entende que os objetivos foram atendidos, pois se abordou tecnicamente uma tecnologia de núcleo disruptiva, cujas características são de garantia da imutabilidade, autenticidade e preservação da custódia através de procedimentos criptográficos.

Importante ressaltar que as opções tecnológicas oferecidas pelo mercado vão desde soluções proprietárias em desenvolvimento, soluções *open source* já disponíveis, até soluções oferecidas como serviço, como *Cloud as a Service* ou *Blockchain as a Service*. Uma das soluções estudadas e que muito contribuiu na construção do modelo foi a GoFabric<sup>47</sup>, que facilita a criação, expansão e a governança de redes blockchains escaláveis.

Algumas ideias aqui apresentadas estão sendo objeto de estudo aprofundado por grupo técnico da Controladoria-Geral da União no processo de desenvolvimento mediante Inovação Aberta em acordo firmado com a Escola Nacional de Administração Pública (Enap), objetivando o aperfeiçoamento do Processo Eletrônico Correccional.

Novas linhas de pesquisa devem derivar deste artigo. O tema cadeia de custódia de provas digitais tem sido objeto de estudos em diversos ramos do Direito, uma vez que a tecnologia digital se incorporou de vez ao mundo jurídico.

---

<sup>47</sup> A plataforma GoFabric tem como objetivo principal orquestrar uma rede Blockchain permissionada baseada na tecnologia Hyperledger Fabric. É um produto desenvolvido pela Startup Brasileira GoLedger.



## Referências

- AJAY, K. **Micro Frontends Architecture**. [S.l.]: [s.n.], 2020.
- ANDERSON, A. **WEB3: Decentralized web the complet guide**. [S.l.]: Edição do Kindle, 2021.
- AP.PETRONI, B. C.; GONÇALVES, R. F. Smart Contracts baseados em blockchain na cadeia de custódia: uma proposta de arquitetura. **ICOFCs**, 2018.
- BADARÓ, G. H. R. I. A Cadeia de Custódia e sua Relevância para a Prova Penal. *In*: SIDI, R.; LOPES, A. B. (Org. ). **Temas Atuais da Investigação Preliminar no Processo Penal**. Belo Horizonte: Editora D'Plácido, 2017. p. 517-538.
- BRASILEIRO DE LIMA, R. **Manual de Processo Penal**. 8. ed. Salvador: Jus Podivm, 2020.
- CERNEV, A.; DINIZ, E. Blockchain: a nova revolução tecnológica nos serviços. *In*: TIGRE, P.; PINHEIRO, A. **Inovação Em Serviços na Economia Do Compartilhamento**. São Paulo: Saraiva, 2019.
- DALLAGNOL, D. M. **As lógicas das provas no processo: prova indireta, indícios e presunções**. 1. ed. Porto Alegre: Livraria do Advogado, 2018.
- DALLAGNOL, D. M.; CÂMARA, J. D. A. S. R. A cadeia de custódia da prova. *In*: SALGADO, D. D. R.; QUEIROZ, R. P. D. (Org. ). **A prova no enfrentamento à macrocriminalidade**. 3. ed. Salvador: Jus Podivm, 2019. p. 529-566.
- FALEIROS JUNIOR, J. L. D. M. **Administração Pública Digital**. Indaiatuba: [s.n.], 2020. ISBN São Paulo.
- JUSTEN FILHO, M. **Curso de Direito Administrativo**. 11. ed. São Paulo: Revista dos Tribunais, 2015.
- KUNTZ, J. **Blockchain Ethereum - Fundamentos de arquitetura, desenvolvimento de contratos e aplicações**. São Paulo: Alura - Casa do Código, 2021.
- LIMA, P. G. C.; ROMANELLI, L. L. A cadeia de custódia a partir da reforma do CPP: atividade probatória de segundo grau. **Revista do Ministério Público Militar**, Brasília, 2021. 65-102.
- LOPES JR., A.; DA ROSA, A. D. M. A importância da cadeia de custódia para preservar a prova penal., 2015. Disponível em: <<https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal>>. Acesso em: 22 Abril 2022.
- OSÓRIO, F. M. **Direito administrativo sancionador**. 7. ed. São Paulo: Thomson Reuters Brasil, 2020.
- PRADO, G. L. M. Ainda sobre a "quebra da cadeia de custódia das provas". **Boletim IBCCRIM**, São Paulo, 262, Setembro 2014. 16-17.
- PRADO, G. L. M. **Prova penal e sistema de controles epistêmicos: A quebra da cadeia de custódia das provas obtidas por métodos ocultos**. São Paulo: Marcial Pons, 2014.
- PRADO, G. L. M. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital., 2021. Disponível em: <<https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/>>. Acesso em: 15 Abril 2022.
- RAMAMURTHY, B. **Blockchain in Action**. Shelter Iland,NY: Manning Publications, 2020.
- REVOREDO, T. **Blockchain - Tudo o que precisa saber**. [S.l.]: Amazon, 2019.
- SHWAB, K. **A Quarta Reoluçãp Industrial**. São Paulo: Edipro, 2016.



SOBRINHA, M. Q. D. L. **CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS: A PERÍCIA TÉCNICA COMO INSTRUMENTO DAS GARANTIAS**. São Cristóvão. 2021.

SOMMERVILLE, I. **Engenharia de Software**. São Paulo: Pearson, 2018.

TAMMAY, R.; MAURICIO, T. **Provas no Direito Digital**: conceito da prova digital, procedimentos e provas em espécie. São Paulo: Thomsom Reuters - Revista dos Tribunais, 2020.

TOURINHO FILHO, F. D. C. **Manual de processo penal**. 15. ed. São Paulo: Saraiva, 2012.

VOSHMIGIR, S. **Economia dos Tokens**: Como a web3 está reinventando a internet e a relação entre os agentes econômicos. Berlin: Token Kitchen, 2021.

WAN, C. Beijing sets up special fund as part of plan to become a blockchain hub by 2022. **The Block**, 30 Junho 2020. Disponível em: <<https://www.theblockcrypto.com/linked/69981/beijing-fund-blockchain-2022>>.

XU, X.; WEBER, I.; STAPLES, M. **Architecture for Blockchain Applications**. Cham, Switzerland: Springer, 2019.