Garantir a autenticidade e o acesso continuado à informação digital: os desafios da preservação digital em arquivos

Cristiana Vieira de Freitas

Arquivo Municipal de Ponte de Lima
Largo Dr. António Magalhães
4990-052 Ponte de Lima
Tel: 258900425
E-mail: arquivo@cm-pontedelima.pt

RESUMO

A presente comunicação visa essencialmente abordar as questões relacionada com a preservação digital, dado que, atualmente, esta deve ser considerada como uma das principais preocupações a ter em conta pelos profissionais da informação de modo a fazer face às ameaças geradas pela rápida evolução das tecnologias de informação e, por conseguinte, pela obsolescência tecnológica que pode ocorrer a vários níveis (*hardware*, *software*, suportes de armazenamento, formatos de arquivo). Torna-se, para o efeito, imprescindível a implementação de estratégias e de políticas adequadas que visem garantir a perenidade e o acesso continuado à informação digital.

PALAVRAS-CHAVE: Preservação digital, autenticidade, informação digital, profissionais da informação.

INTRODUÇÃO

É sabido, que desde a Antiguidade que a fidedignidade dos documentos como prova está estreitamente relacionada com os conceitos de memória perpétua e de pública fé que só poderia ser atribuída se os documentos fossem preservados em locais públicos, tais como arquivos, que surgem de forma espontânea ou, mais concretamente, com o intuito de preservar a memória dos atos registados ao longo do tempo. Nesta perspetiva, emergem no século XVII os princípios gerais de uma nova ciência, a Diplomática, com a finalidade de estabelecer regras para comprovar a autenticidade de documentos régios e eclesiásticos e cujo objeto não é qualquer documento escrito, mas apenas o documento de arquivo, ou seja, os documentos produzidos ou recebidos por uma pessoa física ou jurídica no decurso da sua atividade.

No entanto, na atualidade, a ampla utilização das Tecnologias de Informação e Comunicação (TIC) aplicadas à produção, processamento, troca, disseminação e armazenamento de informação levanta problemas críticos de preservação a longo prazo da informação digital, indispensável aos propostos operacionais da organização. Assim sendo, a fragilidade física dos suportes, a obsolescência tecnológica e a vulnerabilidade do meio digital são obstáculos a ultrapassar na preservação digital a longo prazo, de modo a garantir a autenticidade, a integridade e a fiabilidade da informação a preservar, isto é, consiste em "garantir os requisitos inerentes à sua produção e aos objetivos do seu produtor/produtores, dada a multiplicidade de atores envolvidos e as implicações administrativas, legais, políticas e económico-financeiras dela decorrentes" (PINTO, 2005, 55), bem como garantir o acesso continuado à informação.

Face ao contexto digital, e aos desafios impostos pela cada vez mais crescente produção e disseminação de informação que se torna necessário preservar a longo prazo, é imprescindível uma abordagem concreta sobre os requisitos e tecnologia necessárias para garantir a autenticidade e o acesso continuado à informação digital a longo prazo, isto é, enquanto essa for necessária à organização e por um período de tempo superior à longevidade tecnológica necessária à sua leitura, interpretação e/ou reprodução.

Nesta conformidade, e considerando que cabe aos profissionais da informação contribuir para o desenvolvimento e implementação de sistemas de informação que garantam a criação, manutenção e preservação a longo prazo e acesso continuado da informação digital autêntica, íntegra, fidedigna, inteligível e utilizável, levantam-se as seguintes questões:

- Pode a presunção da autenticidade ser transferida para o contexto digital?
- Quais os requisitos que garantirão a autenticidade, integridade, fidedignidade, inteligibilidade e usabilidade da informação?
- Quais as implicações no conceito de documento?
- Qual o posicionamento da Arquivística?
- Como garantir a autenticidade e o acesso continuado da informação digital a longo prazo?

A AUTENTICIDADE EM AMBIENTE DIGITAL

O conceito de autenticidade, cujo âmago encontramos na Diplomática, refere-se à manutenção da fidedignidade da informação após a utilização, transmissão e preservação a longo prazo. Assim sendo, segundo a teoria Diplomática, se um documento/informação apresenta todos os elementos formais quando é gerado ou recebido (isto é, se é autêntico), esse documento é aquilo que pretende ser (isto é, genuíno) e o seu conteúdo é de confiança (isto é, fidedigno).

Estes conceitos, outrora válidos quando os procedimentos, as regras e as rotinas de criação/produção de documentos eram tão rigorosos que impossibilitavam a criação de documentos formalmente corretos noutros locais que não fossem as chancelarias e os notários, entre outros, já não são atualmente válidos, particularmente, quando os sistemas eletrónicos participam nos procedimentos de produção e de manutenção e preservação dos documentos/informação.

Figura 1: Binómio Informação-Documento

Isto significa que a informação digital apresenta maiores problemas do que a informação registada em suporte analógico, no que se refere à autenticação, devido à forma como são produzidos e transmitidos e ao facto de poderem ser mais facilmente alterados, sendo a sua origem difícil de determinar.

Na verdade, a autenticidade da informação digital é ameaçada sempre que há intercâmbio entre utilizadores, sistemas e aplicações, ou sempre que a obsolescência tecnológica obriga a atualizações ou substituição do *hardware* e/ou *software* utilizado para armazenar, processar e comunicar essa mesma informação. Por conseguinte, a presunção da autenticidade dos objetos digitais deve assentar nas evidências fornecidas pela metainformação que por sua vez fornece elementos sobre as estratégias de preservação utilizadas, o histórico da custódia, o formato dos ficheiros, a estrutura do conteúdo, entre outros.

Desta forma, a questão da presunção da autenticidade no contexto digital, tal como refere Pinto (2007), "está agora muito mais fragilizada implicando o envolvimento e um trabalho estreito entre o produtor e o "gestor da informação", dado que a segurança da informação, o garantir da sua autenticidade, integridade, fidedignidade e inteligibilidade devem ser pensadas mesmo antes da mesma ser produzida, isto é, quando os próprios sistemas tecnológico-organizacionais que sustentarão a criação da informação estão a ser planeados e concebidos".

Apesar das inúmeras vantagens introduzidas pela era digital na rotina dos profissionais da informação, tais como, entre outros, o processamento automático, as Bases de Dados, uma maior capacidade de armazenamento e disseminação de conteúdos digitais, por outro lado acarretou novos desafios no que se refere à preservação a longo prazo da informação digital e acesso continuado à mesma (ROTHENBERG, 2010, 1). Para fazerem face aos desafios do novo contexto digital os profissionais da informação têm de ser capazes de entender que, apesar de algumas reformulações e da necessidade de uma nova abordagem arquivística, os princípios arquivísticos tradicionais – valor probatório e informativo, princípio da proveniência, critérios de ordenação e descrição e, ainda, a avaliação – continuam a reger a prática arquivística.

Efetivamente, esses princípios e práticas podem contribuir significativamente para a identificação dos requisitos necessários para a implementação de sistemas de informação digital capazes de criar, manter e preservar objetos digitais autêntico, o que implica, conforme já foi referido, um maior envolvimento entre o produtor e o profissional da informação.

Quer isto dizer, que a autenticidade é garantida através da adoção de métodos que asseguram que a informação não é manipulada, alterada ou, melhor dizendo, falsificada após a sua criação, nem durante a transmissão, manipulação e preservação, dentro dos sistemas de gestão e de preservação de informação. Para o efeito, tal como é referido nas *Diretrizes do Preservador* deverá: i) manter-se a custódia ininterrupta dos documentos arquivísticos; ii) implementar-se e monitorizar-se procedimentos de segurança e controlo; iii) garantir que o conteúdo dos documentos arquivísticos e as anotações e elementos da forma documental não sofram alterações após a reprodução (INTERPARES 2 Project).

Isto significa que a garantia da autenticidade, bem como a preservação digital, tem início na conceção e implementação da plataforma tecnológica que abarca todo o ciclo de vida da informação (com base na norma ISO 15489, que pode ser complementada/integrada com outras normas, designadamente as ISO 30300 e 30301), desde a produção, captura, recolha, processamento, organização, circulação, avaliação, armazenamento, uso e disseminação, bem como no *software* utilizado, nos formatos adotados, na recolha atempada de metainformação administrativa, técnica, descritiva e de preservação, que agirão sobre os diferentes níveis de abstração do objeto digital (físico, lógico, conceptual).

PRESERVAÇÃO DIGITAL

A preservação digital, definida por Ferreira (2006, 20) como a "capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada

no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação", visa ultrapassar a fragilidade física dos suporte, a obsolescência tecnológica e a vulnerabilidade do meio digital de modo a garantir a autenticidade, a integridade, a fidedignidade, bem como o acesso continuado à informação a preservar, sendo esta a única forma de garantir e fomentar a memória coletiva e institucional.

No que se refere à preservação digital e considerando que esta exige recursos substanciais no que se refere a capacidades tecnológicas e conhecimento tecnológico, deverá ter-se em conta que é fundamental a definição de modelos de financiamento sustentáveis, sendo desejável que essas despesas sejam incluídas no orçamento das organizações. Por outro lado, é importante salientar que a preservação digital deverá integrar, para além do orçamento, os objetivos das organizações, através da adoção de políticas, normas e procedimentos adequados que abranjam todos os aspetos da preservação digital.

Grácio (2011, 82) representa os aspetos da preservação digital divididos em três grupos e a respetiva relação/interdependência existente entre eles: (i) *organizacional* (objetivos da instituição; política de preservação digital; responsabilidades; equipa multidisciplinar; recursos financeiros e autenticidade), (ii) *técnico* (seleção e avaliação; modelos, padrões e iniciativas; infraestrutura tecnológica; estratégias de preservação; suporte e metadados); (iii) *legal* (leis; direitos de autor; atos administrativos).

Figura 2: Aspetos da preservação digital (GRÁCIO, 2011, 83)

Considerando os aspetos mencionados, torna-se imprescindível que cada organização proceda ao desenvolvimento do seu próprio sistema de preservação e à definição e implementação de políticas de preservação adequadas que englobem todo o ciclo de vida da informação (conceção, produção, armazenamento, manutenção, avaliação/seleção e acesso aos recursos digitais) e que se materializem em planos e medidas de modo a assegurar a autenticidade, a integridade, a fidedignidade, a inteligibilidade e a usabilidade da informação durante tanto tempo quanto a organização dela necessitar.

Deverá criar-se, para o efeito, uma equipa multidisciplinar para a elaboração e implementação de um plano de preservação digital, onde constem os aspetos organizacionais, técnicos e legais relacionados com a preservação digital, e onde estejam devidamente definidas as estratégias de preservação mais adequadas e os esquemas de metainfomação apropriados (EAD, PREMIS, METS, NISO Z39.87, Dublin Core, etc.), bem como os formatos de preservação (TIFF, PNG, PDF/A, etc.), as aplicações informáticas e soluções de armazenamento, ou seja, toda a infraestrutura tecnológica adequada, e ainda os recursos humanos e financeiros associados.

Deverá igualmente considerar-se no plano de preservação digital eventuais ameaças tal como:

- Falhas do *Hardware* e/ou *Software*;
- Erros nos canais de comunicação;
- Falhas na rede;
- Obsolescência tecnológica (ao nível físico e lógico);
- Erros do operador;
- Desastres naturais;
- Ataques externos e internos;
- Falhas organizacionais e económicas.

O paradoxo da preservação digital

A definição e a avaliação da autenticidade são tarefas complexas que implicam determinadas atividades teóricas e operacionais/técnicas, que passam pelo desenvolvimento de recomendações e políticas para a construção de repositórios confiáveis e a identificação precisa de cada componente da função da custódia.
Nesta conformidade, torna-se necessário definir como e em que base a autenticidade tem de ser gerida na preservação digital de modo a garantir a confiabilidade da informação digital, tendo em consideração que não é possível preservar os objetos digitais na sua forma e estrutura original e que, por conseguinte, terão de ser modificados com alguma periodicidade.
Quer isto dizer, que os objetos digitais podem sofrer adaptações em função dos avanços tecnológicos ao longo do tempo – "ao nível do hardware, redes, arquiteturas de software, sistemas de gestão, esquemas e necessidades [de] metadados, e até alterações à tutela responsável pela conservação dos registos" (FERREIRA et al., 2012).
Trata-se, por conseguinte, de um paradoxo, dado que enquanto a autenticidade carece de fixidez (armazenamento seguro que mantenha o objeto digital completo e inalterado no que se refere ao conteúdo informativo, estrutura lógica e contexto da informação)

a preservação implica alteração/mudança. Isto é, por um lado pretende-se manter a informação digital intacta tal como foi produzida e por outro lado, pretende-se aceder a essa informação de forma dinâmica e com recurso às ferramentas tecnológicas mais avançadas, dado que, devido à obsolescência tecnológica, torna-se imprescindível adotar estratégias de preservação mais adequadas para transferir periodicamente a informação digital de uma determinada geração tecnológica para outra diferente daquela utilizada no momento da criação da informação original.

Se por um lado, a preservação digital requer procedimentos específicos e técnicas apropriadas para cada tipo de formato e suporte (ARELLANO, 2004, 25), por outro lado, raramente é discutido o facto de a maioria das estratégias propostas, incluindo a migração, basearem-se em sucessivas conversões dos objetos digitais para novos formatos ao longo do tempo e que, inclusivamente, algumas dessas abordagens não tentarem sequer preservar o objeto digital no seu formato original, o que faz com que haja, inevitavelmente, corrupção e degradação dos mesmos à medida que vão sendo convertidos para novos formatos (Rothenberg, 2010, ix-x).

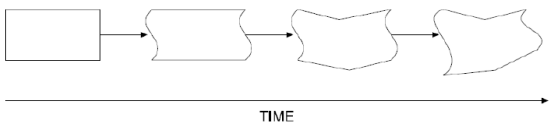

Figura 3: Degradação do objeto digital ao longo de sucessivas migrações (FERREIRA, 2006, 40)

Por sua vez a integridade do objeto digital é igualmente colocada em risco sempre que o recurso a uma estratégia de preservação leva à alteração do *bitstream* original. Contudo, manter o *bitstream* original também não é suficiente para garantir que a integridade está preservada, sendo igualmente crucial a correta interpretação desse *bitstream* devendo, para o efeito, recorrer a um *software* e *hardware* apropriados, caso contrário a integridade do original é corrompida (ROTHENBERG, 2010, 13).

Plano de preservação digital

A elaboração do plano de preservação digital, documento estratégico que contém políticas e procedimentos orientados para a constituição de uma estrutura técnica e organizacional que visa a preservação a longo prazo de informação digital, bem como a seleção das estratégias de preservação mais apropriadas, deve resultar de um esforço de colaboração entre o serviço de arquivo e o serviço de informática, envolvendo uma participação ativa de todas as unidades orgânicas implicadas na produção de informação digital.
Mais concretamente, este documento tem como principais objetivos: i) garantir que os documentos de arquivo eletrónico sejam conservados de forma legível e acessível, mantendo simultaneamente as suas propriedades de autenticidade e integridade durante tanto tempo quanto a organização deles necessitar; ii) permitir identificar quais as funcionalidades que devem ser implementadas e a forma de as implementar, para manter a integridade e usabilidade dos documentos de arquivo eletrónicos ao longo do tempo (BARBEDO et al., 2010, 8).
São considerados como pré requisitos fundamentais para a elaboração do plano de preservação digital: o plano de classificação, a tabela de seleção, a caracterização dos sistemas de informação e identificação dos requisitos da informação digital (análise e caracterização do sistema informacional e suas funcionalidades e a análise dos processos de negócio, tradicionalmente designados por séries documentais).
No planeamento da estratégia de preservação mais adequada à organização em causa, devem ser consideradas as seguintes questões de modo a garantir a autenticidade e o acesso continuado à informação digital:

- Definição de estratégias de preservação (migração, encapsulamento, emulação, preservação da tecnologia, arqueologia digital, transferência para suportes analógicos, pedra roseta digital, refrescamento);
- Definição de formatos de preservação (escolha de formatos abertos e independentes em detrimento de formatos proprietários, cobertos por patente ou *copyright*);
- Escolha de aplicações informáticas ou *software* (para a produção, manipulação, gestão e preservação de informação digital);
- Escolha de soluções de armazenamento (considerando os seguintes critérios: custo, escalabilidade, interoperabilidade, segurança de dados e facilidade de programação);
- Escolha de esquemas de metainformação (descritiva, técnica, estrutural e de preservação).

No que se refere especificamente à infraestrutura tecnológica (*hardware* e *software*), aspeto fundamental da preservação digital e acesso continuado, deverão considerar-se os seguintes questões apontadas por Grácio (2011, 145):

- Definição de *hardware* e *software*;
- Sistema de armazenamento com alta capacidade e dispositivos de acesso adequados;
- Estrutura de cópias de segurança (*backups*) fiável;
- Sistema de redundância de banco de dados e *hardware*;
- Sistema de deteção e recuperação automática de falhas;
- Escolha dos suportes de armazenamento para preservação, *backups* e acesso;
- Definição dos tipos, ou seja *off-line* e/ou *online*;

- Estrutura de rede de computadores adequada para acesso dos utilizadores ao sistema de informação;
- Sistemas de armazenamento com mecanismos de segurança, com senhas seguras para acesso à Base de Dados;
- Definição de formatos de armazenamento lógico e fisco.

Em suma, pretende-se, com a definição de politicas e estratégias apropriadas de preservação digital, minimizar os riscos de perda irremediável da informação que pode ocorrer de diversas formas – adulteração da informação digital; definição de formatos não adequados na migração e refrescamento; alteração ou perda da estrutura da informação digital original; perda de informação e/ou metainformação sobre as ações realizadas sobre o objeto digital durante a processo de preservação e da metainformação de contexto e, ainda, obsolescência do *hardware* e *software* necessários para o acesso, leitura e interpretação dos *bits* armazenados.

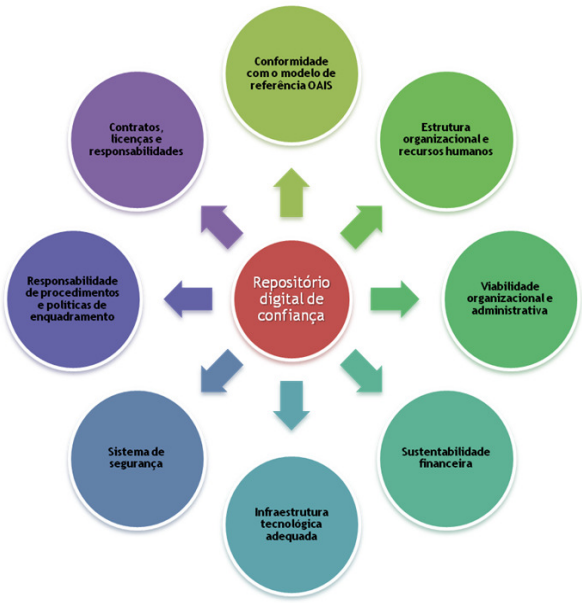

Figura 4 Atributos e responsabilidades dos repositórios digitais de confiança

Repositório digital de confiança

Tendo em conta a preservação da autenticidade e integridade da informação tal qual como quando foi gerada, é fundamental a adoção de um sistema de arquivo digital, isto é, um repositório capaz de albergar os objetos, de facilitar a implementação dessas políticas e respetivas estratégias de preservação e, ainda, de facilitar a gestão dos objetos, bem como a sua localização (FERREIRA, 2009, 47).

Nesta conformidade, preservar num repositório digital, significa que se cumprem os determinados objetivos: i) os dados são mantidos no repositório sem serem danificados, perdidos ou adulterados; ii) os dados podem ser encontrados, recuperados e disponibilizados ao utilizador; iii) os dados podem ser interpretados e entendidos pelo utilizador (não basta preservar a *bitstream* que representa a informação preservada, o desafio reside em assegurar que os utilizadores podem aceder ao conteúdo tal como este foi depositado no repositório; iv) todas as condições referidas podem ser mantidas ao longo do tempo (FERREIRA, 2011, 72).

Para satisfazerem os objetivos que se propõem, os repositórios digitais de confiança deverão cumprir determinados atributos e responsabilidades que constam do documento TRAC (*Trustworthy Repositories Audit & Certification: Criteria & Checklist*), recentemente adaptado a ISO 16363:2012, "que reúne um conjunto de requisitos que vão desde a gestão organizacional, às infraestruturas de suporte, e que são considerados vitais no estabelecimento de um clima de confiança em torno do repositório digital" (FERREIRA et al., 2012).

Para além da identificação de potenciais riscos e ameaças, constam entre os atributos a necessidade do repositório digital (Eprints, DSpace, Fedora, entre outros) estar em conformidade com o modelo de referência OAIS.

O modelo de referência OAIS (*Open Archival Information System*), publicado em 2002 pela *Consultive Committee for Space Data System* (CCSDS) e aprovada como norma internacional ISO 14721:2003, teve a pretensão de criar um consenso sobre quais os requisitos necessários para o desenvolvimento de arquivos capazes de garantir a preservação a longo prazo e o acesso continuado à informação digital, bem como pretendeu definir conceitos chave, normalizar a terminologia e, ainda, definir as entidades internas (a ingestão, o repositório de dados, a gestão de dados, a administração, o planeamento da preservação e o acesso) e externas (produtor, administrador e consumidor) que o compõem, bem como os objetos de informação trocados no seu interior.

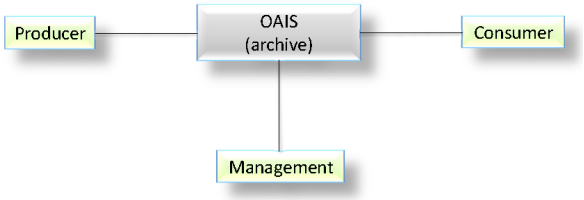

Figura 5: Modelo OAIS (CCSDS, 2009, 2-2)

Mais concretamente, o modelo de referência OAIS teve como objetivos: i) identificar e analisar os desafios da preservação digital; ii) localizar os pontos do procedimento de preservação para os quais era

necessário desenvolver novos padrões; iii) enumerar um conjunto de requisitos mínimos que devem se cumpridos pelos repositórios digitais; iv) servir de referência aos fornecedores interessados em desenvolver produtos e serviços de preservação digital (SERRA SERRA, 2008, 124).

Tal como o TRAC, outros documentos há que visam a autoavaliação de repositório digitais, como é o caso do DRAMBORA (*Digital Repository Audit Method Based on Risk Assessment*), cuja abordagem é essencialmente centrada "na identificação e gestão de risco com o objetivo de racionalizar as incertezas e prevenir ameaças" (FERREIRA, 2012).

Para que os dados contidos num repositório digital fidedigno e confiável estejam na base de uma futura avaliação da autenticidade, será necessário que os profissionais da informação continuem a associar metainformação aos objetos digitais, que servirão para que os utilizadores entendam e acedam à informação digital no futuro. Isto significa que, tendo em conta os critérios de avaliação da autenticidade, deverá ser conservada como parte integrante do objeto digital a metainformação relativa aos diversos contextos associados à sua produção – isto é, os contextos jurídico-administrativo, proveniência, procedimento, documental, tecnológico – bem como sobre alterações sofridas desde a sua produção. Conforme refere Borbinha et al. (2002, 80) "a todos os níveis – conteúdo, estrutura, contexto – têm de ser definidos os elementos que, não estando presentes em determinado momento, tornam o documento em qualquer coisa diferente do que ele pretende ser, inviabilizando a sua utilização para os fins que justificaram a sua conservação".

Contudo, Ferreira et al. (2012) constatam que ainda é reduzido o número de repositórios com políticas e estratégias consolidadas no domínio da preservação digital e que "ainda subsistem dúvidas, incertezas e lacunas quanto aos papéis e responsabilidades, isto é, quem deverá ser responsável pela preservação e curadoria, a qualidade e interoperabilidade dos repositórios, ou a inexistência de enquadramento jurídico apropriado em termos de preservação digital". Apesar destas conclusões se referirem especificamente a repositórios de acesso aberto podem certamente, à exceção do RODA (Repositório de Objetos Digitais Autênticos), alongar-se aos restantes repositórios institucionais.

AUTENTICIDADE COMO PROVA E EVIDÊNCIA LEGAL

Conforme é referido no *Manifesto para a Preservação Digital,* numa perspetiva arquivística, a autenticidade está intrinsecamente ligada à capacidade probatória dos documentos, não apenas num sentido estritamente jurídico, mas num sentido mais amplo de testemunho autêntico dos atos, ações e atividades que representam. Essa é a principal característica diferenciadora de um arquivo relativamente a outros repositórios de documentação, o que não lhe retira dimensão informativa, antes lhe acrescenta um papel de responsabilização dos intervenientes nas atividades documentadas (BORBINHA [et al.], 2002, 80).

Recentemente, no domínio da segurança informática e da segurança de dados, devido em certa medida ao o rápido crescimento da rede de utilizadores da *Internet*, o conceito de autenticidade – entendida como um critério para admissibilidade legal como prova – é usado para indicar que os processos irão assegurar que a transação eletrónica é genuína e que a mensagem não foi alterada ou corrompida na transmissão.

Neste sentido, foram desenvolvidas diversas técnicas e dispositivos de segurança tais como a criptografia, a assinatura digital, a marca de água, as chaves públicas, entre outras.

Não obstante a legislação regular a validade, eficácia e valor probatório dos documentos eletrónicos e da assinatura digital, outras questões se levantam, nomeadamente no que se refere à utilização da assinatura digital como prova de autenticidade e integridade da informação digital e, especificamente, à sua preservação a longo prazo.

Neste sentido, Maurício (2009) levanta as seguintes questões: a tecnologia atual consegue garantir a preservação da autenticidade e assinatura dos documentos ao longo do tempo? Como é que os sistemas garantem ou garantirão a médio e longo prazo que determinado documento foi assinado por determinada pessoa?

De fato, se por um lado a assinatura digital confere autenticidade e integridade à informação digital, por outro lado os avanços tecnológicos (incluindo avanços criptográficos, revogação e expiração/caducidade da assinatura digital) não garantem a sua preservação a longo prazo, o que levanta inúmeros problemas/desafios. Pois, tal como alude Jiménez (2008, 38) "*Los documentos firmados o compulsados digitalmente, o que han recibido un sello de tiempo, hoy por hoy pueden parecer estables porque se trata de una tecnología actual y aprobada, pero no sabemos qué puede pasar en un futuro. La estabilidad a largo plazo no está probada, por lo tanto su autenticidad e integridad tampoco están garantizadas*".

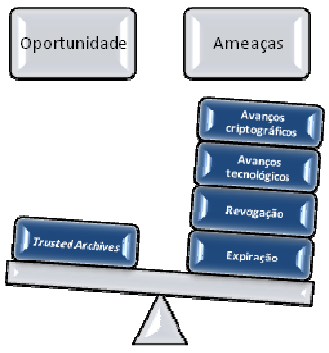

Figura 6: Ameaças e oportunidades associadas à assinatura digital

O diagrama, abaixo representado, apresenta o ciclo de vida da assinatura digital em quatro etapas distintas, isto é: i) assinatura criada pelo signatário e enviada ao destinatário; ii) verificação inicial efetuada pelo destinatário; iii) efetuada a validação, a informação assinada digitalmente é arquivada com vista à preservação da evidência; iv) em caso de litígio a informação assinada digitalmente é apresentada ao juiz, procedendo-se novamente à sua verificação, de modo a apurar a identidade do signatário e a integridade da informação (BLANCHETTE, 2004, 22).

Pretende-se, deste modo, que a evidência concedida pela assinatura digital seja preservada ao longo do tempo juntamente com a informação, para acesso no futuro, devendo, para o efeito, preservar-se a informação e respetiva assinatura de forma inteligível e acessível, bem como assegurar a sua verificação de modo a avaliar a validade da assinatura.

Contudo, entre as verificações da assinatura efetuadas durante a etapa 2 e a etapa 4, há necessariamente um hiato de tempo, que pode ser de vários anos, durante o qual ocorre inevitavelmente a obsolescência tecnológica.

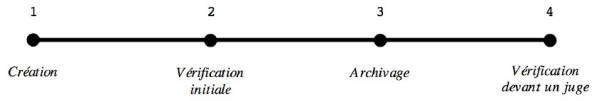

Figura 7: Ciclo de vida da assinatura digital (BLANCHETTE, 2004, 22)

Posto isto, tendo em conta a preservação a longo prazo da informação digital com assinatura digital – que podem ser embebidas (*enveloped*) ou independentes (*detached*) – a solução poderá passar por separar a assinatura da informação digital. Desta forma, toda a informação contida na assinatura digital (nome de quem assinou, data, hora, entidade certificadora, etc.) seria convertida em metadados que, por sua vez, seriam preservados juntamente com a respetiva informação digital.

Digital Records Forensics

Com o intuito de aplicar métodos cientificamente comprovados para verificar a autenticidade, a integridade e a fiabilidade da informação digital, de modo a fornecer prova/evidência, surge o *Digital Records Forensics Project*, que envolveu investigadores da Universidade de British Columbia, em colaboração com o Departamento de Polícia de Vancouver, e cujo âmago consiste no desenvolvimento de conteúdos teóricos e metodológicos de uma nova disciplina e ciência designada por *Digital Records Forensics*, que resulta de uma interdisciplinaridade, representada na figura 8.

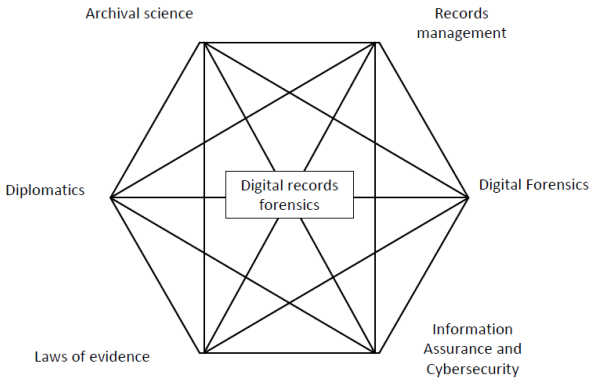

Figura 8: Digital Records Forensics Project (DURANTI, 2010)

Mais concretamente, consiste em: "*the application of computer science and investigative procedures for a legal propose involving the analysis of digital evidence after proper search authority, chain custody, validation with mathematics, use and validated tools, repeatability, reporting, and possible expert presentation*" (DURANTI, 2009, 42).

A autenticação dos objetos digitais é o ponto chave para a aplicação da forense digital nos arquivos, designadamente no que se refere à verificação/interpretação dos selos digitais de tempo (garantem a comprovação da existência da informação na data e hora indicadas), à capacidade de recuperar cópias autênticas dos objetos digitais, à capacidade de extrair metainformação significativa a partir do sistema de informação original e, ainda, permitir a verificação do histórico e de outros detalhes da composição da informação, bem como, identificar falsificações, fato aparentemente inevitável no mudo digital (KIRSCHENBAUM et al., 2010, 12). Em suma, essas ações têm o intuito de permitir a reconstituição de procedimentos de natureza criminosa que possam ocorrer nos equipamentos digitais, tais como, uso ilício ou não autorizado da informação digital.

CONCLUSÃO

A preservação digital deve ser encarada numa perspetiva ampla de gestão de informação digital, que inclua todo um conjunto de políticas, planos de contingência, estratégias e metodologias apropriadas, e não como uma questão meramente tecnológica.

Conforme refere Arellano (2004, 16) "o desafio é muito mais um problema social e institucional do que um problema técnico, porque, principalmente para a preservação digital, depende-se de instituições que passam por mudanças de direção, missão, administração e fontes de financiamento".

No contexto digital não é suficiente armazenar os objetos digitais num suporte adequado. O maior desafio que se coloca aos profissionais da informação consiste em pensar nos requisitos que permitam a pesquisa, a recuperação e a utilização da informação para uso futuro, preservando o conteúdo, a integridade e a

autenticidade.

Além disso, sabemos, que a preservação da memória institucional e coletiva constitui, igualmente, um dos maiores desafios que se colocam atualmente aos profissionais da informação, sendo que esta questão deixou de ser colocada à posterior – quando a informação passa para entidade custodial, que assegura a sua preservação e utilização a longo tempo – para ser colocada à priori, isto é, quando os sistemas de informação estão a ser planeados e implementados.

Todavia, considerando o grande volume de informação digital produzida e/ou recebida, e mesmo correndo-se o risco de perda de informação para as gerações vindouras, tornar-se impensável conservar tudo. Nesta conformidade, torna-se primordial, no que respeita à preservação digital, preservar apenas a informação de valor continuado, cujos critérios de seleção terão de ser feitos de acordo com os objetivos da instituição e das necessidades das comunidades de utilizadores. Quanto maior for o volume de informação maior será o custo associado à escalabilidade da tecnologia de armazenamento e à aplicação de estratégias para ultrapassar a obsolescência tecnológica.

De modo a garantir a preservação a longo prazo da informação digital autêntica e o acesso continuado à mesma devem ser cumpridos determinados requisitos, tais como: i) mecanismos de preservação que assegurem que a informação não será danificada nem perdida inadvertidamente ao longo do tempo; ii) medidas de segurança que assegurem que a informação não é intencionalmente modificada por razões financeiras, ideológicas ou políticas; iii) mecanismos de verificação que comprovem a correta e consistente aplicação dos procedimentos de preservação e de segurança (ROTHENBERG, 2010, 64). Para tal, será inevitável que haja, por parte das organizações, um investimento substancial em infraestruturas, equipamentos e conhecimentos.

Para além da definição de políticas e da escolha de estratégias de preservação mais adequadas, é imprescindível a adoção de um repositório. Para que um repositório digital seja efetivamente confiável terá de evidenciar, de forma contínua, o seu correto funcionamento através de auditorias que abranjam os diferentes contextos – a infraestrutura organizacional, a gestão de objetos digitais e a infraestrutura tecnológica, técnica e a segurança – de modo a serem criadas condições para a sua certificação.

Terminamos com uma frase de Gary King (Apud Goth, 2012, 12), que bem evidencia os desafios que atualmente enfrentados pelos profissionais da informação: "*Preservation is the promise of keeping things in perpetuity. That's a long time. Figuring out that is really hard*".

REFERÊNCIAS BIBLIOGRÁFICAS

ARELLANO, Miguel Angel (2004) – Preservação de documentos digitais. **Ciência da Informação** [em linha]. Vol. 33, nº 2 (2004), p. 15-27. [Consult. 15 set. 2012]. Disponível em WWW: <http://www.scielo.br/pdf/ci/v33n2/a02v33n2.pdf>.

BARBEDO, Francisco; CORUJO, Luís; SANT'ANA, Mário (2010) – **Recomendações para a produção de planos de preservação digital** [em linha]. Lisboa : DGARQ. [Consult. 15 Set. 2012]. Disponível em WWW: <http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf>.

BLANCHETTE, Jean-François (2004) – **La conservation de la signature électronique: perspectives archivistiques** [em linha]. Paris: Direction des Archives de France. [Consult. 12 set. 2010]. Disponível em WWW: <http://polaris.gseis.ucla.edu/blanchette/papers/daf.pdf>

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (2012) – **Reference model for an Open Archival Information System (OAIS)** [em linha]. Washington : CCSDS. [Consult. 13 set. 2012]. Disponível em WWW: <http://public.ccsds.org/publications/archive/650x0m2.pdf>.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (2011) – **Audit and certification of trustworthy digital repositories** [em linha]. Washington : CCSDS. [Consult. 13 set. 2012]. Disponível em WWW: <http://public.ccsds.org/publications/archive/652x0m1.pdf>.

DURANTI, Luciana (2010) – **Digital records as evidence: toward a digital records forensics** [em linha]. Singapore : [s.n], 2010. [Consult. 13 set. 2012]. Disponível em WWW: <http://www.interpares.org/display_file.cfm?doc=ip3_canada_dissemination_cs_duranti_singapore_2010b.pdf>

DURANTI, Luciana (2009) – From digital diplomatics to digital records forensics. **Archivaria** [em linha]. Vol. 68 (Spring 2009), p. 39-66. [Consult 12 set. 2011]. Disponível em WWW: <http://journals.sfu.ca/archivar/index.php/archivaria/article/view/13229/14548>. ISSN 0318-6954.

FERREIRA, Carla Alexandra Silva (2011) – **Preservação da Informação Digital: uma perspectiva orientada para as bibliotecas** [em linha]. Coimbra : [s.n]. [Consult. 21 set. 2012]. Dissertação de mestrado. Disponível em WWW: <http://hdl.handle.net/10316/15001>

FERREIRA, Miguel; SARAIVA, Ricardo; RODRIGUES, Eloy (2012) – **Estado da arte em preservação digital** [em linha]. [S.l. : s.n.]. [Consult. 13 set. 2012]. Disponível em WWW: <http://projecto.rcaap.pt/index.php/lang-pt/consultar-recursos-de-apoio/remository?func=startdown&id=351>.

FERREIRA, Miguel (2006) – **Introdução à Preservação Digital: Conceitos, estratégias e actuais consensos** [Em linha]. Guimarães : Escola de

Engenharia da Universidade do Minho. [Consult. 13 set. 2012]. Disponível em WWW: <http://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. ISBN 9728692307.

GOTH, Gregory (2012) – Preserving digital data. **ACM** [em linha]. Vol 55, nº 4 (Abril 2012), p. 11-13. Disponível em WWW: <http://www.renci.org/wp-content/uploads/2012/04/2011-April-Preserving-Digital-Data-goth-copy.pdf>.

GRÁCIO, José Carlos Abbud (2011) – **Preservação digital na gestão da informação: um modelo processual para as instituições de ensino superior** [em linha]. Marília : Faculdade de Filosofia e Ciências. [Consult. 13 set. 2012]. Disponível em WWW: <http://www.athena.biblioteca.unesp.br/exlibris/bd/bma/33004110043P4/2011/gracio_jca_dr_mar.pdf>. Tese de doutoramento.

INTERPARES ([s.d.]) – Diretrizes do preservador: a preservação de documentos arquivísticos digitais: diretrizes para organização [em linha]. [Consult. 15 set. 2012]. Disponível em WWW: <http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>.

KIRSCHENBAUM, Matthew G.; OVERDEN, Richard; REDWINE, Gabriela (2010) – **Digital forensics and born-digital content in cultural heritage collections** [em linha]. Washington, D.C.: Council on Library and Information Resources. [Consult. 16 set. 2012]. Disponível em WWW: <http://www.clir.org/pubs/reports/pub149/pub149.pdf>. ISBN 978-1932326-37-6.

SOLER JIMÉNEZ, Joan (2008) – **La preservación de los documentos electrónicos** [em linha]. Barcelona : Editorial UOC. [Consult. 15 set. 2012]. Disponível em WWW: <http://pt.scribd.com/doc/73864504/La-Preservacion-Documentos-Electronicos >. ISBN 9788497883085.

MAURÍCIO, Rui (2009) – A garantia de segurança digital na prova da relação jurídica. **Tendências judiciais de admissibilidade legal de documentos eletrónicos como prova documental** [documento eletrónico]. [Lisboa] : DGARQ.

PINTO, Maria Manuela Gomes de Azevedo (2007) – Da acção à informação: o desafio digital. In CONGRESSO NACIONAL DE BIBLIOTECÁRIOS ARQUIVISTAS E DOCUMENTALISTAS, 9, Ponta Delgada, 2007 – **Bibliotecas e Arquivos: Informação para a cidadania, o desenvolvimento e a inovação: actas** [em linha]. Lisboa : BAD. [Consult. 13 set. 2012]. Disponível em WWW: <http://badinfo.apbad.pt/Congresso9/COM63.pdf

PINTO, Maria Manuela Gomes de Azevedo (2005) – Do "efémero" ao "sistema de informação": a preservação na era digital. **Páginas a&b: arquivos e bibliotecas** [em linha]. Vol. 15, p. 63-178. [Consult. 13 set. 2012]. Disponível em WWW: <http://ler.letras.up.pt/uploads/ficheiros/3083.pdf>. ISSN 0873-5670.

ROTHENBERG, Jeff (2000) – Preserving authentic digital information. In COUNCIL ON LIBRARY AND INFORMATION RESOURCES - **Authenticity in a digital environment** [em linha]. Washington, D.C. : Council on Library and Information Resources. [Consult. 13 set. 2012]. Disponível em WWW: <http://www.clir.org/pubs/reports/pub92/pub92.PDF>. ISBN 1-887334-77-7. p. 51-68.

ROTHENBERG, Jeff; et al. (2010) – Addressing the uncertain future of preserving the past: towards a robust strategy for digital archiving and preservation [em linha]. [S.l.] : RAND.[Consult. 16 set. 2012]. Disponível em WWW: <http://www.rand.org/pubs/technical_reports/2007/RAND_TR510.pdf>.

SERRA SERRA, Jordi (2008) – **Los documentos electrónicos: qué son y como se tratan**. Asturias : Ediciones Trea. ISBN 978-84-9704-395-3.