Direito Digital e a manutenção da cadeia de custódia em evidências digitais do tipo SSD

Marcelo Felipe Maia Hor-Meyll Alvares
Mestre em Engenharia Elétrica pela Universidade Federal de Pernambuco em 2009. Graduado em Engenharia de Comunicações pelo Instituto Militar de Engenharia em 1999. Graduado em Direito pela Universidade Federal da Paraíba em 2012. Oficial do Exército Brasileiro do QEM – 1999-2003. Perito Criminal Federal da Polícia Federal da área de Telecomunicações e Eletrônica – 2003-2023. Promotor de Justiça Militar – 2023-.
CV Lattes: http://lattes.cnpq.br/6803937427585760
E-mail: marcelo.hor-meyll@mpm.mp.br

Data de recebimento: 03/06/2024
Data de aceitação: 05/07/2024
Data da publicação: 13/11/2024

RESUMO: O Direito Digital, enquanto releitura do Direito tradicional, trouxe a necessidade de adaptação às novas tecnologias de comunicação e virtualização das relações sociais. Gradativamente, a jurisprudência brasileira vem se adequando a essa mudança, exigindo que as provas digitais colhidas na fase investigativa sejam íntegras e confiáveis. Novas tecnologias de armazenamento, como os SSD, apresentam peculiaridades que requerem novas técnicas de validação da prova.

PALAVRAS-CHAVE: Direito Digital; Direito 4.0; indústria 4.0; SSD; Hash; cadeia de custódia; integridade.

ENGLISH

TITLE: Legal Technology and the maintenance of the chain of custody in SSD digital evidences.

ABSTRACT: The Legal Technology, as a reinterpretation of traditional Law, brought the need to adapt to the new communication technologies and the virtualization of social relations. Gradually, Brazilian jurisprudence has been adapting to this change, demanding the digital evidence collection in the investigative phase to be complete and reliable. New mass storage technologies such as SSDs present features that require new evidence validation techniques.

KEYWORDS: Legal Technology; Computational Law; Legal Tech SSD; industry 4.0; SSD; hash; chain of custody; integrity.

SUMÁRIO

1 INTRODUÇÃO

O Direito digital é considerado pela doutrina (Pinheiro, 2021) uma releitura do Direito tradicional, uma nova perspectiva, e não um novo ramo. Trata-se de uma imprescindível evolução para permitir a adaptação às recentes tecnologias e formas de comunicação, em

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

especial, relacionadas ao uso em massa da Internet e da crescente virtualização das relações humanas.

Segundo Klaus Schwab, Presidente do Fórum Econômico Mundial, estaríamos vivendo a 4ª revolução industrial, caracterizada pela interconexão das etapas produtivas, digitalização de informações e gestão massiva de dados. As três revoluções industriais anteriores estão associadas, respectivamente, com: o desenvolvimento da máquina a vapor e a exploração do carvão mineral; o uso sistemático da energia elétrica e petróleo; e o surgimento do computador, desenvolvimento das telecomunicações, Internet e globalização.

A preocupação com os conflitos sociais decorrentes desse novo cenário virtualizado e interconectado requereu uma abordagem inovadora, levando a Ciência Jurídica a criar o conceito de Direito 4.0, terminologia inspirada na 4ª revolução industrial e, no conceito alemão de indústria 4.0, baseada em fábricas inteligentes.

O Direito 4.0 se preocupa com duas frentes: a aplicação dessas tecnologias na prestação da atividade jurisdicional, é o chamado Computacional Law, Legal Technology ou Legal Tech; mas também com a regulação e proteção do ser humano em face dos riscos do progresso tecnológico.

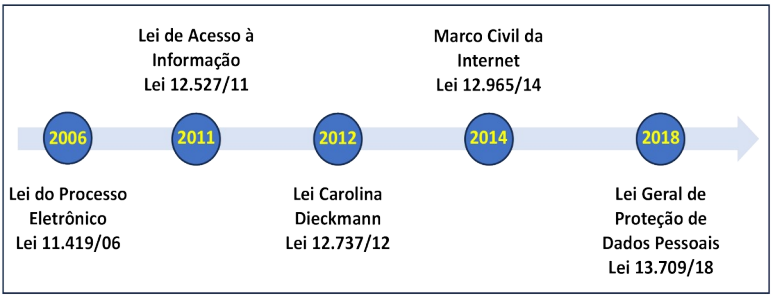
Prova da existência desses riscos, foi a inclusão no Código Penal do tipo específico de invasão de dispositivo informático trazido pela Lei Carolina Dieckmann (Lei 12.737/12), editada após a atriz sofrer invasão em seus computadores, tendo como consequência o vazamento de conteúdo pessoal.

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

Um dos primeiros passos do Brasil na tendência do Direito Digital foi a edição da Lei 11.419/06, que dispõe sobre o processo judicial eletrônico, tratando sobre a sua tramitação, comunicações de atos e transmissão de peças. Destaca-se ainda o Marco Civil da Internet (Lei 12.965/14), considerado verdadeira Constituição do Direito Digital no Brasil e que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. É um dos principais marcos do Direito Digital e foca na proteção de dados, privacidade, acesso à informação estabelecendo a obrigação dos provedores de guarda de registros.

A Lei Geral de Proteção de Dados (Lei 13.709/18) também contribuiu de forma relevante para o reforço na tutela da proteção de dados. E, mais recentemente, por meio da Emenda Constitucional 115/22, o direito à proteção de dados, inclusive nos meios digitais, foi consagrado como direito fundamental, expressamente previsto no artigo 5, LXXIX, da CF.

A linha do tempo a seguir ilustra algumas das principais leis relacionadas ao Direito Digital.



Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

O tema é bastante desafiador em razão da velocidade de evolução das novas tecnologias e na adesão em massa a elas, criando um impacto social que não pode ser ignorado pelos operadores do Direto.

Segundo a Corte Interamericana de Direitos Humanos (Corte IDH), as investigações brasileiras não vêm se preocupando suficientemente com o tema. Em diversas oportunidades envolvendo o Brasil, a Corte identificou problemas na integridade da cadeia de custódia de evidências, muitas delas derivadas digitalmente.

Em 2021, no relatório da Corte IDH sobre o Brasil (OEA, 2021), no capítulo referente à impunidade, itens 371 e 372, a Corte IDH apontou falhas significativas na fase preliminar das investigações criminais, evidenciando problemas no isolamento e preservação das cenas de crime, bem como na coleta de provas por autoridades que não fazem parte da cadeia de custódia. Essas falhas comprometem não apenas a eficácia dos trabalhos periciais, mas também a própria confiabilidade do sistema de Justiça Criminal.

As críticas acerca do comprometimento das provas nas investigações brasileiras também podem ser encontradas, por exemplo, nas sentenças de condenação do Brasil pela Corte IDH nos casos "Trabalhadores da Fazenda Brasil Verde *vs*. Brasil" – julgado em 2016 – e "Favela Nova Brasília *Versus* Brasil" – julgado em 2017 (Corte Interamericana de Direitos Humanos, 2022). Nos termos das decisões, destacou-se que a falta de uma cadeia de custódia adequada implica falhas graves na investigação de crimes, levando a violações dos direitos humanos e contribuindo para a impunidade.

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

A jurisprudência pátria vem se deparando com o problema da cadeia de provas digitais. Em fevereiro de 2023, a Quinta Turma do STJ decidiu que: "[...] são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, da autenticidade e da confiabilidade dos elementos informáticos" [STJ. 5ª Turma. RHC 143169/RJ, Rel. Min. Messod Azulay Neto, Rel. Acd. Min. Ribeiro Dantas, julgado em 7/2/2023 (Info 763)].

No caso dos autos (A cadeia […], 2023), um homem foi denunciado por, supostamente, fazer parte de organização criminosa que praticava furtos eletrônicos. A defesa alegou ter havido quebra da cadeia de custódia. No seu voto, o ministro Ribeiro Dantas afirmou que a metodologia de acondicionamento e extração de dados não foi registrada, não sendo possível assegurar que os dados periciados são íntegros, destacou que:

> […] antes mesmo de ser periciado pela polícia, […] o conteúdo extraído dos equipamentos foi analisado pela própria instituição financeira vítima [...].
> [...]
> Não existe nenhum tipo de registro documental sobre o modo de coleta e preservação dos equipamentos, quem teve contato com eles, quando tais contatos aconteceram e qual o trajeto administrativo interno percorrido pelos aparelhos, uma vez apreendidos pela polícia. Nem se precisa questionar se a polícia espelhou o conteúdo dos computadores e calculou a *hash* da imagem resultante, porque até mesmo providências muito mais básicas do que essa – como *documentar* o que foi feito – foram ignoradas pela autoridade policial. (Brasil. STJ, 2021b, p. 6, destaque original)

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

Essa decisão não é isolada, o STJ vem reforçando a importância da cadeia de custódia de provas em seus julgamentos, como garantia de aplicação da justiça, conferindo legitimidade nas condenações e efetiva proteção das vítimas (HC 653.515 RJ e AGRRHC 143.169) (Brasil. STJ, 2021a; 2021b).

Nesse contexto do Direito Digital e, considerando a importância da manutenção da cadeia de custódia de evidências derivadas digitalmente, passa-se a analisar questão relacionada às particularidades da tecnologia dos Discos em Estado Sólido (*Solid State Disk* – SSD).

2 CADEIA DE CUSTÓDIA DE IMAGENS DE DISCOS SSD PRESERVADA AINDA QUE COM *HASHES* DIFERENTES

A tecnologia SSD (*Solid State Drive*) de armazenamento de dados vem gradativamente substituindo os antigos HDD "mecânicos" (*Hard Disk Drives*) no nicho de dispositivos de memória de grande capacidade, utilizados não apenas em *desktops* e *laptops*, mas também em *datacenters* e DVR.

As principais vantagens do SSD em relação às tecnologias anteriores são: alta durabilidade e confiabilidade por não apresentarem partes móveis (como os HDD); maior velocidade de acesso aos dados; alta eficiência energética; baixo peso; nenhuma produção de ruído de funcionamento; e retrocompatibilidade com os HDD.

Todos esses avanços levaram à sua adoção como padrão na indústria de tecnologia, fazendo com que fossem produzidos em

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

massa e a baixo custo, tornando-os presentes na maioria esmagadora dos dispositivos computacionais de trabalho nos dias atuais.

Ocorre que toda essa inovação tecnológica trouxe sérios revezes para as forças forenses.

Com vistas a garantir a cadeia de custódia da prova, quando um equipamento computacional é apontado como sendo de interesse para determinada investigação, o procedimento padrão da equipe policial é: identificar os dispositivos de armazenamento (HDD/SSD) desse computador; removê-los; e apreendê-los em embalagem de segurança. Há, contudo, situações peculiares (ex. casos pedofilia) que requerem que o equipamento seja ligado *in locco* e que um perito realize uma análise prévia no conteúdo dos discos, com vistas a materializar minimamente o crime e subsidiar a conversão da prisão em flagrante em preventiva.

Tradicionalmente, a inviolabilidade da cadeia de prova de evidências digitais é confirmada mediante comparação de *hashes*: o calculado no momento da apreensão, confrontado com um cálculo posterior no decorrer do processo. *Hashes* idênticos garantem prova íntegra, no entanto, veremos que esse conceito precisa ser relativizado para os SSD.

Inicialmente, é importante esclarecer o que é a função Hash – trata-se de uma operação matemática que mapeia, idealmente de maneira única[1], um bloco de dados de qualquer tamanho (ex: todo o

[1] Apesar de o ideal ser a identificação de maneira única, isso normalmente não é possível. Mas, em razão da característica de dispersão dos algoritmos, os casos de identidade de *hash* apresentam blocos de dados de entrada muito diferentes, não comprometendo a utilidade do algoritmo.

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

conteúdo de um disco), em uma sequência de caracteres de tamanho fixo.

Essa sequência de caracteres, resultado do processo, é conhecida pelas seguintes expressões sinônimas: *hash*; *hashes*; valores *hash*; código *hash*; soma *hash*; *checksum*.

Dada a dispersão do algoritmo, a função *hash* apresenta algumas características desejáveis para a sua utilização como vetor de segurança de dados: pequenas modificações num bloco de dados de entrada geram sequências de caracteres (somas *hash*) bastante diferentes – evidenciando a mudança; apesar de indesejáveis, mas estatisticamente possíveis, blocos de dados diferentes que geram o mesmo *checksum* terão conteúdos bastante diferentes, o que impossibilita o uso dessa limitação para fins ilícitos.

Concebida para identificar e referenciar de maneira rápida e única longas sequências de dados, a função *hash* tem ampla aplicação no ramo forense. A mais conhecida delas é garantir a integridade da cadeia de provas de evidências digitais, mas, também é usada em processos de indexação de grandes volumes de arquivos digitais gravados nas mídias, permitindo buscas rápidas durante as análises investigativas.

Voltando para a tecnologia SSD, para garantir as características de eficiência, confiabilidade e alta velocidade de acesso, os SSD possuem controladores eletrônicos embarcados que rodam constantemente, em segundo plano e de forma autônoma, algoritmos de otimização de armazenamento dos dados, apagando arquivos descartados e realocando dados constantemente. Essa

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

característica gera imediatamente duas consequências indesejadas do ponto de vista forense:

A primeira é que um SSD poderá apresentar *hashes* da sua imagem global diferentes, ainda que nenhuma modificação externa tenha sido feita. Em outras palavras, ainda que a cadeia de custódia tenha sido preservada, é possível que, cada vez que um SSD seja ligado, ocorra um novo arranjo no armazenamento das informações gravadas, de forma que, ainda que o conteúdo de arquivos seja o mesmo, o *hash* da imagem global do disco pode ser diferente.

A segunda: a possibilidade recuperação de arquivos apagados, técnica bastante comum e relativamente eficaz no passado recente, se tornou mais complexa e improvável. Os SSD excluem ou tornam ilegíveis cerca de 95 a 100% dos dados imediatamente. Considerando que os algoritmos de otimização dos SSD são proprietários de cada fabricante e protegidos por direitos autorais, são remotas, por ora, as chances de que sejam desenvolvidas ferramentas forenses para recuperar dados apagados desse tipo de mídia.

É importante destacar que ainda são muito comuns outros tipos de mídias que não apresentam esse tipo de tecnologia como: unidades de HDD, cartões SD e memórias *flash* USB (*pendrives*). Neles os dados excluídos ainda possuem grandes chances de recuperação.

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

3 CONCLUSÃO

Afinal, como é possível garantir a cadeia de custódia para os SSD? nicialmente, cabe esclarecer que, se no momento da apreensão foram calculados os *hashes* de todos os arquivos individualmente (o que é incomum por demorar muito), não haverá divergência, pois, o único *hash* que sofre alteração com o comportamento do SSD é o da imagem global do disco (ISO). O mais usual e rápido durante apreensões é que se calcule um *hash* global da imagem completa do disco (ISO), nessa hipótese, serão necessárias medidas extras para garantir a integridade da prova.

Em todo caso, a solução é preservar física e documentalmente a integridade da cadeia de custódia mediante controle estrito das embalagens de segurança/lacres e fazer a documentação histórica do manuseio do vestígio nos termos do art. 158-A e ss do CPP. Uma vez rompidas as embalagens de segurança para a realização dos exames, é fundamental que o vestígio deslacrado seja manuseado por um perito especialista da área de informática, que deverá descrever minuciosamente a metodologia dos exames realizados.

Na linha das considerações expostas, seja por influência da ordem internacional ou por um despertar para o Direito Digital pátrio, impõe-se à polícia judiciária uma atuação mais técnica e ao Ministério Público um controle externo mais apurado, em especial no que se refere à preservação da integridade da cadeia de provas digitais para

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238

garantir a preservação da prova e promover a justiça na aplicação da lei penal.

REFERÊNCIAS

A CADEIA de custódia no processo penal: do Pacote Anticrime à Jurisprudência do STJ. *STJ Notícias*, 2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx. Acesso em: 14 jun. 2023.

BRASIL. STJ. *EDcl no AgRg no Recurso em Habeas Corpus nº 143.169-RJ*, 2021b. Relator: Ministro Ribeiro Dantas. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=28/03/2023. Acesso em: 14 jun. 2024.

BRASIL. STJ. *Habeas Corpus nº 653.515-RJ*, 2021a. Relator: Ministro Rogerio Schietti Cruz. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=141279576&tipo=5&nreg=202100831087&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220201&formato=PDF&salvar=false. Acesso em: 14 jun. 2024.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. *Caderno de Jurisprudência da Corte Interamericana de Direitos Humanos nº 36*: Jurisprudência sobre o Brasil. San José, C.R.: Corte IDH, 2022. ISBN 978-9977-36-289-2. Disponível em: https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo36_2022_port1.pdf. Acesso em: 14 jun. 2024.

OEA. *Situação dos direitos humanos no Brasil*. Comissão Interamericana de Direitos Humanos, 2021. ISBN 978-0-8270-7176-6. Disponível em: https://www.oas.org/pt/cidh/relatorios/pdfs/brasil2021-pt.pdf. Acesso em: 14 jun. 2024.

PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2021.

Revista do Ministério Público Militar, a. 51, n. 44, Edição especial: Seminário "Sistema jurídico militar comparado Brasil e Itália", Brasília, novembro 2024, pp. 235-246, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.13972238