UNIVERSIDADE FEDERAL DO AMAZONAS (UFAM)
INSTITUTO DE CIÊNCIAS HUMANAS E LETRAS (ICHL)
DEPARTAMENTO DE ARQUIVOLOGIA E BIBLIOTECONOMIA (DAB)
CURSO DE ARQUIVOLOGIA

Manoel Pedro de Souza Neto

A preservação digital em uma instituição judiciária: o caso da assinatura digital nos processos judiciais como requisito de autenticidade aos documentos arquivísticos

Manaus
2013

MANOEL PEDRO DE SOUZA NETO

A preservação digital em uma instituição judiciária: o caso da assinatura digital nos processos judiciais como requisito de autenticidade aos documentos arquivísticos

Trabalho de conclusão de curso, apresentado ao Departamento de Arquivologia e Biblioteconomia da Universidade Federal do Amazonas, como requisito parcial à obtenção do título de Bacharel de Arquivologia.

Orientadora: Professora Carla Mara da Silva Silva

Manaus
2013

S726p

A preservação digital em uma instituição judiciária: o caso da assinatura digital nos processos judiciais como requisito de autenticidade aos documentos arquivísticos / Manoel Pedro de Souza Neto. – Manaus, 2013.

120 f. : Il; cm

Monografia (Arquivologia – Graduação) - Curso de Arquivologia, Universidade Federal do Amazonas, 2013.

Orientado por Profª. Carla Mara da Silva Silva

1 Arquivologia 2 Preservação Digital I Título

CDD: 025.0634

UNIVERSIDADE FEDERAL DO AMAZONAS (UFAM)
INSTITUTO DE CIÊNCIAS HUMANAS E LETRAS (ICHL)
DEPARTAMENTO DE ARQUIVOLOGIA E BIBLIOTECONOMIA (DAB)
CURSO DE ARQUIVOLOGIA

FOLHA DE APROVAÇÃO

Título: A preservação digital em uma instituição judiciária: o caso da assinatura digital nos processos judiciais como requisito de autenticidade aos documentos arquivísticos

Autor: Manoel Pedro de Souza Neto

Departamento: Arquivologia e Biblioteconomia

Trabalho de Conclusão de Curso submetido à Comissão Examinadora designada pelo Departamento de Arquivologia e Biblioteconomia, da Universidade Federal do Amazona como requisito parcial para obtenção do título de Bacharel em Arquivologia

Trabalho de Conclusão de Curso apresentado em: 12 de novembro de 2013

Aprovado por:

_____
Professora Carla Mara da Silva Silva
Presidenta-orientadora (UFAM/DAB)

_____
Professora Marcielli Brondani de Souza
Membro interno (UFAM/DAB)

_____
Professora Dayse Enne Botelho
Membro interno (UFAM/DAB)

A Deus meu amigo fiel, meu maior protetor, mais essa conquista em minha vida

AGRADECIMENTOS

Muitas pessoas trilharam o meu percurso nessa minha decisão retornar ao banco de faculdade para cursar mais uma graduação. Esta pela qual tenho profundo AMOR e foi onde me encontrei profissionalmente. Durante essa trajetória muitos atores fizeram-se principais e outros coadjuvantes, mas cada qual teve a sua parcela de contribuição e ficarão guardados no meu coração.

Agradeço à Professora Carla Mara da Silva Silva que foi a minha preceptora (orientadora) nessa trajetória final do curso de graduação.

Aos meus pais Maria Rosilene de Oliveira Souza e Francisco de Assis Mendonça de Souza que acompanharam-me nessa nova trajetória, sempre apoiando-me e torcendo por mais essa conquista.

Às minhas irmãs Juçara de Oliveira Souza e Julieta Mendonça de Souza Neta que, também, acompanharam o meu esforço e a minha obstinação em chegar ao final deste curso.

Ao meu amigo, parceiro, ***Pablo Augusto da Paz Elleres***, onde em muitos momentos eu recorri e você prontamente estava ali para ajudar-me, sobretudo, em um momento delicado da sua vida conseguiste tirar forças inimagináveis para, mais uma vez, colaborar com o seu conhecimento, experiência, prática, vivência, labor para a construção nesse trabalho. Obrigado por me mostrar e aprender mais da sua área de Tecnologia da Informação. Meus agradecimento especial a você e admiração profunda a ti.

À Marlúcia Araújo dos Santos, amiga/irmã de trabalho que durante esses mais de 07 anos de amizade sempre me orientou, me ajudou profissionalmente, em tantos momentos que precisei.

Aos meus colegas de trabalho Fátima, Lessandra, Carlisman, Anselmo, Alexandra, Seu Nunes, Socorro, Mário, Paulo Max, Nazir que estão dando o suporte necessário sempre quando tive que me ausentar para a minha jornada de estudante.

Aos meus ex-estagiários e os recentes. Não vou nominar, pois posso incorrer no erro de esquecer algum. Vocês também ajudaram nessa trajetória profissional-arquivística a dar fôlego à instituição na qual atuo.

Ao presidente do Tribunal de Justiça Desembargador Ari Jorge Moutinho da Costa que possibilitou o desenvolvimento desta pesquisa na instituição.

A todos os nossos professores do curso de Arquivologia que puderam repassar os seus conhecimentos para formar os profissionais **arquivistas da 1ª Turma de Arquivologia da Região Norte do país**.

RESUMO

Esta pesquisa se propõe a contribuir com o processo de preservação informacional, identificando se o requisito de autenticidade da assinatura digital estão incorporados aos processos judiciais eletrônico de modo que possam garantir a sua preservação em longo prazo. Para isso optou-se pela pesquisa descritiva, a partir da abordagem qualitativa, a qual se fundamentou de pesquisa bibliográfica e de campo, tomando por base o método de estudo de caso, onde o instrumento de coleta de dado foi aplicado ao setor responsável pelo tratamento direto da informação judiciária, afim de cumprir com as prerrogativas metodológicas exigidas nos trabalhos científicos. Espera-se com esta pesquisa, contribuir com a melhoria da prática arquivística, a qual vem sendo trabalhada na instituição judiciária definida no objeto de estudo.

Palavras-chave:
Arquivologia. Preservação digital. Autenticidade eletrônica. Processo judicial digital. Documentos arquivísticos

ABSTRACT

This research has the purpose to contribute with the informational preservation process, identifying if the digital signature requirement of authenticity are incorporated into the electronic processes in order to ensure their long-term preservation. For this fact we chose for the descriptive research, from the qualitative approach, which was based from literature search and field, based on the method of case study, where the data collection instrument was applied to the sector responsible for direct treatment control of judicial information in order to fulfill with the required prerogatives of the methodological scientific works. It is expected that this research contribute to the improvement of archival practice, which has been worked on judicial institution defined in the object of study.

Keywords
Achival. Digital preservation. Electronic authenticity. Digital judicial proceeding. Archival documents

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURA E SIGLAS

AC – Autoridade Certificadora

AIIM – Association for infomation and image management

AMAZONJUS – Amazonas Justiça

CD – Certificação Digital

CF – Constituição Federal

CBN – Central Brasileira de Notícias

CNJ – Conselho Nacional de Justiça

CPC – Código de Processo Civil

CRC – Cyclic Redundancy Check

CTDE – Câmara Técnica de Documentos Eletrônicos

CONARQ – Conselho Nacional de Arquivos

DSA – Digital Signature Algorithm

DSS – Digital Signature Standard

HD – Hard Disk

IN – Instrução Normativa

ICP-Brasil – Insfraestrutura de Chaves Públicas Brasileiras

ITI – Instituto Nacional de Tecnologia da Informação

JECC – Juizados Especiais Cíveis e Criminais

LAI – Lei de Acesso à Informação

MD – Message Digest

MP – Medida Provisória

METRO-MAO – Rede Metropolitana de Manaus

OCLC – Online Computer Libray Center

PDF – Portable document format

PJE – Processo Judicial Eletrônico

PROJUDI-PR – Processo Eletrônico do Judiciário do Paraná

RG – Registro Geral

RSA – Ron Rivest, Adi Shamer, Landleman

RLG/OCLG – Research Library Group/Online Computer Library Center Report

SHA – Secure Hash Algorithm

SOA – Arquitetura Orientada ao Serviço

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SAJ – Sistema de Automação de Justiça

SIPAM – Sistema de Proteção da Amazônia

SOFTPLAN/POLIGRAPH – Sistemas Integrados para Mercados Específicos de Negócios

TIC – Tecnologia da Informação e Comunicação

TJ/AM – Tribunal de Justiça do Amazonas

TJPR – Tribunal de Justiça do Paraná

TRF – Tribunal Regional Federal

UKLON – United Kingdom Office for Library Networking

UNESCO - Organização das Nações Unidas para a Educação, Ciência e Cultura

VSAT - Very Small Aperture Terminal

VECUTE – Vara Especializada em Crimes de Uso de Tráfico de Entorpecentes

SUMÁRIO

INTRODUÇÃO

O Tribunal de Justiça do Estado do Amazonas, enquanto instituição judiciária, vem acumulando e custodiando um rico acervo. Isso lhe permite assumir o papel de relevo que lhe cabe historicamente na administração pública e entre seus congêneres.

Sem o caráter prescritivo e sem se esgotar com a temática lançada, esta investigação buscou mapear no contexto macro a preservação digital e no micro a autenticidade da assinatura digital como requisito aos documentos arquivísticos em uma instituição judiciária no estado do Amazonas.

Esta, portanto, foi tarefa bem delicada, mas acredita-se que ao final bem sucedida, visto que o investigador ao mesmo tempo em que confirma, reitera a necessidade do diálogo de profissionais de outros campos próximos à Arquivística: Ciência da Informação, Informática, Administração a juntos caminharem e propor soluções adequadas à preservação da informação arquivística no meio digital.

Se as instituições não tiverem a consciência e disposição para encarar a preservação dos documentos digitais como uma questão-cerne no processo de transposição do meio físico para o virtual pode ter um impacto negativo na memória coletiva, pública e privada com repercussão em questões legais e organizacionais.

A preservação digital – objeto de reflexões desta investigação – se consolida como um tema contemporâneo e revela interfaces com a gestão do conhecimento, pois à medida que se tem uma política de preservação digital institucional consegue-se dar condições de acesso ao material custodiado no meio eletrônico.

É válido citar, também, a construção do arcabouço técnico-legislativo foi construído ao longo dos anos com a implantação de alguns procedimentos, como por exemplo: a tramitação eletrônica dos atos gravados em fita magnética; a gravação eletrônica de dados e recepção das duplicatas mercantis; a recepção e transferência eletrônica das petições entre outras e culminou na Lei 11.419 de 2006 do processo judicial eletrônico.

Diante da explosão e diversidade informacional, chamar a responsabilidade para si e assumir o papel que lhe cabe no contexto judicial não tem sido trivial. De modo particular, o meio digital pode oferecer dificuldades frente à quantidade de informação a ser gerenciada e preservada ao longo do tempo.

Isto só é percebido à medida que há disposição de conjugar a realidade de seu campo de trabalho a um campo da investigação; de buscar referenciais na área estudada e construir uma base de apoio para experimentações empíricas, no intuito de unir o conhecimento prático ao teórico.

Para alcançar o objetivo maior deste trabalho de identificação das estratégias adotadas de autenticidade eletrônica dos processos judiciais em um tribunal no Estado do Amazonas, debruçou-se sobre os aspectos legislativos da informatização nos tribunais; identificação das estratégias de preservação existentes na literatura; verificar se estão enquadradas na etapa da criação de uma política de preservação digital e identificar regulamentações internas que tratem de um política de preservação digital.

Em síntese, pode-se dizer que o desenvolvimento desta investigação agrega à literatura da área arquivística reflexões acerca da assinatura eletrônica como um dos requisitos que garante a autenticidade aos documentos arquivísticos produzidos no meio eletrônico posicionando-o no centro das preocupações de preservação digital.

Como se observa, ao longo dos anos, a sociedade está sendo impactada, direta ou indiretamente com uma grande quantidade de informações produzidas, recebidas e acumuladas nos mais variados suportes e formatos. Tal crescimento deveu-se à disponibilidade dos meios e das mídias de comunicação que ao longo dos tempos utilizam-se desse desenvolvimento para melhor se comunicarem e transmitirem a informação; da evolução da sociedade que se permitiu crescer culturalmente buscando cada vez mais conhecimento fazendo uso dos meios e das mídias supramencionados; da (r)evolução tecnológica, sua variedade e disponibilidade, do barateamento dos instrumentos e do amadurecimento das ciências que em suas trajetórias produzem dados e resultados em suas respectivas áreas, as quais corroboraram para a crescente quantidade de informações que se produziu no século XX e tem se produzido no século XXI, mais conhecida como a era da Sociedade da Informação.

Acompanhando essa era, está a consolidação da tecnologia da informação da comunicação (TIC’s) que chegam como aliados na melhoria do recolhimento, do armazenamento, da transmissão, da análise e apresentação de dados. Estima-se que com o passar dos anos esse movimento – informacional – tende só a aumentar

e uma parcela significativa desta deve ser produzida, recebida, registrada e transmitida em suportes e formatos digitais.

Nessa esteira, erigem-se dois atores: a sociedade e o Poder Judiciário. A primeira vem, gradativamente, conscientizando-se sobre seus direitos e buscando cada vez mais a justiça para solucionar os seus conflitos, a reparação de algum dano ou simplesmente fazendo valer o seu direito. Mostra disse são os 90 milhões de existente até o ano de 2012. Desse total, 63 milhões são processos pendentes de julgamento e 26 milhões são novos[1]

É fato que com a aceleração do processo de informatização nos tribunais todos ganham – partes, advogados, magistrados, servidores –, em certa medida, pois se desburocratiza os procedimentos de acesso aos autos, sendo realizado diretamente nas páginas dos tribunais; facilitou-se a vida dos patronos com a criação do sistema *push* onde ele se cadastram e recebem, via e-mail, toda e qualquer movimentação referente a processo em que ele advoga e ao magistrado a possibilidade em tempo real saber sobre quantos processos estão pendentes de despachos e sentença, sobre o andamento da serventia em que é titular, entre outros.

Todavia, contraditoriamente ou não, provém das TIC's o principal paradigma – segurança –. Decerto, destacam-se alguns atributos básicos de: confidencialidade, integridade, disponibilidade e autenticidade, necessitam de monitoramento constante devido à transitoriedade das mídias. Thomaz e Soares (2004) apud Lusenet (2001) destaca três questões de um conjunto de problemas relacionados à preservação digital que precisam ser compreendidos e, necessariamente, monitorados:

> 1) as mídias são suportes transitórios que prestam sua função somente por um período limitado de tempo e que a transferência para novas mídias é absolutamente necessária; 2) o software e o hardware tornam-se obsoletos em questão de anos, ao invés de décadas, e que embora as versões sucessivas de programas possam ser compatíveis, os fabricantes de software normalmente não garantem a compatibilidade por um longo período; e 3) o software proprietário é problemático não somente porque é protegido e o código fonte não está disponível mas, também, porque normalmente está documentado de forma inadequada tornando a conversão de dados muito mais complexa (THOMAZ; SOARES, 2004, p.01)

[1] CNJ em ação mostra divulgação do relatório justiça em números. http://www.cnj.jus.br/noticias/cnj/21953:cnj-em-acao-mostra-divulgacao-do-relatorio-justica-em-

Há de se coadunar com as questões levantadas pelo autor, pelos seguintes motivos: 1. As ações e a conscientização preservacionistas não avançam na mesma medida que a tecnologia progride; 2. Por mais que se tenha um contrato formal, os quais explicitam os deveres e obrigações do contratante e contratado, por exemplo, entre o poder público e o privado, há algumas cláusulas passam "despercebidas" e requerem intervenção dos atores envolvidos para minoração de problemas futuros ou às vezes maquiam visando ludibriar a contratante; 3. Ter empresas terceirizadas gerenciando as informações das atividades fim e meio deixam as instituições reféns, visto que o código fonte não lhe será fornecido ou quando o fazem o caminho a percorrer demora mais do que o necessário causando problemas de ordem não mensuráveis.

O processo de informatização no Poder Judiciário, indelevelmente, veio contribuir para a melhoria da prestação jurisdicional, promovendo maior acesso às informações. Não obstante a essa premissa, é um tanto quanto assustador a rapidez com que está sendo feita essa transição do analógico para o digital levantando-se a seguinte questão: será se os atuais registros judiciais que agora estão sendo tramitados de forma digital estarão disponíveis para o acesso e pesquisa daqui a alguns anos? Tal questionamento tem implicações mais amplas, visto que se observou quando Cetto e Alonso Gamboa (2010) citando Inarelli (2007, p.03) afirma que "a humanidade ainda não tem prática e nem experiência para a memória digital". Hoje a tecnologia é um meio para se chegar e não o princípio de tudo, ou seja, ela por si só não resolve todas as questões envolvendo a preservação digital. Tal afirmativa é identificada quando Cetto e Alonso Gamboa (2010) citando Inarelli (2007, p.03) informam acerca de vários fatores que cercam a preservação digital, pois "a cada dia em virtude da obsolescência das tecnologias, da deterioração das mídias digitais e principalmente pela falta de políticas de preservação digital", visto que a memória da sociedade está ameaçada.

As instituições judiciárias que não tiverem, desde o início, a preocupação em desenvolver políticas de preservação digital, as quais visam controlar a documentação que foi convertida em virtual ou aquelas que já nasceram digitais serão as principais responsáveis pela lacuna histórica da perda de informação, visto que Ferreira (2006, p.12) afirma que "o tema da preservação digital é, ao mesmo tempo, um tema novo, vasto e complexo". É novo, porque se está saindo do físico para o digital (mudança de suporte). Torna-se vasto porque ainda surgirão muitas

questões teóricas-práticas a serem exploradas (perspectiva preservacionista) e complexas porque transcendem questões vão além de um de um simples armazenamento das informações em um HD externo, por exemplo.

O Poder Judiciário, dentre os demais tem evoluído rapidamente, assim como os sistemas de gerenciamento das informações quer sejam administrativos ou judiciais. Advindo dessa evolução surgem, também, problemas reais, os quais necessitam de resposta efetivas. É claramente identificado quando Cetto e Alonso Gamboa (2010) citando Inarelli (2007, p.04) quando diz que é necessária a "interferência humana e de políticas para a preservação digital". Partindo desse pressuposto, formularam-se outras questões, que por hora, só poderão ser respondidas no desenvolvimento deste trabalho: Existe uma gestão documental integral para a manutenção dos documentos em ambiente físico ou eletrônico seguro? Será se os documentos digitalizados ou aqueles natos digitais estarão disponíveis para o acesso e para a reutilização daqui a alguns anos? Os sistemas atuais estão preparados para desenvolverem a gestão para os documentos digitais?

Pela coragem intelectual, o trabalho de conclusão de curso preservação digital em uma instituição judiciária: o caso da assinatura digital como requisito de autenticidade aos documentos arquivístico, dá ao leitor a certeza de que se trata de um trabalho inicial no meio acadêmico, o qual requer maior aprofundamento na perspectiva de construção e contribuição de mais reflexões e praxes na pesquisa entorno da Arquivística contemporânea.

2. FORMAÇÃO DO PODER JUDICIÁRIO

A história mostra que o Poder Judiciário no mundo surgiu há mais de 250 anos. Foi idealizado pelo francês Charles-Louis de Secondat, após realizar um estudo sobre as instituições políticas inglesas. Ele elaborou a teoria da separação dos poderes como é atualmente consagrada em muitas modernas constituições: legislativo (função de elaborar as leis), executivo (função de administrar ou executar) e o judiciário (função jurisdicional).

Essa teoria apareceu em sua obra mais famosa: O espírito das Leis (L'Espirit des lois, em 1748), onde se discutia a respeito das instituições e das leis e se buscava compreender as diversas legislações existentes em diferentes lugares e épocas.

No que diz respeito ao Brasil, esse poder chegou com os portugueses, em 1500. Portugal exerceu forte influência na colonização desse país. Sendo assim, a história do poder judiciário não seria diferente. Isto é constatado na citação de Ituassú (2000, p.01) quando diz:

> A atividade judiciária brasileira nasceu em Portugual, a que então o Brasil pertencia desde a descoberta em 1500, até a proclamação da independência em 1822. E assim mesmo, as regras jurídicas lusitanas continuaram a vigir por largos anos, disciplinando a vida jurídica de nosso país.
> Quando D. Afonso de Portugal faleceu, seu sucesso foi seu filho D. Sebastião, que morreu jovem na batalha de Alcacer Kibir, sendo substituído no trono por D. Henrique seu tio, Prior do Crato, que exercitou seu reinado por pouco tempo.
> Não deixando herdeiros, assumiu o trono português seu primo Felipe I da Espanha, que de 1580 a 1640 uniu as duas coroas, assim permanecendo durantes os reinado de Felipe II e Felipe III.
> D. Afonso editou o primeiro código, inspirado no *Corpus Júris Romanorum* e seu código tomou seu nome em 1466 e publicado somente em 1786, constando cinco volumes: o primeiro tratava dos Oficiais da Corte, com o encargo de aplicar o Direito e a Justiça; o segundo tratava dos atos judiciais e da ordem processual; o terceiro contendo a relação das leis e ordenação a serem observadas; o quarto dos atos concernentes aos contratos e sua regulamentação e o quinto as ordenações sobre crimes e respectivas penas.

À guisa de explicação, nessa época, a distribuição das matérias, seguida ainda pelas linhas gerais das Ordenações Afonsinas, era exercida pelas capitanias hereditárias. Essa função cabia ao capitão donatário[2] que reunia as atribuições de administrador, juiz e chefe militar.

---

[2]Era um cargo tardo-feudal criado nas ilhas atlânticas e no Brasil onde vigorava o regime da donataria. Cabia ao capitão-donatário a representação na capitania dos interesses do donatário,

Essas ordenações vigeram no Brasil após as descobertas, quando foi implantado um sistema de Governos Gerais, em 1548. Esse Governador-Geral passou a ser assessorado pelo Ouvidor-Geral nos assuntos relativos à justiça. Em 1609, foi instalado, com sede na Bahia, o primeiro tribunal no país, denominado de Relação do Estado do Brasil.

Mais de um século após a instalação deste tribunal, surge, em 1753, a Relação do Rio de Janeiro. Sua propositura, nesse Estado, foi em consequência da transferência de toda estrutura política, administrativa e judiciária, ocorrida em 1751.

Em 1808, com a chegada da Família Real ao Brasil, o Tribunal de Relação passou a denominar-se Casa da Suplicação do Brasil – funcionando como um tribunal de terceira e última instâncias –, à qual competia julgar os agravos ordinários e apelações, pois se tornaria inviável a remessa desses autos à Casa de Suplicação de Lisboa.

Em mais de cinco séculos de descoberta no Brasil, foram elaboradas sete constituições: *Constituição de 1824*, promulgada após a Proclamação de Independência do Brasil. *Constituição de 1891*, tendo seu início em 1890. *Constituição de 1934*, que assegurava à Nação cinco pilares fundamentais: a *unidade, a liberdade, a justiça e bem-estar social e o econômico. Constituição de 1937,* é a quarta. *Constituição de 1946*, somente consagrou-se à liberdade expressa na Constituição de 34. *A Constituição de 1967* garantiu função do poder constituinte originário ilimitado e soberano. E por fim, a *Constituição de 1988,* que ainda vigora. Nesse período, o Poder Judiciário do Brasil sofreu várias modificações em sua denominação, passou a ser conhecido como: *Corte de Apelação, Tribunal de Apelação* até chegar ao *Tribunal de Justiça.* Essas modificações foram significativas para entender essas fases transitórias até chegar ao que hoje se denomina.

A síntese da formação do Poder Judiciário para compreensão do que hoje é um Tribunal de Justiça demonstra o quanto este ramo foi e continua sendo importante para o desenvolvimento dos estados brasileiros na perspectiva proferir decisões e dizer o direto àqueles que buscam o judiciário para resolverem os seus conflitos.

---

garantindo os seus proventos e administrando os seus bens. Serviam ainda de interlocutor entre as populações e o donatário (GARCIA, 2004)

2.1 Composição dos órgãos judiciários STF, STJ, CNJ, Justiça Estadual e suas competências

2.1.1 Supremo Tribunal Federal - STF

A CF, no artigo 101, seção II, descreve este órgão, o Supremo Tribunal Federal, composto de 11 Ministros, aprovados pelo Senado Federal e nomeados pelo Presidente da República, dentre cidadãos brasileiros natos, com mais de trinta e cinco anos e menos de sessenta e cinco anos de idade, de notável saber jurídico e de reputação ilibada (BRASIL, 1988)

O STF é o guardião da Constituição Federal. Compete-lhe, dentre outras tarefas, julgar as causas em que esteja em jogo uma alegada violação da CF. Ele aprecia uma ação direta de inconstitucionalidade ou um recurso contra a decisão que, alegadamente, violou algum dispositivo da Constituição.

2.1.2 Conselho Nacional de Justiça – CNJ

Compõe-se de 15 membros com mais de trinta e cinco anos e menos de sessenta e cinco anos de idade, com mandato de dois anos, admitida uma recondução.

Este órgão foi criado pela emenda constitucional nº 45, de 08 de dezembro de 2004, com a função de controlar a atuação administrativa e financeira dos órgãos do Poder Judiciários brasileiro. Também é encarregado da supervisão do desempenho funcional dos juízes.

2.1.3 Superior Tribunal de Justiça – STJ

O Superior Tribunal de Justiça compõe-se de 33 Ministros, nomeados pelo Presidente da República, depois de aprovada a escolha pela maioria absoluta do Senado Federal, dentre Juízes, Desembargadores, advogados e membros do Ministério Público, com base no sistema previsto na Constituição Federal.

O STJ é o guardião da uniformidade da interpretação das leis federais. Desempenha esta tarefa ao julgar as causas decididas pelos Tribunais Regionais

Federais ou pelos Tribunais dos Estados, do Distrito Federal e dos Territórios, que contrariem lei federal ou deem à lei federal interpretação divergente.

2.1.4 Justiça Estadual

No artigo 125 da Constituição Federal é determinado que os estados organizem a Justiça Estadual, observando os princípios constitucionais federais. Sua composição, via de regra, dá-se por duas instâncias, o Tribunal de Justiça – TJ – e os Juízes Estaduais (BRASIL, 1988)

Os Tribunais de Justiça dos Estados possuem competências definidas na Constituição Federal, bem como na Lei de Organização Judiciária dos Estados. Têm a competência de, em segundo grau, revisar as decisões dos juízes, em primeiro grau, determinadas ações em face de determinadas pessoas.

Determina, ainda, a CF que os estados instituam representação de inconstitucionalidade de leis e atos normativos estaduais e municipais frente à Constituição Estadual, geralmente apreciada pelos TJs. Contudo, é facultado aos estados criar a Justiça Militar Estadual, com competência sobre a polícia militar estadual. Seus integrantes de primeiro grau são chamados de Juízes de Direito e de segundo grau, de Desembargadores.

2.2 Marco legislativo da informatização dos atos processuais nos Tribunais Brasileiros

Partindo-se do pressuposto que os processos físicos sofrem uma morosidade nas estanterias do judiciário, ocasionando, muitas vezes, a falta de controle sobre o andamento de cada, os quais comprometem o poder judiciário no tocante a efetiva prestação jurisdicional e o acesso mais célere à justiça.

Buscando mudar esse quadro, surge o projeto de Emenda Constitucional nº 45, passando a vigorar no dia 31 de dezembro de 2004. Propunha incluir o inciso LXXVIII do artigo 5º da Constituição da República Federativa do Brasil de 1988, introduzindo "a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação".

Com essa propositura Dias Soares diz que:

> Uma reformulação das rotinas processuais internas, com vistas à desmaterialização dos atos processuais e à racionalização dos procedimentos, bem como à otimização da prestação jurisdicional e dos serviços judiciários, conferindo-se concretude aos princípios da celeridade processual, da economicidade e da instrumentalidade e ao direito fundamental à efetividade, a partir do abandono de formalidades arcaicas na tramitação do processo. (DIAS SOARES, 2011)

Face ao exposto, talvez, a perspectiva que se tinha quando se pensava em melhorar as rotinas internas era informatizar. A utilização de recursos tecnológicos, no judiciário, assim como em outras áreas abriria oportunidades imagináveis. Dessa forma, cabe citar: a melhoria no controle, o qual se tornaria mais eficaz, a redução de custos financeiros, à medida que se liberta de sistemas privados, a geração de sinergia de conhecimento entre outros.

A presente abordagem visa identificar os tribunais que iniciaram um projeto de informatização em suas respectivas unidades, fazendo uma análise das regulamentações existentes.

A Seção I dos Poderes, dos Deveres e da Responsabilidade do Juiz, art. 125, II, já determinava que houvesse a rápida solução do litígio, assim como os dispositivos que tratavam do procedimento sumário e a tutela antecipada [3]

[3] é o ato do juiz, por meio de decisão interlocutória, que adianta ao postulante, total ou parcialmente, os efeitos do julgamento de mérito, quer em primeira instância quer em sede de recurso. Disponível em: <http://pt.wikipedia.org/wiki/Tutela_antecipada>. Acesso em: 14 de nov. de 2013.

revelavam-se como em seus parágrafos e artigo. Contudo, o *modus operandi* ficaria a cargo das instituições.

A Lei 9.099 de 25 de setembro de 1995, que dispôs sobre a criação dos Juizados Especiais Cíveis e Criminais (JECCs) cumpriu bem o papel para a qual foi criado: facilitou o acesso à justiça a milhares de pessoas que buscavam o judiciário, visto que antes se esbarrava na burocracia existente de recolhimento das custas, na necessidade de contratação de advogado, entre outros. Esta, não tratou, especificamente, da possibilidade de tramitação eletrônica. Identificou-se na Seção IV, § 3º que apenas abriu a possibilidade de atos poderem ser gravados em fita magnética ou equivalente, mas depois do trânsito em julgado da decisão, elas poderiam ser inutilizadas.

A Lei nº 9.492, de 10 de setembro de 1997, que definiu competência, regulamentou os serviços concernentes ao protesto de títulos e outros documentos de dívida e deu outras providências, trouxe em seu art 8º, parágrafo único a previsibilidade de, por meio magnético ou de gravação eletrônica de dados, recepção das duplicatas mercantis e de prestação de serviços.

Já na Lei nº 9.800, de 26 de maio de 1999, conhecida como Lei do Fax, permitiu a recepção e transferência eletrônica das petições e chegando aos tribunais elas eram impressas e juntadas ao processo físico, ou seja, a forma física era mantida, visto que a Lei não dispensava às partes entregar os documentos originais, conforme predizia o art. 2º. Como praxe inovadora diz-se desta Lei a possibilidade de transmissão eletrônica das petições.

Diferentemente da Lei 9.099/1995 (criação dos Juizados Especiais Cíveis e Criminais) sobreveio a Lei 10.259 de 12 de julho de 2001 que disciplinou os Juizados Especiais Cíveis e Criminais Federais, trazendo em seus dispositivos inovações para alavancar a informatização do processo nas unidades afetas. Possibilitou, aos tribunais, os serviços de organização da intimação das partes e o recebimento de petições pelo meio eletrônico (art. 8º § 2º) sem, contudo, “obrigar” a entrega a *posteriori* da peça física nas unidades judiciárias. Foi além no sentido de possibilitar que as reuniões dos juízes que integravam as Turmas de Uniformização jurisprudenciais, caso estes residissem em cidade diferentes, utilizassem a comunicação eletrônica (§ 3º. do art. 14). Por fim, determinou ao Centro de Estudos Judiciários do Conselho da Justiça Federal e as Escolas de Magistraturas dos

Tribunais Regionais Federais a criação de programas informáticos para subsidiar a instrução das causas e aperfeiçoamento dos magistrados e servidores (art.24).

Os TRF's desenvolveram o e-*processo*, ou simplesmente e-*proc* que possibilitou a "eliminação" do documento físico, dispensando, ainda, a ida dos advogados às sedes dos Tribunais. Se o sistema se apresentasse instável fazia-se necessário o recebimento das peças físicas, as quais eram digitalizadas e entregues aos advogados quando da audiência de conciliação. Quando não logravam êxito, acumulavam-se nos arquivos das unidades judiciárias. Registra-se que o e-proc não oferecia um módulo que garantisse a validade de identificação de usuários, ou seja, qualquer pessoa poderia se passar por outra. Existia, também, a questão da autenticidade dos documentos inseridos.

A partir dessa problemática, produziu-se a Lei 10.358 de 27 de dezembro de 2001, que alterava os dispositivos da Lei nº 5.689 (Código de Processo Civil) com o propósito de combater o problema. Inseriu-se, então, o art. 154, parágrafo único do CPC com a seguinte redação:

> atendidos os requisitos de segurança e autenticidade, poderão os tribunais disciplinar, no âmbito da sua jurisdição, a prática de atos processuais e sua comunicação às partes, mediante a utilização de meios eletrônicos (BRASIL, 2001)

A tentativa não fora recepcionada, pois nesse parágrafo, pois na época o Presidente da República Fernando Henrique Cardoso, vetou, apresentando as suas razões. Fundamentou dizendo:

> A superveniente edição de Medida Provisória nº 2.200 de 2001 que institui a Infra-estrutura de Chaves Públicas e Privadas – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras, que, aliás, já está em funcionamento, conduz à inconveniência da adoção da medida projetada, que deve ser tratada de forma em prol da segurança jurídica (BRASIL, 2002)

O Poder Judiciário, muitas vezes, sempre esteve à frente do seu tempo, à medida que buscava soluções para resolver as questões de informatização dos tribunais. No entanto, o Presidente da República sancionando tal dispositivo no CPC possibilitava que cada tribunal desenvolvesse sistema de certificação eletrônica

próprios, em detrimento de uma padronização técnica unificada. Numa análise temporal, a Medida Provisória (MP) retrocitada já vigorava meses do aludido Projeto de Lei, bastava cumprir.

O veto foi assertivo, pois impossibilitou aos tribunais criarem estruturas próprias de certificação ou filiarem-se a outras. Mais, ainda, objetivou evitar uma insegurança jurídica, pois reconhecia e credencia o ICP-Brasil como certificadora oficial capaz de validar os documentos jurídicos produzidos em relação a terceiros, conforme exposto no art.10 da MP 2.200.

A mensagem presidencial do veto retorna ao Congresso Nacional para adequar-se à MP. Assim, produz-se a Lei 11.280 de 16 de fevereiro de 2006, introduzindo o parágrafo único do art. 154 do CPC com a seguinte redação:

> Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meio eletrônicos, atendidos os requisitos de autenticidade, integridades, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileiras ICP-Brasil

O dispositivo regulador encontra-se vigente, mas vê-se dissonâncias práticas de alguns tribunais que preferem não seguir. O judiciário brasileiro, como instituição de vanguarda para os feitos judiciais eletrônico, vem ao longo dos anos realizando um trabalho de consolidação de marco legislativo para dar legalidade às questões de informatização de seus atos processuais nos tribunais. Mais ainda servir de modelo a outros poderes ou, quiçá, a instituições congêneres de outros países.

Em continuidade ao mapeamento legislativo, identificou-se a Lei 11.341, de 07 de agosto de 2006 que alterou o parágrafo único do art. 541 do Código de Processo Civil – Lei nº 5.689 de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na internet, entre as suscetíveis de prova de divergência jurisprudencial, existindo resistência de uma parte e de outra. Assim, o recorrente, caso entendesse, que cabe recurso especial ou extraordinário, tem a possibilidade de recorrer visando garantir a aplicabilidade do princípio da segurança jurídica.

> Quando o recurso fundar-se em dissídio jurisprudencial, o recorrente fará a prova da divergência mediante certidão, cópia autenticada ou pela citação do repositório de jurisprudência, oficial ou credenciado, inclusive em mídia eletrônica, em que tiver sido publicada a decisão divergente, ou ainda pela reprodução de julgado disponível na Internet, com indicação da respectiva

> fonte, mencionando, em qualquer caso, as circunstâncias que identifiquem ou assemelhem os casos confrontados (BRASIL, 2006)

O dispositivo retrocitado alerta os tribunais para a necessidade de regulamentação no âmbito de suas instituições, visto que a lei estabelece alguns requisitos para o recorrente fazer uso de prova: certidão, cópia autenticada, citação do repositório de jurisprudência ou reprodução de julgado disponível na internet, mencionando sua fonte.

Sob essa perspectiva, o Superior Tribunal de Justiça, atento às modificações legislativas publicou a Instrução Normativa (IN) nº 01, de 11 de fevereiro de 2008, a qual dispôs sobre o registro dos repositórios autorizados e credenciados da jurisprudência, em mídia impressa e eletrônica, e em páginas em portais da Rede Mundial de Computadores.

A IN informa quais serão as publicações válidas e os repositórios oficiais do STJ válidos para os recorrentes fazerem uso deles. Considerou, ainda, como repositórios oficiais de jurisprudências os Tribunais Regionais Federais e Tribunais de Justiça que preenchessem os requisitos: ser certificado pela Infra-estrutura de Chaves Pública Brasileiras (ICP-Brasil); apresentassem a íntegra dos acórdãos; possuíssem base de dados próprias; permitissem a utilização de diversos navegadores e disponibilidade do sítio de no mínimo 99,9%. Atualmente existem 44 repositórios autorizados e credenciados que fazem uso da jurisprudência do STJ.

No mesmo ano, foi sancionada a Lei 11.382, de 06 de dezembro de 2006, que alterou vários dispositivos da Lei nº 5.689 de 11 de janeiro de 1073 – Código de Processo Civil, relativos ao processo de execução e a outros assuntos. Os dispositivos inovaram no sentido de permitir a execução de título extrajudicial ser realizada a penhora *on line* e o leilão *on line.*

Esses institutos possibilitaram a utilização do recurso eletrônico melhorando a prestação jurisdicional. Antes, o juiz expedia ofício ao Banco Central determinando o levantamento de valores nas contas do executado. Esse procedimento poderia demorar dias. Hoje, se houver valores, o juiz realiza o bloqueio até o valor da dívida e intima o executado para se manifestar. Não contestando considerar-se-á verdadeiros os fatos da inicial.

Todas as leis sancionadas serviram para que o judiciário fosse implementando soluções paulatinamente, as quais serviram para melhorar a prestação jurisdicional, pois o que se torna mais prejudicial à população é a

morosidade da justiça. O quadro que se apresentava reverteu-se com auxílio da tecnologia que vem transformando as instituições judiciárias em ilhas de excelência.

O ciclo legislativo avança e completa-se com a aprovação da Lei 11.419 de 14 de dezembro de 2006 que dispôs sobre a informatização do processo judicial; altera a Lei nº 5.869 de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

O Capítulo I trata da informatização do processo judicial utilizando-se do meio eletrônico para a tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais (art.1º), mas requer que todas as práticas processuais sejam realizadas mediante a assinatura eletrônica.

O Capítulo II, possibilitar aos tribunais a criação do Diário da Justiça eletrônico, via sítio da rede mundial de computadores, objetivando publicizar seus atos através deste meio.

Já no Capítulo III, refere-se ao processo eletrônico diz que os tribunais poderão desenvolver sistemas para o processamento das ações dos autos totais ou parcialmente, utilizando-se preferencialmente, da rede mundial de computadores cujo acesso será por meio de redes internas ou externas (art.8º). Os atos serão assinados eletronicamente para que esta possua validade.

Os documentos digitalizados e juntados aos autos dos órgãos da justiça e seus auxiliares, o Ministério Público e seus auxiliares, as procuradoria, as autoridades policiais, repartições públicas e advogados tem a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada antes ou durante o processo de digitalização (§1º). Poderá ser arguida a falsidade documental antes ou durante a fase de digitalização. Constatada alguma “irregularidade” posterior à finalização da digitalização não prospera, visto que precluiu o direito.

Se houver sido arguida a falsidade da documentação a lei determina a preservação pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para a interposição de ação rescisória, conforme prevê o art. 11§ 2º.

Quando se tratar de grandes volumes ou ilegibilidade determina a lei o seu processamento físico e após o trânsito em julgado estes serão devolvidos aos seus detentores.

Os tribunais deverão desenvolver sistemas e construir uma política de gestão de processos e documentos que garantam a segurança, a integridade, e a

preservação da informação em todo o seu ciclo de vida, pois o meio digital possui particularidades e são necessárias soluções para combater:

> a fragilidade intrínseca do armazenamento digital (degradação física do suporte); rápida obsolescência da tecnologia digital (*hardware*, *software* e formatos); Necessidade de tratamento adequado das entidades integrantes do documento digital: objeto físico (suporte), lógico (software e formatos) e conceitual (conteúdo); complexidade e custos da preservação digital e complexidade dos controles para garantir a autenticidade, a confidencialidade, a integridade e a disponibilidade desses documentos (CONARQ, 2004)

Chama-se atenção para o art.12 § 5º da Lei 11.419 que diz:

> A digitalização de autos em mídia não digital em tramitação ou já arquivados será precedida de publicação de editais de intimações ou da intimação pessoal das partes e de seus procuradores, para que, no prazo preclusivo de 30 (trinta) dias, se manifestem sobre o desejo de manterem pessoalmente a guarde de algum dos documentos originais.

A análise deste parágrafo apresenta informações importantes, pois como se tratava de procedimento “novo” a virtualização/processo eletrônico, a publicidade dos atos era fundamental. Alinhado a esse corolário permitiu que o tribunal, ao iniciar o processamento eletrônico dos autos em mídia não digital (suporte físico), em tramitação, possibilitasse às partes e/ou advogados a manifestação de ter para si algum dos documentos originais, no prazo preclusivo de 30 dias.

Na mesma esteia de informações importantes que o aludido parágrafo traz, ratifica-se a necessidade de ser ter arquivista(s) atuando em sintonia com a unidade responsável quer seja na discussão de um planejamento estratégico voltado para o processo eletrônico, quer seja na pronta resposta à administração superior da necessidade ou não de digitalização dos autos já arquivados (fase intermediária), pois se empreender esforços no sentido de implementar uma política de gestão da informação, torna-se desnecessária a digitalização de processos arquivados.

Em sua maioria, as instituições judiciárias, fizeram vistas grossas para o sobredito parágrafo, atropelando o rito, na perspectiva de digitalizando os autos em tramitação tornar-se-iam mais céleres. Em certa medida conseguiram, visto que, dentre muitas vantagens, com os autos digitalizados a visualização torna-se mais rápida e as decisões dos juízes são conhecidas quase que em tempo real. Na outra ponta estão os arquivos dos tribunais, os quais se encontram no, mínimo, com os espaços físicos abarrotados ou chegando ao seu limite. Sobrevém os documentos judiciais digitalizados para, também, ser gerenciado por essas unidades.

O capítulo IV que trata das disposições gerais e finais reforça a necessidade do desenvolvimento de sistemas que possuam código aberto. Muitos tribunais, sobretudo, os de justiça antes do advento do processo eletrônico tornavam-se dependentes de sistemas privados e se despendiam um grande monta do orçamento da instituição para pagar às empresas a utilização do *software*.

Quando se utiliza o *software* livre tem-se como uma grande vantagem o não pagamento de licenças de uso. Isso pode representar, significativamente, no orçamento de um tribunal percentual que poderiam ser investidos na aquisição de mais computadores, na política de treinamento, na melhoria da banda larga da internet etc.

O processo eletrônico hoje nos tribunais é algo irreversível. Nesse diapasão e atento a essa evolução de virtualização nos tribunais, Conselho Nacional de Justiça (CNJ) chama para si a responsabilidade do desenvolvimento de:

> [...] um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais pelos magistrados, servidores e demais participantes da relação processual diretamente no sistema assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho. (TUPINAMBÁ, 2011)

Esse esforço, alinha-se as muitas iniciativas oriundas do Conselho objetivando que os tribunais de todo o país possuam um sistema único, gratuito que contenham, dentre outros os requisitos de segurança, confidencialidade, interoperabilidade, trilha de auditoria, etc.

Mais recentemente sobreveio a Lei 12.527, de 18 de novembro de 2011 que regulou o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; alterou, também, a Lei 8.112, de 11 de dezembro 1990; revogou a Lei nº 11.111 de 5 de maio de 2005 e dispositivos da Lei nº 8.159, de 08 de janeiro de 1991. Ela surge para regulamentar o acesso a informações públicas e na tentativa de dar mais transparência as ações dos Poderes da União, Estados, Distrito Federal e Municípios, permitindo à sociedade cobrar dos representantes melhoria na gestão pública.

A Constituição Federal (CF), no inciso XXXIII do Capítulo I – dos Direitos e Deveres Individuais e Coletivos – dispõe que:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

A CF de 1988, mais conhecida como Constituição cidadã inovou trazendo à lume o Capítulo I, que dispõe sobre os direitos e deveres individuais e coletivos. Destaca-se no arcabouço legislativo deste capítulo a obrigação dos órgãos públicos prestarem as informações de interesse particular ou interesse coletivo ou geral, resguardando aquelas cujo sigilo era imprescindível. Todavia, ela não informava qual era o prazo do requerente para o recebimento das informações e se não prestasse quais seria as suas penalidades.

A Lei 12.527/2011 segue a tendência internacional de muitos países que já possuíam regulamentações sobre o direito de acesso. Em análise, a lei abrangeu todos os poderes e todos os entes federativos e, ainda, as entidades privadas sem fins lucrativos que recebem recursos públicos. Tendo como premissa básica que o sigilo é a exceção e o acesso à informação como regra.

Destacam-se os principais comandos da Lei para simplificar o seu entendimento: o franqueamento das informações de forma ágil, transparente, clara e de fácil compreensão; a disponibilização de informações de interesse público independentemente de solicitações; a gestão da informação de forma transparente, objetivando o seu amplo acesso. Esses principais comandos dão mostra da necessidade de profissionais de arquivologia em projetos que visam gerenciar a informação desde a sua produção até a destinação.

A Lei de Acesso à informação (LAI) trouxe ainda conceitos de informação, documento, informação sigilosa, informação pessoal, tratamento da informação, disponibilidade, autenticidade, integridade e primariedade. Neste arcabouço conceitual considerado pela LAI, traz-se à discussão o tratamento da informação: "*conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação".* (BRASIL, 2011). Ele sintetiza o trabalho de uma instituição preocupada com o gestão da informação desde o nascedouro, visando o controle e gerenciamento desta.

Prevê, ainda, um conjunto de obrigações mínimas que o administrador precisa para divulgar as informações na internet (transparência ativa); a não existência da motivação do pedido, o qual tem um período de 20 dias para ser respondido, prorrogável por mais 10 dias (transparência passiva). Manteve a proteção de dados pessoais, relativas à intimidade, vida pública, honra e imagem das pessoas, cujas exceções são: expresso consentimento da pessoa; apuração de irregularidade, cumprimento de ordem judicial, defesa dos direitos humanos e proteção de interesse público preponderante.

Tratou, por fim, de excluir a classificação denominada "confidencial". Ratificou a classificação da "reservada" em 5 anos. Diminuiu em 5 anos as classificações "ultrassecretas" e "secretas". Nessa perspectiva LAI se diferencia, pois estimula à disponibilização de dados (caráter inovador) juntando-se às demais leis vigentes dos países que regulamentaram o acesso.

2.3 Problema da pesquisa

Hoje as instituições judiciárias estão com esforços concentrados para digitalização e focam-se tão-somente para isso, não percebem que em breve poderão ser questionadas sobre como estão sendo preservadas essas informações. Importam-se, algumas, em adquirir *Data Centers*[4] e depositar toda a confiança neles, mantendo-os incólumes.

Observa-se que as instituições judiciárias, por hora, não estão se voltando para as questões de preservação digital. Muitos sistemas vem sendo desenvolvidos por profissionais de várias áreas: administradores, analistas de TI e muitas vezes não existem um diálogo dos profissionais da TI com os de Arquivo. Vendem uma ideia, equivocada, para a administração superior de que a digitalização/virtualização

[4] É uma modalidade de serviço de valor agregado que oferece recursos de processamento e armazenamento de dados em larga escala para que organizações de qualquer porte e mesmo profissionais liberais possam ter ao seu alcance uma estrutura de grande capacidade e flexibilidade, alta segurança, e igualmente capacitada do ponto de vista de hardware e software para processar e armazenar informações. Disponível em:< http://www.projetoderedes.com.br/artigos/artigo_datacenter.php>. Acesso em: 19 de abril de 2013.

resolverá todos os problemas relacionados ao acesso, gerenciamento etc., mas onde fica a preservação digital?

Após a aprovação da Lei 11.419 de 19 de dezembro de 2006, observou-se que instituições judiciárias vêm passando por essa transição e se o processo de virtualização não for devidamente planejado e exaustivamente discutido com a administração superior estes poderão estar fadados ao fracasso no tocante à preservação da informação no meio digital. Ademais, a sociedade contemporânea passar por um dinamismo, o qual não permite amadorismo ou testes, sobretudo, quando se trata do Poder Judiciário. Os requerentes buscam resolver os conflitos jurisdicionais, muitas vezes trazem à baila questões complexas para serem decidida, tais como: o direito a vida, à liberdade, etc.

A informação, em sua essência, precisa ser preservada, mas não é apenas adquirindo *storages*[5] que se resolverá a questão da obsolescência tecnológica. Eles são uma parte de e não o conjunto de estratégias para a preservação digital. É mister construir conjuntamente com os setores de TI e Arquivo modelos e padrões que permitam a gestão e preservação da documentação digital por longo prazo. Nesse sentido, destaca-se a reportagem do Diretor do Arquivo Nacional, Prof. Jaime Antunes (2012), durante evento realizado na UNICAMP sobre preservação digital:

> São necessários requisitos para aquilo que não é tangível, como os documentos digitais. Portanto, se o documento passou por reformatação, ele não pode ser corrompido. Um bom programa de gestão vai garantir capacidade de acompanhamento, de ter cópia de segurança, de ter garantias de que ele possa ser permanente enquanto informação e possa ser acessado a qualquer momento (ANTUNES, 2012)

Existe, também, uma corrente que está pensando em, primeiramente, digitalizar todo o acervo e a *posteriori* verificar o desenvolvimento de métodos que contemplem a conservação desses suportes. Refuta-se, que adiar o desenvolvimento de uma política de preservação digital é praticamente comparar com uma doença que o ser humano adquire, a qual fica protelando os cuidados, quando ele resolver tratar-se poderá estar em estágio avançado e não terá mais condições de ter a cura plena.

---

[5] *Storage* é um hardware que contém slots para vários discos, ligado aos servidores através de ISCSI ou fibra ótica. O storage é uma peça altamente redundante e cumpre com louvor a sua missão, que é armazenar os dados [...]. Disponível em:< http://www.infob.com.br/site/hardware/storage-um-item-essencial/>. Acesso em 19 de abril de 2013.

Há de se ressaltar, também, que o procedimento de digitalização pode, muitas vezes, ficar a cargo de empresas terceirizadas, as quais não se preocupam com a qualidade e sim a quantidade de imagens digitalizadas por segundo. Do outro lado, está a contratante que não exerce o poder de fiscalizar da forma imposta contratualmente quer seja pela acúmulo de atividades ou por acreditar que estas empresas possuem *know-how* e *expertise* necessárias para desenvolver a atividade licitada. Os efeitos só serão sentidos posteriormente quando se identificar alguma situação que esteja fora da normalidade. Adiciona-se, também, a questão da inserção dessa documentação digitalizada em sistemas que não contemplem metadados[6] necessários à recuperação das peças do processo digital.

A sociedade contemporânea está altamente dinâmica. Isso é fruto da revolução tecnológica, pelo menos, nos últimos 15 anos com a consolidação da Web. Hoje não é permitido o amadorismo em questões envolvendo a preservação digital. Estabelecer padrões e melhores práticas é o assunto que está em voga.

Portanto, faz-se necessário empreender esforços para os estudos preservacionistas que contemplem o acesso por longo prazo e privilegiem ações integrais desde a sua produção e pelo tempo de guarda que for definido em tabela de temporalidade de documentos em tramitação que foram digitalizados e aqueles que já nascem digitais.

Na perspectiva de contribuir, na vida acadêmica, tentar alertar e colaborar com os tribunais que estão migrando para o meio digital, desenvolveu-se a seguinte problematização: Como está sendo aplicada a preservação digital nas instituições judiciárias?

[6]Definindo o prefixo “meta” como primeiro elemento de compostos eruditos com a ideia de “mudança”, “posterioridade”, “além”, “transcendência”, “reflexão crítica sobre” o que nos remete à ideia de metalinguagem, ou seja, “linguagem para descrever outra linguagem ou qualquer sistema de significação: todo discurso acerca de uma língua, como as definições dos dicionários as regras gramaticais, etc (FERREIRA, 1986).

2.4 OBJETIVO GERAL

Identificar as estratégias de autenticidade eletrônica dos processos judiciais adotadas pelo Tribunal de Justiça do Amazonas.

2.4.1 Objetivos Específicos

- Contextualizar as estratégias preservação digital existentes na literatura;
- Verificar se as estratégias de preservação digital encontradas estão enquadradas na etapa da criação de uma política de preservação digital;
- Apontar a existência de regulamentações institucionais que serviriam como início de uma política de preservação digital;

2.5 Justificativa

No ano de 2005, iniciava a trajetória de melhorar e democratizar a prestação jurisdicional no Tribunal de Justiça do Amazonas (TJAM), através do projeto denominado “Justiça Efetiva”. A proposta do projeto era a integração das Comarcas do interior com o TJAM, o STJ e o STJ, por link de satélite do SIPAM, para trafegar dados, voz e imagem, possibilitando minorar a falta de infraestrutura, agravada pela vastidão territorial do Estado, o baixo índice populacional, a grande concentração econômica da Capital.

Até esse mesmo ano, o Amazonas possuía 57 Comarcas no interior do Estado cujo percurso entre elas e Manaus é de até 15 dias de viagem por barco, se o rio estiver navegável. Caso contrário o acesso só será possível por avião, nos municípios com campo de pouso. Somente cinco municípios tinham ligação rodoviária com a Capital. Só alguns deles possuíam transporte aéreo com frequência regular; a maioria, não tinha campo de pouso.

Como se trata de um Estado *sui generis*[7], identificaram-se alguns problemas que necessitavam de soluções, quais sejam: completo isolamento físico das serventias do interior, a ausência de instrumentos modernos de trabalho e a falta de

[7] Forma única de ser, singularidade. Disponível em:< http://www.dicionarioinformal.com.br/sui%20generis/>. Acesso em: 14 de nov de 2013.

treinamento e de capacitação dos servidores.

Às dificuldades expostas, somam-se às necessidade: dotar as Comarcas de uma ferramenta de trabalho adequada à melhoria do serviço e prestação jurisdicional; gerar processos de trabalho e conduta homogênea dentro da Instituição, com utilização da mesma ferramenta de trabalho usada na Comarca de Manaus. O projeto continha “Justiça Efetiva” perlustrava sete objetivos:

> 1º: Ligar a sede do TJA à rede de telecomunicação por satélite do SIPAM, através de um link de voz de 64 Kbps, com o quê o TJA poderá se comunicará por telefone e fax com todas as 43 Comarcas onde têm terminal remoto instalado por aquele Órgão;
> 2º: Ligar o Fórum de Manaus à rede de telecomunicação por satélite do SIPAM, mediante instalação de um link de dados de 256 Kbps;
> 3º: Instalar e implementar o SAJ nas 43 Comarcas do Interior onde têm instaladas antenas VSAT/SIPAM, a) inicialmente, em rede local, interligando os Juizes, os Cartórios, o Ministério Público e a Defensoria Pública; e b) na rede de telecomunicação do Poder Judiciário do Amazonas, à medida que forem sendo configuradas as rotas de comunicação para acesso ao banco de dados em Manaus;
> 4º: Instalar e implementar o SAJ nas 14 Comarcas do Interior do Estado onde não têm instaladas antenas VSAT do SIPAM;
> 5º: Cumpridos os objetivos 1º ao 4º, conectar referida rede ao PORTAL do STF, objetivando a conectividade ao STF, STJ e Conselho Nacional de Justiça;
> 6º: Interligar a rede AMAZONJUS à Rede Metropolitana de Manaus (METRO-MAO), uma rede em fibra óptica, em forma de anel, a ser erigida na Cidade de Manaus, entrelaçando pela comunicação órgãos públicos federais, estaduais e municipais, órgãos de pesquisa, ensino e saúde e;
> 7º: Interligar a rede AMAZONJUS ao barco Catuiara do projeto “Justiça e Cidadania”, para facilitar a comunicação “on-line” de dados e imagens, da prestação jurisdicional à população ribeirinha, no que tange a registros civil, de casamento e óbito, concessão de carteiras de identidade e de solução de conflitos. (BANDIERA, 2006)

Esse, talvez, tenha sido o primeiro esforço concentrado e planejado do TJAM para a trafegabilidade de dados, voz e imagem do interior para a capital, através de sistema informatizado. A partir deste projeto e acompanhando as mudanças legislativas a partir 1995 quando da publicação da Lei n. 9.099, que dispôs sobre a criação dos Juizados Especiais Cíveis e Criminais (JECCs) e entre seus artigos e incisos possibilitou a gravação dos atos em fita magnética ou equivalente, as quais depois do trânsito em julgado da decisão, poderiam ser inutilizadas.

Na perspectiva de se cooperar e melhorar o acesso à justiça no Estado do Amazonas e sob as justificativas de: crescimento na demanda cível de processos distribuídos nos Juizados Especiais Cível, provocando a dilatação cada vez maior para a realização de audiências de instrução; do Projeto “Justiça Efetiva”, o qual visa

informatizar todo o interior do Estado do Amazonas para iniciar a implantação do processo virtual em todos os municípios do Estado; na redução de despesas com pessoal, diante da desnecessidade de realização de uma série de rotinas processuais com a implantação do procedimento virtual, aprovou-se em 24 de agosto de 2006, Resolução nº 10/2006-TJAM, que Determinava à Coordenadoria Geral dos Juizados Especiais Cíveis e Criminais que desse início à implantação gradual de processo eletrônico (virtual) em todos os Juizados Especiais Cíveis e Criminais da Capital, nos moldes do Projeto "Justiça Efetiva", devendo estar em pleno funcionamento até o final do mês de novembro daquele ano.

O TJAM ao aprovar a Resolução sobredita, apostava todas as fichas nas vantagens que o processo virtual traria para a instituição. O conteúdo do ato normativo apresenta os seguintes aspectos: A criação de comissões para a implementação rápida do procedimento virtual (Art.1º § 1.º); estudos para a implementação da gravação de audiências realizado pela Coordenadoria do Juizados Especiais Cíveis e Criminais (Art.1º § 3.º); Com o suporte da Coordenadoria de Informática, determinou-se a implementação do serviço de peticionamento eletrônico, por intermédio de portal eletrônico, disponível às partes e advogados mediante a certificação (Art. 3º).

Passados cento e dez dias do ato normativo supramencionado, o TJAM edita novo marco regulatório – a Resolução nº 14 de 14 de julho de 2006 – que dispôs sobre a virtualização da 5ª, 8ª, 9ª e 10ª Varas de Família, Sucessões e Registros Públicos da Comarca de Manaus. Esta não trouxe inovações conceituais ou de praxes, apenas ampliou as unidades judiciárias que passariam a processar os feitos virtualmente.

No dia 19 de dezembro de 2006 é sancionada a Lei 11.419 que trata de regular a informatização do processo eletrônico no âmbito do Poder Judiciário. Tal ato, foi um divisor de águas nos tribunais visto que determinava a eles o desenvolvimento de sistemas e a construção de uma política de gestão de processos e documentos que garantissem a segurança, a integridade e a preservação *da* informação em todo o seu ciclo de vida. Essa medida asseguraria o armazenamento de dados sob o formato digital por longo prazo.

Mais uma vez o TJAM avança na produção de outro ato regulatório, a Resolução nº 27, de 26 de dezembro de 2007, construída após a promulgação da lei do susomencionada. Esta, portanto, tratou de implantar o processo eletrônico nas

Varas Especializadas em Crimes de Uso e Tráfico de Entorpecentes (VECUTE), a qual predizia: enquanto não houver um equílibrio quantitativo de processos entre as três varas especializadas, apenas a terceira vara receberá e funcionará com processo eletrônico (Art. 2º).

A trajetória do processo informatizado no TJAM foi construída, praticamente, através de ações mais práticas. Não se identificam registros de um projeto descrito e divulgado para os usuários internos (servidores e magistrados), usuários externos (partes e advogados) e a sociedade em geral, onde sejam visualizadas as etapas de implementação e seu desenvolvimento iniciados na digitalização dos autos físicos (suporte papel) daqueles já recebido no meio virtual (nato digitais).

Nesse diapasão é apresentado por Arellano um conceito bastante abrangente quando se pensa a preservação digital:

> Em meio digital, a preservação digital compreende a preservação **física, lógica e intellectual dos documento digitais**. A preservação física está focalizada nos conteúdos armazenados em suportes magnéticos (casseste, *VHS*, cassetes de música etc.) e nos suportes ópticos (CD-ROM`s, discos, *WORM* etc.), que levam à necessidade de definição de regras para a migração dos formatos em que os documentos estão registrados. A preservação lógica procura na tecnologia formatos atualizados para a introdução de dados (material audiovisual, correio eletrônico etc.) e novas aplicações de *hardware* e *software* que mantenham em atividade os seus *bits* para conservar a sua capacidade de leitura. (ARELLANO 2004, p.17) (grifo nosso)

Conforme demonstrado pelo autor, refuta-se a ideia de preservação digital atrelada somente aos armazenamento da informação em *storages*, como pensam a maioria dos informáticos. Ferreira (2006, p. 20) diz que é necessário um “conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação e restante património cultural existente em formatos digitais”. Em continuidade reitera a necessidade atrelar-se, ainda, ao conteúdo, ao contexto e a estrutura “para garantir que a informação digital permanence acessível e com qualidades de autenticidade suficientes para [..] ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação”. (Ferreira, 2006, p.20).

Em 02 de julho de 2012, o sítio CBN Manaus, blog Ronaldo Tiradentes

noticiava: “Sistema SAJ do Tribunal de Justiça segue fora do ar”[8], o qual relatava a seguinte situação:

> O site do Tribunal de Justiça está for a do ar neste momento. Há mais de 10 dias que o sistema estava funcionando precariamente.
> O peticionamento eletrônico está inoperante. Várias audiências estão sendo suspensas por causa da falta de acesso aos processos.
> O TJAM não se manifestou até agora para explicar o que está acontecendo. (TIRADENTES, 2012)

Já no dia 03 de julho de 2013, o advogado Christhian Naranjo[9] publicava em seus blog a seguinte notícia: “O grande culpado”

> O caos que vivemos está ligado aos novos equipamentos/softwares do TJAM, que fazem as máquinas travarem. Em virtude de demora na licitação, compra e entrega do novo servidor de “backup”, não houve tempo para a realização todos os testes necessários, mas mesmo assim, os novos servidores foram postos em atividade. Tantos foram os travamentos que o funcionamento do banco de dados do primeiro grau foi comprometido. Acionaram os fornecedores/fabricantes para identificar a causa e a solução, até agora desconhecida, mas uma coisa é certa: o SAJ nada tem a ver com o caos que vivemos.
> As redes de todos os fóruns estavam sendo refeitas, um anel de fibra ótica estava em implantação quando o projeto simplesmente parou, pergunta-se: ordem de quem?
> Para minimizar o estrago, o servidor antigo deve retornar até que os novos sejam devidamente configurados, permitindo então o restabelecimento dos serviços essenciais, entre eles o S.A.J. (NARANJO, 2013)

Ambos os sítios traziam informações a respeito da inoperância do Sistema de Automação Judicial (SAJ) iniciada no dia 29 de junho de 2012 que perdurou até o dia 03 de julho de 2013, ou seja, durante 05 (cinco) dias as atividades judiciárias e administrativas praticamente não funcionaram, visto que tanto os sistemas administrativos quanto os judiciais são gerenciados por sistemas privados.

Registra-se, por oportuno, que essa inoperância, afetou milhares de cidadãos que buscaram durante esses dias o judiciário na tentativa de resolverem seus conflitos. Mais ainda, impossibilitou, talvez, ao magistrado decidir questões urgentes.

Sem acesso pleno aos sistemas informatizados a presidência do TJAM publicou a Portaria n.1.662 de 03 de julho 2012, com os seguintes considerandos:

---

[8] Disponível em: <http://www.cbnmanaus.com.br/ronaldotiradentes/sistema-saj-do-tribunal-de-justica-segue-fora-do-ar/>. Acesso em 15 de agosto de 2013.

[9] Disponível em:< http://www.diariodeumadvogado.adv.br/2012/07/03/a-verdade-sobre-o-s-a-j/>. Acesso em 15 de agosto de 2013.

> CONSIDERANDO a indisponibilidade do sistema da Automação Judicial – SAJ nos dias 29/06; 02/07 e 03/07, no âmbito do 1º Grau, na Capital, por força de manutenção no sistema e migração do banco de dados para os novos equipamentos adquiridos pelo Tribunal de Justiça;
> CONSIDERANDO que a indisponibilidade resultou, inclusive, na impossibilidade de acesso à visualização aos processos judiciais eletrônicos, dificultando, por isso, até o peticionamento por meio físico;
> CONSIDERANDO que o sistema de automação judicial será restabelecido no decorrer do dia 03 de julho do corrente ano;

Assim, ficaram suspensos os prazos processuais no período de 29 de junho de 2012 a 03 de julho do ano corrente (Art. 1º). Apesar da presidência assumir o *mea culpa* não se pode quantificar os prejuízos advindo das manutenção ou migração do banco de dados que causaram a paralisação dos sistemas.

Como exemplo real e fato motivador para o desenvolvimento desta pesquisa, pode-se citar: O setor de licitação vem desenvolvendo suas atividades de forma virtual, conforme determinou a administração superior. Tudo ocorre dentro da normalidade, licitações em andamento, outra já homologadas e assinadas digitalmente pelo ordenador de despesa, edital de intimação publicado convocando o(s) vencedor(es) etc. O presidente da licitação recebe uma ligação do licitante questionando várias coisas, dentre as quais ele informava que foi conferir a autenticidade do documento assinado pelo presidente, mas não estava registrada na entidade certificadora. Então, o servidor informou que formalizasse o pleito e encaminhasse à presidência para verificar a questão.

Como se observa, não se pode atribuir credibilidade total a sistemas eletrônicos quando não se tem perspectiva de se implantar, desde o início, uma política de segurança, de trilha de auditoria, de política de *back-up*, de preservação digital, dentre outras. O fato relatado, apesar de referir-se à documentação administrativa, ilustra bem o grande desafio que os profissionais da informação têm pela frente e, inexoravelmente estes, ser-lhe-ão postos à prova para dar soluções a essas e outras questões em termos de gestão da documentação produzida no meio digital.

Outra questão importante a ser observada, durante a trajetória de utilização de sistemas de automação para o judiciário amazonense diz respeito à migração de sistemas, isto porque toda ação tem sua consequência, perda de dados. Isto é um fato. Anterior ao ano de 2002, os processos físicos eram gerenciados pela empresa de Processamento de Dados do Amazonas S/A, cuja razão social dela é uma

sociedade de economia mista, de capital fechado, com controle acionário do Governo do Estado. Foi criada pela Lei N° 941, de 10 de julho de 1970, tendo iniciado suas operações em setembro de 1972.

A partir do ano supra, o TJAM contratou uma empresa privada – SOFTPLAN/POLIGRAPH - para fazer o gerenciamento dos processos físicos da capital. Sua trajetória no desenvolvimento de sistemas vem desde a década de 90 quando iniciou as suas atividades. No poder judiciário amazonense, ampliou suas atividades não somente gerenciando os processos físicos judiciais, mas também os administrativos e recentemente os digitais tanto das áreas meio quanto a fim.

Para as comarcas do interior, primeiramente, os processos começaram a ser gerenciados por um sistema *off-line*, desenvolvido por servidor do TJAM, conhecido como SISPRO. Funcionava, basicamente, como um sistema de registro de movimentação e localização física no cartório. Algumas comarcas que possuíam Juizados Especiais Cíveis e Criminais, em história recente, aderiram ao Projudi disponibilizados pelo CNJ, tendo funcionado até o final do ano de 2012. Na cerimônia de lançamento do PJe, em maio do mesmo ano, na Comarca de Iranduba, distante 22Km da Capital, o juiz auxiliar da presidência, Roberto Taketomi observou que "a Justiça já trilhava o caminho da modernização desde 2006, através do Projudi". Em continuidade, destacou[10] que:

> O CNJ interrompeu o processo porque identificou que não era a ferramenta ideal. Chegamos a instalar os sistemas de tramitação eletrônica em algumas comarcas do interior, mas os múltiplos sistemas acabaram criando barreiras para o trabalho dos advogados, que precisam se adaptar a cada uma das plataformas. (TAKETOMI, 2012)

O evento supramencionado, tratava de inaugurar mais uma fase no TJAM, a implantação de mais um sistema – Processo Judicial Eletrônico (PJe) – concebido e desenvolvido pelo CNJ. Entretanto, o projeto, no momento, foi abandonado para ser utilizado um outro sistema, o Projudi-PR. Este foi cedido pelo Tribunal de Justiça do Paraná (TJPR), o qual está sendo implantado nas comarcas do interior do Estado. Optou-se por ele, visto que é considerado o mais estável, o mais seguro e o que serve de referência para todos os tribunais. Todavia, não se descartou a hipótese de adoção do PJe no futuro. A justificativa para não utilização, por hora, dele no TJAM

[10] Disponível em: http://www.cnj.jus.br/noticias/judiciario/19469-pje-e-instaurado-em-iranduba-pelo-tjam>.Acesso em 17 de jul. de 2013.

é que se encontra em fase de desenvolvimento pelo CNJ.

Muitas questões têm sido discutidas pelo mundo a fora. EUA, Canadá, Austrália e Reino Unido, têm se destacado sobre o desenvolvimento de uma política de preservação digital. Apesar de haver conectividade em relação as estratégias já desenvolvida pela comunidade Internacional até o momento, existe uma lacuna por parte do Poder Judiciário, onde não se verificam informações sobre uma política nacional.

No obstante às questões relatadas, tratar-se-á, especificamente, da assinatura digital como elemento garantidor de autenticidade, integridade, confiabilidade e não-repúdio aos documentos digitais produzidos e recebidos durante a trajetória de virtualização das unidades organizacionais de um tribunal no estado do Amazonas

Preservar digitalmente os documentos é o grande desafio do século XXI. Primeiramente, é necessário convencer as administrações e alocar grandes recursos para o desenvolvimento de tecnologias. Arellano tem advertido nesse sentido:

> É preciso chamar a atenção para a importância de informar o contexto do objeto digital a ser registrado (e preservado) para que, dessa maneira, futuros usuários possam entender o ambiente tecnológico no qual ele foi criado. A preservação dos documentos continua a ser determinada pela capacidade de o objeto informacional servir às utilizações que lhe são imputadas, às suas atribuições que garantem que ele continue a ser satisfatório às utilizações posteriores. (ARELLANO 2004, p.15)

Problemas de toda a ordem podem surgir na complexa missão de virtualização e digitalização da documentação administrativa quanto à judicial. De nada adianta, por exemplo, realizar um esforço concentrado nos processos judiciais em trâmite transformando-os em virtuais se não tiver, também, uma definição de estratégias, políticas e técnicas, as quais visam garantir a preservação e acessibilidade destes dados ao longo do tempo.

Indubitavelmente, pretende-se com este tema trazer à baila a discussão da preservação digital, quer seja no âmbito local, quer seja nacional. Mais, ainda, tentar alertar e conscientizar as administrações superiores dos tribunais sobre a importância de se garantir a inalterabilidade dos registros digitais desde à concepção do documento digital.

2.6 HIPÓTESE

Apesar de o suporte em papel ser considerado a mídia mais estável, os tribunais têm emprendido esforços de toda a ordem para substitui-lo pelo meio digital. Decerto, este possui vantagens se comparado ao físico, mas também apresentam problemas de ordem técnica que necessitam de solução, pois com esse avanço tecnológico, as instituições judiciárias têm deixado muitas questões, tais como a autenticidade, os riscos e às vulnerabilidade que os sistemas podem apresentar para ser tratada em outro momento o que colabora com o que Sayão (2006) chamou de amnésia digital.

As instituições judiciárias vêm acelerando o processo de digitalização e virtualização no âmbito das suas unidades organizacionais. Embora possam perceber a preocupação que os usuários têm em conhecer a origem, a história, a qualidade e a utilidade da informação que disponibilizam, não vem atuando de forma proeminente no sentido de apresentar soluções adequadas para a preservação digital.

Presume-se que as questões supramencionadas quando tratadas em segundo plano, vão de encontro com os princípios que a Arquivologia preconiza, visto que não se terão garantias de acesso ao processo judicial digital a médio ou a longo prazo. Ademais, projetos dessa envoltura são, muitas vezes, desenvolvidos e gerenciados pelas TIs que não contam com a participação de profissionais de arquivo para que juntos possam desenvolver diretrizes que garantam a perenidade e acessibilidade ao processo judicial eletrônico.

Assim, reforça-se a investigação acerca da assinatura digital como requisito de autenticidade aos processos judiciais digitais visando garantir a integridade e comprovação de autoria aos documentos arquivísticos digitais, as quais convergirão em uma política de preservação digital.

3. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados os conceitos relacionados à arquivologia, o qual passa do conceito básico do que é o documento até chegar a preservação digital, objeto desta investigação.

3.1 **Arquivologia:** conceitos iniciais

A palavra documento é comum ao vocabulário cotidiano. Das bases de registros pessoais às relações sociais interligam-se as informações básicas, que asseguram a identidade, a atividade, as obrigações e os direitos. Essas informações estão invariavelmente registradas no que chamamos de documento. Algumas delas são importantes e outras fundamentais. Há informações, entretanto, que são pouco interessantes e outras que possuem valor tão-somente histórico.

Para definir documento, Paes utiliza-se da seguinte definição:

> Documento - registro de uma informação independentemente da natureza do suporte que a contém.
> Documento de arquivo – 1. Aquele que, produzido e/ou recebido por uma instituição pública ou privada, no exercício de suas atividades, constitua elemento de prova ou de informação. 2. Aquele produzido e/ou recebido por pessoa física no decurso de sua existência. (PAES, 2004, p.26)

A autora esclarece, de uma forma didática, que independentemente de seu suporte, a informação pode tornar-se um documento. Porém, os documentos de arquivo que nascem na instituição ou são delas recebidos, quando reunidos, constituem um fundo documental e as informações neles contidas devem ser preservadas para fins de prova ou de informação.

Referenciando documento em Direito, obteve-se a conceituação de ser “um objeto corpóreo, resultado da atividade humana, que pelos vestígios de confiabilidade, representa, por si só, permanentemente, um fato idôneo” (WIKIPÉDIA, 2013)

Constata-se, juridicamente, que se dá ao documento uma representatividade e confiabilidade permanentemente idônea, ou seja, ele é capaz de bem exercer sua função nas organizações: fornecer informação, a qual se obtém através dos

resultados das atividades humanas.

Guinchart e Menu (1994, p.41) dizem que “documento é um suporte material do saber e da memória da humanidade”. É, por conseguinte, todo e qualquer suporte físico, palpável, gráfico, iconográfico, plástico, fonético, onde o indivíduo pode se expressar e fixar suas informações por um tempo durável, transmitindo e testemunhando as atividades humanas.

Observa-se, então, que, sob as mais diversas formas, o homem tem produzido e armazenado a informação. Isto só foi possível, porque houve a evolução do conhecimento e os mais diversos suportes acompanharam esse progresso, do surgimento do papel ao advento do computador.

Sob esse enfoque verifica-se, indelevelmente que a informação representa uma ponte para o conhecimento, alterando o cognitivo de quem a recebe. Estimula, ainda, a buscá-la incessantemente de modo a ser disseminada por outros que a procuram.

Partindo para o conceito de documento de arquivo definido por Delmas (2010, p.62) assim diz: “documento de arquivo é o resultado de uma ação passada que se pretende guardar, ao longo do tempo, por um prazo mais ou menos extenso, para necessidades futuras”. Se perguntássemos às pessoas comuns para quê elas guardam os documentos particulares (certidão de nascimento, certidão de casamento, certidão de óbito etc), talvez obtería-se a mesma resposta, mas de forma simplificada: para provar algo.

Nesse contexto, o autor informa que as praxes vêm ocorrendo de uma maneira natural e ao longo do tempo vai se acumulando a documentação quer seja na vida pessoal, quer seja nas instituições. De forma mais simplista, muitas vezes, passa despercebida pelos homens e as organizações essa trajetória de controle do seu fluxo, a qual objetiva dar uma temporalidade para que a documentação, depois de atingida as suas razões tenha a sua gestão.

O primeiro autor insere o documento de arquivo numa contextualização, digamos assim “histórica”, obviamente que não menos importante para os esses dois autores que apresentam o seguinte conceito: “Documento de arquivo é aquele que, produzido ou recebido por uma instituição pública ou privada no exercício de suas atividades, constitua elemento de prova ou de informação.” (ROUSSEAU e COUTURE 1998, p.137). Assim, eles surgem como uma questão mais prática da

vivência relacional da sociedade com as instituições de vice-versa.

Ele é reforçado e coadunado pelo entendimento de Belloto (2005) quando diz: “[...] É a razão de sua origem e de seu emprego que determina sua condição de documento de arquivo.” Todos os autores, cada um em seu tempo, disseram que ele possui uma relação *sin qua non* com função para a qual foi criado.

Para que seja considerado documento de arquivo, sobrevêm algumas características para a sua identificação: 1. É produzido e/ou recebido por uma pessoa física ou jurídica, pública ou privada, no exercício de sua atividades. Um documento meramente escrito produzido no computador de uma pessoa ou da instituição se não exercer uma função (subsidio informacional) ele pode ser considerado somente documento.

Como segunda característica tem-se: Forma um conjunto orgânico. Antes de adentrar no mérito dessa particularidade é necessário fazer um nexo entre informação orgânica e o conjunto. Entendida como aquela que foi elaborada enviada ou recebida no âmbito da missão de uma pessoa física ou moral. Sob esse aspecto – informações orgânicas – os autores (ROUSSEAU e COUTURE, 1998, p.65) afirmam que: “[...] são agrupados todos os documentos, seja qual for o seu suporte e idade, produzidos e recebidos pelo organismo no exercício de sua atividade das funções”. De forma exemplificativa, pode-se citar o Poder Legislativo, cuja função precípua é a elaboração de leis. Assim, as informações produzidas ou recebidas têm que coadunar com a sua missão institucional.

Em continuidade, apresenta-se a terceira característica: reflete as atividades a que se vinculam. Esta, portanto, possui conexão com o termo organicidade. Nesse sentido, (BELLOTO, 2005) qualifica-o da seguinte forma: “organicidade é a qualidade segundo a qual os arquivos refletem a estrutura, funções e atividades da entidade produtora, acumuladora em suas relações internas e externas”. Sob essa lógica a autora reafirma que os documentos produzidos ou recebidos no órgão devem possuir relação com a(s) atividade(s) que são desenvolvidas no âmbito de sua estrutura; as informações contidas no(s) documentos(s) são úteis à administração e é possível classificá-lo de acordo com a sua estrutura, funções e atividade.

A última característica, por fim, do documento de arquivo é que: expressa os atos de seus produtores no exercício de suas funções. Significa dizer que após identificar-se com a relação orgânica da estrutura da organização – compatibilidade

– o responsável dará andamento, visto que o evento ao qual o documento liga terá alguma consequência.

Perlustrando o meio digital – objeto deste trabalho – chega-se para referenciar e analisar o conceito de documento digital. A Câmara Técnica de Documentos Arquivístico (CTDE) do Conselho Nacional de Arquivos (CONARQ), no documento "Diretrizes para a presunção de autenticidade de documentos arquivísticos", define apresenta o seguinte conceito: "informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional". Próximo a esta conceituação estão, também, Ribeiro e Andrade (2012, p.91), os quais dizem: "os documentos digitais, como qualquer arquivo digital, são cadeias de código binário (compostas de zeros e uns) capazes de serem reconhecidos por computadores". Significa dizer que os dados estão de forma bruta, o qual necessita de um hadware (computador) e software (sistema de informação) para que possa ser decodificada e lido seu conteúdo.

Com efeito, traz-se à discussão a partir de (MICHEL 2000 apud SIQUEIRA 2012, p.134), a qual trouxe em seu artigo L`Information et documentation- un domaine d`activité professionnelle en mutation[11], no qual reforça a posição sobre o conceito de documento digital, mas também salienta a necessidade dos profissionais da informação e da Documentação repensarem suas atividades à luz das novas tecnologias de comunicação e informação, destacando o papel do documento digital e seu impacto no contexto desses profissionais. No texto, em referência, faz-se uma análise sobre o que é documento digital, não meramente sob um contexto objetivo, mas destacando características combinadas que este deve possuir.

Michel (2000) continua a apontar as principais características do documento digital: 1. a facilidade de ser armazenado, localizado e recuperado; 2. A disponibilidade instantânea à distância e 3. Poder relacionar-se com outros documentos (hiperdocumento). Depreende-se das características que distancia o documento tradicional, visto que pode-se ter economia de espaço, ganho de produtividade, otimização dos fluxos de trabalho, facilidade de acesso aos estoques de informação e a facilidade de geração e distribuição de dados e informações digitais.

Bodê (2011), em seu blog Preservação Digital no Brasil, ao mesmo tempo em

[11] A Informação e a documentação: uma área de ocupação em mudança (tradução nossa)

que questiona, apresenta uma definição operacional sobre documento digital:

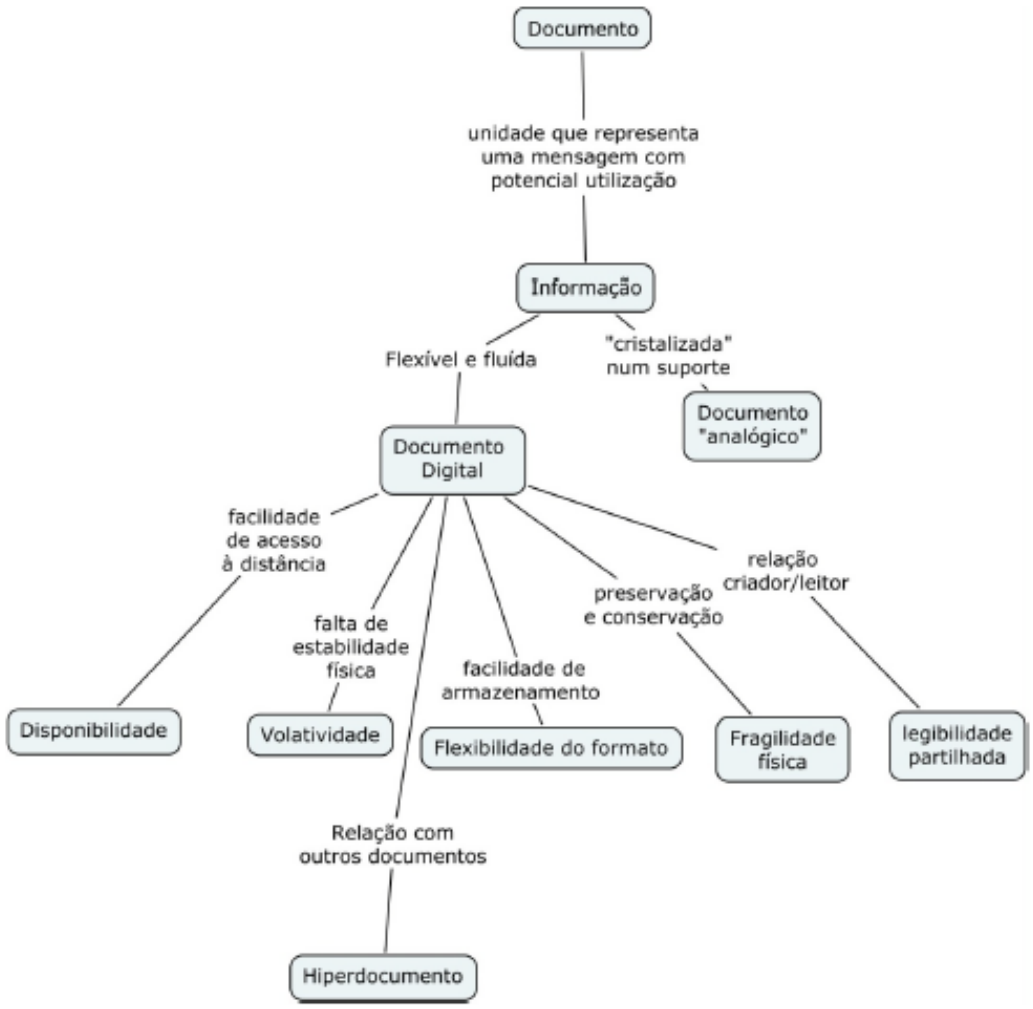
> Um documento digital é o equivalente a uma sequência de códigos binários registrados em algum tipo de tecnologia de memória. Organizados de acordo com determinado formato de arquivo computacional e mensurado através da quantidade de bytes total desse arquivo. Dependendo do tipo de conteúdo, haverá outras características específicas como a representação de cores, som ou texto. A interpretação desses códigos para humanos ocorrerá através de sistemas computacionais de software e hardware.

Este autor classificou a definição de Bodê (2011) como triádica, pois ao mesmo tempo em que ela é operacional, demonstra-se, também, didática e contextual. Na operacional ele cita que se deve expressar-se através de operações que possam ser utilizadas para caracterizá-las em termos físicos conhecidos e aceitos. Nesse contexto, apresenta como exemplo um vídeo digital, um documento digitalizado, um mensagem eletrônica, um texto digitado ou qualquer outro exemplo reforçando a ideia de que é possível ter uma definição comum operacional para o todos os casos. Apresenta-se como didática, pois ao mesmo tempo que introduz termos técnicos explica-os como ele é processado no contexto dos sistemas de informação. Por fim, apresenta-se, porque insere informações da atualizadas, utilizando-se da camera digital – e convidando o leitor a realizar tal operação e chegar aos mesmos resultados, convergindo no que ele chamou de meio eficiente de comunicação.

Siqueira (2012, p.136) foi muito feliz ao sintentizar o conceito de documento digital a partir de um mapa conceitual:

Figura 1 – Mapa conceitual

Figura 1- Mapa conceitual de Documento Digital



Fonte: Elaboração do autor

Fonte: Siqueira, 2012

A partir deste mapa e autora mesmo subdividindo o documento em “análogico” e “digital” deixa claro a necessidade fixar o conteúdo (informação) em algum meio para que seja considerado documento.

O que se pode concluir até aqui é que ambos apresentam vantagens, bem como desvantagens. Para o analógico, reside, dentre muitas, a questão de limitação do acesso e alocação física, mas como vantagem sobrevêm a perspectiva de durabilidade do suporte, se tomadas as medidas necessárias. Já o digital estão, dentre muitos, o fato de preservação dos dados e a dificuldade em garantir a integridade dos documentos e como vantagem garantir o acesso a distância. Silva

(2006) citando Siqueira (2012, p.137) diz: “Ainda, ressalta-se que na verdade, o que importa não é o suporte em que a informação está registrada, mas a informação em sim”.

Felizmente, a gestão arquivística dos documentos, independentemente do suporte, não é uma receita de bolo. Requer estudos constantes e profissionais da informação e documentação conectados para compreendam a nova ordem – gestão e preservação de documentos eletrônicos – e se chegar ao ideal (senão o possível).

4. PRESERVAÇÃO DIGITAL

4.1 O homem e a vida social

Não se tem conhecimento precisamente de como se iniciou a vida social do homem. Deduz-se que tenha começado a partir do surgimento dos primeiros vilarejos, aproximadamente, no sétimo milênio a.C (GONTIJO, 2004). Com esse surgimento o homem necessitou manter uma interação com as demais pessoas que ali conviviam para uma troca de experiências estimulando, ainda, a comunicação, a qual se convergiu na produção e troca de conhecimento.

A partir dessa acumulação verificou-se a necessidade de reuni-las objetivando concentrar as informações para se ter o acesso organizado. Corrêa (2010, p.12) informava que “os sistemas de registro, inventados por volta do nono milênio a.C., utilizados até então, para, por exemplo, contabilizar e controlar as colheitas e os rebanhos, não eram suficientes.”. Como se observa, desde os auspícios sentia-se a necessidade de sistematização e registro do que se produzia com dois objetivos: acumulação (guarda) e disseminação (acesso), pois “a intenção de registrar sempre esteve associada à necessidade de lembrar” (GONTIJO, 2004).

Equipara-se a lembrança como uma necessidade básica (comer, beber etc), pois ela é o resultado das praxes do cotidiano – produção de informação diária – quer seja de uma pessoa ou instituição. Segundo Delmas (2010, p.26-27) diz “É o resultado da necessária continuidade da vida dos indivíduos como organismos, isto é, a continuidade de cada uma de suas ações”. O exemplo mais claro dessa sequência ocorre quando da mudança/substituição de chefia quer seja num plano maior ou menor. Ela vem acompanhada, na maioria das vezes, da transferência dos registros e de documentos, sintetizada em uma palavra: arquivos.

Registra-se, também, quando Corrêa (2010, p.12) diz que “a importância do patrimônio enquanto memória sempre foi reconhecida e manipulada conforme as conveniências para determinado grupo ou governante”. Infelizmente percebe-se que tal prática encontra-se “arraigada” durante o desenvolvimento da sociedade. Este “círculo vicioso” é demonstrado na citação de Chagas (2002, p.135) que diz: “o ato de preservação sempre esteve submetido ao exercício de poder, mas este não é

apenas repressor, é também promotor de memórias e esquecimentos[12]".

É no mínimo interessante, para não dizer trágico ligar a sobrevivência da memória registrada a ação da natureza, pois conforme diz Corrêa (2010, p.12) ao longo do tempo ocorre o "desgaste natural dos suportes de registro quando em contato com o ar, sol, umidade e terremotos". Há, também, a ação humana – considerada sob a ótica deste autor a mais grave –. Muitas vezes são causadas pela falta de tratamento adequado para a preservação ou mesmo com a intenção de destruir aquilo que serve à coletividade.

Obviamente existem muitas outras prioridades no âmbito governamental, tais como saúde, educação, moradia, infraestrutura, lazer, entre outros. Porém, não existe uma conscientização dos governantes de que se conservando preventivamente onera-se menos o erário. Contudo, não se pode deixar de reconhecer as várias políticas públicas destinadas à preservação.

Não obstante à necessidade descrita, a humanidade vem perpetuando a sua história através da preservação do patrimônio quer seja ele histórico, artístico, cultural, documental, de conhecimento, de objetos etc, produzidos pelas sociedades passadas e, preservados pelas gerações que estão lhe sucedendo. Esta dinâmica – quando mantida – representa uma fonte inesgotável de pesquisa.

Assim, é dispensável enfatizar a contribuição da revolução industrial seguida da revolução tecnológica que propiciaram um maior volume de informações em todo o seu desenvolvimento.

4.2 Arquivologia a serviço da ciência da computação.

Presente hoje em todas as áreas, bem como na arquivologia, a computação veio como uma ciência que colabora para a continuidade da gestão de documentos de arquivos, desde o momento de sua produção até a sua gestão (eliminação ou guarda definitiva). Isto posto, Delmas (2010, p.98) alerta dizendo que "o arquivista deve intervir logo na concepção dos documentos eletrônicos, para introduzir os metadados capazes de assegurar sua conservação e perpetuidade dos dados"

[12]Esquecer e perder não são males absolutos, abrem espaço para o novo e para o criativo (Chagas, 2002)

Assim, percebe-se que se está vivendo numa época em que há o maior trafego de informações no meio computacional e cuja tendência é a ampliação dos canais e meios para a produção e disseminação das informações. Sob esse espectro Arellano (2004, p.15) dar-se-á ênfase “à geração e/ou aquisição de material digital, em vez de manter a preservação e o acesso a longo prazo aos acervos eletrônicos existentes”.

Não é preciso ir muito longe para se compreender a necessidade de se preservar documentos produzidos neste meio. Até pouco tempo a sociedade produzia suas fotografias pelo meio analógico e cuja tendência era utilizar-se dos birôs/lojas para revelar os negativos e ter a possibilidade de visualização das imagens. Geralmente, as pessoas constituíam os seus álbuns fotográficos a partir dessa ação.

Acompanhando essa contemporaneidade e com o avanço tecnológico surgem as câmeras digitais ampliando o espectro do registro. As possibilidades são infinitas, isto porque algumas registram, captam a imagem pelos movimentos, filmam etc. No processo de modelagem pode-se aplicar filtro às fotografias, se não gostar da pose apaga-se e faz-se novo registro. Ao final você descarregava-nas no computador e lá deixava armazenado ou as salvava em disquetes de 3.5 polegadas.

Com o avanço tecnológico o mercado foi sucumbido pela obsolescência tecnológica e em pouco mais de 10 anos – março de 2003 – a fabricante Dell Computer Corporation anunciava que os seus computadores deixariam de integrar dispositivos capazes de ler os disquetes 3.5 polegadas, fazendo com que as demais fabricantes seguissem a mesma tendência. Hoje, ainda é possível adquirir dispositivos capazes de ler os disquetes 3.5 polegadas, mas o mercado posiciona-se para a produção e armazenamento em CD-ROM, HD, que são as mídias, por hora, mais utilizadas. Todavia, insurge-se com a sua temporalidade até quando elas estarão disponíveis no mercado?

Ferreira (2006, p.19) bem coloca dizendo que:

> A obsolescência tecnológica não se manifesta somente ao nível dos suportes físicos. No domínio digital, todo o tipo de material tem obrigatoriamente de respeitas as regras de um determinado formato. Isto permite que as aplicações de software sejam capazes de abrir e interpretar adequadamente a informação armazenada. À medida que o software vai evoluindo, também os formatos por ele produzidos vão sofrendo alterações.

É interessante a observação do autor, pois a obsolescência atingi não somente os suportes físico, assim como os softwares e hardwares. Fazendo uma alusão ao processo arquivístico de gestão de documento e se utilizando da teoria das três idades com as suas devidas adaptações, é como se cada meio (suporte físico, *software* e *hardware*) possuísse a sua temporalidade, cumprindo, assim, um prazo na fase corrente – período em que se tem uma frequência de uso constante –. Após, ocorre a sua substituição, mais ainda assim é possível acessar – fase intermediária –. Depois, tem a sua destinação final, a completa substituição.

Compreende-se que o homem é o produto do meio e se o mundo está evoluindo em relação à informação digital e seus meios, natural que ocorram essas mudanças. Entretanto, é preciso alertar na perspectiva de conscientizar as instituições que estão enveredando para o caminho do meio digital, isto porque Arellano (2004, p.15) diz que se faz necessário a "aplicação de estratégias de preservação para documentos digitais [...], pois sem elas não existiria nenhuma garantia de acesso, confiabilidade e integridades dos documentos a longo prazo".

Visando garantir as estratégias supramencionadas, faz-se necessário compreender o que cada termo significa. O dicionário *online* Houaiss apresenta nove significações para a palavra *acesso*. Para este trabalho, utilizar-se-á apenas duas que possuem mais proximidade, vejamos:

> 1 possibilidade de alcançar (algo difícil)
> ‹ *poucos têm a. ao saber* ›
> 2 *inf* possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados. (HOUAISS, 2013)

Para que o conteúdo de um documento digital continue disponível, acessível e interpretavél através de sistemas computacionais é necessário criar mecanismos e estratégias para o seu alcance.

Acompanhado dessa estratégia para o acesso – neste caso entendível como de longo prazo – ao documento arquivístico encontra-se a *confiabilidade*. O Glossário da Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CTDE-Conarq), diz que confiabilidade significa a:

> Credibilidade de um documento arquivístico enquanto uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza da forma do

> documento e do grau de controle exercido no processo de sua criação. (BRASIL, 2010, p. 9)

A confiabilidade/credibilidade se dá a partir da produção do documento arquivístico, pois este consubstanciará um fato. Assim, Moreira (2012, p.62) diz que a questão da "confiabilidade pressupõe indagar porque costumamos atribuir aos documentos um caráter de (trans)portadores de fatos verdadeiros."

No entendimento das estratégias de preservação para os documentos digitais o termo *integridade* relaciona-se com a completude e inalterabilidade, quer dizer que não houve corrupção ou alteração não autorizada nem documentada (ISO, 2007, p.07).

Após perfilhar em um contexto introdutório como iniciou, talvez, a vida social do homem, tratar a questão da obsolescência tecnológica a partir da exemplificação de uma grande empresa de informática, e discorrer a cerca da noção terminológica que encadeia as estratégias para a manutenção dos documentos a longo prazo, chega-se a uma abordagem conceitual do que é preservação digital. Mas antes, faz-se necessário refletir a cerca da constituição do conceito de patrimônio digital:

> consiste de recursos exclusivos do conhecimento humano e de expressão. Abrange fontes culturais, educacionais, científicas, administrativas, técnicas, legais, médicas e outros tipos de informação criados digitalmente ou convertidos a partir de um suporte analógico. [...] Materiais digitais pode ser textos, base de dados, imagens fixa (fotografias, gravura, pintura) ou em movimento, gravações sonoras, *software* e paginas da internet entre muitos outros tipos que não param de ser criados. Geralmente são efêmeros e exigem manutenção para serem preservados para a geração presente e para as futuras (UNESCO, 2003)

Oportuno destacar que a UNESCO foi bastante abrangente no sentido de englobar várias áreas do conhecimento humano quem vêm ao longo do tempo aperfeiçoando as suas técnicas e procedimentos, gerando informação de maneira digital ou convertendo-as para este meio. Significa dizer, também, que muitos desses dados possuem relevância, são significativos, necessitam estar protegidos e serem preservados não somente para a geração atual, assim como as futuras.

Partindo-se do termo preservação, analisando a sua significação a partir da consulta ao dicionário *on-line* Houaiss (2013) a palavra possui três acepções. Para este trabalho utilizar-se-ão apenas duas que se ligam melhor ao objetivo proposto: O ato ou efeito de preservar e é:

> **1** m.q. conservação ('conjunto de medidas')
>
> **2** série de ações cujo objetivo é garantir a integridade e a perenidade de algo; defesa, salvaguarda, conservação
> *‹ p. de um bem cultural › ‹ p. da democracia constitucional ›* (HOUAISS, 2013)

Como a própria significação referencia, preservar significa dizer que é necessário a aplicação de um "conjunto de medidas", objetivando garantir a integridade física de algo. No contexto do formato tradicional – suporte em papel –, o conceito é bastante atual e por mais que não se tenha conhecimento aprofundado sobre tais medidas, intuitivamente, o responsável pelo acervo proceder-se-á as ações primeiras visando manter incólume a documentação sobre sua guarda.

Entretanto para o meio digital a integridade física não é suficiente, visto que o momento em que a sociedade tem passado em relação aos avanços tecnológicos impostos pela nova ordem – a computação – faz-se necessário, conforme Cunha e Lima (2007, p.03) dizem a utilização de "dispositivos que tornem acessíveis os conteúdos para o acesso humano (os discos rígidos, cd's, disquetes etc)". No entanto, mantê-los armazenados nestas mídias não garante a preservação das informações, tampouco a perpetuidade do acesso, isto porque, conforme relatado por Cunha e Lima (2007, p.03) "leva a uma necessidade de preservação também dos *software*, bem como dos equipamentos necessários […]" à sua utilização.

Após revisar o termo preservação a partir do vocábulo da língua, partir-se-á para a análise conceituológica dos autores e organizações que vêm definindo a preservação digital em suas áreas e/ou projetos. Ressalta-se que as conceituações mais utilizadas são *Online Computer Library Center (OCLC), Association for Information and Image Management (AIIM)*, a *United Kingdom Office for Library Networking (UKLON),* dentre outras.

A *Association for Information and Image Management (AIIM)* citada por Cunha e Lima, (2007, p.03) apresenta a seguinte definição: "habilidade de manter documentos digitais e arquivos acessíveis por períodos de tempo que transcendam avanços tecnológicos sem afetar por alteração ou perda da legibilidade".

No conceito proposto pela AIIM, ela sintetiza em uma palavra: habilidade. Significa dizer que o pessoal envolvido em projetos que privilegie a preservação digital possuem esta característica/qualidades e, portanto, estão aptos para dar resposta e resolver as situações novas que se lhe apresentam e agindo de maneira mais apropriada aos fins a que visa durante a trajetória da mudança para o meio

digital. Isto é possível a partir da acumulação de conhecimentos técnicos e procedimentais no desenvolvimento de soluções do qual tenham, inexoravelmente, atuado em projetos cujo foco tenha sido acesso contínuo e a longo prazo na perspectiva da preservação de documentos digitais.

Em continuidade, Ferreira (2006, p. 20) apresenta o seguinte conceito: “designa-se, assim, por preservação digital o conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo-prazo à informação e restante patrimônio cultural existente em formatos”. Constatou-se que ele retoma o conceito proposto pela UNESCO substituindo a palavra “digital” pela “cultural”, mas ao final chega-se ao mesmo denominador.

Ao introduzir o termo *cultural* subentende-se que ele considera os bens materiais, imateriais que se referem à identidade, à ação e a memória dos diferentes grupos formadores da sociedade: as formas de expressão, os modos de criar, fazer, viver; as criações científicas, artistísticas e tecnológicas; as obras, objetos, documentos, edificações e demais espaços destinados às manifestações artístico-culturais; os conjuntos urbanos e sítios de valor histórico, paisagísticos, artístico, arqueológico, paleontológico, ecológico e científico (FUNDARPE, 2013) , aproximando-se do que a UNESCO considerou como recursos exclusivos do conhecimento humano e de expressão.

Após aproximar o conceito de patrimônio como proposto pela Organização, Ferreira (2006, p.20) continua conceituando preservação digital: “consiste na capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro [...].”. Ele coaduna-se do conceito perlustrado pela AIIM, mas acrescentando outra variante a “autenticidade”, visto que ao tratá-la como um requisito a CTDE (2012, p.02) reitera que o documento digital deve possuir “qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração”.

À autenticidade ainda compõem-se de: “identidade” e “integridade”. A CTDE (2012, p.12) diz que a identidade “é o conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (ex.: data, autor, destinatário, assunto, número identificador, [...])”. Em continuidade ela diz que a integridade “é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem

sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos".

Sob esta égide, observa-se que a autenticidade (e seus componentes) é um dos requisitos fundamentais (se não o mais), pois a partir dele denota-se nas evidências um alto grau de certeza que ao longo dos tempos foram utilizadas, pois conforme menciona a CTDE (2012, p.01) as "tecnologias e procedimentos administrativos que garantiram a sua identidade e integridade" ou em especial, "pelo menos, minimizaram os riscos de modificações dos documentos a partir do momento em que foram salvos pela primeira vez em todos os acessos subsequentes" (CTDE, 2012, p.01).

Mais uma citação a cerca da preservação digital é a *Research Library Group/Online Computer Library Center Report (RLG/OCLG)*, na qual diz que: "a preservação digital, refere-se a uma série de atividades gerenciadas necessárias para assegurar o acesso contínuo e preservação de materiais digitais (CHAPMAN, 2001 apud CUNHA; LIMA, 2007, p.04 tradução dos autores).

A partir do conceito do Chapman (2001), os autores consideram outra característica "gerenciamento de atividades". Cada autor em seu respectivo tempo colaborou para imbricar as "características" a partir dos seus estudos e análises. Compreende-se que nenhuma é excludente e sim, complementar a outra. Isto porque o técnico precisa ter as "habilidades" necessárias para "gerenciar as atividades" de preservação digital com qualidades de "autenticidade" para a perpetuidade do acesso contínuo de documentos digitais.

Traz-se ao contexto, também, o que Hedstrom (1997/1998 apud THOMAZ; SOARES 2004, p.01) considerou como duas definições básicas de preservação digital ou arquivamento digital:

> Planejamento, alocação de recursos e aplicação de métodos de preservação e tecnologias necessárias para que a informação digital de valor contínuo permaneça acessível e utilizável por longo prazo, considerando-se neste caso longo prazo, o tempo suficiente para preocupar-se com os impactos de mudanças tecnológicas. A preservação digital aplica-se tanto a documentos "nato-digitais" quanto a documentos convertidos do formato convencional para o formato digital.

Partindo do pressuposto que toda ação necessita de planejamento e quando se trata da preservação digital o espectro, necessariamente, precisa ser ampliado, visto ser um assunto relativamente recente, o qual requer amadurecimento sobre conceitos, analisar os prováveis problemas e desenvolver requisitos e estratégias

para a manutenção e acesso por longo prazo dos documentos digitalizados e aqueles nato-digitais.

Destaca-se, ainda, do conceito formulado as frases como “longo prazo” e “tempo suficiente para preocupar-se com os impactos de mudanças tecnológicas”. Nesse aspecto, iniciavam-se discussões sobre as questões preservacionistas de modo que tinha que se preocupar com o impacto tecnológico. Quinze anos depois se verifica que: Ou se constroem bases para a preservação digital de maneira proeminente ou se perderão muitas informações no meio digital.

Em continuidade Task Force on Archiving of Digital Information (1996) apud Thomaz; Soares (2004, p.01) dizem que:

> A capacidade de manter a integridade e a acessibilidade da informação digital por longo prazo. Esta preservação da integridade e acessibilidade não se limita, apenas, a proteger a informação digital contra o acesso não autorizados mas, também, contra o uso inadequado resultante da má interpretação ou má representação da informação por parte dos sistemas computacionais. Percebe-se, aqui, o aspecto da inseparabilidade entre as atividades de preservação e acesso ao mundo digital.

Muitos autores, ao longo da construção textual sobre o termo preservação digital destacaram o que consideravam importante sobre a temática, mas acredita-se que todos sem dúvidas preocupavam-se com a questão-chave é: como manter o acesso continuado e de longo prazo da informação em formato digital e com qualidades autênticas?

Esta pergunta, talvez, seja uma das mais importantes que reside na mente dos profissionais que o longo das últimas décadas vêm estabelecendo diretrizes e padrões, definindo técnicas e procedimentos e escolhendo as estratégias mais adequadas – ao tempo – para a preservação digital.

4.3 Estratégias de preservação digital

Ao longo dos anos vêm sendo construídas diversas estratégias de preservação digital. Vislumbra-se que algumas delas possam adequar-se à realidade das instituições que optaram por seguir o meio digital. Entretanto, antes de se pensá-las faz-se necessário o total envolvimento, interação e disposição de profissionais de várias áreas ligados com a criação, com o desenvolvimento, com o armazenamento e com os disseminadores desses documentos. Na fase inicial, talvez, este seja o maior desafio – conter de brios –, pois ninguém é autosuficiente que não possa precisar de profissionais de outras áreas[13].

Muitas soluções têm sido desenvolvidos há pelo três décadas e um conjunto de normas, também, vêm sendo produzidas durante esse período. Assim, coaduna-se do mesmo pensamento de Sayão (2006, p.118) quando ele afirma não um "corpo de conhecimentos plenamente consolidados". Por mais que se tenha um *corpus* consolidado, Corrêa (2010, p.25) diz que "talvez ainda não tenha decorrido tempo suficiente para ser possível comprovar a eficiência das estratégias adotadas[14]"

Há uma clara propensão dessas soluções fixarem apenas um requisito: a obsolescência tecnológica. Justamente, o foco principal talvez seja esse, devido "pela vida curta que as mídias, dos *hardwares*, dos *softwares* e dos formatos" (CONARQ, 2004 p.02; SAYÃO, 2006 apud CORRÊA, 2010, p 25-26) que ameaçam a longevidade e o acesso incondicional aos documentos. Não obstante, "é válido lembrar que a rápida evolução e obsolescência tecnológica se apresentam vantajosas e essenciais na competição pela supremacia em um mercado bastante competitivo" (RIVERA DONOSO, 2009, p.13; SAYÃO, 2006 apud CORRÊA, 2010, p. 26). Obviamente que o transcurso de projetos de preservação digital possam surgir algumas estratégias, mas cada terá a sua contribuição no arcabouço conceitual, metodológico e prático, visto que "nenhuma estratégia se mostrou completa o suficiente" (ROTHENBERG, 1999) e a utilização de mais de uma é a mais aceitável.

---

[13] Em muitos casos, o responsável pelas duas ações é o mesmo. No entanto, pode ser preocupante que a preservação digital dependa apenas de um indivíduo, pois ele pode não ter todos os recursos necessários para garanti-la a longo prazo. (OWEN, 2007)

[14] Por outro lado, já passou tempo suficiente para termos a certeza de que políticas de preservação cuidadosamente elaboradas precisam ser implantadas com urgência!

Assim, Ferreira (2006, p. 31-45) lista algumas prováveis estratégias a serem utilizadas, vejamos:

Preservação de tecnologia: Reside na conservação e manutenção de todo o hardware e software necessário a correta apresentação de objetos digitais[15]. De maneira exemplificativa Ferreira (2006, p.21) considera que os objetos sejam: "documentos de texto, fotografias digitais, diagramas vetoriais, bases de dados, sequência de vídeo e audio, modelos de realidade virtual, páginas da Web e aplicações de software" são alguns exemplos que ele considera como um objeto digital.

Refrescamento: Consiste na transferência de informação de um suporte físico de armazenamento para o mais atual. Por exemplo: a documentação que foi salva em um disquete deve ser transferida para outro suporte, neste caso, o CD-ROM, DVD, visto que com o passar dos anos não poderá ser equipamentos para lê-la, o que ocasionará a perda da informação. Entretanto, Ferreira (2006, p. 33) alerta que o refrescamento de suporte não constitui uma estratégia de preservação por si só. Deverá, em vez disso, ser entendido como um pré-requisito para o sucesso de qualquer estratégia para a sua completude.

Emulação: Este tipo de estratégia, consiste na utilização de software, designado emulador, capaz de reproduzir o comportamento de uma plataforma de *hadware* e/ou *software*, numa outra que a partida seria incompatível. Importante ressaltar que este tipo consegue preservar, com um alto grau de fidelidade, as características e as funcionalidades do objeto digital.

Migração/Conversão: Consiste na transferência periódica de material digital de uma dada configuração de hardware/software para uma outra, ou de uma geração de tecnológica para outra subsequente. Significa dizer que a migração/conversão você muda geral de um *software* para outro. De forma exemplificativa, tem-se um programa de arquivamento que atende às necessidades

[15] Um objecto digital pode ser definindo como todo e qualquer objecto de informação quem possa ser representado através de uma sequência de dígitos binaries. Esta definição é suficientemente lata para acomodar tanto, informação nascida num contexto tecnológico digital (objectos nado-digital), como informação digital obtida a partir de suportes analógicos (objectos digitalizados)

da instituição, mas identificaram outro que possuem mais recursos etc. A instituição, então, decidi adquiri-lo e resolve migrar para esse novo *software*. É feita a transferência da base de dados do antigo para o novo. Apesar de ser uma das estratégias de preservação, e ser utilizada como tal, refuta-se, a sua utilização, pois sempre há perdas de informação. Há, entretanto, todo um trabalho das equipes de TIC's para minorar, mas seus efeitos só são sentindo no dia a dia quando os casos surgirem.

Migração para suportes analógicos: Consiste na inversão de papéis. O objeto é migrado para o suporte físico (papel, microfilme, etc) considerado mídias mais duradouras, mas sem esquecer a conservação entorno deste. Obviamente que esta estratégia só é possível aqueles objetos digitais que possuam uma representação aproximada em suportes analógicos, ou seja, documentos de texto ou imagens.

Atualização de versões: Consiste em software capazes de abrir ou importar objetos digitais produzidos por versões anteriores dessa mesma aplicação, a qual se denomina de atualização da versão do formato. De forma exemplificativa, tem-se a seguinte situação: A instituição já utiliza um programa de arquivamento, mas a equipe de TI ou o próprio setor identifica que há uma atualização desse melhorando alguns recursos e parte de segurança. Então, basta atualizar o *software* e não mudar/migrar para o outro. O que diferencia a migração/conversão para a estratégia de preservação atualização de versões é que esta última é realizada apenas como uma complementação.

Conversão para formatos concorrentes: Consiste em converter um objeto digital para um outro formato que não fora desenvolvido pela empresa atual que possui a propriedade do software. A utilização dessa estratégia é bem recorrente pois há uma constante descontinuidade das empresas no desenvolvimento dos produtos. Em certa medida, garante às instituições uma certa "autonomia", pois independemente do sucesso econômico do fabricante ou do produto do software elas não ficam à mercê destes. Na atualidade, há um fluxo migratório para formatos que não dependem de qualquer aplicação de software. Exemplo disso são os formatos de imagem que podem ser convertidos para JPEG, TIFF, PNG,

possibilitando a conversão entre formatos análogos, indepentendemente da aplicação utilizada na sua criação.

Aderência a padrões (inclui-se a técnica de normalização): Cunha e Lima (2007, p.06) trazem como uma outra estratégia "A adesão a padrões abertos estáveis e largamente utilizados ao criar e arquivar recursos digitais", pois é o que está sendo amplamente divulgado pela comunidade internacional. E Cunha e Lima (2007, p.06) justificam dizendo que "eles não estão presos a plataformas específicas de hardwares e softwares o que resguarda por algum tempo a mais o recurso digital da obsolescência tecnológica". Optando-se por modelos normalizados, garante assim a uniformização desde o momento da produção até seu potencial reuso.

Migração a pedido: Técnica utilizada para manter sempre a conexão com o objeto original. Significa dizer que quando é realizada uma migração sempre do objeto de partida (original) as suas características mantêm-se incólumes. Para tanto, dependerá, fundamentalmente, da qualidade dos conversores utilizados e da capacidade que o formato de destino possui para acomodar o conjunto de propriedades do formato de partida, evitando-se, assim, a perda de alguma particularidade quando da realização da migração do objeto digital na atual versão para uma mais nova.

Migração distribuída: Trata-se de uma migração que introduz arquiteturas distribuídas de conversores. Esses conjuntos de serviços de conversão encontram-se acessíveis através da internet e poderão ser utilizados remotamente recorrendo a uma pequena aplicação-cliente. Ferreira (2006, p. 42) informa que o *Lister Hill National Center for Biomedical Communications* desenvolveu um serviço web que converte objetos digitais de cinquenta formatos distintos para PDF. E continua dizendo que a Universidade do Minho está desenvolvendo uma *Arquitetura Orientada ao Serviço* (SOA) que disponibiliza várias centenas de serviços de conversão, avaliação e recomendação.

Encapsulamento: Este tipo de estratégia de preservação digital, conforme Cunha e Lima (2007, p.06) informam, consiste em "reunir em conjunto com o recurso digital e o que quer que seja necessário para manter o acesso a ele. Isto pode incluir

metadados, software visualizador e arquivos específicos constituintes do recurso digital". Dá *corpus* prático aos conversores e emuladores a serem desenvolvidos no futuro para garantir a preservação da coleção do objeto digital, visto que a informação poderá consistir, por exemplo, numa descrição formal e detalhada do formato do objeto preservado.

Pedra de Rosetta digital: Possui esse nome porque em 1799 um grupo de soldados franceses havia descoberto no delta do Nilo um bloco de granite onde se encontrava escrito três línguas distintos (egípcio hieroglífico, cursivo e grego clássico) um decreto emitido em 196 a.C por Ptolomeu V Epifânio. Vinte e três anos depois o paleógrafo francês Jean-François Champollion decodificou a versão egípcia do texto. A partir desse trabalho inúmeros textos egípcios encontrados nos mais variados locais e suportes (monumentos, rochas, papiros) foram decodificados. Nessa estratégia, em vez de se preservar as regras que permitem traduzir o objeto digital, reúnem-se amostras de objetos que sejam representativas do formato que se pretende recuperar. Este modelo baseou-se em três momentos diferentes: processo de preservação do conhecimento [1] registro da codificação do formato de arquivo e do conteúdo em binaries; [2] recuperação dos dados e [3] reconstrução dos documentos a partir das especificações construídas na primeira etapa (CUNHA e LIMA, 2007, p. 07). Por fim, Ferreira (2006, p. 45) alerta que esse tipo de estratégia deverá ser considerada apenas em situações em que todos os esforços de preservação falharam, visto que se trata de uma ferramenta de arqueologia digital e não propriamente de uma estratégia de base para preservação de objetos digitais.

Após revisitar as 12 estratégias de preservação digital propostas na sistematização de Ferreira (2006), verifica-se que está longe de construir uma proposta única para as instituições que migram para o meio digital. Essa diversificação de estratégias abre um leque para as organizações optarem para a sua utilização, mas o mais importante é a conscientização de profissionais que gerenciam todos esses dados terem a percepção de preservarem as informações sob os parâmetros arquivísticos para o seu reuso.

O próximo capítulo é dedicado à assinatura digital, definição de conceitos, requisitos e a certificação digital. Mas cabe neste capítulo abrir um aparte – dedicado às estratégias de preservação digital – e introduzir o conceito de autenticidade.

Ferreira (2006, p.49) diz que "O conceito de *autenticidade* está muito longe de ser consensual entre os profissionais da preservação", isto porque são "facilmente duplicados, distribuídas, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes" (CTDE-CONARQ, 2012, p.1). Contudo, tê-los em mente torna-se bastante significativo, pois dessa forma terão condições de interagir com os profissionais que gerenciam os sistemas e a documentação neles contida, informando-os sobre os riscos a que a instituição está exposta e que se medidas assertivas não forem tomadas ter-se-á uma massa documental que não possui autenticidade, tampouco são íntegras.

Na complexa missão de definição conceitual existe duas áreas, a história e a Arquivologia, que possuem visões distintas a cerca do termo autenticidade. "Para um históriador um objeto é autêntico se a sua identidade e integridade não forem comprometidas, se for possível aferir que um objeto é realmente aquilo que se propõe ser.". Nesta definição revigora a necessidade de se ter a identidade (autor, destinatário, assunto, data etc) mantida (não sofreu revés) em sua trajetória, documentada e possuir conteúdo verdadeiro. Sob o ponto de vista da arquivologia, "a autenticidade de um documento não pressupõe uma legitimação da sua veracidade ou até mesmo utilidade". Sua preocupação está voltada para a capacidade do documento servir como prova. Ferreira (2006, p.49) diz que ele pode até "conter incorreções, erros ou até falsidades, mas isso não invalida a sua importância como testemunho de algo que aconteceu". Nesse contexto, existem três aspectos que ligam a autenticidade de documentos arquivísticos: legal, diplomático e histórico (CTDE, 2012, p.03).

Quanto aos documentos que são legalmente autênticos, Moreira apresenta a sua visão:

> A autenticidade legal, sob o ponto de vista dos documentos públicos, decorre da intervenção feita pelo agente público, por meio de sua assinatura, ao final do processo de produção de um registro. A assinatura completa o rito de produção do documento, dá autoria ao ato jurídico e também lhe confere legitimidade (que se confirmará mediante a aferição da competência do agente para praticá-lo) (MOREIRA, 2012, p.53)

Um documento arquivístico – no expectro de documentos públicos – para ser considerado autêntico, requer necessariamente que o agente público, investido do

cargo que ocupa, possua legitimidade para o ato (fé pública) para apor a sua assinatura após a finalização de sua produção, surtindo assim os efeitos requeridos, bem como garantindo a sua genuidade.

Em relação aos documentos diplomaticamente autênticos "são aqueles que foram escritos de acordo com a prática do tempo e do lugar indicados no texto e assinados pela pessoa (ou pessoas) competente para produzi-los" (CTDE, 2012, p. 03). Desse modo, ele encontra-se ligado à trajetória jurídica, social e tecnológica, bem como respeita o contexto no qual foi inserido. Moreira (2012, p.53) apresenta como exemplo: "a fonte exigida para a produção de um documento oficial for Time New Roman e ele estiver escrito em fonte *Lucida handwriting*" existem evidências fortes que no aspecto diplomático se houve modificação da fonte o documento torna-se inautêntico, mas não necessariamente que ele seja inautêntico sob o aspecto legal e histórico.

Em última análise verificar-se-á a autenticidade histórica do documento. Para este aspecto, o fato ou o evento realmente aconteceu ou as informações transcritas possuem veracidade. Moreira apresenta o seguinte exemplo:

> Uma certidão de nascimento expedida dentro da normalidade pelo órgão oficial responsável e comprovadamente autêntica sob os pontos de vista legal e diplomático, pode não ser historicamente autêntica se, por um erro de digitação, atribuir (por exemplo) a data de nascimento 28/09/2007 a alguém que tenha na realidade nascido no dia 27/09/2007. (MOREIRA, 2012, p. 54)

Para o direito, diz-se que houve um "erro material", o qual pretende que se restaure, supra ou retifique assento no registro civil, através da ação denominada "Retificação ou Suprimento ou Restauração de Registro Civil". Saneada a questão jurídica, verificar-se-á que "a autenticidade histórica tange o conteúdo dos registros, ela se delinea com uma noção complexa que versa diretamente sobre a possibilidade de existir uma 'verdade histórica'" (MOREIRA, 2012, p.54).

Constata-se, portanto, nos três aspectos da autenticidade dos documentos arquivísticos que cada um possui uma independência e relevância, "de tal maneira que um documento não atestado por uma autoridade pode ser diplomática e historicamente autêntico, mas sempre será legalmente inautêntico" (CTDE, 2012, p.03).

Para os documentos eletrônicos Atheniense (2010, p.125 apud MOREIRA 2012, p. 53) apresenta o seguinte conceito:

> O documento eletrônico original e autêntico é aquele cuja autoria possa ser aferida de forma inequívoca. Enquanto nos documentos em papel a autenticidade é comprovada por firma que eventualmente poderá ser reconhecida por um tabelião que atestará sua legitimidade nos documentos eletrônicos, **a assinatura digital emitida por meio de um certificado digital de uma autoridade certificadora é que atribuirá a autoria**. (grifo nosso)

Não restam dúvidas em relação à comprovação de autenticidade dos documentos eletrônicos para o autor. Convém salientar no caso de documentos públicos oficiais requer do agente público que ele possua uma assinatura digital, a qual deve estar registrada, necessariamente, em uma autoridade certificadora para que seus atos sejam autênticos (possua autoria identificável), íntegros (impossíveis de ser alterados de maneira imperceptível) e válidos (assinatura registrada da entidade não tenha expirado).

5. CRIPTOGRAFIA

Esse tópico destaca informações relevantes acerca de criptografia, o histórico dos avanços da ciência e tecnologia criptográfica, conceitos, formas, assinatura digital, os requisitos necessários da assinatura digital, a criação da Assinatura digital, a certificação digital e a autoridade certificadora, e para finalizar a capacidade de segurança.

5.1 Avanços na tecnologia criptográfica (histórico)

Durante os auspícios da formação da sociedade reis, rainhas buscavam a melhor forma de transmissão da mensagem para o pessoal das forças armadas e de governo seu país. Para tanto, era necessário que as informações importantes, chegassem de através de código para que fossem lidas por aqueles que possuíam a “chave” para a decifração. Todavia durante a trajetória histórica da criptografia não se identificam registros precisos sobre o seu surgimento. Behrens (2005, p.21) mostram que “estudos […] giram em torno do Egito, da China, da Índia e Mesopotâmia” .

As formas codificação, ao longo do tempo, foram evoluindo à medida que os seus utilizadores sentiam a necessidade de proteção maior dos dados transmitidos

O primeiro mais conhecido informado por Behrens (2005, p.21) “data de 475 a. C quando os gregos e esparta utilizaram o primeiro sistema criptográfico aplicado às mensagens militares, denominado como ESCÍTALA”. A composição, conforme apresentado por Behrens (2005, p.21) era “bastão de madeira envolto por uma tira fina de pergaminho, que apresentava a escrito da mensagem secreta”. Entretanto, tiveram outros episódios no transcurso da história que ilustram bem o uso da criptografia.

O segundo, refere-se ao imperador romano Júlio César (110 a.C 44 a.C) que se utilizava da criptografia para enviar mensagens a seus generais. Ficou conhecido como “cifra de César”. O código consistia em trocar cada letra de uma mensagem pela terceira letra seguinte. Assim, na decifração do código, o receptor precisava saber que o "A" virava "D", o "B" se tornava "E" e assim por diante. Poder-se-ia dizer que a partir deste sistema iniciou-se um estudo mais orientado a cerca do método.

Já o terceiro, refere-se ao pintor Leonardo Da Vinci (1452-1519). Ele utilizava-se de um método curioso visando proteger-se daqueles “bisbilhoteiros”. Seu método consistia em escrever da direita para a esquerda de modo que seus textos só podiam ser lidos diante de um espelho. Esses foram apenas três de muitos exemplos possíveis de serem encontrados na história da “velha ciência” que a cada dia torna-se nova.

5.2 Conceitos de Criptografia

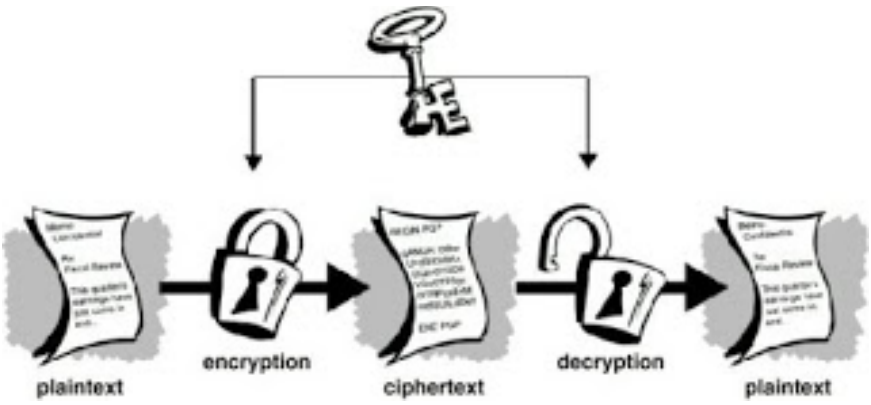
A criptografia é denominada a ciência ou a arte de grafia oculta, com intuito de esconder uma informação envida via rede de computadores entre o emissor e o receptor, evitando o acesso de terceiros desautorizados a esse conteúdo. Ou seja, a informação é enviada de modo ilegível para garantir a sua privacidade e ao chegar ao destino volta novamente ao formato legível.

Para Castro entende-se o seguinte conceito:

> a criptografia consiste numa técnica de codificação de textos de tal forma que a mensagem se torne ininteligível para quem não conheça o padrão utilizado. Sua origem remonta às necessidades militares dos romanos (Escrita cifrada de César)”. (CASTRO, 2001, p.01).

A figura 2 destaca um exemplo de como funciona a criptografia, onde há um texto que é encriptografado pelo emissor ao ser enviado e ao chegar ao destino é decriptografado para respectiva leitura do receptor.

Figura 2 – Criptografia



Fonte: VIANNA, 2011.

A este processo de codificação dá-se a nomenclatura de cifragem ou encriptação. De acordo com Trinta e Macêdo:

> A palavra criptografia tem origem grega (*kriptos* = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem. (TRINTA; MACÊDO, 1998).

Esse processo de inversão da mensagem pode ser feito de duas maneiras um método de transposição que basicamente embaralha a ordem das palavras e o método de substituição no qual as palavras são trocadas com base em uma tabela de ciframento. Trinta e Macêdo (1998) discorrem sobre os métodos mencionados anteriormente da seguinte maneira:

> A primeira delas procura esconder o conteúdo da mensagem através de códigos predefinidos entre as partes envolvidas na troca de mensagens. [...] O outro método usado para criptografar mensagens é a cifra, técnica na qual o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso ao ciframento. Os principais tipos de cifras são:
>
> a. **Cifras de Transposição**: método pelo qual o conteúdo da mensagem é o mesmo, porém com as letras postas em ordem diferente. Por exemplo, pode-se cifrar a palavra "CARRO" e escrevê-la "ORARC". (TRINTA; MACÊDO, 1998).

Trata-se de uma cifra bem simplória a qual faz uso de algoritmos (softwares de computador) que fazem com que cada caractere introduzido pelo usuário ou

ainda, existente em um documento, seja invertido em ordem oposta a original protegendo a informação, de modo que qualquer interceptação dela deixe sem sentido esse conteúdo. Os autores descrevem ainda sobre o outro modelo de cifra relacionada à substituição. Trinta e Macedo continuam a afirmar:

> b. **Cifras de Substituição**: neste tipo de cifra, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. As cifras de substituições podem ser subdivididas em: **1) Cifra de substituição simples, monoalfabética ou Cifra de César**: é o tipo de cifra na qual cada letra da mensagem é substituída por outra, de acordo com uma tabela baseada geralmente num deslocamento da letra original dentro do alfabeto. Ela é também chamada Cifra de César devido ao seu uso pelo imperador romano quando do envio de mensagens secretas. César quando queria enviar mensagens secretas a determinadas pessoas, substituía cada letra "A" de sua mensagem original pela letra "D", o "B" pelo "E", etc., ou seja, cada letra pela que estava três posições a frente no alfabeto. **2) Cifra de substituição polialfabética**: consiste em utilizar várias cifras de substituição simples, em que as letras da mensagem são rodadas seguidamente, porém com valores diferentes. **3) Cifra de substituição de polígramos**: utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da mensagem. Por exemplo, "ABA" pode corresponder a "MÃE" e "ABB" corresponder a "JKI". **4) Cifra de substituição por deslocamento**: ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra "CARRO" utilizando o critério de rotação "023", seria substituir "C" pela letra que está 0(zero) posições a frente no alfabeto, o "A" pela letra que está 2 (duas) posições a frente, e assim por diante, repetindo-se o critério se necessário. A principal vantagem das cifras em relação aos códigos é a não limitação das possíveis mensagens a serem enviadas, além de ser tornarem mais difíceis de serem decifradas. As cifras são implementadas através de algoritmos associados a chaves, longas sequências de números e/ou letras que determinarão o formato do texto cifrado. (TRINTA; MACÊDO 1998) (grifo do autor)

Assim, é possível afirmar que a tecnologia se utiliza desses dois tipos de métodos para garantir a integridade, autenticidade, legitimidade e inalterabilidade das informações que trafegam em uma rede de computadores. Porém hão de serem usadas as cifras ou chaves que irão permitir o acesso ao documento. Ainda parafraseando Trinta e Macêdo:

> Do ponto de vista do usuário, as chaves de criptografia são similares as senhas de acesso a bancos e a sistema de acesso a computadores. Usando a senha correta, o usuário tem acesso aos serviços, em caso contrário, o acesso é negado. No caso da criptografia, o uso de chaves relaciona-se com o acesso ou não à informação cifrada. O usuário deve usar a chave correta para poder decifrar as mensagens. Tomando-se ainda a comparação aos sistemas de acesso a computadores, senhas dos serviços descritos acima podem possuir diferentes tamanhos, sendo que quanto maior for a senha de um usuário, mais segurança ela oferece. Assim

> como estas senhas, as chaves na criptografia também possuem diferentes tamanhos, e também seu grau de segurança está relacionado com sua extensão. Na criptografia moderna, as chaves são longas sequências de bits. Visto que um bit pode ter apenas dois valores, 0 ou 1, uma chave de três dígitos oferecerá $2^3 = 8$ possíveis valores para a chave. Sendo assim, quanto maior for o tamanho da chave, maior será o grau de confidencialidade da mensagem. (TRINTA; MACÊDO 1998).

Portanto, fica a critério dos administradores dessa rede optarem pelo melhor e mais adequado método que irá atender as suas necessidades, pois cada um tem suas características, vantagens, desvantagens e fazem uso de algoritmos específicos que são associados as chaves de criptografia, os quais foram sendo aprimorados no decorrer da evolução dessa ciência, conforme mencionado anteriormente no item 5.2

5.3 Formas de Criptografia

Existem duas maneiras simples de criptografias, a que se baseia no modo assimétrico e o simétrico que serão melhor explicitadas nos itens 5.3.1 e 5.3.2.

5.3.1 Simétrico

Essa é a forma de criptografia simples e foi a primeira a ser utilizada, na qual as chaves são iguais e, portanto, deverão permanecer em segredo, também denominada de simétrica ou chave privada. Esta chave normalmente é uma senha que deve ser utilizada tanto pelo emissor, quanto pelo receptor da informação. Parafraseando Oliveira:

> O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra. (OLIVEIRA, 2012, p 02).

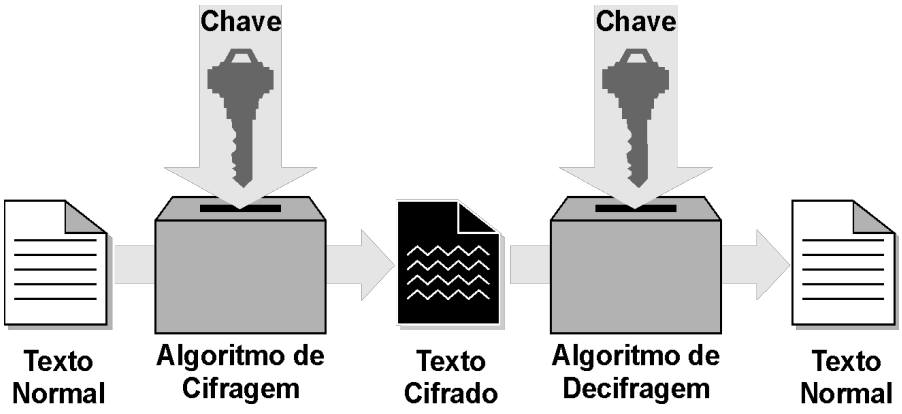
Esse tipo criptográfico tem a vantagem de ter seus algoritmos executados mais rapidamente, e também dispor de um custo mais acessível. Contudo, há de

existir um canal de comunicação seguro, com uma confidencialidade maior, pois a chave utilizada aqui é uma senha idêntica tanto para o emissor, quanto para o receptor.

> A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.
> O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem. (OLIVEIRA, 2012, p.02)

A figura 3 demonstra o formato de criptografia simétrico, no qual a mesma chave utilizada para envio será também usada para o recebimento no destino.

Figura 3 – Criptografia Simétrica



Fonte: TRINTA e MACÊDO, 1998.

5.3.2 Assimétrico

Forma criptográfica mais complexa do que a simétrica por não fazer uso somente de senhas idênticas, mas sim de chaves sendo uma privada e outra

pública, as quais são utilizadas para codificar e decodificar a informação para que apenas seja vista pelo receptor. Por conseguinte, esse tipo de criptografia requer uma complexidade maior no algoritmo que a controla, o que certamente demando um tempo maior para implementá-la e um custo no mesmo nível. Oliveira define a criptografia assimétrica como:

> Modelo de criptografia criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública. Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem. A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Por outro lado, o tempo de processamento de mensagens com criptografia assimétrica é muitas vezes maior do que com criptografia simétrica, o que pode limitar seu uso em determinadas situações. (OLIVEIRA, 2012, p. 03).

A figura 4 destaca a criptografia de forma assimétrica, na qual o emissor possui uma chave privada e envia um documento via internet até um receptor que dispõe de uma chave pública e poderá acessar o conteúdo do documento utilizando-a. A diferença entre as chaves é que o segredo da privada não é compartilhado.

Figura 4 – Criptografia Assimétrica

Fonte: CASTRO, 2007.

O fato do segredo da chave privada não ser divulgado proporciona uma segurança maior nesse formato criptográfico, o que torna a confidencialidade da mensagem garantida. Ainda parafraseando Oliveira:

> A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens. O óbice deste sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional. (OLIVEIRA, 2012, p. 04).

Portanto, esse tipo de criptografia é o mais utilizado em instituições que necessitam de maior confiabilidade e confidencialidade no envio/recebimento de documentos via Internet. Nunan, Farias e Santiago afirmam:

> A criptografia assimétrica não substitui a simétrica – na verdade a complementa. O desempenho computacional dos algoritmos simétricos é muito inferior aos dos assimétricos, o que torna seu uso pouco prático na cifragem de grandes quantidades de dados. Nesse caso os algoritmos assimétricos continuam sendo a melhor opção. (NUNAN, FARIAS e SANTIAGO, 2010, p. 207).

Existe, porém, outros recursos de segurança que podem ajudar a manter a integridade das informações que trafegam em uma rede, como a assinatura digital que será descrita no próximo tópico.

5.4 A Assinatura Digital e a Assinatura Digitalizada

Todo documento impresso necessita de uma validação seja por meio de uma marca d'água (timbre), um carimbo ou uma assinatura. No ambiente *web* surgiu a necessidade de se pensar em algo como a assinatura digital de modo que pudesse ser equivalentes à assinatura no documento impresso. Nesse sentido, é bastante contemporâneo e adequado o que Brasil (2013) diz:

> [...] a lei vem em nosso socorro fazer a devida equiparação e assim permitir que o fato social, já definitivamente consagrado, possa ser aceito com uma

> norma pacificadora dos conflitos por acaso existentes neste ambiente novo, que é a internet (BRASIL, 2013)

Ferreira (2004, p.100) define assinatura como: “Ato ou efeito de assinar; o nome escrito, firma [...]”. Fato que proporciona a identificação e autenticidade do documento. Assim como os documentos impressos, os digitais também precisam dessa autenticação que permitirá que as negociações *online* sejam lucrativas e seguras. Vieira a define do seguinte modo:

> A assinatura digital é um método de autenticação de informação digital tratada como análoga à assinatura física em papel. Embora existam analogias, também existem diferenças que podem ser importantes. O termo assinatura eletrônica, por vezes confundido, tem um significado diferente: refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica. A legislação pode validar, por vezes, tais assinaturas eletrônicas como endereços Telex e cabo, bem como a transmissão por fax de assinaturas manuscritas em papel. (VIEIRA, 2009).

Dessa forma, receptor e emissor estarão acordados de que o emissor de um documento ou serviço é realmente quem ele diz ser e os usuários podem navegar pela internet e acessar sites que utilizam as suas informações pessoais sem preocupar-se de serem enganados ou furtados. Existem algumas características sobre os documentos conforme destaca Volpi Neto (2002, p.50 apud BEHRENS, 2005, p. 34).

> Identificativa: Indica que é o autor do documento. Declarativa: significa assumir o conteúdo do documento pelo seu autor. Probatória: permite identificar se o autor da firma é efetivamente aquele que foi identificado como próprio naquela assinatura.

Ou seja, o fato de assinar digitalmente um documento proporciona a identificação dos partícipes no negócio, a declaração acerca do conteúdo disponível no documento, e a prova de que autor é aquele, em tese, disponível na assinatura. Levanta-se, a tese, porque no meio virtual nada é cem por cento, visto que a assinatura digital pode ser usada, transferida ou informada a outrem que não o próprio possuidor. Mas nos tempos modernos é a que dá relativa garantia aos procedimentos realizados no meio virtual e podem basear-se nas características dos documentos impressos.

Nesse sentido, utiliza-se da assinatura digital, a qual identifica a pessoa física ou jurídica e também serve para vincular ao documento eletrônico que se houver

qualquer alteração ao documento esta torna-se inválida. Sem a identificação inequívoca o documento não teria validade e estaria suscetível à fraude e modificação do conteúdo.

Esse recurso também faz uso das chaves públicas e privadas mencionados anteriormente no item que discorre sobre a criptografia assimétrica, porém a assinatura tem a finalidade de verificar quem enviou e quem assinou digitalmente o material enviado por rede de computadores, para conferir a veracidade do mesmo.

Assim, Devegili e Santos (2004, p. 205 apud Behrens 2005, p. 38), explicam o funcionamento da assinatura digital por meio de exemplificação, “se Alice encripta um documento com sua chave privada, qualquer pessoa pode usar a chave pública de Alice para decriptar o documento verificando, portanto, que este realmente foi assinado por Alice”. Oliveira em concordância com Devegili e Santos explica a criptografia e assinatura digital da seguinte maneira:

> O sistema de criptografia assimétrica ou de chave pública também é utilizado como um meio de assinatura digital. A pessoa que assina usa sua chave privada para criptografar uma mensagem conhecida, e o texto cifrado pode ser decifrado por qualquer um usando a chave pública desta pessoa, assim como uma assinatura em papel, consiste em um bloco de informação adicionado à mensagem que comprova a identidade do emissor, confirmando quem ele diz ser. O processo se baseia em uma inversão do sistema, onde o funcionamento da assinatura digital pode ser descrito como: o emissor cifra (ou seja, atesta autenticidade) a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá verificar a validade da assinatura digital, utilizando para isso a chave pública do emissor, reconhecendo de fato, que a mensagem não foi adulterada. Como a chave pública do emissor apenas decifra (ou seja, verifica a validade) mensagens cifradas com sua chave privada, obtém-se a garantia de autenticidade, integridade e não repudiação da mensagem, o que é apoiado pela função hashing (algoritmo), pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés do próprio emissor, o sistema de verificação não irá reconhecer a assinatura digital dele como sendo válida. (OLIVEIRA, 2012).

Face ao contexto digital e o grande tráfego de informação no meio virtual, resta a necessidade do documento eletrônico possuir a assinatura digital para que ele tenha validade do seu conteúdo.

Há que se ressaltar também de um modo que a sociedade vem se utilizando: assinatura digitalizada. No contexto jurídico não se vislumbram qualquer garantias de ser a mesma pessoa que assinou digitalmente o documento, o qual poderá ser questionado. Face ao contexto arquivístico e considerando à preservação digital verifica-se que:

- É a digitalização da manuscrita;
- Pode ser obtida de modo estático e dinâmico;
- É uma imagem;
- A sequência de bits pode ser colada e copiada diversas vezes e;
- Não pode garantir integridade, tampouco autenticidade do seu conteúdo.

Resta claro que todo documento eletrônico que possui a assinatura digitalizada, mesmo que realizada perante um agente público pode ser questionada e não se enquadrará aos princípios arquivísticos tradicionais.

5.4.1 Requisitos necessários da assinatura digital

O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, sendo a primeira autoridade da cadeia de certificação - AC Raiz.

O conceito de *autenticidade*, encontrado na diplomática é utilizado, também, como requisito da assinatura digital. Como fonte de prova, Rondinelli (apud FONSECA 1998, p.36) apresenta o seguinte conceito:

> Autenticidade: a autenticidade está ligada ao processo de criação, manutenção e custódia, os documentos são produto de rotinas processuais que visam ao cumprimento de determinada função, ou consecução de alguma atividade, e são autênticos quando criados e conservados de acordo com procedimentos regulares que podem ser comprovados, a partir de rotinas estabelecidas.

O documento arquivístico foi criado com um fim específico, ou seja, ele tem relação umbilical com alguma função ou atividade da Instituição. Assim, existe uma conectividade, conforme mencionado por Duranti (1998, p.06) “entre um fato a ser provado e o fato que o prova”.

À luz da MP-2.200 que regulamentou em um dos seus artigos a certificação digital (registro no ICP-Brasil), revigora dizendo que um documento produzido ou recebido em meio digital para possuir presunção de autenticidade faz-se necessário que ele seja assinado digitalmente, o qual conferirá a ela validade jurídica daqueles

assinados de próprio punho.

Em continuidade, tratar-se-á o termo confiabilidade requerido pela certificação digital ao documento arquivístico. As diretrizes elaboradas pela CTDE-CONARQ trazem como significação do termo confiabilidade “credibilidade de um documento arquivístico enquanto uma afirmação do fato”, ou seja, presumir-se-ão e sustentar-se-ão verdadeiros e confiáveis a informação contida nele, a qual é “estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção.

O termo integridade vincula-se diretamente à assinatura digital, significa dizer que foi estabelecida uma “imutabilidade lógica de seu conteúdo” (Instituto Nacional de Tecnologia da Informação - ITI, 2013), ou seja, posto a assinatura digital, a simples inserção de apenas um ponto final esquecido durante o processo de confecção do documento eletrônico, invalida a assinatura, pois já houve “adulteração” ao documento, deixando, portanto, de ser íntegro.

A Lei 11.419 de 19 de dezembro de 2006, que tratou sobre a informatização do processo judicial, já previa que os documentos gerados em sistemas eletrônico devessem ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garantisse a preservação e integridade dos dados (Art. 12 § 1º). Trazia o entendimento de que um documento após assinado digitalmente não tivesse seu conteúdo alterado. Para tanto, faz-se necessário preparar os sistemas eletrônicos para que ele identifiquem qualquer alteração não autorizada ao conteúdo. Isto é possível através de uma trilha de auditoria, por exemplo.

O último requisito que compõe a assinatura digital diz respeito ao *não-repúdio*, o qual impede as partes de negarem a participação no negócio do processo eletrônico.

Na prática, a certificação digital, funciona como uma carteira de identidade virtual e surge como um instrumento técnico-jurídico que assegura que os requisitos de autenticidade, integridade, confiabilidade e não repúdio estarão presentes durante o trâmite do documento no transcurso de determinada ação.

5.4.2 Criação da Assinatura Digital

As tecnologias estão disponíveis para todos com o intuito de melhorar e dar celeridade no processo de acesso à informação. Nesse sentido, a assinatura digital ou também denominada de assinatura eletrônica utiliza-se de mecanismos como os algoritmos com base em fórmulas matemáticas para proporcionar a segurança dessa informação.

Para tanto, existem diversos tipos de técnicas que irão identificar o emissor e receptor de um documento/informação em meio eletrônico. Volpi (2001 apud BEHRENS 2005, p. 39), expõe as técnicas aplicadas na assinatura digital:

> A checksum, a checagem de redundância cíclia (CRC), a função Hash, os algoritmos RSA e os algoritmos DAS (Digital Signature Algorithm). Todas essas técnicas trabalham sobre algoritmos de autenticação, por meio da aplicação de um processo lógico-matemático, levando ao alcance da assinatura pretendida.

Cada técnica apresentada por Volpi tem métodos e características diferentes que proporcionam um resultado satisfatório à necessidade de quem faz uso dele.

Para tanto, faz-se mister conhecer essas peculiares para que se possa optar pela que melhor irá atender a instituição a qual se deseja implantar a assinatura.

No quadro 1, estão resumidamente em destaque os algoritmos de CRC, RSA e DSA mencionados anteriormente, com as respectivas informações sobre cada um deles.

Quadro 1 – Algorítmos Aplicados na Assinatura Digital

Algorítmos	
CRC	A verificação de redundância cíclica (*Cyclic Redundancy Check* – CRC) é uma técnica de detecção de erros muito usada em redes de computadores. Uma mensagem deve ser enviada com o código de CRC calculado para que possa ser verificada no receptor. O cálculo de CRC é realizado através de uma operação de divisão. O emissor antes de enviar os dados realiza essa divisão na qual são gerados e adicionados alguns bits ao valor inicial e transmitidos ao receptor que também deverá realizar um cálculo e esse deve ser idêntico ao valor inicial para que a assinatura seja dita como correta.
RSA	O RSA (sigla baseia-se nos nomes de seus criadores – Ron Rivest, Adi Shamir e Len Adleman) é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma da criptografia assimétrica, há uma chave pública e uma chave privada, e a segurança do sistema baseia se na dificuldade da

	fatoração de números grandes.
DSA	Inventado pela NSA é patenteado pelo governo americano, o *Digital Signature Algorithm* (DSA), unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão *Digital Signature Standard* (DSS). Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Essa técnica é semelhante a anterior porém a diferença se dá pelo uso de uma chave pública irreversível.

Fontes: BATISTA, 2009, OLIVEIRA, 2012.

Os algoritmos em destaque no quadro supra, apresentam basicamente as mesmas característica mencionadas no início desse tópico. Entretanto, existem peculiaridades das referidas fórmulas matemáticas as quais se baseiam que os difere. Contudo, o funcionamento é basicamente o mesmo. Procedem como uma função denominada de *hash* que é bastante comum e trabalha assim como descrito no quadro 1 o RSA, porém com a peculiaridade de que cada arquivo ou documento enviado receberá uma assinatura digital diferenciada. Oliveira afirma:

> A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, é necessário o emprego de um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função *hashing*. Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente cifradas com a chave privada de alguém, ao invés disso, é empregada uma função *hashing*, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho, para oferecer agilidade nas assinaturas digitais, além de integridade confiável. (OLIVEIRA, 2012).

Para melhor explicitar a função *hash* o quadro 2, irá destacar os diferente tipos de técnicas existentes concernentes a essa função.

Quadro 2 – Principais Funções Hashing

Funções Hashing	
Funções	**Descrição**
SHA-2	O *Secure Hash Algorithm* (SHA-2) por outro lado significativamente difere da função *hash* SHA-1, desenhado pelo NSA é uma família de duas funções *hash* similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512. Eles diferem no tamanho, o SHA-256 utiliza 256 bits e o SHA-512 utiliza 512 bits. Há também versões truncadas de cada

	padrão, conhecidos como SHA-224 e SHA-384. O ICP-Brasil em suas mudanças anunciadas adotadas para o novo padrão criptográfico do sistema de certificação digital implantou em 2012, o uso do SHA-512 em substituição ao seu antecessor, o SHA-1. Um novo padrão proposto de função de *hash* desenvolvido, pela programação do NIST a competição que apresenta esta nova função *hash*, com a seleção de uma função vencedora, que denomina-se de SHA-3.
SHA-1	O Secure Hash Algorithm (SHA-1), uma função de espalhamento unidirecional inventada pela NSA, gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte do MD5, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Em 2005, falhas de segurança foram identificados no SHA-1, ou seja, que uma fraqueza matemática pode existir, o que indica que o uso de uma função *hash* mais forte é recomendável, o que motiva o uso preferencial de SHA-2.
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa *message digest*. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função *hashing* prévia de Rivest: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia.

Fonte: OLIVEIRA, 2012.

Quadro 2 – Principais Funções *Hashing* (Continuação)

Funções Hashing	
Funções	**Descrição**
MD5	Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor *hash* de somente 128 bits é o que causa maior preocupação; é preferível uma função *hashing* que produza um valor maior.
MD2 e MD4	O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um *hash* de 128 bits. A segurança do MD2 é dependente de uma permutação aleatória de bytes. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções *hash* citadas e acredita-se que seja menos seguro.

Fonte: OLIVEIRA, 2012.

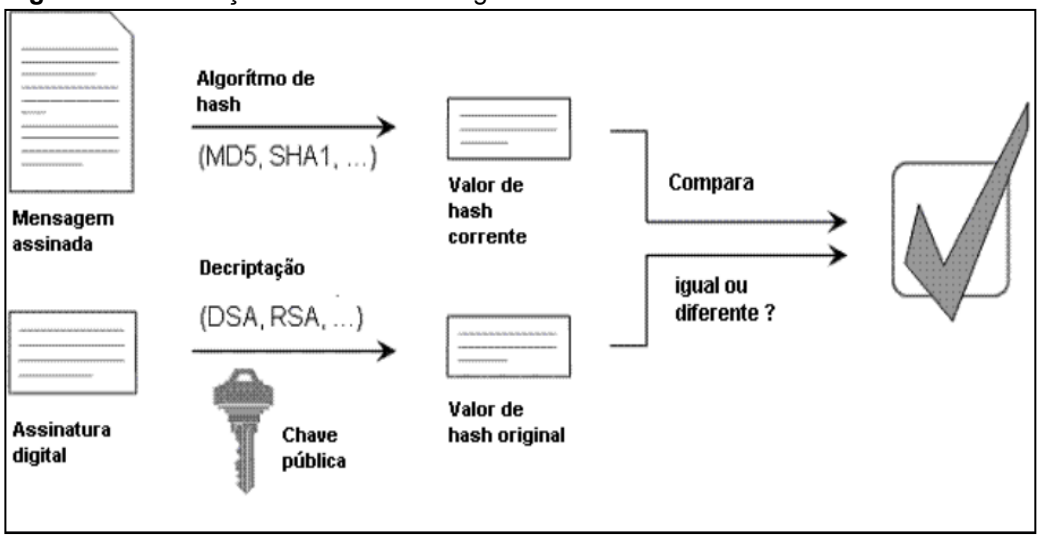
Conforme visto no quadro 2, a função *hash* vem sofrendo modificações para melhorar a questão do tamanho da manipulação de dados, a qual inicialmente tinha a capacidade de 128 bits e no ano passado foi anunciado a elaboração do *Secure Hash Algorithm* (SHA-2) que por sua vez consegue trabalhar com 512 bits de informações.

Portanto, cabe também ao administrador da rede de computadores que irá implantar a assinatura digital a opção de escolha no que tange o algoritmo de assinatura digital e a função *hashing* (que cifra apenas a parte que compõe a *message digest*, ou seja os códigos *hash* criados) a qual será utilizada para melhor atender as suas necessidades. Nunan, Farias e Santiago destacam:

> As funções digesto (ou mensagem digest) permite obter autenticação sem precisar aplicar operações de cifragem/decifragem a toda uma mensagem, recebendo como entrada blocos de dados de qualquer tamanho e retornando valores de tamanho fixo, de tal forma que qualquer alteração no bloco de entrada causa uma alteração no valor resultante do digesto. Algumas dentre essas funções digesto mais utilizadas são o MD5 e o SHA-1. Foram descobertas vulnerabilidades no MD5 de forma que o o SHA-1 e extensões (SHA-256, SHA-384 e SHA-512) são mais recomendados para uso. (NUNAN, FARIAS e SANTIAGO, 2010, p. 246).

A figura 5 destaca na parte superior da ilustração, a comparação do documento sendo encriptado (sendo enviado), no qual roda um algorítmo de *hash* que se utiliza da função digesto MD5 e SHA-1 (tendo uma chave de *hash* corrente), e na parte inferior da imagem após o envio ao destinatário o documento com a assinatura digital sendo decriptado por um algoritmo de DAS e RSA, os quais verificam a chave pública e fazem a comparação com o valor de *hash* original. Feita a comparação, se não houver nenhuma modificação na mensagem e nem na assinatura digital o documento é considerado válido.

Figura 5 – Verificação de Assinatura Digital



Fonte: adaptado de NAKOV, 2002 apud RIBEIRO, 2004, p.5.

A seguir Ribeiro (2004, p.06) relata algumas razões para invalidar as assinaturas digitais:

> No processo criptográfico de verificação, há pelo menos três possíveis razões para resultar em assinatura digital inválida:
>
> - Se a assinatura digital é adulterada (ela não é verdadeira) e é decifrada com a chave pública verdadeira, o valor original obtido não será o valor de '*hash'* original da mensagem original, mas algum outro valor;
> - Se a mensagem foi alterada (adulterada) após a assinatura, o valor de '*hash'* corrente calculado dessa mensagem adulterada será diferente do valor de '*hash'* original porque as duas mensagens diferentes correspondem a valores de '*hash'* diferentes;
> - Se a chave pública utilizada não corresponde à chave privada usada para efetuar a assinatura digital, o valor de '*hash'* obtido por decriptação da assinatura não será igual ao valor de '*hash'* corrente obtido a partir da mensagem.
>
> Se a verificação falhar, indica que a assinatura que está sendo verificada não foi obtida assinando a mensagem que está sendo verificada com a chave privada que corresponde à chave pública usada para a verificação. A verificação mal sucedida não significa necessariamente que uma tentativa de adulteração da assinatura digital foi detectada. Às vezes, a verificação pode falhar porque uma chave pública inválida é usada. Tal situação poderia ser obtida quando a mensagem não é emitida pela entidade que se esperou emití-la ou quando o sistema de verificação da assinatura tem uma chave pública incorreta para esta entidade. É mesmo possível para uma entidade possuir diversas chaves públicas válidas diferentes junto com certificados válidos para cada uma delas e do sistema ter tentado verificar uma mensagem recebida desta entidade com alguma destas chaves públicas, mas não com a correta (a que corresponde à chave privada usada na criação da mensagem assinada). (RIBEIRO, 2004, p. 6).

Outra questão relevante se faz em relação a certificação digital e como obtê-la, ou seja, a qual instituição ou autoridade certificadora se deve recorrer para isso. Essa situação poderá ser melhor explicitada no item 4.1.7 a seguir.

5.4.3 O Certificado Digital e a Autoridade Certificadora

Até aqui nota-se que a criptografia, a assinatura eletrônica e os demais recursos são complementares e que juntos permitem garantir a autenticidade das informações em rede. Nunan, Farias e Santiago explicam:

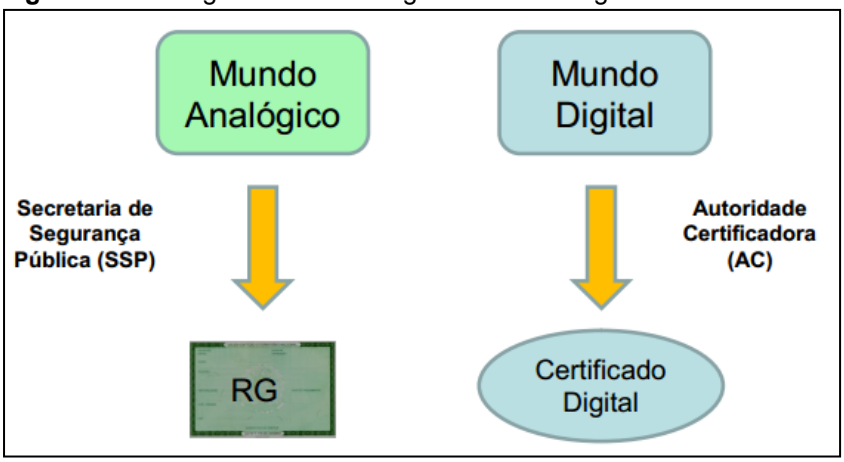
> A solução mais utilizada para a distribuição de chaves assimétricas é o certificado digital (CD): documento que vincula informações a uma chave pública assinado por um ente confiável. Este ente, emissor dos certificados, é chamado de Autoridade Certificadora (AC). (NUNAN, FARIAS e SANTIAGO, 2010, p. 247).

Desta feita, o certificado digital funciona como a validação em meio eletrônico de um documento ou arquivo o qual se deseja enviar de um emissor a um receptor, utilizando uma chave criptográfica e um ente (pessoa física ou jurídica, aplicação ou computador).

Esse certificado é concedido através de uma autoridade certificadora (como se fosse um cartório, que dá autenticação ou validade aquele documento).

A figura 6 expõe o mundo analógico que faz uso do Registro Geral (RG) para identificação dos cidadãos da sociedade humana o qual é emitido pela secretaria de segurança pública de cada estado. E o mundo digital que se utiliza do certificado digital para identificar as informações que tramitam no meio virtual o qual é emitido pela autoridade certificadora.

Figura 6 – Analogia Mundo Analógico x Mundo Digital



Fonte: USP, SD.

No Brasil existe a ICP – Brasil, entidade certificadora a qual emite os certificados digitais para controlar os documentos e informações dos usuários no mundo digital.

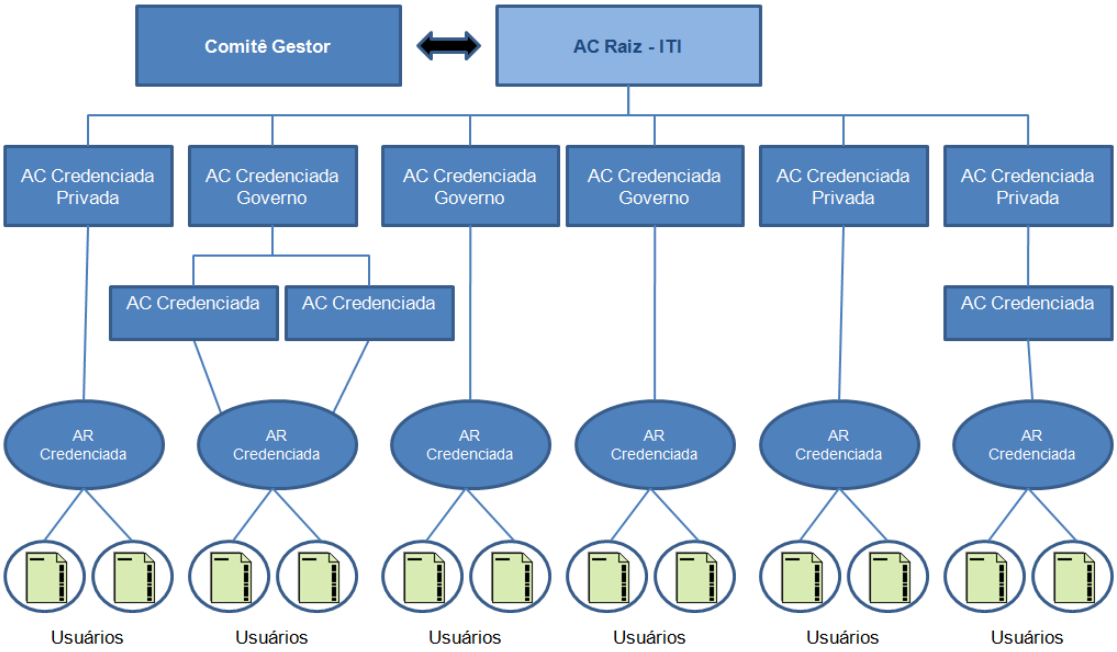
Fora instituída pela Medida Provisória N° 2.200-2/2001 com a finalidade de garantir a validade jurídica, integridade, confidencialidade e autenticidade de documentos no formato eletrônico.

Assim qualquer entidade que necessitar dispor de uma estrutura de segurança própria para validar sua documentação, possuir as suas respectivas chaves públicas. Nunan, Farias e Santiago descrevem claramente a estrutura hierárquica da ICP-Brasil.

> A ICP-Brasil (figura 6) apresenta uma estrutura hierárquica sendo autoridade certificadora raiz (AC Raiz) responsável por emitir certificados para as AC subordinadas.
> A AC Raiz é gerenciada pelo Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada ao Gabinete Civil. Observa-se que o modelo adotado pelo Brasil foi o de certificação com Raiz única, sendo que o ITI além de desempenhar o papel de Autoridade Certificadora Raiz – AC Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. (NUNAN, FARIAS e SANTIAGO, 2010, p. 245).

A figura 7 exibe o organograma hierárquico do ICP no Brasil, explicado nitidamente por Nunan, Farias e Santiago.

Figura 7 – Organograma da Hierarquia do ICP no Brasil



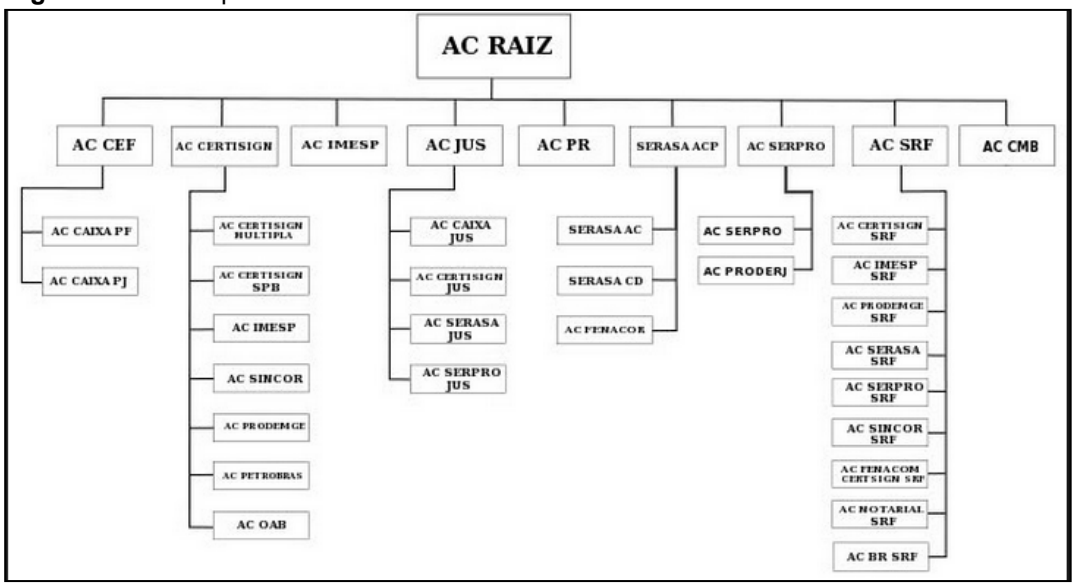
Continuando a descrição da hierarquia do ICP-Brasil, Nunan, Farias e Santiago discorrem:

> Opcionalmente a ICP também pode possuir Autoridades de Registro (AR) [...] que permitem descentralizar algumas funções das Autoridades Certificadoras, sendo que a maior parte destas relacionadas com os usuários/entidades finais. [...] Entretanto, a emissão dos certificados só pode ser feita pela Autoridade Certificadora (RCF 4210, 2010). (NUNAN, FARIAS e SANTIAGO, 2010, p. 244).

A figura 8 apresenta a hierarquia do ICP-Brasil com todas as suas autoridades certificadoras credenciadas (governo e privadas) e as Autoridades de Registro existentes.

Através da imagem nota-se que empresas e instituições financeiras, entidades governamentais compõem essa estrutura hierárquica, dentre as quais: a caixa econômica federal, Receita federal, Serpro, Serasa, Justiça federal, Presidência da República. Fica claro que nessa infraestrutura do ICP no Brasil só existem ACs, não havendo nenhuma AR.

Figura 8 – Hierarquia da ICP Brasil



Fonte: TUPINAMBÁ, 2010.

Todas as entidades que desejarem possuir uma Autoridade Certificadora subordinada a ICP-Brasil deverão ingressar com um processo de credenciamento junto ao Instituto. Esses processos serão avaliados e aprovados pela ITI. Os interessados podem solicitar essas autorizações por meio do site do Instituto Nacional de Tecnologia da Informação (www.iti.gov.br), conforme figura 9.

Figura 9 – Site do ITI – ICP – Brasil

5.4.4 Capacidade de Segurança

A sociedade mundial evolui e continua a desenvolver-se no âmbito da tecnologia, a cada dia que passa as TIC's, vem trazendo a sofisticação, a velocidade e a informação de maneira global ao alcance de todos. Até as pessoas que vivem em locais mais longínquos como a Amazônia com toda a sua imensidão e a dificuldade relacionada à logística fazem uso do aparato tecnológico existente: desktops, notebooks, *tablets* e *smartphones*.

Há vários ambientes que disponibilizam nesses municípios e no País os equipamentos mencionados no parágrafo anterior, como: laboratórios de informática, lan *houses*, telecentros de inclusão digital e outros que possibilitam a inclusão digital. Sem falar nas instituições como: a esfera judiciária, universidades e centros tecnológicos que levam a capacitação aos populares dessas localidades:

> Com a evolução da(s) TIC, particularmente no final do século XX e princípio do século XXI, assistiu-se a uma mudança global do mundo físico para o virtual. Quando a informação, e com ela a cultura humana, começa a viajar cada vez mais num ambiente digital, mediado por computadores, as infra-estruturas computacional e de comunicações devem ser expandidas para prover os mecanismos fundamentais necessários para apoiar na totalidade a cultura humana. (CRUZ, 2009, p. 49).

Nesse sentido, esse aparato tecnológico requer tecnologias relacionadas à segurança da informação que conforme Cruz menciona, "um desses mecanismos, amplamente reconhecido, mas pouco entendido, é a segurança, particularmente no que se refere à Segurança da Informação e das Comunicações (SIC)". (CRUZ, 2009, p. 49).

Esta é utilizada por toda essa clientela, pois as transações no meio virtual como: o comércio eletrônico, as transferências online, a troca de informações e outros fazem com que a criptografia seja fundamental para manutenção da segurança no ambiente digital. Parafraseando o autor supra diz que:

> A Associação Brasileira de Normas Técnicas (ABNT) estipula, por meio da norma ABNT NBR ISO/IEC 17799, que 'Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio' (ABNT, 2005, p. ix). E acrescenta a ABNT (2005, p. 1) que a Segurança da Informação consiste da 'preservação da confidencialidade da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade,

> responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas'. (CRUZ, 2009, p. 50).

Contudo, para assegurar a informação e sua confidencialidade, integridade e autenticidade utiliza-se de artifícios disponíveis na ciência da criptografia que dispõem de métodos que irão proporcionar segurança ao meio digital. Ainda seguindo as contribuições de Cruz:

> A questão da segurança da computação vista nos anos 1970 evoluiu para um problema de segurança de redes do século XXI. Alguns problemas foram resolvidos com relação ao passado, outros persistem, e muitos novos têm surgido. Igualmente importante é o fato de que novas ferramentas agora estão disponíveis. Nos anos 1970, a criptografia era primitiva, em comparação com os desenvolvimentos atuais. Dois aspectos da criptografia especialmente cruciais para a segurança computacional — a criptografia de chave pública e a função de *hash* criptográfico, estavam no seu nascedouro. Igualmente importante, a NSA, cujo monopólio de erudição criptográfica era maior do que agora, era a principal apoiadora das pesquisas de segurança computacional, mas desencorajou a aplicação de muitas técnicas criptográficas ao problema da pesquisa ostensiva. A peça final dos quebra-cabeças é o custo sempre decrescente de computadores. Agora é aceitável dedicar a capacidade computacional à segurança, numa escala inimaginável até pelo menos dez anos atrás. (CRUZ, 2009, p. 57).

Assim, os algoritmos criptográficos com base em fórmulas complexas de matemática estão a cada dia mais sofisticados e apresentam técnicas que são baseadas em ataques já ocorridos, e portanto, permanece o velho ditado, primeiro espera-se que o invasor adentre para poder solucionar o problema de segurança. Para Rezende:

> O projeto de um sistema criptográfico seguro deve ser feito somente após o modelo de ameaças ter sido compreendido. Este trabalho é o tema central da criptologia, e é muito especializado. A criptografia mescla várias áreas da matemática: teoria dos números, teoria da complexidade, teoria da informação, teoria da probabilidade, álgebra abstrata, análise formal, dentre outros. Poucos podem contribuir apropriadamente para esta ciência, onde um pouco de conhecimento é muito perigoso: criptógrafos inexperientes quase sempre projetam sistemas falhos. Bons criptógrafos sabem que nada substitui a revisão extensiva feita por colegas e anos de análise. Sistemas de qualidade usam algoritmos e protocolos publicados e bem compreendidos: usar elementos não provados em um projeto é no mínimo arriscado. O projeto de sistemas criptográficos é também uma arte. O projetista precisa atingir um equilíbrio entre segurança e acessibilidade, anonimidade e responsabilização, privacidade e disponibilidade. A ciência sozinha não garante segurança: somente a experiência e a intuição nascida da experiência podem guiar o criptógrafo no projeto de sistemas criptográficos e na busca de falhas em sistemas existentes. Bons sistemas de segurança são feitos de pequenos módulos independentemente verificáveis (e que tenham sido verificados), cada um provendo algum serviço que claramente se resuma a uma primitiva. Existem vários sistemas

> no mercado que são muito grandes para serem verificados em tempo razoável. (REZENDE, 2002, p. 07).

Esses projetos de sistemas criptográficos têm por base algumas possibilidades que devem ser verificadas em no âmbito digital, como: realização de downloads de arquivos em meio seguro, proteger transações de bancos e operadoras de cartões de crédito e outros são alguns dos objetivos a serem alcançados por esses sistemas, que conforme Corrêa (2002 apud BEHRENS 2005, p. 47) descreve:

- Tornar original uma mensagem enviada por correio eletrônico, mediante a utilização de assinaturas digitais;
- Tornar documentos pessoais inacessíveis e, assim privados;
- Verificar a identidade de outra pessoa online, que esteja acessando a rede;
- Verificar a fonte provedora de um arquivo que está sendo copiado; em outras palavras, tornar o 'download' mais seguro;
- Proteger transações financeiras;
- Habilitar o fluxo de caixa digital na Internet;
- Proteger a propriedade intelectual;
- Evitar opiniões ilegais e puni-las;
- Proteger a identidade e a privacidade de todos.

Dessa forma, os sistemas criptográficos usam seus métodos e mantém as transações virtuais menos vulneráveis. E o uso do recurso da assinatura digital só faz complementar a minoração dos problemas relacionados a segurança de TI, a qual resguarda a integridade da informação. De acordo com a afirmação de Bertol:

> O documento eletrônico juntamente com a assinatura digital confirma sua validade ao decifrar a assinatura digital com a chave pública do signatário, obtida no certificado digital. O resultado da decifração é o valor *hash* do documento eletrônico, conforme gerado pelo signatário. A seguir é realizado um novo cálculo do valor *hash* do documento e o compara com o valor *hash* recebido junto com o documento. Se forem iguais, significa que o documento eletrônico está íntegro e que é possível identificar o signatário por meio do certificado digital. Caso contrário, a assinatura digital é inválida. [...] Por si só, uma assinatura digital não diz nada sobre a verdadeira identidade do signatário e sua chave pública deve ser evidenciada a partir de um certificado digital. Na ICP-Brasil, o certificado digital deve ser criado por uma autoridade certificadora credenciada, o que lhe oferece u alto grau de confiabilidade. (BERTOL, 2009, p. 68).

Face ao recurso do certificado digital atrelado à assinatura digital, é importante salientar a questão da utilização da chave privada da autoridade certificadora, pois é por meio dela que será validada a assinatura via chave pública e

assim dar a garantia de que o documento eletrônico foi examinado pela cadeia de entidades da ICP-Brasil.

Outra característica imprescindível sobre a certificação digital esta relacionada a não reutilização da firma conforme Zoccolli alega:

> [...] não-reutilizabilidade, uma vez que a firma digital é gerada a partir de um cálculo efetuado em função do conteúdo específico de cada documento, não havendo possibilidade de transferência da firma digital, de um documento para outro, bem como a possibilidade do não-repúdio, uma vez que a pessoa que recebe um documento eletrônico portador de firma digital não necessitará, em nenhuma hipótese, de ajuda ou intervenção do autor para reconhecimento de sua firma digital – garantindo-se, assim, a autenticidade, uma vez que não será possível o autor, eventualmente, sustentar uma negativa de autoria. (ZOCCOLLI, 2000, p.190 apud BEHRENS, 2005, p. 49).

Os recursos tecnológicos até aqui aludidos são de suma importância para promover a validação jurídica, confiabilidade e segurança em todos os processos concernentes ao certificado digital. A concatenação de: criptografia, assinatura digital e certificação digital por meio de uma autoridade certificadora compõem o mix de segurança disponível no mercado.

Assim, todos esses recursos técnicos atrelados a *hardware*, *software* e *peopleware* treinados formam um grupo harmônico que afiançam a segurança da informação no mundo digital.

6. PROCEDIMENTOS METODOLÓGICOS

Ao final da trajetória acadêmica, muitas vezes, é necessário a elaboração do trabalho de conclusão de curso para obtenção do título de formação para o qual perlustrou a sua vida de estudante universitário. Nesse sentido, faz necessário o estabelecimento de algumas ações, orientando-se com os objetivos, definição de método etc até chegar à conclusão do objeto de trabalho. Dessa forma, vislumbra-se que "[...] a metodologia pode ser vista como conhecimento geral e habilidade que são necessários ao pesquisador para se orientar no processo de investigação, tomar decisões oportunas, selecionar conceitos, hipóteses, técnicas e dados adequados." (THIOLLENT, 2005, p.28).

Em continuidade ao conceito metodológico, Eva Lakatos (2001) posiciona-se da seguinte forma:

> [...] o conjunto das atividades sistemáticas e racionais que, com maior segurança e economias, permite alcançar o objetivo – conhecimentos válidos e verdadeiros -, traçado o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista" (LAKATOS, 2001, p. 83)

A partir da observação dos dois autores, ratifica-se a necessidade de ter um posicionamento metodológico para seguir, visando ao pesquisador chegar a resultados mais precisos. Por outras palavras, como se estivesse cumprindo um passo a passo, mas sem perder o foco durante a pesquisa.

6.1 Quanto à natureza

Tomando por base o procedimento metodológico defendido por Sylvia Vergara (2003, p.37), esta pesquisa optou pela abordagem qualitativa, uma vez que se visa analisar os "[...] microprocessos, através do estudo de ações sociais individuais e grupais, realizando um exame intensivo dos dados […]", objetivando não só estudar o fenômeno, mas também de entender seu funcionamento. No caso deste estudo as causas que estão a subsidiar a prática da assinatura digital como requisito de autenticidade aos documentos arquivísticos eletrônicos

6.2 Quantos aos fins

Devido o objetivo proposto, esta investigação optou pela pesquisa descritiva, e conforme citado por Cervo (1996, p.52) ela tem como escopo tentar "[...] descobrir, com a precisão possível, a frequência com que um fenômeno ocorre, […] sem manipulá-los". Nesse diapasão, procurar-se-á compreender como se dá o registro das assinatura digital aos documentos arquivísticos eletrônicos, visando conhecer e compreender a realidade diagnosticada, sem modificá-la.

6.3 Quanto ao meio

Entende-se como o meio, o método pelo qual o pesquisador trilha a sua investigação. Em outras palavras, é o *modus operandi* que seguirá com a pesquisa, visando atingir os objetivos propostos.

Nesse sentido, a investigação será realizada através de pesquisa bibliográfica, a partir de leituras de fontes primárias e secundárias, bem como a pesquisa de campo, a fim de estabelecer um estudo *in loco.* Para isso, Guerra (2001, p.44), diz ser necessário "[…] a escolha de uma pessoa, situação ou local para fazer uma análise intensiva, do tipo 'estudo de caso.'", pois partindo deste pressuposto ter-se-á uma investigação mais consubstanciada, ampla e detalha para a pesquisa.

6.4 Universo e amostra

Pelo fato de que o foco de estudo, a priori, estará voltado para os setores responsáveis pelo tratamento das informações judiciais, o universo a definido voltou-se para os profissionais do setor de TI da instituição pesquisada

6.5 Instrumento de coleta

Como procedimento metodológico, utilizar-se-á para a investigação as seguintes técnicas: questionário e entrevista, para subsidiar o desenvolvimento deste trabalho.

Optou-se por realizar uma entrevista gravada, com perguntas abertas e fechadas aplicadas ao profissional da área de TI da instituição objetivando conhecer se a instituição pesquisada possui estratégias de preservação aos documentos digitalizados e aqueles nato digitais.

6.6 Análise dos resultados

Como já mencionado, esta investigação seguirá a abordagem qualitativa. Neste contexto, o processo de análise de dados dar-se-á a partir do estudo de conteúdo, pois, conforme explica Goode (1979, p.400) “quando se aplica o código qualitativo ao conteúdo dos vários meios de comunicação […], ele é denominado análise de conteúdo”.

Por outras palavras, e utilizando-se da explicação de Campos (2004, p.611) “o método análise de conteúdo constitui-se em um conjunto de técnicas utilizadas na análise de dados qualitativos”, como será no caso desta investigação.

7. APRESENTAÇÃO E INTERPRETAÇÃO DOS RESULTADOS

No meio acadêmico é aceito que toda a pesquisa que se baseia em estudo de caso, estrutura-se em duas partes. Ela é ratificada por Terra quando informa o *modus operandi*:

> a primeira, associada à apresentação da ideia que se deseja investigar ou demonstrar como verdade e a segunda, associada à apresentação do estudo prático, juntamente com o processo de análise, de modo a comprovar ou negar as hipóteses construídas como verdades (TERRA, 2013, p.212)

Nesse sentido, esta investigação, escolheu como estudo de caso o Tribunal de Justiça do Amazonas (TJ/AM). Optou-se por essa instituição, pois entre as suas congêneres ela encontra-se bastante avançada no tocante à virtualização dos processos, pois a praxe vem sendo realizada, em tese, desde o ano de 2006.

Procurando alertar e contribuir para a melhoria da preservação digital na instituição judiciária pesquisada e observando que o processo de virtualização tem estabelecido mudanças internas, pois se está saindo do documento em papel para o meio virtual. Frisa-se, portanto, que se deve ir além da mera expectação de visualizar cada documento digitalizado, através do sistema informatizado. Deve-se trabalhar, ainda, para que estas informações estejam acessíveis ao longo do tempo e minorar ao máximo qualquer forma de corrupção dos sistemas, para que a confiabilidade e autenticidade não esteja ameaçada.

Nesta investigação buscou-se verificar como a instituição vem tratando à temática preservação digital no âmbito do processamento das ações voltadas ao processo judicial digital. Para isso, focou-se a Divisão de Tecnologia da Informação (DIVTIC), a qual é a responsável pela implementação. Assim, foi realizada a entrevista a partir da análise do *olhar interno*.

7.1 Análise do *olhar interno*

Conforme já apresentado ao longo desta investigação, a assinatura digital é elemento fundamental para garantir a autenticidade aos documentos judiciais digitais. Com base na resposta fornecida pelo entrevistado, notou-se que o TJ/AM apesar de estar trabalhando de modo totalmente virtual na capital, por algum tempo

utilizou-se da assinatura digitalizada (partes e advogados) para validar os processos. Isso é claramente demonstrado quando diz:

> Não soube informar o tratamento e foram perguntar a outro servidor, pois informaram que cuidavam especificamente do PROJUDI, o qual já possuía a assinatura digital
> Também não soube informar acerca da questão suscitada, muito embora tenha noção que início da virtualização os processos dos juizados especiais cíveis e criminais tenha se utilizado da assinatura digitalizada. (ENTREVISTADO N. 01, 2013).

Enquanto instituição judiciária decidida avançar na virtualização, tornando-se, quiçá, uma instituição pioneira no estado, observou-se que durante essa trajetória, esse conceito não era tão presente.

Quando se fala em autenticidade, envolve-se conceitos bem mais abrangentes, conforme dito por Ferreira (2006, p.50) "[...] integridade, completude, veracidade, validade, conformidade com o original, significância e adequabilidade ao fim a que se destina".

No contexto mais abrangente e como forma de comprovação de requisitos supramencionados, a simples aposição de uma assinatura digitalizada não garante por si só a confiabilidade ao documento original, porque pode haver corrupção durante a sua trajetória ou má fé nesse momento.

É primordial, também, ter sistemas confiáveis, em conformidade com as normas reguladoras vigentes, o que não se verificou na instituição pesquisada, visto que se questionou acerca do conhecimento da Resolução n. 91 de 2009 do CNJ, obtendo-se como resposta do entrevistado n.1: "Afirmou que não possui conhecimento acerca da resolução sobredita"

O mote que levou o Conselho Nacional de Justiça (CNJ) a aprovar uma Resolução acerca da matéria baseou-se a partir das questões suscitadas por Campos (2009, p.09) de "o como preservar, a responsabilidade pela preservação, os custos envolvidos, as autorizações de acesso e estratégicas para assegurar eficiência em todo o ciclo de vida do documento digital".

A partir da implementação dos requisitos consolidados pela normativa, ter-se-á condições e garantias mínimas que os procedimentos, por exemplo de captura e armazenamento, estejam assegurados, visto que seguiu uma diretriz (Resolução) emana de um órgão superior (CNJ):

> Que além de colocar em pauta a questão da preservação digital, procurou soluções por meio da adoção de um modelo de requisitos para sistemas informatizados do Judiciário, visando garantir a confiabilidade, a autenticidade e acessibilidade dos documentos e processos geridos por esses sistemas. (MOREQ-JUS, 2009, p.06)

A adoção desse modelo de requisitos determinado pelo CNJ garantirá a uniformização da produção, da tramitação, da guarda, da destinação, do armazenamento, da preservação, da recuperação, do arquivamento e do recebimento de processos e de outros documentos digitais, nato-digitais ou híbridos geridos pelos sistemas informatizados do Judiciário.

Seguindo questionou-se acerca de uma política especial para a preservação digital em longo prazo para os processos judiciais, a qual obteve como resposta:

> Deteve-se, especificamente, ao sistema PROJUDI-PR. Informava que todos os processos que são digitalizados ou aqueles nato digitais são armazenados numa pasta de um diretório e são gravados (back-up) no data center da instituição. De tempos em tempos esses arquivos são gravados em fita para que fiquem retidos por tempo indeterminado.
> Informa, também, que o TJAM possui outros sistemas como o SAJ-PG5 que gerencia os processos judicias de primeira instância. Para esse sistema ele diz que são gravados em banco de dados. Ele também recebe o tratamento de back-up e posteriormente são gravados em fita. Informou que no caso do PROJUDI-PR a realização de estrutura back-up, visto que facilita, na hora de fazer a comunicação com o interior, visto que a internet no interior do estado é bastante precária e dificultaria na replicação dos dados (ENTREVISTADO N. 01, 2013)

O entrevistado n. 01 considerou como uma política de preservação digital o armazenamento no data center da instituição e posteriormente a sua gravação em fita, embora a literatura referenciada no capítulo 3 desta investigação considere ser estratégias. Frisa-se que a política de preservação digital perpassa o estabelecimento de diretrizes, a definição de procedimentos para a gestão, a preservação e o acesso contínuo aos documentos arquivísticos digitais do TJ/AM, o que não se verificou haver na instituição pesquisada.

Quanto ao procedimento de controle para quem produz (partes/advogado/servidor etc) e para quem preserva (arquivo do TJ/AM) os documentos arquivísticos digitais e como ele é realizado, obteve-se como resposta:

> O controle é realizado a partir da assinatura, pois todo o documento que é emitido pelo advogado/servidor é necessário finalizá-lo com o token ou o certificado que é gerado pelo sistema para poder ser validado. Afirma que todos os servidores que vão trabalhar/movimentar os processos possuem assinatura digital.

> Em relação a quem preserva (arquivo) afirma que não tem procedimento para os arquivos, pois considera que o documento digital pode estar acessível a qualquer tempo. Considerou que a preservação digital para quem preserva não está bem estruturada na instituição (ENTREVISTADO N. 01, 2013).

Mediante a resposta do entrevistado, tornou-se fácil compreender a não existência de participação das unidades organizacionais da instituição. Ou seja, todo e qualquer decisão parte da DIVTIC e como gestora define todos os procedimentos necessários à implementação de ações relacionadas à virtualização do tribunal.

Pela entrevista concedida o que se tem de efetivo são: o armazenamento dos dados em data center, a duplicação desses dados armazenados em fita, atualmente a autenticidade garantida através do sistema PROJUDI possuir requisitos para requerer a assinatura digital, apenas daqueles que possuem token para assinar.

O objetivo geral desta investigação Identificar as estratégias de autenticidade eletrônica dos processos judiciais adotadas pelo Tribunal de Justiça do Amazonas. Ressalta-se que a instituição tem melhorado gradativamente na área de TI, esforçando-se, inclusive, para garantir que a informação judicial esteja acessível, mas falha na procedimentação, visto que não sistematiza as etapas e não as cumpre.

O meio digital é bem diferente do contexto físico. Engana-se quem pensa que a preservação do suporte ou da cadeia de bits garante, por si só que a informação continue acessível. A preservação da informação digital, de acordo com Ferreira (2006, p.51) “consiste, por vezes, em modificar ou transformar deliberadamente o objeto físico ou lógico que transporta a mensagem (ver Migração/Conversão)” como estratégias de preservação. Por isso, Ferreira (2006, p.51) reitera dizendo que urge a necessidade de definição de “quais propriedades da mensagem que deverão ser asseguradas durante o processo de transformação”.

Frisa-se que o conjunto de estratégias não é definitivo, tampouco estático, mas deverá ser levado em conta a natureza da instituição, as característica do acervo que deve preservado e, acima de tudo, levar em consideração que comunidade poderá ter interesse.

Destaca-se que apenas uma estratégia de preservação não é suficiente. Deve-se ter em mente o contexto da instituição, o tipo de documentação que ela produz e recebe para que possa ser definido o conjunto de estratégias a serem utilizadas para que se coaduna em uma política de preservação que contemplem os

processos e outros documentos digitais, não-digitais ou híbridos desde à produção até o arquivamento.

A título de exemplo e para entendimento didático de um tema complexo e ao mesmo tempo importante no atual contexto da sociedade e fazendo-se uma adaptação ao exemplo proposto por Ferreira (2006, p.52) trouxe para o contexto judicial o seguinte: Considere-se o arquivo responsável por preservar os processos judiciais (o repositório institucional de um tribunal, por exemplo). Se a sua política de preservação apenas especificar a propriedade significativa: preservação do conteúdo textual dos processos judiciais de guarda permanente, estes estarão, então, adequadamente preservados se apenas os caracteres ASCII [16] que os constituem forem conservados. Se por outro lado a política de preservação especificar propriedade significativas adicionais como a disposição do texto na página ou a sua formatação, então a preservação dos caracteres ASCII deixa de ser suficiente e passa-se a recorrer a formatos mais complexos, como por exemplo o PDF.

Os atuais preservadores (Divisão de TI) da instituição pesquisa custodiam toda a documentação no data center ou no banco de dados (da empresa contrata) e os mantém incólume para uma vez ou outra ser acessado.

Essa constatação sugere que os atuais gestores do acervo documental digital dialoguem com a demais unidades interessadas para que juntos formulem uma política de preservação digital, regulamentem as questões relacionadas ao valor probatório dos documentos eletrônicos, buscando a uniformização dos procedimentos aprovados pela Lei 11.419 de 2006.

[16] American Standard Code for Information Interchange. Trata-se de um conjunto de códigos capaz de reprenserntar letras, dígitos e outros símbolos, amplamente utilizado por computadores para a troca de informação textutal.

8. CONSIDERAÇÕES FINAIS

A instituição pesquisada pauta fundamentalmente seus objetivos, metas e ações nas expectativas do cidadão que procura o judiciário. Grandes e significativas mudanças ocorreram durante os últimos sete anos desde a implantação do processo judicial eletrônico. Com essas mudanças, surgiram necessidades de melhorias práticas de gestão eletrônica da documentação judicial para tornar a prestação jurisdicional mais rápida, eficiente, com qualidade, mas sobretudo pautada em ações preservacionista para que não se incorra em uma amnésia digital.

A pesquisa perlustrou um tema pouco explorado no nível do Poder Judiciário, visto que tentou identificar se os requisitos de autenticidade, integridade, confiabilidade e o não-repúdio da assinatura digital em processos eletrônicos estavam garantidos, conforme preconiza o ICP-Brasil.

Em continuidade, este trabalho tentou responder a três objetivos específicos: a) contextualizar as estratégias preservação digital existentes na literatura. Identificou-se na literatura existente no mínimo doze tipos de estratégias de preservação, conforme referenciado por Ferreira (2006) e Cunha e Lima (2007). A instituição pesquisa utiliza-se do migração/conversão, mas destaca-se que essa estratégia sempre há perda de informação e do refrescamento, o qual não é armazenado em mídia de dvd, por exemplo, e sim num banco de dados. Ressalta-se que a instituição apesar de utilizar-se de ao menos dois tipos de estratégia, encontra-se bastante incipiente a preservação, visto que não existe diálogo com outras áreas, como arquivo e tudo é decido no âmbito da Divisão de TI

Outro objetivos específicos perlustrados foram: b) verificar se as estratégias de preservação digital encontradas estão enquadradas na etapa da criação de uma política de preservação digital e c) apontar a existência de regulamentações institucionais que serviriam como início de uma política de preservação digital. Optou-se por reuni-los na resposta em virtude item c, pois no TJAM não há nenhuma regulamentação acerca de uma política de preservação digital, a qual defina procedimentos para gestão, a preservação e acesso contínuo aos documentos arquivísticos digitais para o Tribunal.

Constatou-se que há um problema de ordem conceitual quando se trata de assinatura digital versus assinatura digitalizada. Os gestores, quando entrevistados, fogem ao conceito quando afirmam categoricamente que todos os processos

judiciais, desde à implantação, no ano de 2006 possuíam garantias de autenticidade, mas da análise dos resultados verifica-se que nos auspícios da implantação muitos processos dos juizados especiais eram assinados através da assinatura digitalizada, a qual não garante autoria e integridade ao documento eletrônico.

Na construção legislativa encontra-se o artigo 216 § 2º da Constituição Federal, o qual assegura uma política de gestão documental e os meios para franqueá-las. A Lei 11.419/2006, em seu art 12 § 1º é claro quando diz que os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados.

Ressalta-se, também, que nenhum sistema computacional encontra-se imune a qualquer corrupção, quer seja ela acidental, quer seja criminosa ou por mal funcionamento, deixando a sua confiabilidade e autenticidade ameaçadas.

Com efeito, o arquivista deve colaborar com a instituição no sentido de alertar, conscientizar e orientar sobre as práticas de preservação digital, o impacto acerca da não implementação de uma política segura, eficiente e eficaz ao processo judicial eletrônico. Desta forma, tentou-se com a pesquisa algo nesse sentido, pois à medida que se identifica as praxes realizadas na instituição, demonstrava aos responsáveis da TIC quão vulnerável encontrava-se a preservação digital aos processos judiciais.

Nesse expectro, resta claro que a instituição deve trabalhar sob dois parâmetros: o legado e a documentação vigente, buscando medidas de segurança que visam aumentar o grau de proteção à documentação produzida no meio digital e de acordo com Moreira (2012, p.145) é “fortificando seu valor de prova (confiabilidade + autenticidade). Assim, no que tange aos processos judiciais digitais, o mais correto é se pensar em níveis de confiabilidade e de autenticidade”.

Verifica-se que das respostas ao questionário os sistemas, tanto o PROJUDI quanto o SAJ não possuem, em sua maioria, os requisitos exigidos pela Resolução n. 91 do CNJ:

> Art. 3° Os sistemas legados que ora servem às atividades judiciárias e administrativas do Conselho e dos órgãos integrantes do Poder Judiciário deverão aderir ao MoReq-Jus, conforme o seguinte cronograma:
> I - Adesão aos requisitos de “organização dos documentos institucionais”, “preservação”, “segurança”, “avaliação e destinação”, até dezembro de 2012.
> II - Adesão aos demais requisitos até dezembro de 2014 (BRASIL, 2009).

Durante a entrevista, constatou-se a falta de conhecimento dos profissionais da TIC acerca do ato normativo, o que ratifica mais ainda a necessidade de revisão dos sistemas para realizar a aderência aos requisitos.

Ademais, por se tratar de uma Resolução, não se identificou por parte do CNJ qualquer tipo de fiscalização ou sanções aos tribunais que não cumprirem os requisitos. Como se trata de uma mudança de cultural e quebra de paradigmas, seria mais interessante, em um primeiro momento, elaborar um estudo estatístico acerca do andamento de implementação da Resolução. Todavia, há uma certeza que nenhum tribunal cumpriu até o ano passado inciso relacionado à gestão documental.

Quanto ao arquivo, verificou-se que não houve tratativas com a unidade organizacional para o iniciar os trabalhos acerca de procedimentos garantidores de manutenção, avaliação, destinação e preservação da documentação nato digital, bem como afirma que a questão da preservação digital na instituição não se encontra bem estruturada.

Durante a entrevista, ouviu-se bastante dos respondentes que não havia a necessidade de eliminação, considerando haver a espaços disponível (terabytes) no data center da instituição. Há uma corrente que vem advogando que com o avanço tecnológico e o barateamento dos dispositivos de armazenamento, não há a necessidade de “eliminação” da informação.

No entanto, as duas reportagem “Sistema SAJ do Tribunal de Justiça segue fora do ar” e o “Grande culpado”, ilustrados na justificativa da pesquisa demonstram que a “pane nos sistemas” pode ter afetado o banco de dados do TJAM. Tratando-se de sistemas, essa inoperância é bem atual e deixam os profissionais da informação bastante preocupados. Na atualidade, não se concebe os profissionais da TI trabalharem de forma isolada. A reportagem ilustrativa, chama a atenção para a incorporação de preceitos de gestão documental, isto porque não apenas eliminaria a informação inútil, bem com a economia de recursos (evitando a aquisição de novos *storages*), muitas vezes tão escassos nas instituições judiciárias.

Durante a trajetória de investigação, buscou-se verificar se os requisitos de autenticidade da assinatura digital estavam sendo resguardados a todos os processos judiciais digitais, os quais estão sendo atendidos integralmente no sistema PROJUDI e parcialmente no sistema SAJ-PG5, visto que nos termos de

audiência de conciliação dos juizados especiais cíveis e criminais, os processos persistem com a assinatura digitalizadas de partes e advogados.

Quanto as sugestões desta investigação para que tanto à autenticidade estejam garantidas, quanto a preservação digital também, propõem-se: a) Envolver o profissional arquivista, no sentido de conscientemente, orientar a preservação daquilo que os documentos têm de mais importante: o caráter de prova; b) Estabelecer uma Resolução que defina diretrizes e procedimentos para a gestão, a preservação e acesso contínuo aos documentos arquivísticos digitais do TJAM; c) propor a mudança da utilização da assinatura digitalizada para a assinatura manual aos processos judiciais dos juizados especiais cíveis e criminais, enquanto não houver procedimentos reais, visando garantir a autenticidade dos processos judiciais digitais; d) Elaborar um modelo plano de preservação digital para documentos jurídicos, visando dar uma linha de orientação para a instituição investigada que produz e depende, em maior ou menor percentagem, de informação criada e mantida em formato digital. Esse modelo servirá para tomar medidas que possam garantir as condições materiais mínimas para preservar informação digital, durante o período pelo qual a organização dela necessite; e) propor um modelo de interoperabilidade entre o sistema automação judicial privado com o sistema de gestão de documentos, permitindo consulta, recuperação, importação e exportação de informações e documentos e seus metadados e; f) desenvolver ou adquirir um repositório digital confiável (software livre) para a preservação de objetos digitais

Por fim, reitera-se que a participação do profissional arquivista em projetos dessa magnitude é indispensável, justamente, pois ele irá colaborar na construção de uma política de gestão documental voltada ao processos judiciais digitais.

REFERÊNCIAS

AMAZONAS. Tribunal de Justiça do Amazonas. **Portaria nº 1662 de 03 de julho de 2012. Declara suspenso os prazos processuais no período de 29 de junho a 03 de julho do corrente ano.** Disponível em:< http://www.tjam.jus.br/index.php?option=com_docman&task=cat_view&gid=496&limit=5&order=name&dir=DESC&Itemid=168>. Acesso em 16 de ago de 2013.

ANTUNES, Jaime. **A contribuição da Unicamp para a preservação digital**. Disponível em:< http://www.unicamp.br/unicamp/noticias/2012/10/24/contribuicao-da-unicamp-para-preservacao-digital>. Acesso em 30 de jun. 2013.

ARELLANO, Miguel Angel. Preservação de documentos digitais. **Ci. Inf**., Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004.

ANDRADE, Nelson Spangler de; RIBEIRO, Sândalo Salgado. A segurança da informação documental nos órgãos públicos. In: **Fonte – Prodemge**, 2012. Disponível em: http://www.prodemge.mg.gov.br/images/revistafonte/revista_12.pdf. Acesso em: 20 de jul de 2013.

BANDIERA. Cezar Luiz. **Justiça Efetiva** (Prêmio Inovare). Disponível em:< http://www.premioinnovare.com.br/praticas/projeto-justica-efetiva-738/>. Acesso em 11 de ago de 2013

BATISTA, Othon M. N. **Cálculo de Cyclic Redundancy Check** – CRC. Disponível em: <http://www.othonbatista.com/arquivos/redes/aulas/redes-othon-crc.pdf>. Acesso em: 12 de set de 2013.

BRASIL, Angela Bittencourt. **Assinatura digital não é assinatura formal**. Disponível em:<http://http://www.e-commerce.org.br/artigos/assinatura_digital.php>. Acesso em 16 de setembro de 2013.

BRASIL. Constituição da República Federativa do Brasil (1988). Diário Oficial da União: Presidência da República, Brasília, 10 out; 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 25/04/2013.

_____. **Decreto-Lei n°. 2.848**, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Presidência da República, Brasília, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em 30/05/2013.

_____. **Decreto-Lei n°. 3.689**, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 30/05/2013

_____. **Lei n°. 5.869**, de 11 de janeiro de 1973. Institui o Código de Processo Civil. Diário Oficial da União: Presidência da República, Brasília, 17 jan. 1973. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5869.htm>. Acesso em 30 de maio de 2013.

_____. **Lei nº 8.159**, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados. Disponível em: <www.planalto.gov.br/ccivil/leis/L8159.htm>. Acesso em 02 de junho de 2013.

_____. **Lei 10.358** de 27 de dezembro de 2001. Altera dispositivos da Lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, relativos ao processo de conhecimento. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10358.htm>. Acesso em 16 de abril de 2013

_____. **Lei n°. 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Oficial da União: Presidência da República, Brasília, 11 jan. 2002. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 15/08/2013.

_____. **Lei n°. 11.280**, de 16 de fevereiro de 2006. Altera os arts. 112, 114, 154, 219, 253, 305, 322, 338, 489 e 555 da Lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, relativos à incompetência relativa, meios eletrônicos, prescrição, distribuição por dependência, exceção de incompetência, revelia, carta precatória e rogatória, ação rescisória e vista dos autos; e revoga o art. 194 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil. Diário Oficial da União: Presidência da República, Brasília, 17 de fev. 2006a. Disponível em:<http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11280.htm>. Acesso em: 15/08/2013.

_____. **Lei 11.341**, de 07 de agosto de 2006. Altera o parágrafo único do art. 541 do Código de Processo Civil - Lei nº 5.869, de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11341.htm>. Acesso em 10 de junho de 2013.

_____. **Lei 11.419**, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Diário Oficial da União: Presidência da República, Brasília, 20 dez. 2006b. p. 2. Disponível em: <http://www.presidencia.gov.br/legislacao>. Acesso em: 28/05/2013.

_____. **Lei 12.527** de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União: Presidência da República, Brasília, 18 de novembro 2011. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 01 de maio de 2013.

_____. **Medida Provisória n°. 2.200-2**, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial da União: Presidência da República, Brasília, 27 ago. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 16/06/2013.

_____. **Mensagem de veto n°. 1.445**, de 27 de dezembro de 2001. Diário Oficial da União: Presidência da República, Brasília, 27 dez. 2001. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/Mensagem_Veto/2001/Mv1446-01.htm>. Acesso em: 16 de junho de 2013.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Instrução normativa n. 01** de 11 de fevereiro de 2008. Dispõe sobre o registro dos repositórios e credenciados da jurisprudência do Superior Tribunal de Justiça, em mídia impressa e eletrônica, e em páginas e portais da Rede Mundial de Computadores. Disponível em:< http://www.stj.jus.br/portal_stj/publicacao/download.wsp?tmp.arquivo=953>. Acesso em 11 de julho de 2013.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Carta para a preservação do patrimônio arquivístico digital**: preservar para garantir o acesso. Disponível em: <www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf>. Acesso em 02 de julho de 2013.

_____.**Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Câmara Técnica de Documentos Eletrônicos (CTDE), 2012.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n°. 91, de 29 de setembro de 2009**. Disponível em: <http://www.cnj.jus.br/atos-administrativos/atos-da-presidencia/323-resolucoes/12206-resolucao-no-91-de-29-de-setembro-de-2009>. Acesso em: 02 de novembro de 2012.

_____. **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)**. Disponível em:< http://www.cnj.jus.br/atos-administrativos/atos-da-presidencia/323-resolucoes/12206-resolucao-no-91-de-29-de-setembro-de-2009>. Acesso em 02 de novembro de 2012.

BATISTA, Othon M. N. **Cálculo de Cyclic Redundancy Check** – CRC. Publicado em: 2009. Disponível em: <http://www.othonbatista.com/arquivos/redes/aulas/redes-othon-crc.pdf>. Acesso em: 12/09/2013.

BEHRENS, Fabiele. **A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira**. Dissertação de Mestrado apresentada a Pontifícia Universidade Católica do Paraná – Centro de Ciências Jurídicas e Sociais – Programa de Pós-graduação em Direito Econômico e Social. Curitiba-PR: PUC-PR, 28 de Julho de 2005.

BELLOTO, Heloisa Liberalli. **Arquivo Permanentes**, 3. Ed. Rio de Janeiro: FGV, 2005.

BERTOL, Viviane Regina Lemos. **Uma Proposta para a Regulamentação da Certificação Digital no Brasil**. Brasíia: UNB – Faculdade de Tecnologia – Departamento de Engenharia Elétrica. Sob Orientação do Prof. Rafael Timótio de Sousa Jr. Publicado em: 07/2009 sob o Número: PPGENE.TD – 042/09.

BODÊ, Ernesto Carlos. **Definição de documento digital 2**. Disponível em:<http://preservedoc.blogspot.com.br/2011/04/na-ultima-mensagem-publicada.html>. Acesso em 01 de setembro de 2013.

CAMPOS, Claudinei José Gomes. Método de análise de conteúdo: ferramenta para análise de dados qualitativos no campo da saúde. In: **Rev. Bras. Enferm**. Ano 57, n.5 (set./out. 2004).

CAMPOS, Fernanda Maria. Informação digital: um novo patrimônio a preservar. In **Cadernos BAB**, Lisboa: APBAD, 2002, p.8-14

CASTRO, Aldemario Araújo. **O Documento Eletrônico e a Assinatura Digital** (Uma Visão Geral). Publicado em: Brasília, 30 de outubro de 2001, pela Universidade Católica de Brasília – Curso de Informática Jurídica e Direito da Informática. Disponível em: <http://www.aldemario.adv.br/doceleassdig.htm>. Acesso em: 12 set de 2013.

CASTRO, Rui Carlos. **Criptografia Assimétrica**. Publicado em: 28/06/2007. Disponível em: < http://assinaturas-digitais.web.simplesnet.pt/criptografia_assimetrica.htm>. Acesso em: 10/09/2013.

CERVO, Amado Luiz [et al.]. **Metodologia científica**: para uso de estudantes universitários . 4ª ed. São Paulo: Makron Books, 1996.

CETTO, Ana María y ALONSO GAMBOA, José Octavio (comps.) In: **Calidad e Impacto de la revista Iberoamericana [En línea]**, 1 ed. México: UNAM, 2011. Disponível em:<http://www.latindex.unam.mx/librociri>. Acesso em 03 de junho de 2013.

CHAGAS, Mário. Cultura, patrimônio e memória. In: INTEGRAR – CONGRESSO INTERNACIONAL DE ARQUIVOS, BIBLIOTECA, CENTRO DE DOCUMENTAÇÃO E MUSEUS, 1., 2002, São Paulo. **Textos**... São Paulo: Imprensa Oficial, 2002, p.135-150.

CORRÊA, Amarílis Montagnolli Gomes. **Preservação digital**: autenticidade e integridade de documentos em bibliotecas digitais de teses e dissertações. São Paulo: USP, 2010 (Dissertação)

CRUZ, Edilson Fernandes da. **A Criptografia e Seu Papel na Segurança da Informação e das Comunicações (SIC)** – Retrospectiva, atualidade e perspectiva.

Publicado em: Julho/2009. Brasília: Universidade de Brasília – Departamento de Ciência da Computação no Curso de Especialização em Gestão de Segurança da Informação e Comunicações. Sob Orientação do Professor: João José Costa Gondim. Disponível em: < https://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/edilson_fernandes.pdf>. Acesso em: 13/09/2013.

CUNHA, Jaqueline de Araújo; LIMA, Marcos Galindo. Preservação digital: o estado da arte. In: **Encontro Nacional de Pesquisa em Ciência da Informação** – VIII ENANCIB. Salvador, 2007. Disponível em:<http:// http://repositorio.ufrn.br:8080/jspui/bitstream/1/34/1/2007Ev_Preservacaodigital_JacquelineAC.pdf. Acesso em 04 de setembro de 2013.

DEFINIÇÃO de documento. Disponível em: http://www.google.com.br/search?hl=ptBR&lr=lang_pt&defl=pt&q=define:Documento>. Acesso em 16 de mar. de 2013 às 09:00.

DEFINIÇÃO de acesso. disponível em: http://houaiss.uol.com.br/busca?palavra=Acesso. Acesso em 22 de agosto de 2013.

DELMAS, Bruno. **Arquivos pra quê?**: textos escolhidos. São Paulo: Instituto Fernando Henrique Cardoso, 2010.

DIAS SOARES, Fernanda. Processo judicial eletrônico: Aspectos gerais e ações iniciais. In: **Âmbito Jurídico**, Rio Grande, XIV, n. 84, jan 2011. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=89000>. Acesso em 14 de abr de 2013.

DURANTI, Luciana. **Diplomatics:** new uses for anold Science. Society of American Archivists, Maryland, 1998.

FERREIRA, Aurélio Buarque de Holanda. **Mini Aurélio** – O dicionário da Língua Portuguesa. 7ª Ed. Curitiba: Positivo, 2004.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e actuais consensos. Portugal: Universidade do Minho, 2006. Disponível em:< http://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. Acesso em 22 de março de 2013.

FONSECA, Maria Odília. **Arquivologia e ciência da informação**. Rio de Janeiro: FVG, 2005.

GOODE, William J. [et al.]. **Métodos em pesquisa social**. 7. ed. São Paulo: Companhia Editora Nacional, 1979.

GONTIJO, Silvana. **O livro de ouro da comunicação**. Rio de Janeiro: Ediouro, 2004.

GUERRA, Isabel Carvalho. **Pesquisa qualitativa e análise de conteúdo**: sentidos e formas de uso. São João do Estoril: Principias, 2006.

GUINCHAR, Clarice; MENU, Michel. **Introdução geral às ciências da informação e documentação**. Brasília: IBICT, 1994.

ISO INTERNATION ORGANIZATION FOR STANDARDIZATION. **ISO 15489-1**: Information and documentation: records management. Set. 2009. Disponível em:<http://www.javeriana.edu.co/archivo/07_eventos/preserciondigital/memorias/index_archivos/norma/iso_15489-1.pdf. Acesso em 28 de agosto de 2013

ITUASSÚ, Oyama. **História do tribunal de justiça do amazonas**. Manaus: Governo do Amazonas, 2000.

LAKATOS, E. M. [et al.]. **Metodologia do trabalho científico** . 6ª ed. São Paulo: Atlas, 2001.

LUSENET, Yola. **Digital heritage for the future**. Cadernos BAD, v. 2, p. 15-27, 2002.

MICHEL, J. L'Information et documentation un domaine d'activité professionnelle en mutation : LCN Les Métiers du Numérique. **H_e_r_m_ès_**, v. 1, n.3, p. 47-64, 2000. Disponível em : <http://www.enpc.fr/~michel-j/publi/JM328.htm> Acesso em: 02 set. 2013.

MOREIRA, Leonardo Neves. **Confiabilidade e Autenticidade de Processos Judiciais Digitais**: caso de uma Ação de Habeas Corpus do Superior Tribunal de Justiça. Brasília: UNB, 2012 (Dissertação).

NARANJO, Christhian. **A verdade sobre o SAJ**. Disponível em:< http://www.diariodeumadvogado.adv.br/2012/07/03/a-verdade-sobre-o-s-a-j/>. Acesso em 15 de agosto de 2013.

NUNAN, Angelo Eduardo; FARIAS, Frank Douglas Cruz de; SANTIAGO, Marcus Fabiano Praciano. **Segurança de Redes**. Manaus: UEA Edições, 2010.

OLIVEIRA, Ronielton Rezende. **Criptografia Simétrica e Assimétrica**: os principais algoritmos de cifragem. Publicado em: 2012, artigo da revista de segurança digital. Disponível em: < http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acesso em: 11 de setembro de 2013.

O QUE É CERTIFICAÇÃO DIGITAL. Disponível em: < http://www.iti.gov.br/perguntas-frequentes/1743-sobre-certificacao-digital> Acesso em: 22 de agosto de 2013.

O QUE É PATRIMÔNIO CULTURAL. Fundarpe. Disponível em:< http://www.cultura.pe.gov.br/patrimonio.html>. Acesso em: 05 de setembro de 2013.

OWEN, John Mackenzie. Preserving the digital heritage: roles and responsibilities for heritage repositories. In: LUSENET, Yola de; WINTERMANS, Vincent (Ed.) Preserving the digital heritage: principles and policies, 2007. P. 45-49. Disponível em:<http://www.knaw.nl/ecpa/publ/pdf/2735.pdf>. Acesso em: 05 de setembro de 2013.

_____. Preserving authentic digital information. [s.d]. Disponível em: http://www.clir.org/pubs/reports/pub92/rothenberg.html. Acesso em 06 de setembro de 2013.

PAES, Marilena Leite. **Arquivo**: teoria e prática. 3 ed. Rio de Janeiro: FGV, 2004.

REZENDE, Pedro A. D. **Criptografia e Segurança na Informática**. Brasília: Universidade de Brasília, Publicado em:2002. Disponível em:< http://www.cic.unb.br/docentes/pedro/segdados_files/CriptSeg1-2.pdf>. Acesso em: 13 setembro de 2013.

RIBEIRO, José Adauto. **Segurança de Rede e de Sistemas**: XML Signature e os Desafios da Utilização de Assinatura Digital. Trabalho de Conclusão de Curso – Faculdade SENAC de Ciências Exatas e Tecnologia. Orientador: Prof. Dr. Volnys Borges Bernal. São Paulo: Faculdade Senac de Ciências Exatas e Tecnologia, 2004.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**. Rio de Janeiro: FGV, 2005.

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

ROTHENBERG, Jeff. **Avoiding technological quicksand**: finding a viable technical foundation for digital preservation. Jan. 1999. Disponível em:< http://www.clir.org/pubs/reports/rothenberg/pub77.pdf>. Acesso em: 06 de setembro de 2013.

SANTOS, Vanderlei Batista dos (org). **Arquivística temas contemporâneos**: classificação, preservação digital e gestão do conhecimento. 2 ed. Distrito Federal: SENAC, 2008.

SAYÃO, Luis Fernando. Preservação digital no context das bibliotecas digitais: uma breve introdução. In: MARCONDES, Carlos H. et al (Org). **Bibliotecas Digitais**: saberes e práticas. 2 ed. Salvador: UFBA, 2006, p.113-143.

SIQUEIRA, Jéssica Câmara. A noção de documento digital: uma abordagem terminological. In: **Em questão**, Porto Alegre, v. 18, n. 1, pag. 125-140, jan/jun 2012. Disponível em:<http://seer.ufrgs.br/EmQuestao/article/view/24172/19793>. Acesso em: 31 de agosto de 2013.

DIAS SOARES, Fernanda. Processo judicial eletrônico: Aspectos gerais e ações

iniciais. In: Âmbito Jurídico, Rio Grande, XIV, n. 84, jan 2011. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8900>. Acesso em 15 de abril de 2013.

TAKETOMI, Roberto Santos. **PJe é instaurado em Iranduba pelo TJAM**. Disponível em: http://www.cnj.jus.br/noticias/judiciario/19469-pje-e-instaurado-em-iranduba-pelo-tjam>.Acesso em 17 de jul. de 2013.

TERRA, Guilhermina de Melo. **Atuação do museu enquanto sistema aberto**: uma realidade possível. Portugal: Universidade do Porto, 2013 (Tese)

TIRADENTES, Ronaldo. **Sistema SAJ do Tribunal de Justiça segue fora do ar**. Disponível em: <http://www.cbnmanaus.com.br/ronaldotiradentes/sistema-saj-do-tribunal-de-justica-segue-fora-do-ar/>. Acesso em 15 de agosto de 2013.

THIOLLENT, Michel. **Metodologia da pesquisa-ação**. 14ª ed. São Paulo: Cortez, 2005.

THOMAZ, Katia P.; SOARES, Antonio José. **A preservação digital e o modelo de referência Open Archival Information System (OAIS)**: digital preservation na the Open Archival Information System (OAIS). DataGramaZero Revista de Ciência da Informação, v.5, n.01, 2004.

TRINTA, Fernando Antonio Mota; MACÊDO, Rodrigo Cavalcanti de. **Um Estudo sobre Criptografia e Assinatura Digital**. Publicado em: Setembro de 1998, pelo Departamento de Informática da Universidade Federal de Pernambuco. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 10 de setembro de 2013.

TUPINAMBÁ, Regina. **Certificação Digital**. Publicado em: 2010. Disponível em: < http://rtupinamba.blogspot.com.br/p/o-que-e-icp-brasil.html#.UjKQmcZJ714>. Acesso em: 13 de setembro de 2013.

UNESCO UNITED NATIONS EDUCATION, SCIENTIFIC AND CULTURAL ORGANIZATION. Charter on the preservation of the digital heritage. Oct. 2003. Disponível em:< http://portal.unesco.org/en/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html>. Acesso em 03 de setembro de 2013

USP. **Certificação Digital e Assinatura Digital**: A Experiência da Usp. Disponível em: < http://www.usp.br/arquivogeral/wp-content/uploads/anexo/palestras/silvio.pdf>. Acesso em: 12 de setembro de 2013.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em Administração**. 4ª ed. São Paulo: 2003.

VIANNA, Ricardo. **Criptografia** – PARTE I – A História da Criptografia. Da origem aos dias atuais. Publicado em: 26/05/2011. Disponível em: < http://prof-

ricardovianna.blogspot.com.br/2011/05/criptografia-parte-i-historia-da.html>. Acesso em: 10 de setembro de 2013.

VIEIRA, André. **Gestão da Informação na Era Digital** – Assinatura Digital. Disponível em: <http://gied.web.simplesnet.pt/assinatura_digital.htm>. Acesso em: 12 de setembro 2013.

APÊNDICE A – QUESTIONÁRIO DA ENTREVISTA

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS HUMANAS E LETRAS
DEPARTAMENTO DE ARQUIVOLOGIA E BIBLIOTECONOMIA
GRADUAÇÃO EM ARQUIVOLOGIA
INSTRUMENTO DE COLETA

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Esta pesquisa pretende analisar a assinatura digital como requisito de autenticidade aos documentos arquivísticos, sob a ótica da preservação digital no Tribunal de Justiça do Estado do Amazonas e está sendo desenvolvida por Manoel Pedro de Souza Neto, discente do Curso de Graduação em Arquivologia, da Universidade Federal do Amazonas para a elaboração do Trabalho de Conclusão de Curso, sob a orientação da Professora Carla Mara da Silva Silva

Os objetivos do estudo são: analisar as estratégias adotadas de autenticidade eletrônica aos processos judiciais em um Tribunal no Estado do Amazonas, identificar se há a existência de políticas de preservação digital a longo prazo dos documentos arquivísticos, verificar se as assinaturas digitais cumprem os requisitos do ICP-Brasil etc

A finalidade deste trabalho é: analisar se os processos judiciais digitais nato digitais e os digitalizados são autênticos.

Esclarecemos que sua participação no estudo é voluntária e, portanto, o(a) senhor(a) não é obrigado(a) a fornecer as informações e/ou colaborar com as atividades solicitadas pelo Pesquisador(a). Caso decida não participar do estudo, ou resolver a qualquer momento desistir do mesmo, não sofrerá nenhum dano. Caso necessite de algum esclarecimento, por favor, entre em contato com Natacha Janes pelos telefones 9351-2990 e 8448-1008, ou pelo email: nettotheone@gmail.com

Esse estudo possui finalidade de pesquisa acadêmica, os resultados da pesquisa serão analisados e publicados, a não ser com prévia autorização, sua identidade não será divulgada, sendo guardada em sigilo.

Manaus, 18 de setembro de 2013.

Entrevistado n.01

Manoel Pedro de Souza Neto
Discente de Arquivologia – UFAM

QUESTIONÁRIO

1. Existe uma política especialmente criada para a preservação digital em longo prazo para os processos judiciais?
Sim
Não

1.1 Em caso positivo, pode descrevê-la como se dá no TJ/AM?

2. Estão determinadas na política as estratégias escolhidas para garantir a preservação do acervo de processos judiciais?
Sim
Não

2.1 Informe as estratégias, ainda assim, adotadas de preservação? Qual(is)

3. Existe algum explicação sobre as estratégias e/ou porquê de sua escolha?

4. Os conceitos de autenticidade e integridade de documentos digitais estão presentes na política de preservação?
Autenticidade: qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração
Integridade: é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo)

Sim
Não

4.1 Em caso positivo, quais foram as definições adotadas pela TIC para esses dois conceitos?

5. Qual(is) são as estratégias e procedimentos adotados para preservação? Podes informá-la?

6. Como a Divisão de Tecnologia da Informação e Comunicação do TJ/AM verifica/audita a autenticidade e a integridade de documento a ser incluído aos processos judiciais virtuais/digitalizados?

6.1 Existem procedimentos de controle para quem produz (partes/advogado/servidor etc)? como ele é realizado?
Sim
Não

6.1.1 Para quem mantém/usa (unidades organizacionais do TJ/AM/advogado). Como é realizado?
Sim
Não

6.1.2 Para quem preserva (Arquivo do TJ/AM) os documentos arquivísticos digitais? Como é realizado?

Sim
Não

6.1.3.1 Quais são os metadados* de preservação adotados pelo TJ/AM?
*Dados que descrevem completamente os dados (bases) que representam, permitindo ao usuário decidir sobre a utilização desses dados da melhor forma possível. São dados que permitem informar às pessoas sobre a existência de um conjunto de dados ligados às suas necessidades específicas (Almeida, 1998)

Como eles são gerados?

6.1.3.2 Que tipo de estratégia o TJ/AM adota para o controle desses metadados?

7. O TJ/AM tem conhecimento acerca da Resolução n. 91/2009*?
*Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário e disciplina a obrigatoriedade da sua utilização no desenvolvimento e manutenção de sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Poder Judiciário
Sim
Não

7.1 Em caso positivo, qual é/foi (mês e ano) que o TJ/AM iniciou a sua implantação?

7.2 Qual(is) sistema(s)* hoje está(ao) sendo abrangido(s) pela Resolução?
*Compreende os sistemas desenvolvidos e/ou adquiridos pelo TJ/AM

8. Já foi constatado algum tipo de alteração em um documento?
Sim
Não

8.1 Em caso positivo, como a alteração foi detectada?

9. Todo o(s) sistema(s) judicial(is) utilizado(s) pelo TJ/AM estão registrados em alguma Autoridade Certificadora?
Sim
Não

9.1 Em caso positivo, qual(is) Autoridade(s) Certificadora estão registrado(s)

9.2 Essa(s) Autoridade(s) Certificadora(s) seguem as regras estabelecidas pelo Comitê Gestor da ICP-Brasil [associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas]
Sim
Não

10. Durante a trajetória de virtualização – desde 2006* – o TJ/AM utilizou-se por algum tempo da assinatura digitalizada (processos dos juizados especiais) e mais recentemente da assinatura digital (aos processos de 1ª e 2ª instâncias). Considerando que a assinatura digitalizada não garante a autoria e integridade do documento eletrônico como a DIVTIC tratou essa questão?

*Resolução n. 10/2006-TJ/AM – Determinava à Coordenadoria Geral dos Juizados Especiais Cíveis e Criminais que desse início à implantação gradual de processo eletrônico (virtual) em todos os Juizados Especiais Cíveis e Criminais, nos moldes do Projeto “Justiça Efetiva”, devendo estar em pleno funcionamento até o final do mês de novembro daquele ano.

10.1 O TJ/AM realiza conversão de formato aos processos judiciais?
Sim
Não

10.1.1 Em caso positivo, considerando que após a conversão de formato a assinatura digital* não corresponde mais a essa nova cadeia de bits e não garante mais autenticidade do documento. Como o TJ/AM está tratando a questão?
*Embora o documento conceitual seja o mesmo, passará a estar relacionado a uma nova cadeia de bits, que não tem mais a assinatura. Desta forma, a assinatura digital garante somente a integridade da cadeia de bits original, mas não a do documento conceitual ao longo do tempo.

11. Todos os documentos digitalizados (processos em tramitação físicos, petições, etc) foram certificados no âmbito da cadeia do ICP-BRASIL?
Sim
Não

11.1 Em caso negativo, explique o por quê?