MARCELO AMARO BUZ

O PROTAGONISMO BRASILEIRO NA DEFINIÇÃO DE PADRÕES INTERNACIONAIS DE ASSINATURA DIGITAL EM DOCUMENTOS DIGITAIS TRANSFRONTEIRIÇOS

Trabalho de Conclusão de Curso - artigo científico - apresentado à Comissão de Avaliação de TCC da Escola Superior de Guerra - *Campus* Brasília, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa

Orientador: Prof. Dr. Julio Menezes

Brasília
2020

MARCELO AMARO BUZ (RG 1070398555 SSP/RS)

MARCELO AMARO BUZ

O PROTAGONISMO BRASILEIRO NA DEFINIÇÃO DE PADRÕES INTERNACIONAIS DE ASSINATURA DIGITAL EM DOCUMENTOS DIGITAIS TRANSFRONTEIRIÇOS

Trabalho de Conclusão de Curso apresentado à Escola Superior de Guerra – Campus Brasília, como exigência parcial para a obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 23 de OUTUBRO de 2020

Prof Dr JULIO MENEZES
Orientador

NADIA XAVIER MOREIRA (CF T MB)
Avaliador 1

THADEU LUIZ CRESPO ALVES NEGRÃO (Cel R1 EB)
Avaliador 2

O protagonismo brasileiro na definição de padrões internacionais de assinatura digital em documentos digitais transfronteiriços

Marcelo Amaro Buz[1]

RESUMO

O ambiente virtual cada dia mais toma conta do cotidiano, com ele o incremento de documentos nato digitais. O Brasil é vanguardista ao assinar acordos bilaterais no meio digital. Um documento digital possui características distintas de um documento físico. A preservação de integridade, autenticidade, autoria e validade jurídica passa por garantir infraestruturas de assinatura digitais seguras. Ainda se confundem muito os conceitos de assinatura eletrônica e assinatura digital. O ordenamento jurídico de cada país tem soberania intramuros ao definir padrões, porém em se tratando de documentos transfronteiriços, com exceção da União Europeia, e mesmo assim restrito aos países membros, não há uma regra internacional que defina padrões de assinaturas digitais em documentos transfronteiriços. Considerando que o Brasil passa a assinar acordos internacionais por meio digital, em não havendo uma atenção a este requisito, se identifica um risco de ameaça potencial a defesa nacional. O presente artigo analisa os conceitos da relevância da integridade, da autenticidade, da autoria e da validade jurídica em documentos digitais e traz à luz o debate da importância do Brasil protagonizar-se na definição destes padrões mundiais de assinatura digital.

Palavras Chaves: Documento Digital. Padrão de Assinatura Digital. Risco à Segurança Nacional.

The Brazilian role in the international digital signature standards in cross-border digital documents definition

ABSTRACT

The virtual environment increasingly takes over the everyday, with it there is an increase of born digital documents. More recent nations begin to sign bilateral agreements in the digital medium. A digital document has characteristics distinct from a physical document. The preservation of integrity, authenticity, authorship and legal validity involves ensuring secure digital signature infrastructures. This theme is very developed in some countries, but the concepts of electronic signature and digital signature are still very confused. The legal system of each country has intramural sovereignty when defining standards, but in the case of cross-border documents, with the exception of the European Union, and even so restricted to member countries, there is no international rule that defines standards for digital signatures on cross-border documents. If there is no attention to this requirement, a national security risk may arise when we find that the Brazilian government signs international agreements through digital means. This article analyzes the relevance the preservation of integrity, authenticity, authorship and legal validity concepts and brings to light the debate on the importance of Brazil to be involved in defining these global digital signature standards

Keywords: Digital Documents. Attributes legal validity. International relations. National Sovereignty

---

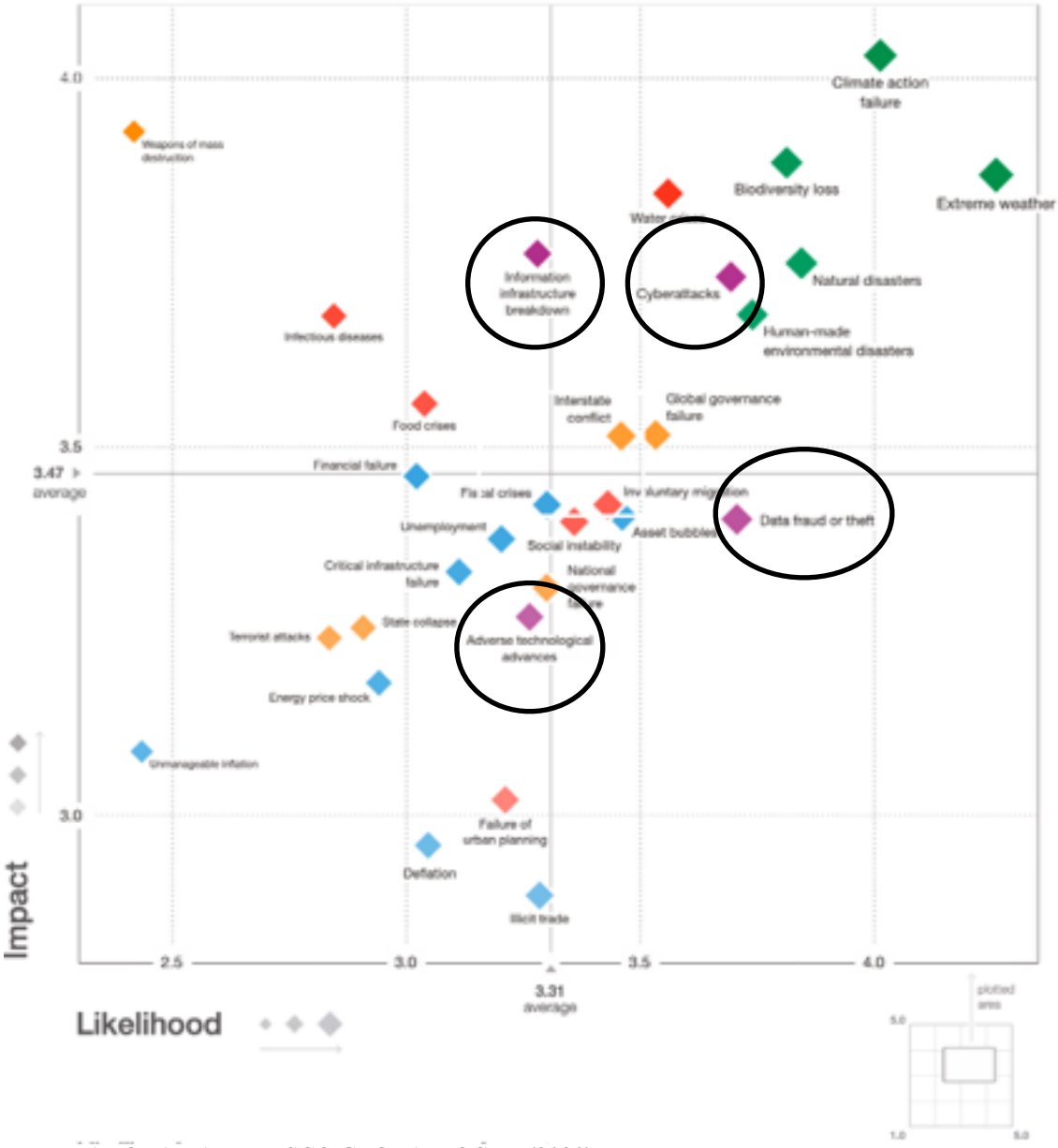
[1] Administrador de Empresas. Ex-presidente do Instituto Nacional de Tecnologia da Informação. Vereador no município de São Leopoldo. Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Guerra (ESG), Campus Brasília, 2020

1 **INTRODUÇÃO**

A cada dia se está mais exposto e vulnerável a ataques cibernéticos. Eles são impossíveis de prever seus limites e atuações, são inúmeros e incontáveis são as tentativas. As engenharias de ataques são mutantes e em constante evolução. Justamente por serem virtuais, possuem a agravante de terem características transfronteiriças. A Estratégia Nacional de Segurança Cibernética - E-Ciber (BRASIL, 2020a), em seu diagnóstico, apresenta o cenário no qual o Brasil está exposto. O Brasil é o 66º lugar no ranking das Organizações das Nações Unidas - ONU de tecnologia da informação e comunicação (TIC), onde apenas 11% dos órgãos federais têm bom nível de governança de TIC. Estas posições do Brasil demonstram o quanto encontra-se deficiente em relação a outras nações. Ainda há um grande caminho a avançar. E quando analisado o ranking do *Global Security Índex,* da International Telecommunication Union - ITU, apud E-Ciber (BRASIL, 2020a), o Brasil ocupa o 70º lugar. Por outro lado, conforme E-Ciber (BRASIL, 2020a), o uso da *internet* tem ganho destaque, pois já são mais de 116 milhões de pessoas, 98% das empresas e 100% dos órgãos federais e estaduais com acesso a rede mundial. Este cenário coloca o Brasil como o 2º país a ter grande prejuízo com ataques cibernéticos. A E-Ciber (BRASIL, 2020a) é enfática ao afirmar que "o risco para a economia brasileira, gerado pela intrusão em computadores e pela disseminação de códigos maliciosos praticados pelo crime organizado já é uma realidade" (BRASIL, 2020a, p. 9). Em termos internacionais, a E-Ciber (BRASIL, 2020a) afirma que em 2017, mais de 70 milhões de pessoas foram vítimas de crimes cibernéticos e 89% dos executivos passaram por alguma ocorrência de fraude em 2018. Estimam-se que os prejuízos decorridos destes crimes chegam na casa de US$ 22,5 bilhões.

As posições brasileiras demonstradas nos rankings acima se tornam ainda mais preocupantes quando analisa-se o Panorama de Riscos Global do Relatório de Risco Global 2020 da OCDE. A Figura 1 - Panorama de Risco Global mostra no eixo das abcissas a probabilidade de um risco ocorrer e no eixo das ordenadas o impacto que o risco pode causar se ocorrido. Os riscos circulados são aqueles vinculados a categoria Tecnologia. Com excessão das adversidades oriundas do avanço tecnológico, os demais riscos inerentes a tecnologia se posicionam nos quadrantes mais elevados, em especial ataque cibernéticos e fraudes e roubos de dados.

FIGURA 1 - PANORAMA DE RISCO GLOBAL



Fonte: PANORAMA DE RISCO GLOBAL, OCDE (2020)

Caso um ataque sistemático seja realizado, o impacto na sociedade, no governo e na democracia pode ser grande. Uma das formas de se mitigar impactos seria adotar cada vez mais padrões criptográficos (Organization of American States - OAS, 2020).

O primeiro acordo internacional assinado digitalmente pelo governo brasileiro, totalmente por meios cibernéticos, foi realizado com Peru no dia 2 de outubro de 2020. O acordo entre as duas nações teve como alcance o reconhecimento mútuo dos respectivos programas

administrados na modalidade segurança da cadeia logística internacional (CRYPTOID, 2020). O acordo impacta o comercio internacional bilateral e regulamenta algumas práticas administrativas de aduanas. Em conversa informal com Dr. Ruy Ramos, Assesor Especial da Presidência do Instituto Nacional de Tecnlogia da Informação - ITI, ele ressaltou que o acordo primeiro acordo internacional entre nações assinado digitalmente só foi possível após realizadas avaliações técnicas das infraestruturas de chaves públicas das partes. Complementa ainda que irão aumentar muito as relações internacionais entre Brasil e Peru, e esta mesma lógica deve ser ampliada para outros países (entrevista)[2].

Outro ato de relações internacionais que evidenciou o avanço de documentos digitais transfronteiriços foi o Acordo de Reconhecimento Mútuo de Assinaturas Digitais no Mercosul assinado em reunião de cúpula no dia 10 de dezembro de 2019. Este acordo possibilitará intercâmbio de documentos fiscais e aduaneiros, assinatura de contratos entre empresas sediadas nos diferentes países do bloco, rastreabilidade de produtos de livre comércio e reconhecimento automático de documentos eletrônicos produzidos a partir de certificados digitais no âmbito das infraestruturas oficiais de cada país, além de assinatura de tratados internacionais entre os chefes de estado. (MERCOSUL, 2019). Além destes dois exemplos, na União Europeia, desde de 2014, a lei que estabelece o *Electronic Identification, Authentication and Trust Services - eIDAS,* que regra os padrões para os documentos digitais com assinatura digital possibilite a interopaerabilidade entre os países membros do Bloco Econômico (PARLAMENTO EUROPEU E DO CONSELHO, 2014).

Com o incremento dos documentos digitais transfronteiriços, as nações tendem a definir atributos padronizados para reconhecimento de documentos digitais. A importância desta padronização diz respeito a validade jurídica dos atos, cujas manifestações de vontades passam a ser manifestados por meio eletrônico, inclusive entre nações. Não estar participando destes debates e até propondo padrões para reconhecimento internacional, podemos estar diante de termos que realizar investimentos que exigirão recursos físicos, humanos e financeiros. Tendo em vista que o país já possui um parque tecnológico instalado, uma serie de infraestruturas que podem servir como suporte para se integrar em uma futura rede de reconhecimento internacional de documentos digitais, não se pode ignorar que a temática pode ter impactos nos

---

[2] Ruy Ramos, Assessor Especial da Presidência do Instituto Nacional da Tecnologia da Informação. Doutor em Engenharia Eletrônica e Computadores pela Universidade do Porto em 2007.

bens nacionais, há o risco de torna-los obsoletos por eventual escolha de padrão no qual não se esteja preparado.

O conceito de segurança nacional "é aquele que considera qualquer fator capaz de comprometer a integridade dos bens do Estado e impedir ou dificultar os seus interesses (ABREU, 2018, p.53)". Um documento digital transfronteiriço pode impactar integridade dos Bens do Estado a partir do momento, que por exemplo, um acordo internacional regrando atividades aduaneiras passa a ser assinado por meio eletrônico. Na Figura 1, pode-se ver que o risco de sermos impactados por alguma ação na categoria Tecnologia. Esta se torna uma ameaça potencial ao Brasil quanto ele passa a ser protagonista do primeiro tratado internacional assinado digitalmente. Abreu (2018) traz a luz a antevisão do risco e o dano que ele pode causar caso não mitigado antes:

> O risco pode ser entendido como a antevisão do resultado de situação impactante indesejável em que se leva em conta a capacidade potencial de um emissor de determinada ameaça de explorar certa vulnerabilidade no sistema de proteção ou defesa, prognosticando um quadro sobre o possíveis damos a serem causados sobre o objeto referente caso não se altere a condição de fragilidade estrutural identificada. (ABREU, 2018, p. 74)

“É possível afirmar que no mundo contemporâneo existem ameaças em que todos os tipos de ambientes, em todos os países do mundo, em todos os níveis de análise. As vezes não percebidas como tal, mas existem” (ABREU, 2018, p. 60). Abreu (2018) afirma ainda que a ameaça é uma variável da percepção de quem a identifica. Tendo em vista que a emissão de documentos digitais transfronteiriços entre nações é uma ocorrência nova e atual, ainda não se tem uma percepção ou estudo do impacto deste risco. Ocorre que eles tendem a serem mais frequentes, expondo o país a riscos que podem caracterizar uma ameaça potencial.

Abreu (2018) fala do interesse nacional como ferramenta de ação política para preservar o que é melhor para a sociedade:

> O conceito de interesse nacional é utilizado na análise política e na ação política. Como ferramenta analítica é empregado para descrever, explicar ou avaliar as fontes de adequação da política externa de uma nação. Como instrumento de ação política, serve como meio de justificar, retificar ou propor políticas. Ambos os entendimentos, em outras palavras, referem-se ao que é “melhor" para a sociedade. (ABREU, 2018, p. 69)

A ausência de padrões de reconhecimento internacional de assinatura digital, e considerando que mesmo assim o Brasil vem assumindo riscos ao assinar acordos que impactam o interesse nacional traz a tona a necessidade de se iniciar o debate sobre a definição destes padrões. Para esta definição, inclusive pelo Brasil ser pioneiro, é importante que seja protagonis-

ta no cenário mundial. Para que os riscos iminentes não se tornem uma ameaça por crimes organizados, ou até conflitos interestatais ou transnacionais. Evidenciando-se assim que o tema a ser desenvolvido se relaciona com o campo de estudos de segurança e defesa nacional. Bem como é intrínseco na temática de Ciber Segurança, pois em se tratando de documentos digitais, seu meio de comunicação é o ambiente virtual. Da mesma forma trata-se de um assunto que pode impactar o Desenvolvimento Nacional, uma vez que, se o país passa a aceitar documentos digitais oriundos de outro país, é preciso garantir suas validades jurídicas.

A Revista Cenários de Defesa 2020 – 2039 (BRASIL, 2017) fala sobre a importância do Brasil adquirir protagonismo na promoção de temáticas crescimento econômico, cooperação e multilateralismo, que "poderiam aumentar o poder relativo brasileiro no contexto mundial, permitindo-lhe maior influência nas decisões globais e, dessa forma, diminuir a possibilidade de soluções bélicas para controvérsias" (BRASIL, 2017, p. 50). A consequência é o incremento do poder nacional e participação decisória do Brasil.

O presente estudo discorre sobre este ambiente de transformação digital, do avanço do documento digital. Faz uma reflexão acerca da importância do Brasil estar a frente do debate de escolha de padrões internacionais a serem adotados. Para tanto, expõem sobre a transformação digital e a estratégia de governo digital, explica-se as diferenças entre documentos físicos e digitais fazendo a incursão sobre a validade jurídica deles, alem de descrever algumas técnicas e atributos de segurança a serem aplicados. Na seqüência descreve a importância da criptografia e a necessidade de se manter a integridade, a autenticidade e a autoria dos documentos digitais bem como a segurança da identificação. Por último, aborda a assinatura em documentos digitais transfronteiriços, sua ameaça potencial aos interesses nacionais e a definição dos padrões internacionais de assinatura digital. O método de pesquisa é o exploratório descritivo em bibliografias disponíveis, dispositivos legais e observações pessoais do autor diante de experiências vividas como Presidente do Instituto Nacional de Tecnologia da Informação - ITI.

2 **TRANSFORMAÇÃO DIGITAL**

Segundo a Organização das Nações Unidas, "O tráfico do Protocolo Global da Internet, o "proxy" para fluxo de dados, cresceu de 100 Gigabytes (GB) por dia em 1992 para 45.000 GB por segundo em 2017... Para 2022 está projetado 150.700GB por segundo" (ONU 2019,

p. XV, tradução nossa). A popularização de telefones móveis, segundo Report Digital 2020 chega a 67% de penetração na população mundial (Hootsuite, 2020, p. 7). Toda infraestrutura que permite com que pessoas, empresas, instituições e governos se relacionem cada vez mais por meios digitais, a informatização da sociedade faz com que o volume dos documentos eletrônicos seja cada dia maior. E não é somente o volume de documentos que cresce, mas também sua relevância, sua importância. Muitos documentos de saúde, contratos entre partes, procurações, escrituras e documentos de identificação civil estão no mundo virtual. Em sua introdução, a Estratégia Nacional de Segurança Cibernética (BRASIL, 2020a) fala da revolução digital que pulsante na sociedade.

> A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à *internet*, da rápida adoção dos recursos de tecnologia da informação e comunicação, e das oportunidades econômicas e sociais oriundas do ambiente digital.
> Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade (BRASIL, 2020a, p. 2).

A guinada do mundo para o ambiente virtual é tamanha, que muitos documentos são nato digitais – não são mais derivados da versão física – nascem em ambiente virtual e nunca passam para o mundo físico. Os atributos de integridade, autenticidade, autoria e rastreabilidade perdem elementos físicos e passam a possuir elementos lógicos. E aí se encontra um desafio técnico de se garantir que quando alterados, corrompidos ou adulterados deixem rastros factíveis de serem periciados.

Intramuros, dentro de uma nação, existem diversas maneiras que podem garantir a segurança de que este ambiente virtual terá validade jurídica. Amparo legal, infraestruturas instaladas e – em última instância em países democráticos – há sempre o Poder Judiciário para realizar a justiça e litigar em torno de eventuais desacordos e contestações em relação a esses documentos. Logo, percebe-se haver segurança interna para que se possa ter no ambiente virtual garantias para se transacionar sem a necessidade de migrar para o ambiente físico, coletar assinaturas manuscritas e arquiva-los fisicamente. Porém, em se tratando de ambiente virtual, as fronteiras entre nações são facilmente ultrapassadas pelos documentos digitalizados. Um documento digital pode atravessar o mundo com a mesma conveniência, e velocidade do que se

for enviado de uma pessoa para outra a poucos metros de distância. E quando transacionado internacionalmente, quando corrompido e/ou alterado, pode provocar fortes impactos negativos em questões de defesa nacional.

E é neste ambiente internacional, de relacionamento transfronteiriço digital que há a necessidade de se utilizar atributos mínimos de segurança, previamente estabelecidos, que permitam as nações manterem confiança e não terem repúdio a documentos digitais, reconhecendo sua autenticidade, integridade e autoria, alcançando-se assim validade jurídica . Desta forma, preserva-se um relacionamento documental onde se pode confiar plenamente na originalidade e autenticidade. Garante-se assim que entes de diferentes países não entrem em rotas de conflitos. “Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais” (BRASIL, 2020a, p.2).

2.1. ESTRATÉGIA DE GOVERNO DIGITAL

Segundo dados do Ministério da Economia, em matéria publicada em abril de 2019, o Governo Federal contava com 621 mil servidores públicos civis concursados. Diante disto, o Governo Federal vem editando e priorizando uma série de medidas que vão ao encontro a este novo cenário de modernização do Estado. Elas tomaram impulso a partir da edição do Decreto 9.319/2018, que instituiu o Sistema Nacional para a Transformação Digital e estabeleceu a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital, cujo eixo temático que se destaca é o terceiro: Confiança no ambiente digital, no qual “o desenvolvimento da economia digital requer confiança no ambiente digital. Nesse sentido, a ação governamental deve estar focada em duas áreas: (i) proteção de direitos e privacidade; e (ii) defesa e segurança no ambiente digital” (BRASIL, 2018, p. 6). Digitalizar sem que se possa confiar no ambiente virtual é um contrassenso, e evidentemente deve ser um fator chave de sucesso.

Mais recentemente, o Decreto 10.332/2020, que instituiu a Estratégia de Governo Digital para o período de 2020 a 2022, diz que os princípios da transformação digital do governo têm objetivo final de reconquistar a confiança dos brasileiros. Naim (2013) fala da degradação do poder e traça correlações entre a confiança dos cidadãos em suas instituições, governos e governantes e a continuidade de determinado poder. Em se tratando de Brasil, uma democracia jovem porém com instituições fortes, manter a confiança da população no Estado demo-

crático de direito é extremamente importante. Neste cenário, esforços na transformação digital são essenciais. Entre os objetivos definidos no Decreto da Estratégia de Governo Digital (2020) encontram-se:

> - oferecer serviços públicos digitais simples e intuitivos, consolidados em plataforma única e com avaliação de satisfação disponível;
> - conceder acesso amplo à informação e aos dados abertos governamentais, para possibilitar o exercício da cidadania e a inovação em tecnologias digitais;
> - promover a integração e a interoperabilidade das bases de dados governamentais;
> - promover políticas públicas baseadas em dados e evidências e em serviços preditivos e personalizados, com utilização de tecnologias emergentes;
> - implementar a Lei Geral de Proteção de Dados, no âmbito do Governo federal, e garantir a segurança das plataformas de governo digital;
> - disponibilizar a identificação digital ao cidadão;
> - adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal;
> - otimizar as infraestruturas de tecnologia da informação e comunicação; e
> - formar equipes de governo com competências digitais (BRASIL, 2020b, p. 3).

Outro dispositivo legal que faz parte deste ambiente de Governo Digital é o recente Decreto 10.222/2020 que aprova a Estratégia Nacional de Segurança Cibernética - E-ciber. Com escopo mais amplo, regulariza diversos termos relacionados não apenas à segurança cibernética, mas também ao grande campo de estudos da segurança da informação. Interessante que na própria metodologia adotada para sua elaboração, ao dividir 3 subgrupos de representantes, já se pode observar a importância que a confiança digital ganha ao ser destacada no "Subgrupo 2 - confiança digital e prevenção e mitigação de ameaças cibernéticas;" (BRASIL, 2020a, p. 3) . Mais uma vez contata-se que para que se obtenha sucesso na digitalização é preciso confiar.

No mundo virtual, nem sempre os vestígios levam a evidências. Esta realidade da digitalização intrínseca aos *bits* e *bytes* fazem com que os mecanismos de perícias forenses sejam, por vezes, ineficazes na coleta de evidências. Cavalcante (2020), afirma:

> No lugar de caneta, papel e impresso, temos conversas, documentos, imagens relações jurídicas em *bits* no ambiente virtual, advindo as provas digitais que para sua validade necessitam observar diversos princípios e ditames legais.
> As leis existentes em nosso país abarcam diversas dessas situações fáticas, mas por vezes existem lacunas que são suprimidas ante a velocidade da evolução tecnológica. Tais lacunas são resolvidas *vide* os costumes, à jurispru-

> dência, aos princípios gerais do direito, à analogia e, também, à equidade. Deixando assim margem a diversas interpretações e ações judiciais.
> Devemos festejar a evolução do direito digital com suas novas normas, mas interpretá-las de acordo com a finalidade maior que vem a ser a proteção às relações jurídicas sem impedir que as mesmas ocorram sem resguardo jurídico em âmbito privado ou público (CAVALCANTE, 2020, p. 291).

Na citação acima pode-se observar que uma transformação digital mal feita pode sofrer reveses inclusive jurídicos, e isto, certamente, impacta na confiança. Buz (2019a), afirma que em se tratando de Estratégia de Governo Digital, perder confiança pode significar instabilidade política e democrática. Não é um tópico cujas escolhas devem ser tomadas a luz do caminho mais rápido e fácil. Digitalizar com segurança é o mantra a ser repetido (informação verbal)[3].

Não obstante os desafios iminentes, pode-se identificar que o Poder Executivo Federal já possui referencial sobre caminhos a serem seguidos neste mundo virtual. As políticas, estratégias, decretos e planos que versam sobre a temática digital traz muitos direcionamentos que vem ao encontro de solucionar questões de padronizações. A E-Ciber (BRASIL, 2020a), i.e, em suas Ações Estratégicas no item 2.3.1 fala em:

> - adotar normas, padrões e modelos de governança reconhecidos mundialmente;
> - adotar, a indústria, padrões internacionais no desenvolvimento de novos produtos desde sua concepção (*privacy/security by design and default*)
> - recomendar a adoção de soluções nacionais de criptografia, observada, para tanto, a legislação específica
> - recomendar a certificação em segurança cibernética, conforme padrões internacionais; e
> - ampliar o uso do certificado digital.
> - estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis.
> - incentivar a adoção de padrões globais de tecnologia, que permitirá a interoperabilidade em escala internacional;
> - incentivar o desenvolvimento de competências e de soluções em criptografia (BEASIL, 2020, p.5)

O Texto para Discussão do IPEA – Instituto de Pesquisa Econômica Aplicada (2013), define o conceito segurança cibernética, como o conjunto de ações no contexto de um planejamento militar, efetivadas no espaço cibernético. Tendo com finalidade "proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuí-

---

[3] BUZ, Marcelo Amaro. Palestra: A importância da certificação eletrônica e a tecnologia blockchain na proteção dos dados no ambiente jurídico e empresarial. **III Seminário de Segurança da Informação No meio Jurídico.** Realização da Comissão de Direito Digital da Ordem dos Advogados do Brasil Santa Catarina. Evento realizado em 10 de dezembro de 2019.

zos aos sistemas de informação do oponente" (JUNIOR, 2013, p. 9). Complementa ainda que se refere a garantir a utilização de ativos de informação estratégicos de maneira protegida, principalmente as infraestruturas críticas. "Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da administração pública federal (JUNIOR, 2013, p. 9).

Segundo o mesmo estudo um dos maiores desafios do século XXI é garantir a defesa no ambiente cibernético, tarefa elencada com riscos significativos para a segurança pública e para a estabilidade global. Um aspecto muito relevante, tendo em vista a característica de não haver fronteiras físicas do ambiente cibernético,é que nenhuma nação superará este desafio isoladamente. A parceria entre nações aliadas, a sociedade civil e o setor privado passa a ser valorizada na Defesa Cibernética (JUNIOR, 2013).

Desde 2012, o Plano Nacional de Defesa do Brasil classifica o setor cibernético como estratégico, citando que "é essencial o domínio crescentemente autônomo de tecnologias sensíveis" (BRASIL, 2012, p. 19) para que o país possa ter autonomia nas questões de ataques cibernéticos. A temática em tela é de alto nível, ao definir que "todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre" (BRASIL, 2012, p. 135):

> O aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos ministérios da Defesa, das Comunicações e da Ciência, Tecnologia e Inovação, e do Gabinete de Segurança Institucional da Presidência da República. (BRASIL, 2012, p. 135)

A Estratégia Setorial de Defesa 2020 – 2031 (BRASIL, 2019c) atenta para o grande volume de dados internacionais, preconiza a importância das parcerias internacionais e cita o termo 'interoperabilidade', que pode ser um fator *sine qua non* para se obter sucesso no reconhecimento internacional de documentos digitais:

> ASD 6.1.5 - Estimular o estabelecimento de parcerias e intercâmbios na área de pesquisa de tecnologias entre as instituições científica, tecnológica e de inovação (ICT) das Forças Armadas e dessas com as instituições civis de interesse da defesa.
> ASD 6.1.6 - Estabelecer parcerias estratégicas internacionais que favoreçam o desenvolvimento de tecnologias de interesse para a defesa.
> ESD 7.2 - Atuar no espaço cibernético de forma efetiva e negar o seu uso contra os interesses da defesa nacional

> ASD 7.2.2 - Promover a interoperabilidade do setor cibernético na defesa nacional. (BRASIL, 2019 c, p. 23)

3 **DOCUMENTOS DIGITAIS E VALIDADE JURÍDICA**

O Michaelis (2020) dentre outras diversas definições, especifica o termo "documento" como um elemento capaz de provar, elucidar, instruir um processo e comprovar a veracidade ou evidência científica de algum fato:

> ...7 Instrumento escrito que, por direito, faz fé daquilo que atesta, podendo legalmente instruir ou esclarecer algum processo judicial; título, contrato, escritura, declaração, atestado, testemunho.
>
> 8 Qualquer objeto, prova, testemunho etc. que possa servir de confirmação para conferir autenticidade a um fato histórico qualquer. (MICHAELIS, 2020, Internet)

Quando analisado sobre o prisma de ato jurídico, o documento "deve possuir os seguintes elementos: a) capacidade do autor do ato; b) imputação do ato realizado por um órgão ao próprio sujeito; c) manifestação de vontade; e d) o objeto do ato deve ser lícito." (MELLO, 2004, p.195)

À luz do Código Civil Brasileiro (BRASIL, 2002), o Artigo 107 traz que "a validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente exigir". Circunstância encontrada no Parágrafo 6º do Artigo 129 da Lei nº 6.015/1973, que dispõe sobre os registros públicos, e dá outras providências, segundo ela:

> "estão sujeitos a registro, no Registro de Títulos e Documentos para surtir efeitos em relação a terceiros... todos os documentos de procedência estrangeira, acompanhados das respectivas traduções, para produzirem efeitos em repartições da União, dos Estados, do Distrito Federal, dos Territórios e dos Municípios ou em qualquer instância, juízo ou tribunal;" (BRASIL, 1973 p. 25)

Mas como se pode observar grifado na Estratégia Brasileira Para Transformação Digital (2018) em referência ao *Communication Building a European Data Economy* (BRUXELAS, 2017), da Comissão Europeia, "num mercado globalizado e interconectado, grandes volumes de dados circulam entre fronteiras nacionais em um fluxo` contínuo de longas e complexas cadeias de valor" (BRASIL, 2018, p. 38). É evidente que as relações internacionais têm se baseado cada vez mais por meios eletrônicos. Porém não se possui marcos legais tampouco padrões para que se conduza este ambiente com segurança jurídica. A Estratégia Brasileira

para Transformação Digital afirma que "é oportuno para o Brasil estabelecer o seu marco legal, protegendo direitos dos cidadãos e conferindo segurança jurídica para investimentos na economia digital (BRASIL, 2018. p.39). O mundo de transações digitais não afeta apenas a Segurança e Defesa Nacional em termos de garantir as Relações Internacionais, mas o "abrangente processo de digitalização dos negócios é o motor de mudanças nas estratégias e gestão das práticas empresariais" (WIRTZ, 2019, p. 2. Tradução nossa). O que traz um aspecto muito importante também de Desenvolvimento Nacional com ambiente de negócios seguros.

Ocorre que há diferenças sensíveis na garantia, atributos como integridade, autenticidade, autoria e rastreabilidade dos documentos quando se migra do ambiente físico para o ambiente virtual. A segurança e validade jurídica perdem elementos físicos que comprovem as manifestações de vontades e migram para elementos lógicos. O Artigo Art. 219 do Código Civil fala que "as declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários" (BRASIL, 2012.). Esta presunção, seguramente se refere às assinaturas manuscritas, cujas propriedades são descritas por Carnelutti (2002) como pressupostos fatídicos inerentes às assinaturas manuscritas que atestam quem é o autor do documento, a sua manifestação de vontade expressa por meio de um sinal único (a biografia comportamental da assinatura). Carnelutti (2002) frisa uma característica inerente do documento físico assinado que é essencial para atestar os atributos de autenticidade, integridade e autoria:

> … tanto esse símbolo, como também a informação lançada, encontram-se ligados a um determinado documento por meio de um processo químico (a tinta lançada penetra nas fibras do papel de modo indelével); e (c) como o documento físico é, a princípio, inalterável (dependendo, para tanto, de uma atuação externa sobre ele para que a informação, uma vez lançada - e portanto, a ele aderente de forma indelével - possa ser modificada), torna-se possível concluir que a pessoa que ali lançou a sua assinatura está de acordo com os fatos ali constantes (CARNELUTTI, 2002, p. 9).

Quando analisado o que o Parecer Jurídico da Procuradoria Federal Especializada do Instituto Nacional de Tecnologia da Informação (BRASIL, 2019a), autarquia vinculada à Casa Civil da Presidência da República que tem como função ser a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil, observa-se que o mesmo raciocínio que abona um documento físico sua validade não é simplesmente acomodado no documento digital. As peculiaridades de forma e meio dos documentos digitais faz com que se te-

nha um desafio maior para se alcançar o seu reconhecimento e validade jurídica internacional. Diferentemente de um documento fisico, cuja adulteração deixará evidências de que houve rasuras, o que é passível de identificação por meio de perícias, um documento eletrônico tem como característica intrínseca a alterabilidade, podendo ser copiados, alterados de forma infinita sem necessariamente deixar rastros e evidências. Um documento eletrônico nada mais é do que a sequencia de *bits*, mesmo em se tratando de imagens, sons ou mesmo documentos, em ultima análise será sempre um compêndio de números que não estão atrelados de formas indissociáveis ou definitiva.

Os documentos digitais não resguardam as mesmas características de segurança, integridade, autenticidade e autoria de um documento físico, mas por outro lado, seu uso tem sido adotado cada vez mais. A Revista Cenário de Defesa (BRASIL, 2017) alerta enfaticamente para os riscos advindos deste novo ambiente:

> Como efeito adverso da ampliação de usuários e aumento da capacidade dos sistemas de comunicação e informação, haverá incremento de atividades cibernéticas maliciosas, incluindo ataques cibernéticos promovidos por atores e organizações estatais (veladas) ou não estatais (criminosas), de cunho ideológico ou não. Haverá, portanto, necessidade de incremento da proteção para sistemas de comunicações e informações, sendo, contudo, improvável o rompimento de infraestruturas globais por tais ações, devido a prejuízos e reações que provocariam na comunidade internacional, ocasionando fortes reações estatais, independentemente de interesses e estratégias político-ideológicas (BRASIL, 2017, p. 16).

3.1 A IMPORTÂNCIA DA CRIPTOGRAFIA

Quando se trata de documentos digitais, especialmente daqueles que tem por finalidade identificar as pessoas, é de suma importância que haja tecnologia possível para garantir autenticidade, integridade e autoria de maneira inseparável e inequívoca. A forma mais usual e conhecida é o uso da criptografia. No Brasil, a criptografia é regida pela Medida Provisória 2.200-2/2001, que estabelece a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, responsável pela emissão das chaves criptográficas brasileiras, chamadas de Certificados Digitais. O Parecer Técnico (BRASIL, 2019 b) traz um resumo sucinto e explicativo do que é o conceito de certificação digital:

> Derivam-se desses processos dois elementos (uma chave pública e privada) matematicamente ligados a fazerem operações aritméticas nos *bits* do documento eletrônico (ou no *hashi* desse), mas distintos um do outro. Essa característica é fundamental na preservação de qualquer assinatura (manifestação de vontade) no meio eletrônico - garante integridade dos dados assina-

> dos e não há compartilhamento de elemento de assinatura. Um é privado, de controle exclusivo e ligado a um titular, e outro público, podendo ser enviado para realizar operações diversas como a verificação de uma assinatura de chave privada ou encriptacão de um ativo digital, garante que tal operação feita com um dos elementos no ato eletrônico somente, e exclusivamente, pode ter vindo do outro (BRASIL, 2019 b, p. 15).

Segundo a Estratégia Brasileira Para a Transformação Digital (BRASIL, 2018) e Menke (2005) o Certificado Digital é uma estrutura de dados, em outras palavras um documento eletrônico, que utiliza chave criptográfica assimétrica de padrão específico (X.509) que contempla a chave pública e privada. Ele contém os dados do seu titular (pessoa física ou jurídica) e ao se realizar uma assinatura eletrônica com ele, fica atestado a identidade de quem manifestou a vontade. Um documento assinado pelo documento eletrônico Certificado Digital, garante a confidencialidade, a autenticidade, a autoria e o tem o status de não repúdio. Pode-se dizer que o certificado digital é este documento de identificação digital seguro capaz de identificar, autenticar e assinar documentos. É um conceito tecnológico da década de 1960, consagrado até hoje e amplamente utilizado em muitos países. Aliados a ele, pode-se usar diversas outras tecnologias como *blockchain,* biometria, carimbo de tempos, serviços em nuvens, entre tantas outras. Mas a base para se realizar o calculo matemático está alicerçada no certificado digital que se utiliza das chaves criptográficas assimétricas para garantir que o esforço computacional para corrompimento da chave privada seja algo praticamente impossível de ser acessada por alguém que não seja o seu titular. A chave pública fica amplamente acessível.

A Lei 14.063/2020 caracteriza como assinatura eletrônica qualificada aquelas regradas pela MP 2.200-2/2001, que institui a ICP-Brasil. É uma cadeia de confiança credenciada abaixo da Autoridade Certificadora Raiz, papel desenvolvido pelo ITI, que credencia, fiscaliza e audita todos os entes credenciados. É nesta infraestrutra com centena de Autoridades Certificadoras e quase 2 mil Autoridades de Registro que o Brasil deposita a confiança do documento digital seguro. As grandes dificuldades da ICP-Brasil são: massificação do certificado digital, interoperabilidade plena do sistema, falta de experiência de uso e ausência de amparo legal para que este documento digital possa se tornar documento de identificação civil.

Conforme se pode observar no sítio eletrônico aquitemcd.iti.gov.br, é neste conceito, que centenas de serviços públicos e privados rodam suas operações e confiam suas transações no mundo digital com quem realmente se diz ser. Em palestra de abertura do 17º CertForum, realizado em setembro de 2019 em Brasília, evento que reúne a indústria da Certificação Di-

gital do Brasil, Buz (b, 2019) afirmou que o Certifica Digital é uma tecnologia que precisa se modernizar, adaptar aos avanços tecnológicos, se desvencilhar de certas amarras burocráticas e legais para que efetivamente possa retornar ao Estado e a sociedade todo o potencial que o Certificado Digital possui (informação verbal)[4].

3.2 INTEGRIDADE, AUTENTICIDADE E AUTORIA

Autenticidade é sinônimo de legitimidade, daquilo que se pode garantir e dar fé, é algo verdadeiro. Integridade, segundo o Parecer Técnico da Diretoria de Infraestrutura do ITI, é a garantia que os dados não podem ser alterados sem autorização. Ademais é importante que os métodos implementados detectem qualquer alteração que por ventura seja realizada. Autoria é se ter certeza do autor de determinada mensagem.

Em um documento físico, estes atributos são atestados por meio de um processo químico de fusão da tinta da caneta às fibras do papel aliados a uma assinatura, que nada mais é do que uma biometria comportamental. Quando um sujeito assina um documento, ele imprime a este documento um rastro inseparável, de forma que se houver qualquer adulteração, ela será facilmente identificável. Desta forma se cria uma marca que garante a integridade e a autenticidade. Para garantir a presunção da autoria, você precisa passar em um cartório e colocar um carimbo de reconhecimento de firma. Assim você tem um terceiro ator, dando fé pública ao seu documento.

Todas estas características são perdidas no mundo virtual. Sua assinatura não possui mais uma biometria comportamental, tampouco alterar um *bit* com certeza deixará vestígios de evidências. Por isto, ao migrar para o mundo virtual, se faz necessário adotar outras técnicas que permitam a preservação destes atributos. Os miotivos são principalmente de ordem jurídica. As manifestações de vontade no mundo virtual precisam ter os mesmos pesos das manifestações de vontade do mundo material. E, em se tratando da coisa pública, mais ainda. Não se pode expor toda uma estratégia de transformação digital a um erro tão elementar a ponto de não adotar padrões tecnológicos que deem segurança para todos, em especial para o Estado, de que o que está sendo tratado é integro, autêntico e esta sendo realizado pela exata pessoa que se diz ser.

---

[4] BUZ, Marcelo Amaro. Palestra Abertura. 17º CertForum. Realização do Instituto Nacional de Tecnologia da Informação em parceria com Associação Brasileira de Identificação Digital - ABRID. Evento realizado em 17 de Setembro de 2019.

Conforme explorados nos Pareceres Técnico e Jurídico do ITI, estes três atributos são indeléveis e prioritários em qualquer processo de digitalização. Mas infelizmente são pouco adotados. Muitas vezes utiliza-se *login* e senha, o mais frágil de todos os mecanismos de autenticação, e sequer assinatura digital podem realizar. A biometria comumente utilizada para se aumentar segurança de identificação pode não ser suficiente. Em que pese a biometria efetivamente trazer um mecanismo mais seguro de preservar a autoria, ela não possui um padrão matemático de vínculo da assinatura ao documento. Apenas com a adoção da matemática, da criptografia aplicada que se pode garantir o obtenção destes atributos.

Neste tema aborda-se tanto procedimentos de autenticação em sistemas quanto a própria assinatura em um documento. É importante esclarecer que o mecanismo que autentica com padrões de segurança inequívoco é o mesmo que assina um documento. Conforme já colocado, um documento de identificação digital, além de identificar, também autentica em sistemas e, aliado a técnicas de criptografia, tem o poder de assinar.

A questão da validade jurídica também precisa ser considerada. Adentra-se dessa forma na seara dos diferentes tipos de assinaturas eletrônicas. O melhor exemplo do mundo para ilustrar e que melhor conseguiu classificar o tipo de assinaturas é o *eIDAS*, Regulamento da União Europeia sobre identificação eletrônica e serviços de confiança para transações eletrônicas no mercado único europeu. O *eIDAS* classifica as assinaturas eletrônicas em três níveis:

> a) Assinatura eletrônica: os dados em formato eletrônica que se ligam ou estão logicamente associados a outros dados em formato eletrônica e que sejam utilizados pelo signatário para assinar;
> b) Assinatura eletrônica avançada: uma assinatura eletrônica que obedeça aos requisitos estabelecidos no artigo 26; e
> c) Assinatura eletrônica qualificada: uma assinatura eletrônica avançada criada por um dispositivo qualificado de criação de assinaturas eletrônica e que se baseie num certificado qualificado de assinatura eletrônica
> d) Certificado qualificado de assinatura eletrônica: um certificado de assinatura eletrônica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I (PARLAMENTO EUROPEU E DO CONSELHO, 2014, p. 84);

No artigo 26 do *eIDAS* (2014) os requisitos para as assinaturas eletrônicas avançadas são estabelecidos de que devem permitir a identificação do signatário de modo único, oferecendo o controle exclusivo pelo signatário e que ao realizada, permita que qualquer alteração do documento seja posteriormente detectável.

Desta feita, observa-se que as Assinaturas Eletrônicas Avançadas e as Qualificadas precisam estar associadas de modo inequívoco ao signatário. Isto é, tanto a emissão da assinatura, uso, e gestão sobre todo o mecanismo/sistema, deve ser controlado única e exclusivamente pelo titular dela. Aliados aos padrões definidos na alínea "d" do Art. 26, ou seja matemática, tem-se os padrões de autenticidade e integridade. Se atendidos os padrões estabelecido no ANEXO I do normativo europeu, a assinatura é qualificada e a partir desta adoção, tem-se a preservação da autoria.

Fica clara a importância que o documento de identificação digital seguro é um aspecto de muitíssima relevância e sua falha pode impactar diretamente na confiança de um sistema informatizado e, principalmente na estratégia de digitalização do estado. É um risco que pode plenamente ser controlável. Interessante e animador, conforme afirmado pela Global Cyber Security Capacity Centre (2020) do Departamento de Ciência da Computação da Universidade de Oxford em estudo encomendado pela Organization of American States - OAS, que o Brasil possui tecnologias e indústria maduras e suficientemente desenvolvidas para atender e entregar esta segurança ao País.

3.3 SEGURANÇA NA IDENTIFICAÇÃO

Acima de tudo, documento de identificação digital é uma temática de segurança de pessoas, empresas, aplicações, instituições, órgãos e governos. E diante da inciativa de se digitalizar a nação, torna-se uma questão de segurança nacional. Também extrapola a barreira de pessoas físicas e jurídicas, avança para artefatos.

Autenticação inequívoca no mundo virtual é um objetivo fundamental para se ter segurança e confiar nas transações eletrônicas, além de garantir a validade jurídica dos atos. É importante se saber que é imprescindível para se ter uma digitalização sólida. Do ponto de vista da identificação de pessoas, conforme já relatado, no Brasil são mais de 50 tipo diferentes de documentos de identificação civil válidos. Esta complexidade do mundo real importa uma problemática para o mundo virtual sem precedentes.

Quando diante de um documento físico, as possibilidades de checagem da autenticidade, integridade e veracidade das informações nele contido são questões fatídicas, que podem ser apuradas instantaneamente. Um documento físico possui requisitos de segurança físicos que podem atestar sua autenticidade, bem como é possível identificar eventuais rasuras, fraudes e adulterações, possibilitando identificar sua integridade. E sua veracidade, muitas vezes

pode ser facilmente verificada através de checagem em base de dados oficiais. Esta tríade autenticidade, integridade e veracidade forma um tripé no qual permite garantir com um certo nível de segurança aceitável, a identificação de indivíduos, instituições e artefatos. Os documentos físicos possuem, por exemplo, carimbos, números e autenticações em cartório, assinaturas de próprio punho e uma série de outras possibilidades de garantia.

Em se tratando de identificação de artefatos, esta não é uma questão muito usual no mundo real, pois a identificação das coisas acaba sendo atestada pela própria presença, por por meio dos sentidos como visão, tato e mecanismos físicos de autenticação. Porém, quando se volta ao mundo virtual, a identificação de pessoas, instituições e objetos são conceitos abstratos. Precisa-se confiar que está se comunicando algo a alguém a quilômetros de distância sem a chance de poder olhar, sentir, e testar atributos físicos de integridade, autenticidade e veracidade. Em suma, a pessoa torna-se número de Protocolo de *Internet* (IP) comunicando-se por meio de *bits* com outro IP. E será que se está fazendo *upload* de dados para a pessoa ou coisa certa? Será que se está recebendo informações da pessoa ou coisa que diz a você que é? Novamente, integridade, autenticidade e veracidade são atributos que agora se precisa passar a confiar.

Principalmente porque a função de um documento físico é somente identificar, já um documento digital pode identificar, autenticar e assinar. São dimensões muito diferentes. É inegável se reconhecer que a força de um documento digital é muito maior que a de um documento físico e, por isto, já avançando a segunda década do século XXI, é inequívoca e célere a digitalização de documentos da economia como um todo. Inclusive entre nações, conforme já relatado na matéria do portal www.CryptoID.com.br do dia 05 de outubro de 2020.

Evidente que certas aplicações ou troca de informações - talvez a maioria - podem ser trafegadas na *internet* sem nenhuma necessidade de uma identificação segura. Mas há uma gama de transações que precisam ser preservadas. Seja para garantir aspectos jurídicos, criar provas inequívocas ou mesmo garantir o sigilo e/ou privacidade

4 **ASSINATURAS EM DOCUMENTOS DIGITAIS TRANSFRONTEIRIÇOS**

Em se tratando de documentos transfronteiriços, é de suma importância atentar ao Artigo 4º da Constituição Federal que fala da “Igualdade entre os Estados” como um dos princípios constitucionais que regem as relações internacionais (BRASIL, 1988). Esta igualdade é

amparada no Princípio do Direito Internacional da Reciprocidade, que segundo Mello (2004) se constitui um dos princípios basilares da cooperação internacional.

Já no ano de 2020, uma das 10 estratégias definidas no Decreto 10.222, de 5 de fevereiro, que estabelece a Estratégia Nacional de Segurança Cibernética - E-Ciber, o item "2.3.8 – Ampliar a cooperação internacional do Brasil em Segurança cibernética" estabelece uma serie de medidas que sustentam a posição do Brasil em ser protagonista na cooperação internacional cibernética:

> - estimular a cooperação internacional em segurança cibernética;
> - incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro;
> - ampliar o relacionamento internacional com os países da América Latina;
> - promover eventos e exercícios internacionais sobre segurança cibernética;
> - participar de eventos internacionais de interesse para o País;
> - ampliar os acordos de cooperação em segurança cibernética;
> - ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos;
> - estimular a participação do País em iniciativas futuras de estruturação normativa, como as relativas à criação de padrões de segurança em tecnologias emergentes, e
> - identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética. (BRASIL, 2020a, p.7)

O *eIDAS*, na União Europeia estabelece um padrão de interoperabilidade nas assinaturas eletrônicas, em especial os embarcados nos documentos de identidade civil digital. Na América do Sul, o acordo assinado em dezembro de 2019, estabelece o reconhecimento mútuo das infraestruturas de assinaturas eletrônicas qualificadas no âmbito do Mercosul. E mais recente o primeiro acordo bilateral assinado entre duas nações, no caso Brasil e Peru apontam a tendência de cada vez mais se adotar o padrão nato digital para firmar acordos, tanto na iniciativa privada, quando entre as nações passa também a ser tendência. Ocorre que estes acordos e regulamentações de assinaturas eletrônicas não possuem caráter de validade global, não definem técnicas e padrões únicos para todos. Se registrem ao seu ambiente de regulamentação.

O próprio acordo no âmbito do Mercorsul não convenciona um padrão único, não permitindo assim sequer a interoperabilidade das assinaturas eletrônicas e tão somente o reconhecimento e confiança das assinaturas realizadas por meio das infraestruturas entre os países signatários. Ao longo do aumento do volume de documentos assinados digitalmente, seguramente haverá a necessidade de definição de padronização em escala global. Pois para se manter a confiança, é necessário que haja um protocolo mínimo de segurança. Inclusive para que se possa ter interoperabilidade das assinaturas.

A ausência de padrão tende a gerar um problema crônico no mundo. Uma infraestrutura de interoperabilidade e reconhecimento global de assinaturas eletrônicas em documento digitais é essencial para que se tenha a segurança e confiança dos documentos digitais transfronteiriços. O grande receio é que em não havendo regramento mínimo, algumas nações adotem práticas não seguras, colorando em risco a integridade dos documentos.

4.1 AMEAÇA POTENCIAL AOS INTERESSES NACIONAIS

Ao ser pioneiro em assinar acordos internacionais por via de documentos digitais, mesmo antes de haver a definição de regras padronizadas que garantam técnica e juridicamente a validade das assinaturas eletrônicas aplicadas ao documento, o Brasil assume um risco eminente de ter seus interesses confrontados. A ameaça é de termos a integridade do documento corrompida, ou a sua autenticidade questionada.

Caso não seja adotado no mínimo uma assinatura eletrônica avançada, não haverá garantia alguma de que o documento preservará sua integridade. E, se o documento digital for corrompido, adulterado ou fraudado, ele não garante a preservação de evidências para uma eventual perícia e comprovação de sua alteração. O risco disto acontecer, seja por intenção de uma das partes, seja por ação de terceiros mau intencionados expões os signatários sobre forte ameaça de seus interesses. Podendo inclusive, ocasionar crises internacionais de confiança. Os interesses nacionais ficam expostos no mundo virtual, podendo o teor de um documento ser alterado ou questionado.

Em não havendo o regramento mínimo de operação das assinaturas eletrônicas, mesmo avançadas, não há como se ter confiança na autenticidade de quem assina. Os atributos de uma assinatura eletrônica são distintos da assinatura manuscrita. O vínculo unívoco e a garantia de que o controle de uma assinatura eletrônica só pode ser operados exclusivamente por quem a assinatura se propõem a identificar é definido em práticas que devem ser regulamentas, fiscalizadas e auditadas. Em situações onde não se tem um regramento mínimo internacional, as partes não possuem garantias jurídicas de que os signatários são realmente quem dizem ser, e que possuem representatividade ou poder para realizar determinado ato.

Assinar acordos internacionais sem o amparo jurídico de um padrão internacional é expor o país a uma potencial ameaça aos bens e interesses nacionais. E dependendo das estruturas de assinaturas eletrônicas utilizadas pelos outros países, pode-se estar expondo o país a insegurança jurídica capaz de atingir a defesa nacional. Ressalta-se que oportunamente, a

ameaça pode vir a ser oferecida por força terceira, *hackers* ou grupos que tenham interesse em dissendiar o relacionamento entre os países. Coloca-se em risco os bens e interesses nacionais e por consequência o risco pode vir a se tornar uma ameaça que necessite de intervenção para evitar uma incursão diplomática, jurídica internacional ou até a necessidade de securitização.

4.2 A DEFINIÇÃO DO PADRÃO INTERNACIONAL DE ASSINATURAS DIGITAIS

O mundo deve se organizar em torno de uma estrutura que possa definir um padrão internacional de práticas mínimas de assinaturas digitais capazes de suportar as assinaturas de documentos digitais transfronteiriços. Este papel de definir, deve recair sobre alguma organização de caráter multilateral. Ocorre que estas definições, se escolhidas práticas de assinaturas eletrônicas diferentes das quais o Brasil adota desde 2001 com advento da MP 2.200-2 que estabelece a ICP-Brasil, forçará o país a reorganizar o arcabouço jurídico e também a própria infraestrutura de emissão de assinaturas eletrônicas qualificadas.

Esta possibilidade pode representar um forte impacto na indústria nacional, uma vez que o país já possui, segundo site do ITI , mais de 6 milhões de certificados digitais ativos. Inclusive emitidos por Autoridades Certificadoras públicas como a da Presidência da República, do Ministério da Defesa e do Ministério das Relações Exteriores. Toda esta industria implementada desde 2001 no país, possui tecnologia de ponta e reúne um arcabouço jurídico, procedimental e estrutural instalados e maduros. O Brasil, é um dos países que administra uma das maiores e mais complexas infraestruturas de chaves públicas qualificadas do mundo. Está na vanguarda deste conceito tecnológico, tanto que é protagonista do primeiro acordo internacional assinado por meio digital.

Ocorre que as práticas e padrões adotados no Brasil não são os únicos existentes. E por isto, por ser um dos países lider em volume de emissão de assinaturas eletrônicas qualificadas, o Brasil pode adquiri posição de protagonista no debate e definição dos padrões internacionais. Desta forma preserva os bens e interesses nacionais representados na indústria nacional de certificação digital, fomenta o desenvolvimento desta mesma indústria, pois pode preparar mercados internacionais para ela atuar bem como zela por um padrão no qual o próprio acordo já assinado e os futuros passam a ter a segurança de estar adequados a regras e procedimentos aceitos internacionalmente.

5 **CONSIDERAÇÕES FINAIS**

A velocidade com que os serviços públicos brasileiros têm se digitalizado, principalmente desde 2019, traz uma esperança de que se conseguirá reduzir burocracias e custos, ganhar eficiência, e escalar da posição 124º no ranking *Doing Business* 2020 do Banco Mundial. Com o avanço destes serviços, cada vez mais aumenta a população usuária. Esta sem dúvida, é uma grande oportunidade para o documento digital prosperar.

Um documento de identificação, como o próprio nome diz, identifica pessoas. Porém um documento de identificação digital tem mais habilidade do que o físico, pois além de identificar, pode autentificar e assinar. Mas não é qualquer documento digital que tem estas funcionalidades ampliadas, conforme já abordado. E é dentro destas possibilidades de que um documento digital pode realizar muito mais função do que apenas identificar, que na migração de serviços públicos para o virtual, se abre um leque de oportunidades para o documento de identificação digital.

Porém é importante que se tenha em vista de que um documento de identificação digital não é o mesmo que um documento eletrônico, ou um documento digitalizado. Em um documento de identificação digital esta-se diante de verdadeira engenharia de sistemas, *software*s e infraestruturas. Bem como, seguramente, diante de padrões criptográficos. O principal motivo disto tudo é: segurança. Assim como um documento físico, com requisitos frágeis de segurança podem ser falsificados ou fraudados, o mesmo vale para documentos digitais de toda a espécie.

Sem dúvida, o mundo virtual deve seguir as regras do mundo real, ele não é um mundo paralelo, tudo que ocorre por lá está sob a égide do ordenamento jurídico, inclusive com algumas leis específicas, como o caso do Marco Civil da *Internet*. Há uma sensível diferença em aplicar as leis no mundo real para o mundo virtual. A *internet* não tem fronteiras, o digital não tem tem DNA, tampouco biometria, mas possui outras características e formas de se criar evidências. Em se tratando de documento transfronteiriços, estas regas de se criar evidência, ou seja, padrões de assinaturas digitais em documentos digitais, capazes de serem reconhecimentos internacionalmente, precisam ser definidos.

Porém não são situações simples e até haver o aumento das fraudes e ataques cibernéticos, não parece estar na prioridade da agenda governamental. Do ponto de vista de autenticação, identificação e assinatura eletrônica o mundo virtual possui uma serie de peculiaridades

das quais o Brasil domina e, inclusive possui uma industria desenvolvida. Estes padrões são vitais para guiar o país e se estar preparado para o momento em que se tiver o desafio de de ser ter a interoperabilidade ou reconhecimento internacional, e principalmente para que não se tenha a transformação dos riscos inerentes da assinatura e aceitação de documentos digitais internacionais em ameaças.

Uma eventual adulteração de um documento digital transfronteiriço realizado sem o amparo jurídico legal de acordos e convenções internacionais de padrões de assinatura digital caracteriza-se como uma ameaça potencial para a defesa nacional. Uma vez que estes documentos avançam a fronteira do privado e passam a ser firmados no âmbito da institucionalidade do governo, coloca-se em risco bens e interesses nacionais. A ausência destes padrões trazem insegurança jurídica e podem acarretar em tensão internacional caso se entre em contestação da integridade de um documento. A definição de padrões se caracterizam em movimentação de Defesa Nacional para que se possa impedir ou mitigar eventuais ameaças.

Considerando que o Brasil possui uma industria nacional consolidada de assinaturas eletrônicas qualificadas, que atendem aos mais altos requisitos de segurança da informação, concatenado com o pioneirismo brasileiro em assinar documentos digitais transfronteiriços imprecam importância no protagonismo brasileiro na definição destes padrões internacionais. A gestão político administrativa deste risco iminente é desejável a fim de mitigar risco de termos nossos interesses nacionais afrontados ou até mesmo a contestação de acordo já firmado.

Neste artigo foram apresentados os conceitos de documentos e assinaturas digitais e o impacto que podem ter na defesa e segurança nacional. Antecipa uma ameaça potencial e reflete sobre a importância do Brasil liderar esta temática. Ainda assim, ele não pretende ser conclusivo sobre como alcançar este protagonismo, tampouco pretende definir quais os padrões a serem definidos internacionalmente. Porém, torna-se evidente que esta temática de *Cyber Security*, transformação digital está mapeada em diversos dispositivos legais, porém não está sendo explorada internacionalmente. Conclui-se que o Brasil pode ser protagonista nesta agenda, e que esta pesquisa possa ser ampliada com a análise de todos os padrões existentes no mundo, bem como uma proposição de agenda para governança internacional de assinaturas e documentos digitais.

REFERÊNCIAS

BRASIL. **Dispõe sobre os registros públicos, e dá outras providências**, Lei nº 6.015, de 31 de dezembro de 1973, Palácio do Planalto. Disponível em <http://www.planalto.gov.br/ccivil_03/LEIS/L6015consolidado.htm>. Acesso em 20 abril 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Palácio do Planalto, Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 09 de abril 2020.

BRASIL. **Código Civil,** Lei nº 10.406, de 10 de janeiro de 2002, Palácio do Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 20 abril 2020.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa (PND e a Estratégia Nacionl de Defesa (END) 2012**. Brasília, DF. Disponível em <http://www.de-fesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 15 de julho de 2020.

BRASIL. **Revista Cenários de Defesa 2020 – 2039** – sumário executivo. Ministério da Defesa. Assessoria Especial de Planejamento. Brasília, 2017.

BRASIL. **Estratégia Brasileira para a Transformação Digital (E-Digital).** Abril de 2018. Ministério da Ciência, Tecnologia, Inovações e Comunicações. MCTIC. Disponível em: <http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf>. Acesso em 25 de março de 2019.

BRASIL. **Parecer n. 00378**, da Procuradoria Federal Especializada Junto ao Instituto Nacional de Tecnologia da Informação. Brasília, 2019a. Disponível em <https://www.iti.gov.br/images/repositorio/publicacoes_tecnicas/parecer/parecer_agu.pdf>. Acesso em 15 março 2020.

BRASIL. **Parecer – DINFRA/ITI - Resposta ao Ofício no 1.282/2019 – COTEC/SUCOR/RFB**, do Instituto Nacional de Tecnologia da Informação. Brasília, 2019b. Disponível em <https://antigo.iti.gov.br/images/repositorio/publicacoes_tecnicas/parecer/parecer.pdf.> Acesso em 15 março 2020.

BRASIL. **Estratégia Setorial de Defesa 2020 – 2031** de 27 de Julho de 2019c. Ministério da Defesa. Disponível em <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj4i6ibjLTtAhWuLLkGHfFUBbAQFjAAegQIBhAC&url=https%3A%2F%2Fwww.gov.br%2Fdefesa%2Fpt-br%2Farquivos%2Flai%2Finstitucional%2Fdiagra_planejamentoa_estrategicoa_17a_04a_2020.pdf&usg=AOvVaw0ogPs3p7_I0-VIurN9JK__V> Acesso em 30 de agosto de 2020.

BRASIL. **Estratégia Nacional de Segurança Cibernética**. Decreto nº10.222, de 5 de Fevereiro de 2020a. Palácio do Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm>. Acesso em 25 de março 2020.

BRASIL. **Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências**, 2020b. Decreto Nº 10.332. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10332.htm>. Acesso em 15 de abril 2020

BRASIL. Ministério da Justiça e Segurança Pública. **O que é o RIC?**. Disponível em <https://www.justica.gov.br/Acesso/governanca/ric>. Acesso em 18 de agosto de 2020.

BUZ, a. Marcelo Amaro. Palestra Abertura. **17º CertForum**. Realização do Instituto Nacional de Tecnologia da Informação em parceria com Associação Brasileira de Identificação Digital - ABRID. Evento realizado em 17 de Setembro de 2019.

BUZ, b. Marcelo Amaro. Palestra: A importância da certificação eletrônica e a tecnologia blockchain na proteção dos dados no ambiente jurídico e empresarial. **III Seminário de Segurança da Informação No meio Jurídico.** Realização da Comissão de Direito Digital da Ordem dos Advogados do Brasil Santa Catarina. Evento realizado em 10 de dezembro de 2019.

CARNELUTTI, Francesco. **A prova Civil. Título original; La prova civile**. Trad. Lisa Pary Scarpa. 2ª Ed. Campinas: Bookseller, 2002. *Apud* Bittar, João Paulo Vinha. **Assinatura e contratos digitais: uma breve abordagem sobre as novas questões trazidas pelos avanços da informática no campo do direito contratual, mais especificamente sobre a validade das assinaturas digitais**. Artigo publicado em 01/11/2011. In Revista Âmbito Jurídico - n° 93 – Ano XIV – Outubro/2011. Disponível em <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10239&revista_caderno=17>. *Apud* **PARECER n. 00378**, da Procuradoria Federal Especializada Junto ao Instituto Nacional de Tecnologia da Informação, Brasília, 2019.

CAVALCANTE, Rodrigo Arantes. Os Meios de Prova e o Direito Digital. In: LÓSSIO, Claudio Joel Brito; NASCIMENTO Luciano; e TREMEL, Rosangela. **Cibernética Jurídica: estudo sobre o direito digital**. Campina Grande. EDUEPB, 2020.

CRYPTOID, Portal. **Primeiro Documento Eletrônico assinado entre dois Países foi emitido em 2 de outubro de 2020**. Disponível em <https://cryptoid.com.br/banco-de-noticias/primeiro-documento-eletronico-assinado-entre-dois-paises-foi-emitido-em-2-de-outubro-de-2020/>. Acesso em 05 de outubro de 2020.

HOOTSUITE. **Report "Digital in 2020. Essential Insights Into How People Around the World Use The Internet, Mobile Devices, Social Media and E-commerce**. Disponível em: <https://datareportal.com/reports/digital-2020-global-digital-overview>. Acesso em 21 de agosto de 2020.

ITI - Instituto Nacional de Tecnologia da Informação, a. **Aplicações com Certificado Digital ICP-Brasil**. Disponível em: <https://aquitemcd.iti.gov.br/>. Acesso em 22 de agosto de 2020

ITI - Instituto Nacional de Tecnologia da Informação, b. **Estrutura ICP-Brasil**. Disponível em: <https://estrutura.iti.gov.br/>. Acesso em 22 de agosto de 2020

JUNIOR, Samuel César da Cruz. **A Segurança e Defesa Cibernética no Brasil e Uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia Para o Espaço Virtual**. IPEA – Instituto de Pesquisa Aplicada: Texto Para Discussão. Brasília : Rio de Janeiro. 2013.

MELLO, Celso D. de Albuquerque. **Curso de Direito Internacional Público**.15ª Ed. Rio de Janeiro: Renovar, 2004.

MENKE, Fabiano. **Assinatura Eletrônica: Aspectos Jurídicos No Direito Brasileiro**. 1ª Ed. São Paulo: Revista dos Tribunais, 2005.

MERCOSUL. **Acordo de reconhecimento mútuo de assinaturas digitais no Mercosul.** Disponível em <https://www.mercosur.int/pt-br/acordo-de-reconhecimento-mutuo-de-assinaturas-digitais-no-mercosul/>. Acesso em 05 de Julho de 2020.

METRÓPOLES, Portal. **Até 2021 um quarto dos servidores públicos federais irão se aposentar**. Disponível em: <https://www.metropoles.com/brasil/servidor-brasil/ate-2021-um-quarto-dos-servidores-publicos-federais-irao-se-aposentar>. Acesso em 3 de agosto de 2020.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Disponível em <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=documento>. Acesso em 09 de maio 2020.

NAÍM, Moises. **O fim do poder**: nas salas da diretoria ou nos campos de batalha em Igrejas ou Estados, por que estar no poder não é mais o que costumava ser?. Tradução Luis Reyes Gil. – São Paulo: LeYa, 2013.

ORGANIZATION OF AMERICAN STATES. ***Cybersecurity: C****apacity Review Federative Republic of Brazil*. Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford, United Kingdom. 2020

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO. **The Global Risks Report 2020** -15th Edition. Disponível em http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf>. Aesso em 18 de agosto de 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Digital Economy Report 2019** – Value Creation and Capture: Implications dor Developing Countries. Nova Iorque. 2019.

PARLAMENTO EUROPEU E DO CONSELHO. **REGULAMENTO (UE) Nº 910/2014**, de 23 de julho de 2014 relativo à identificação eletrônica e aos serviços de confiança para as transações eletrônicas no mercado interno e que revoga a Diretiva 1999/93/CE. Disponibilizado em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910&from=PT>. Acesso em 20 de agosto de 2020.

WIRTZ, Bernard. W. Wirtz. **Digital Business Models**. Speyer: Springer, 2019.

WORLD BANK. **Doing Business Doing Business 2020 Comparing Business Regulation in 190 Economies**. Disponível em <https://openknowledge.worldbank.org/bitstream/handle/10986/32436/9781464814402.pdf>. Acesso em 15 de agosto de 2020.