PERDA DE INFORMAÇÕES E DE BENS EM ARQUIVOS E INSTITUIÇÕES RESPONSÁVEIS POR GUARDA DO PATRIMÔNIO: SEGURANÇA DA INFORMAÇÃO E O VIÉS DIGITAL

Vanderlei Batista dos Santos I Arquivista, mestre e doutor em Ciência da Informação pela Universidade de Brasília. Servidor da Câmara dos Deputados, onde é o atual Diretor da Coordenação de Arquivos. É docente em cursos de pós-graduação em Ciência da Informação, consultor em projetos de gestão de documentos e informação. Componente da Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (2002-2020).

> *As tecnologias que uma sociedade usa para registrar, armazenar e compartilhar informações, terão um papel crucial na determinação da riqueza, ou escassez, de seu legado (Nicholas Carr, 2016).*

É cada vez mais usual ouvir ou ler frases afirmando que a informação é um recurso estratégico. O crescimento exponencial da internet e o surgimento e ampliação do acesso a novas tecnologias permitem a produção cada vez mais rápida, e talvez com menor rigor, de conteúdos na forma de textos, imagens, multimídias etc. Já se fala, neste contexto do *Big Data*, na gestão de dados como recurso estratégico.

Essa valorização da informação é um fato evidente, mas, na contramão do que esse entendimento parece indicar, não se tem notícia de alteração nos investimentos feitos para a melhoria das estruturas organizacionais que permitam uma jornada segura em direção a uma conclamada transformação digital, ou em treinamentos e adoção de políticas de gestão e preservação de documentos arquivísticos nas instituições públicas e, quiçá, nas privadas.

As instituições de memória e o tratamento e disponibilização de seus acervos não são foco de investimentos frequentes por parte dos Governos, senão, e aqui corro o risco de estar exagerando, quando pressionadas pela opinião pública manifestada por meio de ações junto ao Ministério Público. Apenas para citar casos recentes, sugere-se a leitura das denúncias feitas quanto à situação do Arquivo Público do Distrito Federal, na capital do país (FURQUIM, 2018), do Arquivo Público da Bahia (LIMA; NASCIMENTO, 2018), do Arquivo Público de Ribeirão Preto (PESQUISADORES..., 2018) e os vários exemplos de prefeituras e câmaras do estado de São Paulo.[1]

Ainda assim, parece mais adequado falar **quando**, e não **se** perderemos parte da nossa história registrada em documentos arquivísticos armazenados em instituições em condições de preservá-los adequadamente.

Mas, retomando o foco, e quanto à segurança das informações arquivísticas? Se defende o entendimento de que informação arquivística é

> aquela acumulada (produzida e recebida) pela instituição no exercício de suas funções e atividades, ou por pessoa física no decurso de sua existência, atendendo ou não aos requisitos de fixidez de forma e conteúdo (documento), servindo para registrar, contextualizar e permitir compreensão de ações envolvendo a instituição [ou pessoa] (SANTOS, 2015, p.114).

Ou seja, embora contemple as informações contidas nos documentos arquivísticos, a definição de informação arquivística não se restringe a eles, abrange também os dados e informações presentes em sistemas de informação, vinculados ou não a documentos geridos por esses sistemas.

[1] O *Centro de Assistência aos Municípios* (CAM), do Arquivo Público do Estado de São Paulo (Apesp), orienta prefeituras e câmara legislativas do estado no que diz respeito a arquivos, gestão documental e Lei de Acesso à Informação (LAI – Lei Federal nº 12.527/2011), além de manter convênios com o Ministério Público e com o Tribunal de Contas do Estado de São Paulo. Segundo o ***Mapa de gestão documental paulista*** (http://www.arquivoestado.sp.gov.br/site/gestao/municipios/mapa_paulista), o CAM já atendeu 88,53% dos municípios do Estado. Os relatórios do Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo/Apesp, demonstram fartos exemplos em que o MP paulista acionou o CAM como instância consultiva para questões relacionadas aos arquivos municipais. Conferir em: http://www.arquivoestado.sp.gov.br/site/gestao/relatorios .

A informação arquivística precisa de proteção, desde sua concepção até sua destinação final, qual seja a eliminação ou sua guarda permanente. De uma forma geral, na profundidade que esse espaço permite, observa-se que a segurança da informação se baseia em três pilares: disponibilidade, integridade e confidencialidade. As informações precisam estar disponíveis para acesso, devem ser íntegras e livres de alterações não autorizadas, e que seja garantido o acesso exclusivamente a quem deve ter, protegendo-se aquelas que não podem ser divulgadas. Envolve, ainda, a identificação e o tratamento de riscos, bem como auditoria de todos os procedimentos adotados.

Em complemento, considera-se ainda atual o estudo realizado pelo Ministério da Justiça canadense, no contexto de uma enquete sobre segurança das informações eletrônicas realizada em 1998, concluindo que as ameaças podem ser agrupadas em quatro grupos (SANTOS, 2011, p.154-155):

> a) de natureza tecnológica, relativa à facilidade de alteração sem registro, à fragilidade dos suportes e à obsolescência tecnológica;
>
> b) falha da instituição na adoção de medidas de segurança adequadas, geralmente ocasionada pela falta de diagnósticos e abordagem correta para confrontar os riscos à informação;
>
> c) ação de usuário autorizados que possuem acesso privilegiado às informações e podem comprometer sua integridade de forma intencional ou não; e
>
> d) ação de usuários não autorizados após invasão com o uso de vírus.

Além da questão financeira, a frequência de ocorrência dos sinistros e as perdas ocasionadas por eles nos arquivos são resultado direto da inexistência de políticas e práticas de segurança da informação, incluindo a gestão de riscos. O conhecimento do risco tem ligação direta com a identificação dos recursos a serem protegidos, o potencial de ocorrência e a mobilização de recursos para enfrentá-lo. É impossível gerenciar a ocorrência e o impacto de riscos desconhecidos.

A literatura é plena de orientações sobre as três possíveis ações que visam a evitar, mitigar as possibilidades de ocorrência de sinistros ou aceitá-los como algo inevitável, investindo na redução de seu impacto. Há orientação para elaboração de planos de prevenção contra desastres, planos de continuidade do negócio e de contingência. Nesse conjunto de ações estão incluídos os planos de evacuação que incluam a identificação dos acervos mais críticos.

É preciso uma mudança cultural na instituição no que se refere à segurança da informação e isso começa pela realização de um diagnóstico sobre como são produzidas, organizadas, acessadas e preservadas as informações custodiadas, identificando as forças e fragilidades e propondo formas de superar as últimas.

Parece correto considerar que um documento arquivístico digital submetido a uma estrutura de plano de classificação e tabela de temporalidade, adequadamente indexado, inserido num sistema informatizado de gestão arquivística, com perfis de acesso bem definidos e que controle suas alterações e tramitação, que o submeta às regras de acesso legais, que mantenha essas funcionalidades com características auditáveis e que, ainda, possua interface com um repositório arquivístico de preservação digital, atende a esses três pilares. Mas quantas instituições utilizam sistemas com esses requisitos?

Quanto à disponibilidade

Se considerarmos que os arquivos têm como função primordial a concessão de acesso à informação custodiada, garantir sua disponibilidade torna-se uma ação crítica. É na busca deste aspecto de segurança da informação que se concentra uma grande parte das ações que precisam ser implementadas pelas instituições, uma vez que abrange procedimentos de produção, de manutenção e de preservação ao longo do tempo.

Os quatro tipos de ameaças afetam a disponibilidade. Pode-se citar, por exemplo, como problemas para a manutenção do acesso à informação a não adoção de formatos padronizados e implementação de políticas de migração, inexistência de repositórios digitais confiáveis, a falta de políticas de backup e planos de contingência para os casos de queda do sistema ou, ainda, a adoção de firewalls e senhas fracos.

Um exemplo do quanto usuários autorizados podem ser danosos aos arquivos está em um caso ocorrido em 2017, no interior do Tocantins, quando uma prefeita, ao terminar seu mandato e antes da assunção de seu sucessor, apagou todos os arquivos da Secretaria de Finanças (EX-PREFEITA..., 2017). Isso só foi possível porque ela deveria ser um usuário administrador, com autorização para realizar o apagamento dos dados.

Outro bom exemplo de ameaça à disponibilidade vem do governo argentino. Segundo reportagem, os documentos públicos relativos aos quatro anos do governo do Presidente Maurício Macri correm o risco de desaparecer, uma vez que o sistema de documentos digitais utilizado, por onde passa toda a informação do Estado, está cheio de falhas, dentre elas, não possui *backup*, não tem garantia de confidencialidade, não existe controle sobre quem o usa, dentre um grande número de fragilidades apontadas pela *Auditoría General de la Nación* (LOS EXPEDIENTES..., 2019). Além disso, mais da metade dos usuários não foi treinada. É um exemplo típico da ação ineficaz da instituição na proteção de suas informações.

Deve-se mencionar, como uma ameaça à segurança da informação, o uso das nuvens nas suas mais diversas formas, inclusive sem uma contratação formal pela instituição, quando utiliza plataformas de redes sociais, como *Facebook, Flickr e Youtube*, para divulgar seus acervos, muitas vezes ignorando a necessidade de replicar, em um contexto controlado, as informações disponibilizadas. Será que as instituições que divulgam seus documentos nessas plataformas estão investindo, também, em cuidados com a preservação de seus originais? Mantém repositórios arquivísticos digitais confiáveis?

A disponibilidade da informação no escopo de instituições públicas envolve, ainda, atenção à garantia de acessibilidade aos mais diversos interessados, mesmo que possuam limitações visuais, auditivas, de mobilidade e, até, de alfabetização, e a inteligibilidade, qual seja, a manutenção da informação em seu contexto de produção para que possam ser adequadamente compreendidas.

Quanto à integridade

Os documentos digitais arquivísticos devem possuir uma série de requisitos para serem considerados íntegros, confiáveis e terem sua autenticidade presumida para além da adoção ou não de um certificado digital. Esses requisitos encontram-se vinculados aos procedimentos de produção, de armazenamento e de preservação de documentos digitais ao longo do tempo e estão, em sua maioria, definidos no *e-Arq Brasil* (CONSELHO..., 2011), em seus requisitos para implementação de Sistemas Informatizados de Gestão Arquivística de Documentos (SIGADs).

A adoção do SIGAD na administração pública resolve parte dos problemas, porém, a realidade brasileira é que nem todas as instituições o adotou e, mesmo naquelas que o fizeram, nem todos os documentos arquivísticos são hoje capturados por esses sistemas. Seu uso é mais comum para documentos e processos que serão tramitados.

O que fazer, então? Investir na robustez dos sistemas de negócio e na proteção dos ambientes computacionais institucionais de forma a dificultar alterações ou apagamento de documentos. E, também, estabelecer procedimentos claros e auditáveis em relação ao arquivamento e manutenção dos documentos.

Após a entrada destes documentos nas instituições arquivísticas, recomenda-se enfaticamente o uso de repositórios digitais arquivísticos confiáveis como medida de proteger os originais de qualquer acesso ou alteração indesejáveis.

Quanto à confidencialidade

No ambiente de gestão documental é imprescindível dispor de controles de acesso por meio de perfis de usuários que contenha sua identificação, níveis de acesso vinculados a categorias de informações com restrição e registro em trilhas de auditoria das ações realizadas. Isso permite identificar se ocorreram acessos indevidos e responsabilizar as pessoas envolvidas e, também, com o estudo de incidentes, melhorar a segurança do sistema.

Outros problemas devem ser considerados. É comum que dados de indexação e cadastro de documentos sejam ostensivos, mesmo que o documento não o seja, mas não é raro que a pessoa que capture o documento no sistema utilize palavras e textos que comprometem esse sigilo. Sendo assim, qual o nível de descrição que as instituições devem adotar relativamente aos seus acervos arquivísticos disponíveis na internet para que não fiquem expostas a problemas quanto à aplicação da lei geral de proteção de dados pessoais ou de implicações relativas ao direito de ser esquecido? Os arquivos que custodiam processos judiciais são um exemplo de instituições para as quais tal questão é crítica. Nesse contexto, a confidencialidade exorbita a disponibilidade e a integridade.

Há casos em que os três pilares da segurança da informação se misturam. Por exemplo, a relação entre a disponibilidade e a confidencialidade encontra-se ilustrada no problema ocasionado pela prática da discricionariedade de algumas autoridades na aplicação da Lei de Acesso à Informação.

A baixa efetividade da fiscalização e punição das instituições quanto à concessão de acesso aos documentos públicos é uma questão que pode, também, representar um problema de segurança no aspecto de impossibilitar tempestividade no conhecimento social sobre informações públicas. Um exemplo recente é a classificação de mensagens de correio eletrônico trocadas entre o Itamaraty e os representantes brasileiros nas Nações Unidas orientando sobre temas relacionados aos diretos das mulheres e ao aborto. Segundo informações pelo autor da denúncia (CHADE, 2020), os documentos foram classificados apenas após a ocorrência de uma solicitação de acesso. Ou seja, a classificação de sigilo parece ter ocorrido por conveniência e não por previsto nas regras de restrição da instituição, o que é um desrespeito claro à Lei de Acesso à Informação que define o acesso como regra e o sigilo como exceção.

A junção de falhas na disponibilidade e na integridade das informações pode resultar no fortalecimento de um fenômeno contemporâneo preocupante, o revisionismo histórico. Não se trata do revisionismo baseado em pesquisas que identificam documentos que permitem repensar ou inserir em um novo contexto um determinado acontecimento ou fato. Aqui o revisionismo é colocado como a negação da história. Seus defensores advogam apagar do passado informações, documentos e monumentos que comprovem a ocorrência de eventos e aspectos sociais que os desabonem pessoalmente ou às suas crenças. Nesse sentido, promovem a destruição de estátuas, mudança de nomes de ruas, queima de livros e documentos ou, de forma mais incisiva, a mudança da história oficial contada em publicações patrocinadas pelo Estado.

Agora imaginem uma situação em que a disponibilidade se limitasse às informações de interesse desses grupos e, pior, sem a adoção de requisitos que garantam a integridade das informações acessadas. Nesse contexto seria muito fácil construir uma nova narrativa histórica baseada em documentos arquivísticos, uma vez que os demais documentos estariam indisponíveis ou mesmo poderiam ser apagados.

Como alertam Araújo e Santos (2007),

> Os arquivos, artefatos e relatos do passado têm sido utilizados como provas de um passado que foi deliberadamente esquecido pelas versões oficiais da história. Procura-se lembrar tudo aquilo que foi deliberadamente colocado no limbo da história. A lembrança, contudo, está vinculada àqueles que têm o poder, pois são eles que decidem quais narrativas deverão ser lembradas, preservadas e divulgadas.

Sim, a transparência da informação governamental, bem como a preservação da história da humanidade estão sujeitas a inúmeros desafios relativos à segurança da informação e ao uso de tecnologias que, embora possam ajudar a enfrentar alguns deles, também, colaboram para gerar novos problemas.

À guisa de encerramento

O mundo digital é instável e preponderantemente sensível às mudanças tecnológicas que conduzem à rápida obsolescência de formatos, mídias e ambientes computacionais. Mas as atividades dos arquivistas no tratamento das informações digitais não se limitam a esse confronto, também estão sujeitas a vários outros, dentre eles os ditames legais. Existem diversos exemplos a serem citados, mas me limito ao mais

recente. A Lei 13.874/2019 aprovou a eliminação de documento arquivístico original uma vez gerado seu representante digital, mas deixou muitas dúvidas sobre a execução desse procedimento, mesmo após a edição do Decreto nº 10.278/2020, que a regulamentou. Tanto que, visando solucionar o problema, o Conselho Nacional de Arquivos (2020) criou uma comissão técnica consultiva com o objetivo de propor resoluções que estabeleçam diretrizes e procedimentos técnicos a serem implementados no processo de digitalização regulamentado pelo decreto e no descarte dos documentos originais.

Os profissionais de arquivo estão sujeitos a uma legislação desconexa que pode conduzir a ações que resultem na perda de informações custodiadas ou de sua integridade. Em outras palavras, existem aspectos da segurança da informação que são ocasionados pela insegurança jurídica existente no país.

O problema de perda da informação arquivística não se esgota nas possibilidades aqui mencionadas. O escopo temático deste número da *Revista do Arquivo* é pleno de possibilidades de pesquisa e de desafios que demandam urgente enfrentamento dos profissionais que lidam com a gestão documental e com a memória dos povos. O próprio exercício profissional oferece possibilidades de perda: uma indexação mal feita, ou uma classificação errada podem reduzir as possibilidades de recuperação da informação, ou pior, pode resultar em descarte ou preservação indevida de um documento.

Ressalto que aqui não foram abordados aspectos relativos à disponibilidade financeira, que impactam diretamente na manutenção dos acervos ou investimento na melhoria de suas condições de preservação. Neste sentido, cabe questionar, por exemplo, quantas instituições possuem depósitos com controle de umidade e temperatura?

Com todas as possibilidades de perda da memória digital dos povos é preciso consciência das instituições públicas e dos profissionais de arquivos na gestão e preservação desses acervos para que a serendipidade não se torne a tônica da história a ser contada no futuro a partir de consulta aos documentos digitais hoje produzidos.

Referências

ARAÚJO, Maria Paula Nascimento; SANTOS, Myrian Sepúlveda dos. História, memória e esquecimento: implicações políticas. **Revista Crítica de Ciências Sociais,** v.79, 2007, pp.95-111. Disponível em: https://journals.openedition.org/rccs/728 Acesso em: 18 set. 2020.

ARQUIVO DO ESTADO DE SÃO PAULO. Mapa da gestão documental paulista. Disponível em: http://www.arquivoestado.sp.gov.br/site/gestao/municipios/mapa_paulista Acesso em: 20 set. 2020.

CENTRO DE ASSISTÊNCIA aos Municípios. Prata da Casa. **Revista do Arquivo**. São Paulo, Ano II, Nº 7, p. 60-70, outubro de 2018. Disponível em: http://www.arquivoestado.sp.gov.br/revista_do_arquivo/07/prata_da_casa.php#inicio_artigo Acesso em: 20 set. 2020.

CARR, Nicholas. When our culture's past is lost in the cloud. **The Washington Post**. Opinion. 25 mar. 2016. Disponível em: https://www.washingtonpost.com/opinions/when-our-digital-memory-is-lost-in-the-cloud-what-becomes-of-our-human-history/2016/03/24/11ed1482-ba46-11e5-99f3-184bc379b12d_story.html Disponível em: 9 set. 2020.

CHADE, Jamil. Itamaraty coloca telegramas sobre aborto e gênero em sigilo até 2025. **UOL**. Coluna. 11 set. 2020. Disponível em: https://noticias.uol.com.br/colunas/jamil-chade/2020/09/11/itamaraty-coloca-telegramas-sobre-aborto-e-genero-em-sigilo-ate-2025.htm Acesso em: 11 set. 2020.

CONSELHO NACIONAL DE ARQUIVOS. **Portaria nº 120, de 28 de julho de 2020**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-120-de-28-de-julho-de-2020-271228562 Acesso em: 17 set. 2020.

CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de Documentos Eletrônicos. **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. 1.1. versão. Rio de Janeiro : Arquivo Nacional, 2011. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/e-arq.

pdf Acesso em: 10 dez. 2019.

EX-PREFEITA apaga todos os arquivos digitais da secretaria de Finanças. **Rede Globo**, Bom Dia Brasil, 4 jan. 2017. Disponível em: http://g1.globo.com/bom-dia-brasil/noticia/2017/01/ex-prefeita-apaga-todos-os-arquivos-digitais-da-secretaria-de-financas.html Acesso em: 7 mar. 2020.

FURQUIM, Gabriella. Ratos, pombos e fungos ameaçam memória da capital do país. **Metrópoles**, Distrito Federal, 21 mar. 2018. Disponível em: Acesso em: https://www.metropoles.com/distrito-federal/transito-df/distrito-federal-transito-df/ratos-pombos-e-fungos-ameacam-memoria-da-capital-do-pais Acesso em: 15 jun. 2020.

LIJALAD, Ari. Los expedientes públicos de los 4 años de Macri corren riesgo de desaparecer. **El destape**, 22 set. 2019. Disponível em: https://www.eldestapeweb.com/nota/los-expedientes-publicos-de-los-4-anos-de-macri-corren-riesgo-de-desaparecer-201992219170 Acesso em: 7 mar. 2020.

LIMA, Fernanda; NASCIMENTO, Vinícius. Abrigo de documentos raros, Arquivo Público da Bahia sofre com descaso. **Correio**, Bahia, 16 set. 2018. Disponível em: https://www.correio24horas.com.br/noticia/nid/abrigo-de-documentos-raros-arquivo-publico-da-bahia-sofre-com-descaso/ Acesso em: 20 ago. 2020.

LOS EXPEDIENTES públicos de los 4 años de Macri corren riesgo de desaparecer. **Chaco día por día**, 23 set. 2019. Disponível em: https://www.chacodiapordia.com/2019/09/23/los-expedientes-publicos-de-los-4-anos-de-macri-corren-riesgo-de-desaparecer/ Acesso em: 12 mar. 2020.

PESQUISADORES denunciam abandono de documentos e criticam transferência do Arquivo Público de Ribeirão Preto, SP. **Jornal da EPTV 1ª edição**, 17 mar. 2018. Disponível em: https://g1.globo.com/sp/ribeirao-preto-franca/noticia/pesquisadores-denunciam-abandono-de-documentos-e-criticam-transferencia-do-arquivo-publico-de-ribeirao-preto-sp.ghtml Acesso em: 27 jul. 2020.

SANTOS, Vanderlei Batista dos. **A Arquivística como disciplina científica**: princípios, objetivos e objetos. Salvador: 9Bravos, 2015.

_____. **Gestión de documentos electrónicos:** una visión archivística. Florianópolis: Bookess, 2011.

WORLD JUSTICE PROJECT. **Índice de Estado de Derecho 2020.** Disponível em: https://worldjusticeproject.org/sites/default/files/documents/WJP-Global-ROLI-Spanish.pdf Acesso em: 17 set. 2020.