INTEGRANDO FUNÇÕES FORENSES E ARQUIVÍSTICAS: UM DIÁLOGO POSSÍVEL

Juan Bernardo Montoya-Mogollón
Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP, São Paulo, Brasil.
https://orcid.org/0000-0001-6697-2986
juan.mogollon@unesp.br

Sonia Maria Troitiño Rodriguez
Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP, São Paulo, Brasil.
https://orcid.org/0000-0002-7204-3283
sonia.troitino@unesp.br

Resumo Considerando as persistentes dificuldades para gerenciar documentos de arquivo digitais, os estudos desenvolvidos na Arquivologia estabelecem relações com outras ciências para dar possíveis respostas. Assim como os estudos da Diplomática são relevantes para a Arquivologia na verificação de autenticidade através da aplicação dos elementos externos e internos nos documentos de arquivo, as pesquisas forenses estão fornecendo subsídios nas rotinas administrativas e arquivísticas, para tentar atingir e garantir a fidedignidade documental (completude, confiabilidade e autenticidade). Desta forma, o objetivo deste artigo é incorporar os conceitos da Ciência Forense Digital na Arquivologia, trabalho que está sendo desenvolvido em projetos internacionais, principalmente nos Estados Unidos e no Canadá, aproveitando a maturidade dos estudos forenses no domínio digital. Para integrar as duas ciências em questão, reflete-se nas funções forenses: identificação, compilação, preservação, verificação, análise e apresentação. Junto com as funções arquivísticas: criação/produção, avaliação, classificação, descrição, difusão, preservação e aquisição. Para isso, a metodologia usada, parte da literatura científica das pesquisas nacionais e internacionais em andamento, que permitam visibilizar, tanto as convergências, como as divergências das fases ou passos forenses, como das funções arquivísticas. Os resultados apontaram a possibilidade de vincular as funções de ambas as ciências refletindo, no entanto, em alguns conceitos que precisam ser melhor definidos, na busca por estabelecer uma ciência Forense-Arquivística. A conclusão deste artigo baseia-se na necessidade de continuar aprofundando nos estudos nacionais, para delimitar os elementos e conceitos e que contribuam para os estudos arquivísticos na realidade digital.

Palavras-chave Arquivologia. Forense Digital. Documentos de Arquivo Natos Digitais. Fidedignidade.

INTEGRATING FORENSICS AND ARCHIVAL FUNCTIONS: A POSSIBLE DIALOGUE

Abstract Considering the persistent difficulties to management the digital records, studies in Archival Science establish relationships with other sciences to offer possible answers. As that the research in Diplomatics is relevant to Archival Science in the ascertaining of authenticity through of application of external and internal records elements, Forensics research are providing supports in the administrative and archival routines attempting to reach and assure the documental trustworthiness (accuracy, reliability and authenticity). Therefore, the objective of this article is to incorporate the elements of Forensics in Archival Science, efforts that are being developed in United States and Canada projects seizing the maturity of the forensics studies in the digital realm. To integrate the two named sciences, the Forensics functions are addressed: identification, collection, preservation, examination, analysis and presentation. Along with the Archival functions: creation/production, assessment, classification, description, outreach, preservation and acquisition. For this, the applied methodology arises of the ongoing national and international scientific literature, that allows makes visible the similarities and differences of Forensics phases and/or steps, as Archival functions. The results appointed the possibility to bring together the functions and steps of both sciences, albeit highlighting, some concepts that need to be better defined in the pursuit of an Archival-Forensics. It is necessary to continues studying in the national research to delimit the elements and concepts that contributes to the Archival studies in the digital context.

Keywords *Archival Science. Digital Forensics. Digital Records. Trustworthiness.*

Submetido em 13/04/2022
Aprovado em 19/07/2022
Publicado em 22/09/2022

1 INTRODUÇÃO

Devido às latentes dificuldades em relação ao gerenciamento e preservação dos documentos de arquivo natos digitais[1], os estudos teóricos e práticos na Arquivologia continuam aprimorando seus conceitos na busca por manter a fidedignidade dos mencionados documentos. Assim, os estudos em andamento na Arquivologia estão em constante busca e interação com outras ciências, que fortaleçam a sua própria estrutura teórica e prática. Nesse processo, tem-se visto a incorporação de princípios e teorias advindas de ciências, como a Diplomática, a História, o Direito e, na atualidade, alguns elementos e ferramentas tecnológicas da Ciência Forense digital[2]. As pesquisas nessa última ciência estão dando interessantes elementos, ferramentas, conceitos e métodos que lidam com objetos digitais.

Assim, este artigo faz parte de uma tese de doutorado defendida em 2021 a qual buscou criar um elo entre a Arquivologia e a Ciência Forense Digital, com o propósito de dar algumas respostas para manter a fidedignidade dos documentos digitais, além dos repositórios arquivísticos nos quais esses documentos são conservados e preservados. Para cumprir tal objetivo, são incorporados limites em relação às fases ou aos passos forenses e as funções arquivísticas que permitam o entendimento das duas ciências em questão, a fim de minimizar ambiguidades ao momento de ser aplicado nas rotinas arquivístico-administrativas e de prova legal.

A Ciência Forense digital encontra-se em um momento ideal (*Forensics Readiness)*[3] como auxílio em ciências, tais como a Psicologia, a Medicina, as Engenharias e a Criminologia, entre outras. Seus estudos atuais, principalmente no contexto internacional, estão gerando profícuas pesquisas no âmbito da Arquivologia. No entanto, por ser uma ciência relativamente nova, surgida no final do século XX, alguns conceitos continuam sendo aprimorados, tanto no seu próprio *corpus* teórico e

[1] Foi escolhido o termo documento de arquivo nato-digital, como sinônimo de documento arquivístico nato-digital, tal como se encontra descrito no decorrer da nossa tese de doutorado defendida em julho de 2021. Nesse sentido, o termo digital faz referência especificamente a esse objeto arquivístico nesse suporte, e não, a um lugar que poderia ser chamado de digital.

[2] Esta ciência pode ser encontrada na literatura internacional como Forense Computacional, no entanto, as aplicações são divergentes da Forense digital.

[3] *Forensics Readiness,* significa ter a capacidade de verificar que os dados digitais analisados em determinadas fontes digitais possam ser admissíveis. Kebante *et al.* (2021, p.2, tradução nossa), destacam que "...estar preparado no âmbito forense (*forensically ready*) pode ajudar às organizações na recuperação rápida de dados, o aprimoramento da continuidade do negócio e o cumprimento de ações legais, ao manter as provas digitais disponíveis".

prático, como na adaptação em outras ciências. Tendo isso em vista, o propósito deste trabalho é discutir, inicialmente, as possibilidades de diálogo entre as duas ciências, considerando também as diferenças conceituais para que sejam aprofundadas, discutidas e adaptadas.

Para estabelecer o vínculo entre as duas ciências, foi necessário, como metodologia, recorrer à literatura,-no contexto internacional, por ser precisamente esses estudos os que estão analisando sua possível integração, não só no modelo clássico do Ciclo Vital do documento, como também em outras perspectivas, a exemplo do *Records Continuum* na Austrália[4] e o projeto *Blockchain* da Universidade da Colúmbia Britânica - UBC, no Canadá[5]. As pesquisas nacionais também são muito relevantes neste trabalho, principalmente em relação às funções arquivísticas. Desse modo, serão analisadas cada uma das fases usadas na Ciência Forense digital, discutindo suas similitudes e diferenças com as funções arquivísticas. Feito isso, serão também analisados as ferramentas, os instrumentos e métodos de cada ciência como suporte para garantir a fidedignidade dos documentos de arquivo natos digitais, isto é, sua confiabilidade, integridade e autenticidade.

Os critérios de escolha da literatura internacional se deu pela oportunidade de conhecer as pesquisas do Projeto do INTERPARES[6] de forma presencial na UBC, em Vancouver, no Canadá, como parte do doutorado sanduíche desenvolvido em 2019. Nesse período, foi possível trocar experiências acadêmicas com pesquisadoras e coordenadoras do projeto mencionado, tais como Luciana Duranti, Corinne Rogers, Victoria Lemieux, entre outros. Da mesma forma, os estudos nacionais foram escolhidos devido a sua melhor adaptação no âmbito brasileiro e suas possíveis convergências com as pesquisas da Ciência Forense digital.

2 DA CIÊNCIA FORENSE À CIÊNCIA FORENSE DIGITAL

No contexto digital, são observadas duas ciências centrais que constituem e reforçam o núcleo da Ciência Forense digital: o Direito e a Ciência da Computação. A primeira é uma área que vem acompanhando a Forense tradicional. No domínio digital, o Direito analisa a prova digital fornecendo suficientes normas legais para que essa prova seja admissível perante a lei. A Computação, de outro lado, foi incorporada à Ciência Forense digital (PALMER, 2001, POLLITT, 2010,

[4] Este projeto está sendo desenvolvido desde o 2018, deixando como resultado, neste momento, a publicação do livro, *Recordkeeping Informatics for a Networked Age,* escrito por Frank Upward, Barbara Reed, Gillian Oliver e Joanne Evans. Em: https://publishing.monash.edu/product/recordkeeping-informatics-for-a-networked-age/

[5] Em:https://www.eventbrite.ca/e/blockchainubc-august-research-talk-ryon-shamloo-tickets-383771519947?aff=ebdsoporgprofile

[6] www.interpares.org

DURANTI, 2010), com o objetivo de fornecer ferramentas e métodos tecnológicos, desde a captura da prova digital para manter a sua integridade.

Assim, a Ciência Forense fundamenta sua estrutura científica e investigativa na análise da prova, a qual, no contexto digital, é chamada de "prova digital". Essa prova digital está determinada, tanto na análise dos dados mantidos dentro dos dispositivos físicos (*hardware*), como de *software,* complementando algumas atividades difíceis de alcançar dentro da Arquivologia. Desse modo, as contribuições trazidas por essa ciência permitem que os arquivistas possam garantir a integridade dos documentos, além dos sistemas em que eles são gerenciados e preservados.

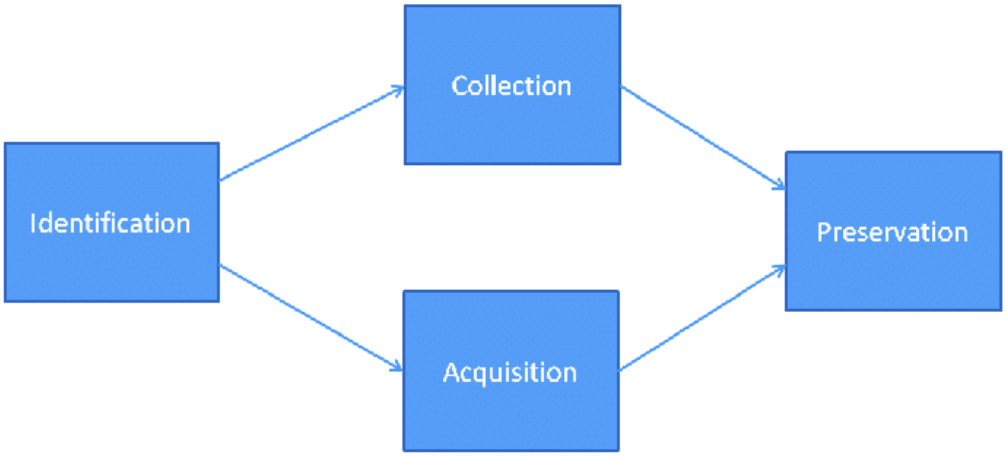
Existem várias definições da Ciência Forense digital, porém, visando abordar a mais adequada para a presente proposta, foi escolhida a feita por Gary Palmer (2001, p. 15, nossa tradução), que a descreve como:

> O uso derivado e provado de métodos científicos para a preservação, compilação, validação, identificação, análise, interpretação, documentação e apresentação da prova digital, derivada de fontes digitais, com o propósito de facilitar ou promover a reconstrução de eventos, considerados como criminosos, ou de ajuda a antecipar ações não autorizadas, que se mostrem prejudiciais às operações planejadas.

Da citação anterior, observa-se cada um dos passos que devem ser seguidos, a fim de estabelecer uma correta sequência ao capturar a prova digital. Ao ser abordado esses passos descritos, foi interessante observar que a metodologia da Ciência Forense digital estabelece certas relações e diferenças com as funções arquivísticas. Portanto, é necessário entender a definição de cada uma das funções descritas, com o objetivo de estabelecer um diálogo entre as duas ciências. Portanto, nossa proposta é chamar essa integração de "Forense-Arquivística".

Cada uma das fases descritas por Palmer na citação anterior é abordada de forma não sequencial, o que pode demonstrar que essas fases estavam em caminho de normalização para, posteriormente, serem melhor entendidas. Portanto, é possível observar na Figura 1 da ISO 27037 de 2013 as mencionadas fases numa ordem padronizada. Para o cientista forense, é relevante acompanhar cada uma das fases nessa ordem a fim de assegurar a correta coleta das provas digitais.

Figura 1 – Processos de tratamento das provas de acordo com a ISO 27037



Fonte: Cloud Security Alliance (2013, p. 11).

Segundo a Figura 1, o primeiro passo é a identificação. Nesse ponto inicial, os profissionais identificam especificamente as possíveis provas digitais que vão ser analisadas. Na sequência, a segunda fase é a compilação e a aquisição. A compilação se relaciona com o processo de coletar itens que contenham potenciais provas digitais. Além disso, essa fase é trabalhada mediante ordens emitidas por autoridades legais e essas provas são encaminhadas e analisadas em laboratórios especializados. A etapa da aquisição, conforme o *Cloud Security Alliance* (2013, p. 11, tradução nossa), é o processo de cópia dos dados dentro de um conjunto definido. Esse processo da aquisição é realizado principalmente em organizações privadas, com o objetivo de garantir a continuidade do negócio.

O quarto passo é o da preservação, definido como o processamento da prova, assegurada desde a etapa da identificação. Nessa etapa, é relevante preservar a cadeia de custódia e a integridade dos dados. Para André Årnes (2018, p. 22, tradução nossa), a fase da preservação

> [...] deve incluir atividades de isolamento, asseguramento e documentação dos dispositivos físicos e digitais analisados. A preservação da prova pode exigir a aplicação de tecnologias para a subsequente cópia da mídia original, estabelecendo a sincronização do tempo e qualquer outra atividade que possa facilitar as atividades forenses.

Nessa ordem, a preservação aparece como uma fase inicial ao momento da coleta da prova digital. A etapa da preservação para o cientista forense adquire um significado e uso diferente do feito dentro dos processos arquivísticos. A preservação Forense se centra em garantir (preservar) a integridade dos dados depois de serem coletados. No entanto, os dados são mantidos somente durante o tempo em que dure o caso legal analisado, após esse processo, os dados são descartados, já que permanece] a prova “original”.

O propósito de "controlar" a prova digital dentro dessas etapas definidas aumenta a possibilidade de assegurar a integridade dos dados como ponto de partida para atingir a fidedignidade forense. Justamente, esse modelo de fidedignidade na Ciência Forense estabelece algumas diferenças com o conceito de fidedignidade construído na Arquivologia. Os elementos que compõem a fidedignidade da Forense digital estão definidos na sua integridade, autenticação, reprodutibilidade, não interferência e minimização (MOCAS, 2004, tradução nossa).

Assim, segundo Sarah Mocas (2004, tradução nossa), a manutenção da integridade é feita por meio da análise *bit* a *bit* dos dados, assegurando que eles permaneçam completos e sem modificações. De igual forma, essa manutenção de integridade é verificada nos sistemas e componentes físicos onde a informação é fixada. A metodologia para garantir a não alteração dos dados é feita através de ferramentas tecnológicas, por exemplo, na criação de uma imagem (*imaging*) ou cópia da informação. Caso a prova digital copiada seja contaminada ou modificada, o expert forense pode verificar de novo a fonte original.

A autenticação é um elemento que difere do conceito de autenticidade. Ela é estabelecida de duas formas: autenticação como parte de segurança do computador, criando uma relação entre o computador e seu autor; a segunda é a autenticação legal, em que se verifica a admissibilidade da prova (MOCAS, 2004). A reprodutibilidade é a garantia da reprodução dos dados em qualquer momento. A não-interferência é um princípio estabelecido para que a prova coletada não seja misturada com outro tipo de provas. A minimização, por último, como explicado por Mocas (2004, tradução nossa), permite que a prova coletada seja relevante nos casos analisados, garantindo a mínima quantidade de dados processados (coletados e/ou examinados).

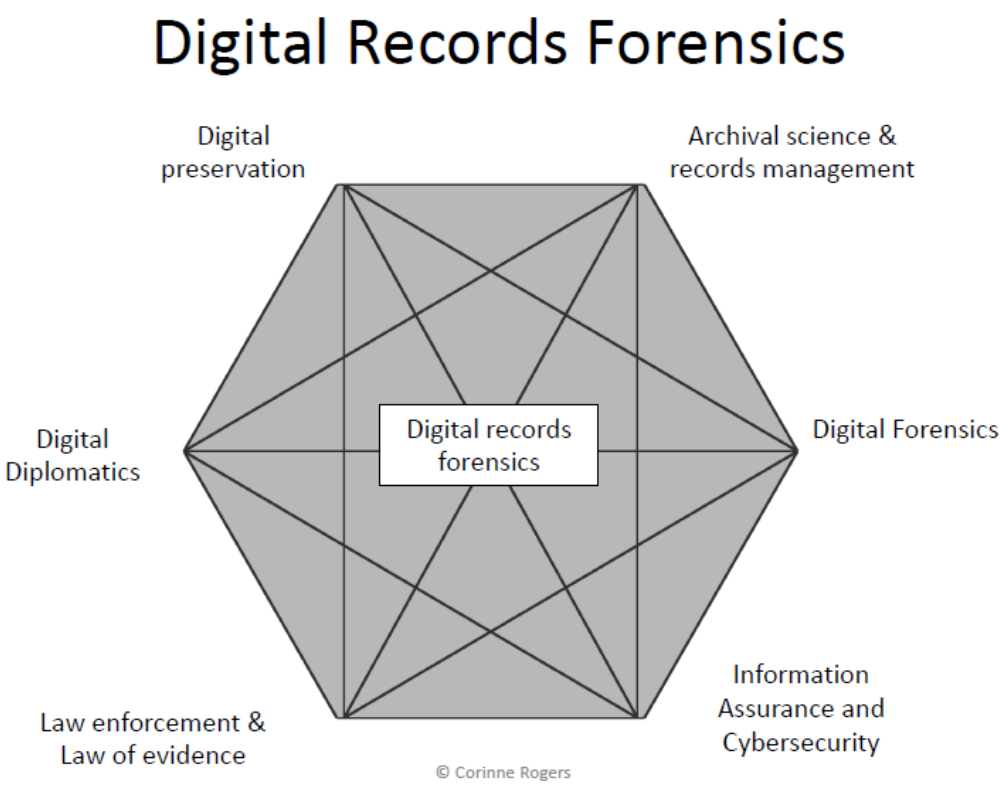
Alguns autores explicam que, desde o surgimento dos estudos da Ciência Forense digital nos anos de 1980, o campo tem passado por um processo de maturidade. Mark Pollitt (2010) estrutura o percurso da Ciência Forense digital em épocas históricas, determinando uma certa suficiência no presente e futuro. Para um melhor acompanhamento da ciência, o autor divide as épocas históricas assim: pré-história (1985), primeira infância (1985-1995), infância (1995-2005), adolescência (2005-2010) e futuro e além (2010-).

Com esse percurso histórico apontado por Pollitt (2010), a Ciência Forense digital encontra-se em seu melhor estágio de maturidade, como apontado por vários pesquisadores. É um momento de desenvolvimento das teorias e práticas do núcleo Forense, possibilitando fornecer subsídios tecnológicos a outras ciências que estão precisando melhorar os mecanismos de autenticidade digital, o qual seria o caso da Arquivologia.

3 INTEGRANDO AS FUNÇÕES DA FORENSE DIGITAL NO PROCESSO ARQUIVÍSTICO

Os estudos na Arquivologia estabelecem relações epistemológicas com outras ciências com o propósito de aprimorar o gerenciamento de documentos de arquivo. Assim, é observado como a Arquivologia tem percorrido um longo caminho histórico, incorporando conceitos, elementos e métodos de outras ciências, tais como a História, o Direito, a Diplomática e hoje a Ciência Forense digital. Desse modo, como observado na Figura 2, o núcleo da ciência é chamado de "Forense nos Documentos de Arquivo Digitais". Na Figura 2, as áreas que estabelecem o vínculo de apoio são: a Arquivologia e Gestão Documental, a Forense Digital, a Garantia da Informação e Cibersegurança, a Aplicação da Lei, a Diplomática Digital e a Preservação Digital.

Figura 2 – Digital Records Forensics



Fonte: Rogers (2019, slide.7).

Dentro da estrutura ilustrada pela Figura 2, a Diplomática digital cumpre um papel relevante. Justamente a incorporação da Diplomática na Arquivologia criou uma forma de verificar a autenticidade dos documentos de arquivo por meio dos tradicionais elementos externos e internos, isto é, a aparência externa do documento e seu conteúdo. A Diplomática nos documentos de arquivo

digitais permitiu também analisar o documento de forma singular e identificar o vínculo com seu autor e com outros documentos que fazem parte do processo arquivístico.

As pesquisas em torno da Diplomática Arquivística ampliaram a análise dos documentos digitais, passando do conceito de "autenticidade" para o de "fidedignidade", isto é, a completude, confiabilidade e autenticidade. Victoria Lemieux *et al.* (2019) aprofundam teoricamente esses atributos, esclarecendo que a completude se relaciona à capacidade de que esses documentos digitais mantenham sua composição interna e externa, e que sejam corretos, verdadeiros e pertinentes. A confiabilidade é definida por meio da consistência dos procedimentos formais da completude, a qual deve ser mantida desde o momento da criação e, finalmente, a sua objetividade/imparcialidade (naturalidade). A autenticidade, por último, é apresentada por meio de dois elementos: integridade e identidade.

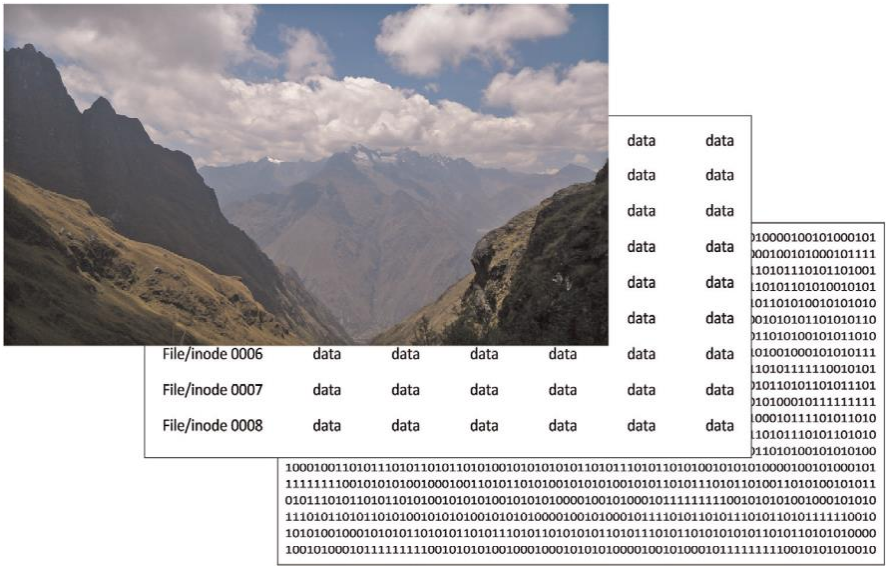
A integridade é a capacidade de manter a estrutura dos bits sem alterações ou com alterações identificáveis. O elemento da integridade é a principal contribuição por parte da Ciência Forense digital. A identidade é o que distingue um documento de outro.

Da mesma forma, as pessoas que interagem no processo documental e na análise da "história" definido arquivisticamente como o princípio de proveniência[7]. No entanto, no domínio digital, esses documentos precisam ser melhor analisados em relação à sua composição tecnológica. Nesse campo, Kenneth Thibodeau (2002) e Corinne Rogers (2015) analisam precisamente a estrutura interna do documento digital, abordando-o por meio de camadas definidas como: físicas, lógicas e conceituais.

Como será mostrado na Figura 3, a camada física é determinada no espaço onde é fixada a informação representada em fluxo de *bits* (codificação computacional em zeros e uns). A camada lógica são os algoritmos processados pelo próprio computador. A camada conceitual é a forma em que a informação é observada e entendida pelos usuários. Assim, a partir desses estudos, é possível analisar como, posteriormente, foi necessária a incorporação da Ciência Forense digital, tanto para entender a tecnologia dos documentos digitais, como fonte de prova para cenários administrativos, arquivísticos e legais.

Figura 3 – Imagem como é observada por um usuário no sistema operativo e pelo *hardware*.

[7] Antonia Heredia-Herrera destaca a importância deste princípio, assinalando nesse sentido, que: (1991, p.33-34, tradução nossa): "[...] cada documento deve estar localizado no fundo documental de onde provêm, e neste fundo em seu lugar de origem.



Fonte: Årnes (2018, p. 41).

O propósito de integrar as pesquisas da Ciência Forense digital na Arquivologia tem como objetivo gerenciar “melhores” documentos de arquivo, possibilitando um diálogo entre cada ciência estudada. Na seção anterior, foram descritas as funções aplicadas na Ciência Forense digital na análise das provas digitais. Feito isto, serão analisadas as funções arquivísticas, na possibilidade de determinar as convergências e divergências na construção da Ciência Forense-Arquivística.

Tomando como referência o trabalho dos canadenses Yves Rousseau e Carol Couture (1998), os autores estabelecem um modelo padronizado de funções arquivísticas as quais podem ser aplicadas de forma geral em vários contextos. As funções descritas por esses autores são: produção/criação, classificação, avaliação, descrição, difusão, preservação e aquisição. Dentro dessa estrutura, existe uma função relevante que não aparece nas escritas anteriormente, a função da identificação. Ana Célia Rodrigues (2012, p.1) destaca a “[...] função da identificação como uma função independente no âmbito da metodologia arquivística”.

> Para a arquivística espanhola, a *identificação* é uma fase independente da metodologia arquivística, qualificada como do tipo intelectual, a qual consiste em estudar analiticamente o órgão produtor e a tipologia documental por ele produzida e que antecede as demais funções (produção, avaliação, classificação e descrição). (RODRIGUES, 2012, p. 3).

Assim, a identificação é caracterizada por ser uma função estudada nos processos arquivísticos da Espanha nos anos de 1980 e incorporada posteriormente nos estudos arquivísticos no Brasil. Portanto, sua inclusão é de importância por representar um elo entre a Diplomática nos processos arquivísticos e, hoje, pela possibilidade de ser integrada nas funções da Ciência Forense digital.

Seguindo com as demais funções, a produção/criação tem como objetivo o controle da criação dos documentos orgânicos (PEREIRA, SILVA, 2019, p. 2). A avaliação tem como objetivo julgar o valor primário e secundário dos documentos de arquivo com o objetivo de planejar sua disposição final. A classificação, segundo o Dicionário Brasileiro de Terminologia Arquivística (2013, p. 9), é definida como a:

> Organização dos documentos de um arquivo (1) ou coleção, de acordo com um plano de classificação, código de classificação ou quadro de arranjo. (2) Análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos. (3) Atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica. Também chamada de classificação de segurança. Ver também desclassificação, documento classificado e documento sigiloso.

A descrição é definida como o "conjunto de procedimentos que leva em conta os elementos formais e de conteúdo dos documentos para elaboração de instrumentos de pesquisa" (ARQUIVO NACIONAL, 2013, p. 67). O conceito de "difusão" é uma função não muito familiar para o contexto nacional e estaria relacionado mais com a fase de "divulgação": "conjunto de atividades destinadas a aproximar o público dos arquivos (2), por meio de publicações e da promoção de eventos, como exposições e conferências" (ARQUIVO NACIONAL, 2013, p. 72). A preservação é a capacidade de conservar, de forma permanente, os documentos de arquivo ao longo do tempo e do espaço.

Por último,

> a palavra "aquisição" não aparece no Dicionário Brasileiro de Terminologia Arquivística, mas aparece como "entrada de documentos", sendo este o ingresso por meio de compra, custódia, comodato, doação, empréstimo, doação, legado, recolhimento, transferência, reintegração ou permuta. (ARQUIVO NACIONAL, 2013, p. 85)

Delimitadas as funções arquivísticas e forenses se passará a analisar as definições e aplicações com o propósito de criar um vínculo que permita trabalhar de forma conjunta para atender às dificuldades no gerenciamento de documentos de arquivo digitais. A proposta neste artigo é nomeá-las como funções Forenses-Arquivísticas.

O primeiro processo é a identificação. Luciana Duranti (2010) explica que essa função é um desafio para as duas ciências ao identificar documentos de arquivo entre todos os objetos produzidos por sistemas interativos e dinâmicos e determinar sua autenticidade. Na primeira questão, ressalta a autora, o trabalho da Diplomática digital é a identificação de documentos de arquivo digitais, como análise de uma ciência secular que estuda a natureza, gênese, as características formais, a estrutura, transmissão e as consequências legais dos documentos de arquivo. A segunda questão a Ciência Forense digital verifica, indiretamente, a autenticidade de documentos de arquivo digitais (DURANTI, 2010, p. 46, tradução nossa).

Assim, a Diplomática digital identifica especificamente os documentos de arquivo digitais, enquanto a Forense digital aborda o conceito de "prova digital", o qual excede o objeto da Diplomática Arquivística digital, analisando tanto a composição interna dos documentos, como os sistemas e repositórios onde os documentos são armazenados. Nesse ponto, é possível ajustar o conceito de "prova digital" para o de "documento de arquivo digital", o qual está estruturado internamente em dados e informação. Dessa forma, a fase da identificação Forense-Arquivística poderia resultar interessante na análise de autenticidade, considerando a diferença entre uma e outra ciência.

A compilação na Forense digital seria uma fase que pode ser considerada nas funções arquivísticas, já que é o asseguramento de possíveis provas digitais que, no caso da Arquivologia, são os documentos de arquivo digitais. Nesse ponto, o trabalho do arquivista é relevante, pois pode determinar, com seu conhecimento, confiáveis documentos de arquivo. A fase da aquisição, como foi explicado na seção da Ciência Forense digital, é aplicada no âmbito privado. Como foi colocado também nas funções arquivísticas, a aquisição tem definição e aplicação diferente. Nesse sentido, poderia ser diferenciado e nomeado como uma fase de "aquisição-forense" aplicada ao gerenciamento dos documentos digitais na gestão documental.

A fase da preservação é analisada de forma diferente, tanto para a Forense digital como para a Arquivística. Preservação, para a Forense digital, refere-se à garantia da proteção da integridade dos dados, de modificações não desejadas ao momento de serem apresentadas às autoridades. Preservação, para a Arquivologia, está relacionada à ação de perpetuar os documentos, devido a sua vital importância como memória organizacional e institucional. Nesse ponto, deveria ser aplicado o conceito de preservação constituído pela Arquivologia, já que a integridade dos dados deve ser mantida desde a própria produção/criação dos documentos digitais.

Outro problema da preservação visto desde uma perspectiva da Ciência Forense é a sua temporalidade. A informação nessa ciência é preservada, ou mantida, somente durante o tempo de duração do determinado caso. Como já foi escrito, a informação trabalhada pelos profissionais forenses é uma cópia da informação "original", evitando que, caso seja apresentado um possível erro, modificação ou contaminação, seja possível copiar de novo os dados da fonte original.

Por tanto, esse recurso de criar cópias de informações poderia ser usado nos trabalhos arquivísticos como formas de *backup*, caso exista algum risco de perda de documentos sensíveis, porém, com a intenção de serem descartados terminada sua função. Outra possibilidade de uso da preservação Forense poderia ser aplicada nos processos de migração, emulação, refrescamento,

encapsulamento para outros sistemas ou repositórios arquivísticos. No entanto, objetivando a permanência definitiva só dos documentos originais.

Como foi destacado no início deste artigo, existem outras fases da Forense digital as quais ainda estão em fase de desenvolvimento. Portanto, além das já mencionadas pela ISO 27037 de 2013, serão elencadas outras fases normalmente aplicadas nos processos dessa ciência. Essas fases são a verificação, a análise e a apresentação da prova digital. Cada uma dessas definições é comparada com as funções arquivísticas no Quadro 1, com o objetivo de analisar suas similaridades e diferenças.

Quadro 1 – Fases Forenses e Funções Arquivísticas.

FASES FORENSES	INSTRUMENTOS E/OU RESULTADOS	FUNÇÕES ARQUIVÍSTICAS	INSTRUMENTOS E/OU RESULTADOS
IDENTIFICAÇÃO: identificar a prova a ser investigada.	"[...] Busca reconhecimento e a documentação de possíveis evidências digitais [...]" (CSA, 2013, p. 11, tradução nossa).	**IDENTIFICAÇÃO:** "[...] estudar analiticamente o órgão produtor e a tipologia documental por ele produzida [...]" (RODRIGUES, 2012).	Documento de arquivo
COMPILAÇÃO: agrupar itens que contenham possíveis provas digitais.	Realiza-se por meio de uma autoridade ou ordem legal e os itens são trasladados a um laboratório especializado para analisar a possível prova digital (CSA, 2013).	**CRIAÇÃO/PRODUÇÃO:** controle da criação dos documentos orgânicos (PEREIRA, SILVA, 2019, p. 2)	Documento de arquivo
AQUISIÇÃO: criação de uma cópia dos dados dentro de um conjunto definido.	Copiar os dados para ser transferidos a um sistema confiável, garantindo a integridade dos dados. Imagem dos dados.	**AVALIAÇÃO:** julgar o valor primário e secundário dos documentos de arquivo com o objetivo de planejar sua disposição final.	Tabela de temporalidade
PRESERVAÇÃO: isolamento, asseguramento e documentação dos dispositivos físicos e digitais analisados (CARRIER; SPAFFORD, 2003, tradução nossa).	Manter e salvaguardar a integridade e a condição original da possível prova digital (CSA, 2013, p. 12, tradução nossa).	**CLASSIFICAÇÃO**: organização dos documentos de um arquivo (1) ou coleção, de acordo com um plano de classificação, código de classificação ou quadro de arranjo. (2) Análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos. (3) Atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica" (ARQUIVO NACIONAL, 2013, p. 72).	Plano de classificação

VERIFICAÇÃO: preparação e extração de possíveis provas das fontes de dados coletados (ÅRNES, 2018, tradução nossa).	*Imaging*	**DESCRIÇÃO:** "conjunto de procedimentos que leva em conta os elementos formais e de conteúdo dos documentos para elaboração de instrumentos de pesquisa" (ARQUIVO NACIONAL, 2013, p. 67).	Instrumento de pesquisa
ANÁLISE: processamento de informação que aborda o objetivo da investigação, com o propósito de determinar os fatos de um evento, a importância da prova e a(s) pessoas envolvidas (ÅRNES, 2018, tradução nossa).	MD5 checksum	**DIFUSÃO (DIVULGAÇÃO):** "conjunto de atividades destinadas a aproximar o público dos arquivos (2), por meio de publicações e da promoção de eventos, como exposições e conferências" (ARQUIVO NACIONAL, 2013, p. 72).	Disseminação da informação; cumprimento do princípio da publicidade (SOUSA, 2013)
APRESENTAÇÃO: realizar relatórios ou laudos para terceira(s) pessoa(s).	Conclusões das provas digitais realizadas materializadas em laudos ou relatórios.	**PRESERVAÇÃO**: capacidade de manter de forma permanente os documentos de arquivo ao longo do tempo.	Manutenção da informação a longo prazo.
		AQUISIÇÃO: [...] ingresso por meio de compra, custódia, comodato, doação, empréstimo, dação, legado, recolhimento, transferência, reintegração ou permuta (ARQUIVO NACIONAL, 2013, p. 85).	Fundo de arquivo

Fonte: Montoya-Mogollón; Troitiño (2022).

No processo de integralização forense-arquivístico proposto, são destacadas duas fases e funções as quais devem ser esclarecidas para criar uma ideal interação. A fase da aquisição, quando incorporada na função arquivística, deveria ser chamada de "aquisição forense", entendendo sua diferença com a Arquivologia. Do mesmo modo, a fase preservação, como foi discutida anteriormente, apresenta alguns desafios acerca da definição e aplicação entre as duas ciências. Portanto, seria possível diferenciar, nesse processo, a preservação da Ciência Forense com a da Arquivologia.

Assim, as funções arquivísticas forenses no domínio digital proposto estaria conformado da seguinte forma: Identificação, Criação/Produção, Compilação, Aquisição Forense, Avaliação, Classificação, Preservação, Verificação, Análise, Descrição, Difusão, Apresentação e Aquisição.

4 CONSIDERAÇÕES FINAIS

Considerando os novos desafios para atender às dificuldades dos documentos de arquivo digitais, novas ciências emergentes como a Forense digital podem ser vistas como interessantes

opções para suprir as demandas surgidas neste contexto digital. Hoje, devido a uma situação especial de pandemia, as interações humanas estão se consolidando em relações especialmente on-line, o que está gerando um aumento desbordado de informação digital. Esse conhecimento criado nas diversas plataformas tecnológicas digitais deve ser propriamente gerenciado, conservado e disponibilizado corretamente para que a memória da sociedade não seja apagada ou modificada, o que poderia criar incertezas da autenticidade da informação no futuro.

A Arquivologia tem um papel fundamental para atingir essas demandas sociais e os arquivistas têm a obrigação de aplicar, integralmente, os conhecimentos estabelecidos pela própria ciência, além de incorporar os elementos, as teorias e práticas de outras ciências que acrescentem ao conhecimento arquivístico. São poucas as pesquisas no país que vinculam o conhecimento arquivístico com o os estudos da Forense digital, motivo pelo qual se faz necessário começar a criar um diálogo entre ambas as ciências. Este trabalho tentou vincular as fases forenses e às funções arquivísticas, com o objetivo de iniciar esse processo de interação entre duas ciências que, como foi visto, concentram alguns conceitos similares com aplicações diferentes. Portanto, o caminho está em construção e é esperado que as pesquisas continuem para tornar possível explorar, ainda mais, ciências que contribuam para o correto gerenciamento e preservação dos documentos digitais.

REFERÊNCIAS

ÅRNES, André. **Digital Forensics**. River Street, Hoboken, USA: John Wiley & Sons Ltd, 2018.

ARQUIVO NACIONAL (Brasil). **Dicionário Brasileiro de Terminologia Arquivística.** Rio de Janeiro: Arquivo Nacional, 2013.BLOCKCHAIN@UBC. www.blockchain.ubc.ca

CLOUD SECURITY ALLIANCE. **Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing**. 2013. Disponível em: https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf Acesso em: 13 abr. 2022.

DURANTI, Luciana. Digital Records Forensics: A New Science and Academic Program for Forensic Readiness**. Journal of Digital Forensics, Security and Law**, USA, v. 5: n. 2, Article 4. DOI: https://doi.org/10.15394/jdfsl.2010.1075. Disponível em: https://commons.erau.edu/cgi/viewcontent.cgi?article=1075&context=jdfsl. Acesso em: 13 abr. 2022.

HEREDIA HERRERA, Antonia. **Archivística general. Teoría y práctica.** Sevilla, España, Diputación Provincial de Sevilla, 1991.

KEBANDE, Victor *et al*. Digital forensic readiness intelligence crime repository. **Security and Privacy**., United Kingdom**,** E1,51, 2021. DOI: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.151 Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.151 Acesso em: 13 abr. 2022.

LEMIEUX, Victoria *et al*. Blockchain Technology and recordkeeping. Project Underwritten by: **ARMA** International, Educational Foundation. Research, Education, Scholarship, Canada, 2019. Disponível em: http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf. Acesso em: 13 abr. 2022.

MOCAS, Sarah. Building theoretical underpinnings for digital forensics research. **Digital Investigation**, USA, v.1, i.1, pp.61-68, 2004. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1742287603000057?via%3Dihub. Acesso em: 13 abr. 2022.

PALMER, Gary. A Road Map for Digital Forensic Research. In: From the **proceedings of The Digital Forensic Research Conference DFRWS**, USA, Utica, NY, pp. 1-42, Aug 7th - 8th2001. Disponível em:https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf. Acesso em: 13 abr. 2022.

PEREIRA, Diogo Baptista; SILVA, Eliezer Pires da Silva. Funções arquivísticas: caracterizando finalidades de instituições de arquivo. **ÁGORA**: Arquivologia Em Debate, Florianópolis, 29(58), 1–22, 2019. Disponível em https://agora.emnuvens.com.br/ra/article/view/754. Acesso em: 13 abr. 2022.

POLLITT, Mark. A history of digital forensics. CHOW, K. P.; SHENOI, S. **Advances in digital forensics VI**. CHOW, K. P.; SHENOI, S (Eds.). Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers. Germany: Springer, 2010. DOI: https://doi.org/10.1007/978-3-642-15506-2_1. Disponível em: https://link.springer.com/content/pdf/10.1007%2F978-3-642-15506-2_1.pdf. Acesso em: 13 abr. 2022.

RODRIGUES, Ana Célia. Identificação arquivística como requisito metodológico do Programa de Gestão de Documentos do Governo de Estado do Rio de Janeiro (PGD-RJ): reflexões sobre a construção teórica dos procedimentos e instrumentos. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 13., 2012, Rio de Janeiro. **Anais**. P.1-20. Disponível em: http://repositorios.questoesemrede.uff.br/repositorios/handle/123456789/576. Acesso em: 13 abr. 2022.

SOUSA, Nascimento Fábio. **Funções arquivísticas**: contribuições para o cumprimento da lei de acesso à informação. 2013. Monografia (Especialização) – Curso de Especialização a Distância em Gestão de Arquivos, Universidade Federal de Santa Maria (UFSM, RS), Cachoeira do Sul, 2013. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/114/Souza_F%C3%A1bio_Nascimento.pdf?sequence=3. Acesso em: 13 abr. 2022.

ROGERS, Corinne. **Digital forensics – intro and history**. Canada. Topics in Archival Automation Digital Records Forensics course. ARST 556H. February 06, 2019. 63 slides. UBC - School of Information.

ROUSSEAU, Jean-Yves; COUTURE, Carol. **Os fundamentos da disciplina arquivística**. Lisboa: Publicações Dom Quixote, 1998.

THE INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS – The InterPARES Project. In: www.interpares.org

THIBODEAU, Francis Kenneth. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. In: **Conference proceedings documentation abstracts**, Inc. Institutes for information science Washington, D.C. Council on Library and Information Resources Washington, D.C. April 24-25, 2002. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.89.3273. Acesso em: 13 abr. 2022.

UPWARD, Frank et al. Recordkeeping Informatics for a Networked Age. In: Australia. Monash University Publishing, 2018.

NOTAS DE AUTORIA

Juan Bernardo Montoya-Mogollón
Doutor (2021) e Mestre (2017) em Ciência da Informação pelo PPCI/UNESP/Marília e estudante de Arquivologia pela UNESP/Marília. Mestrado e Bolsista FAPESP no Doutorado. Pesquisador nos seguintes grupos de pesquisa: "Acervos: Dimensões do documento, da memória e do patrimônio", da Universidade Federal Fluminense/UFF. "Acervos Fotográficos" da Universidade de Brasília/UnB. Trabalho no estudo da Diplomática e da Forense digital em do Documental, realizando a organização de documentos de arquivo em diferentes entidades públicas e privadas.

Sonia Maria Troitiño Rodriguez
Possui graduação em História pela Universidade de São Paulo, formação em Patrimônio Cultural pela Fundación Duques de Sória e Ministério de Cultura de España e em Arquivística pela Fundación Sanchez-Albornoz/ Universidad de Valladolid (Espanha). Atuou como diretora do Centro de Arquivo Permanente do Arquivo Público do Estado de São Paulo, além de trabalhar prestando consultoria nas áreas de pesquisa histórica e organização de acervos para diversas instituições. Doutora em História Social pela Universidade de São Paulo, tendo desenvolvido pesquisa na linha temática Historiografia e Documentação. Docente da Faculdade de Filosofia e Ciências da Unesp (FFC) nos cursos de Arquivologia e Biblioteconomia do Departamento de Ciências da Informação e docente permanente no Programa de Pós-Graduação em Ciência da Informação da UNESP.