Assinaturas eletrônicas e segurança cibernética: uma análise da Lei 14.063/20 à luz da tríade CIA

Samuel Nunes Furtado
Acadêmico de Direito pela Universidade Federal de Uberlândia (UFU)
Membro discente dos Grupos de Pesquisa e Extensão "Comunidade Internacional de Estudos em Direito Digital (CIED)" e "Laboratório de Direitos Humanos (LabDH)"

Victor Rodrigues Nascimento Vieira
Advogado
Pós-graduando em Jurimetria – Ciência de Dados aplicada ao Direito pela Unyleya
Especialista em Direito Digital pelo Complexo de Ensino Renato Saraiva (CERS)

RESUMO

O presente artigo tem por objetivo estudar os aspectos fundamentais da lei de assinatura eletrônica 14.063/20, comparando com legislações estrangeiras e produções acadêmicas sobre a temática. Foram realizadas interpretações teleológicas dos conceitos e classificações à luz dos princípios basilares da segurança de informação, utilizando o método dedutivo. Em suma, o trabalho concluiu que a adoção das assinaturas no modelo rígido imposto pelo legislador, sem considerar a análise da segurança em nível contextual, implica a restrição da atuação dos entes públicos na garantia da segurança da informação, e vai de encontro à análise preventiva da proteção dos sistemas de informação.

Palavras-chaves: Segurança da Informação. Assinatura eletrônica. Lei 14.063/20. Administração Pública.

ABSTRACT

This article aims to study the fundamental aspects of the electronic signature law 14.063/20, comparing it with foreign legislation and academic productions on the subject. Teleological interpretations of concepts and classifications

were carried out in light of the basic principles of information security, using the deductive method. In short, the work concluded that the adoption of signatures in the rigid model imposed by the legislator, without considering the analysis of security at a contextual level, implies the restriction of the performance of public entities in guaranteeing information security, and goes against the preventive analysis. protection of information systems.

Keywords: Information security. Electronic signature. Law 14.063/20. Public administration.

Introdução

A revolução das tecnologias da informação e comunicação (TICs), muito embora tenha dinamizado a interação entre as pessoas em nível global, trouxe diversos desafios ao Direito enquanto ciência, porquanto alterou fundamentalmente os supostos normativos construídos a partir da realidade fática social e econômica. A superficialidade do mundo eletrônico, baseado essencialmente no conhecimento dedutivo-débil, traduziu riscos imensuráveis no espaço cibernético, com a difusão em larga escala de estratégias técnicas de manipulação de dados, em detrimento da consistência e segurança das informações.

Visando resguardar esses binômios no âmbito da administração pública, sem deixar de mencionar a tutela da confiança no meio eletrônico, é que a Lei nº 14.063, de 23 de setembro de 2020, cujo escopo tem por fim a regulação do uso de assinaturas eletrônicas em interações com entes públicos, foi aprovada pelo Congresso Nacional e sancionada pelo Presidente do Brasil. Ela criou dois novos conceitos para assinatura eletrônica de documentos públicos, com o objetivo de facilitar o uso de documentos assinados eletronicamente e, com isso, ampliar o acesso aos serviços públicos digitais, torná-los mais eficientes, agilizar trâmites burocráticos, economizar recursos e, de forma indireta, contribuir com a proteção ao meio ambiente, reduzindo a utilização de papel.

A iniciativa está intimamente relacionada com o desenvolvimento de uma série de ações, coordenadas pelo poder público, tendentes à digitalização dos serviços, que são uma consequência direta do impacto da pandemia de coronavírus[1].

[1] Segundo dados da Agência Brasil, publicados em 07 de junho de 2020, mais de 150 serviços públicos foram digitalizados durante a pandemia.

A legislação tem como propósito, também, garantir a segurança desses serviços prestados em ambiente eletrônico, bem como proteger as informações pessoais e sensíveis dos cidadãos, conforme preveem a Lei Geral de Proteção de Dados[2] e os incisos X e XII do *caput* do art. 5º da Constituição Federal.

Para garantir a segurança pretendida nas comunicações entre pessoas físicas, jurídicas e Administração Pública, a lei cria a figura da assinatura simples, da assinatura avançada e faz menção à já existente assinatura eletrônica qualificada, a qual utiliza certificado digital[3]. A questão da segurança, sob o ponto de vista legal, está relacionada à criação de parâmetros de nivelamento da confiabilidade condicionada à modalidade de assinatura, que é atribuída à informação, considerando as tecnologias utilizadas e os procedimentos envolvidos, em uma espécie de gradação.

A importância do tema é crescente, porquanto se relaciona de igual modo à validade dos atos jurídicos quando, taxativamente, subordina certas informações ao tipo de tecnologia de segurança que lhe é atribuída. Os fatores para a preocupação com a segurança são vários, entre os quais se destaca o aumento do número de delitos informáticos tendentes a violar a integridade de dados e arquivos, como a intrusão informática, a inserção de softwares maliciosos, a modificação de linhas de programação para inutilizar arquivos (SYDOW, 2015, p. 75) e o uso intensivo de engenharia social.

Resta saber se a lei em questão é adequada para atingir os objetivos a que se propõe. Diante disso, a problemática que se apresenta é a seguinte: em que medida o nível de confiabilidade sobre a identidade e manifestação de vontade do titular da assinatura, baseado na classificação das assinaturas eletrônicas criada pela lei, pode ser utilizado como parâmetro de segurança e responsabilidade, considerando-se a tríade CIA - *Confidentiality* (confidencialidade), *Integrity* (integridade) *and Availability* (e disponibilidade)[4]?

A digitalização foi uma das consequências da necessidade de redução de aglomerações e do distanciamento social. Veja mais em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-06/mais-de-150-servicos-publicos-sao-digitalizados-durante-pandemia Acesso em 09 de outubro de 2020.

2 Lei nº 13.709, de 14 de agosto de 2018.

3 Prevista na Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

4 A tríade CIA nos remete aos objetivos estruturantes da Segurança da Informação, quais sejam: *Confidentiality* (confidencialidade), *Integrity* (integridade) *and Availability* (e disponibilidade). Em breve síntese, a

Na busca de debater a questão colocada, este estudo terá como objetivo geral analisar os conceitos e as classificações da Lei 14.063, de 23 de setembro de 2020, à luz da tríade CIA. Os objetivos específicos, por seu turno, são: apresentar a lei desde a sua origem, delineando o âmbito de sua aplicação; conceituar, definir e classificar os tipos de assinatura eletrônica, e problematizar o nível de confiabilidade e segurança à luz da tríade CIA e da responsabilidade pelas interações entre a Administração e a iniciativa privada, conforme passará a expor.

1 Considerações iniciais sobre o trâmite da Lei 14.063/20

A iniciativa legislativa apresentada pelo Poder Executivo teve como origem a Medida Provisória nº 983, de 2020 (MP 983/20), publicada no dia 17 de julho de 2020, no Diário Oficial da União (DOU). Ela recebeu 87 emendas em relação ao projeto original e foi transformada na Lei Ordinária nº 14.063, de 23 de setembro de 2020, nesta data. A enquete a respeito da MP 983/2020 teve 12 votos, sendo que 67% dos votantes concordaram totalmente com o teor da proposta[5].

A referida lei trata do uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde. Foi publicada no DOU de 24 de setembro de 2020[6], tem seis capítulos, vinte artigos, teve sete dispositivos vetados e entrou em vigor na data de sua publicação. Ela versa sobre as licenças de softwares desenvolvidos por entes públicos e altera a Lei nº 9.096, de 19 de setembro de 1995[7], a Lei nº 5.991, de 17 de dezembro de 1973[8], e a Medida Provisória nº

confidencialidade é a propriedade que limita o acesso à informação a quem é legitimado para tanto. É ela que busca garantir o sigilo das informações. A integridade é um atributo que visa garantir que os dados ou informações mantenham a sua incolumidade desde a sua origem até o seu destino. A disponibilidade, última propriedade, visa assegurar ao usuário legítimo que a informação esteja disponível, isto é, que ele consiga acessá-la.

5 A enquete está disponível em: https://forms.camara.leg.br/ex/enquetes/2255363/resultado Acesso em 09 de outubro de 2020.

6 Disponível em: https://www.in.gov.br/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931 Acesso em 09 de outubro de 2020.

7 A Lei nº 9.096, de 19 de setembro de 1995, dispõe sobre os partidos políticos, disciplinando a criação, organização, fusão, incorporação e extinção destes.

8 A Lei nº 5.991, de 17 de dezembro de 1973, dispõe sobre o Controle Sanitário do Comércio de Drogas, Medicamentos, Insumos Farmacêuticos e Correlatos em todo o território nacional.

2.200-2, de 24 de agosto de 2001 (MP nº 2.200-2/2001)[9]. Dispõe, ainda, que todos os sistemas públicos que utilizem assinaturas eletrônicas e que não atendam ao disposto na lei deverão se adaptar às novas regras até o dia 1º de julho de 2021. A iniciativa cria, portanto, um espaço fora do sistema da Infraestrutura de Chaves Públicas brasileira (ICP-Brasil) para tratar do tema de assinaturas eletrônicas.

Vale ressaltar que a nova lei não revogou a MP 2.200-2/2001. Isso porque ela tem característica de texto legal especial em relação à MP, com a abrangência restrita ao âmbito dos entes públicos. Ademais, a MP 2.200-2 adotou classificação "bipartida" de assinaturas eletrônicas (enquanto a Lei 14.063/2020 tem classificação "tripartida"), equiparou a assinatura digital ICP-Brasil à assinatura manuscrita e facultou a utilização de outros mecanismos de comprovação de autoria para o meio eletrônico, o que não se observa na nova iniciativa legislativa.[10]

1.1 Âmbito de aplicação da lei de assinatura eletrônica

Inicialmente, cabe destacar que a lei sob análise visa à regulação e ao uso da assinatura eletrônica nos atos compreendidos na interação com os entes públicos em geral, não se restringindo a documentos eletrônicos. O âmbito de aplicação da lei está previsto no art. 2º. Conforme disposição do inciso I do referido dispositivo, a legislação se aplica à interação[11] interna dos órgãos e entidades da Administração Direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federados. Os

---

9 A Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (MP nº 2.200-2/2001), institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e transforma o Instituto Nacional de Tecnologia da Informação em autarquia. A ICP-Brasil, segundo o artigo 1º da MP, foi instituída 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.

10 MENKE, Fabiano. A MP 983 e a classificação das assinaturas eletrônicas: comparação com a MP 2.200-2. CryptoID, 2020. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-mp-983-e-a-classificacao-das-assinaturas-eletronicas-comparacao-com-a-mp-2-200-2-por-fabiano-menke/?fbclid=IwAR2nAf3Ac_y7ZJ4Y8nW1cIq-YERt8ReDLiwkTO_E3K6XbRtzt1KMcSYzND0. Acesso em: 09 de outubro de 2020.

11 A interação seria qualquer tipo de comunicação que ocorre no dia a dia da administração pública.

entes federados da Administração Direta representam os compartimentos internos da República Federativa, sendo eles a União, os Estados, o Distrito Federal e os Municípios. Os Poderes são as estruturas internas destinadas à execução de certas funções, sendo eles: Executivo, Legislativo e Judiciário.

As autarquias são as pessoas jurídicas de Direito Público interno que gozam de autonomia administrativa, econômica e financeira nos limites das leis que as criam e não são subordinadas a nenhum órgão do Estado (MELLO, 2015, p. 164-165), a exemplo das Agências Reguladoras (ANEEL[12], ANTT[13], ANP[14], entre outras). As fundações surgem quando um determinado patrimônio é destacado por aquele que o funda, ao qual é atribuída uma personalidade jurídica, com o fim de atender a uma finalidade específica.

O conceito de fundação suscita debates na doutrina, a qual aceita a criação de fundações públicas ou governamentais sob o regime de direito público ou privado[15]. São exemplos de fundações a Funai[16], a Funasa[17], o IBGE[18], entre outras. Por sua vez, os órgãos constitucionalmente autônomos são instituições estatais relevantes, com sede constitucional, que desempenham papel estratégico no sistema das garantias coletivas (CARVALHO FILHO, 2017, p. 41), como o Tribunal de Contas da União, o Ministério Público e a Defensoria Pública.

Nos termos do inciso II da lei de assinaturas eletrônicas, o regime jurídico por ela disposto aplica-se de igual modo quando a interação ocorrer entre pessoas naturais ou pessoas jurídicas de direito privado e os entes públicos citados anteriormente. Este inciso, portanto, pode ser exemplificado em uma situação em que um particular (um empreendedor ou uma corporação)

12 Agência Nacional de Energia Elétrica
13 Agência Nacional de Transporte Terrestre
14 Agência Nacional do Petróleo
15 Marya Sylvia Zanella di Pietro destaca que se formaram duas correntes acerca do tema. Uma defende a natureza privatística de todas as fundações instituídas pelo Poder Público. A outra entende que é possível a existência de fundações com personalidade pública - como modalidade de autarquia - ou privada. A autora posiciona-se entre os que defendem a possibilidade de o Poder Público atribuir às fundações personalidade de direito público ou privado. (DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 27. ed. São Paulo: Atlas, 2014. p. 505).
16 Fundação Nacional do Índio
17 Fundação Nacional de Saúde
18 Instituto Brasileiro de Geografia e Estatística

dirige um requerimento (assinado eletronicamente) ao Município com o intuito de regularizar alguma pendência do seu estabelecimento, como o alvará de funcionamento.

Já o inciso III, da legislação supracitada, versa que a medida se aplica à interação entre os próprios entes públicos. Em outras palavras, qualquer que seja a pessoa, física ou jurídica, de direito público ou privado, quando interagir com a administração pública, deverá observar os ditames da Lei nº 14.063/20.

Lado outro, o parágrafo único do art. 2º desta lei, a seu turno, traz algumas exceções, sendo inaplicável aos processos judiciais[19], aos sistemas de ouvidoria de entes públicos, aos programas de assistência às vítimas e às testemunhas ameaçadas, às interações entre pessoas naturais ou jurídicas de direito privado, às interações em que seja permitido o anonimato, às interações em que seja dispensada a identificação do particular e às outras hipóteses nas quais deva ser dada garantia de preservação de sigilo da identidade do particular na atuação perante o ente público.

Cite-se, ainda, que restaram afastadas da aplicação da lei de igual modo as relações havidas exclusivamente entre agentes privados, sejam pessoas jurídicas ou físicas. Essas relações, no entanto, continuam sendo regidas pelo Código Civil, pela MP nº 2.200-2/2001, pelo princípio da liberdade das formas de declaração da vontade[20], pelas legislações específicas aplicáveis a cada caso, bem como pelo direito das partes em empregar os meios probatórios legais e moralmente legítimos[21].

2 Criptografia e certificado digital

Antes de adentrar nos conceitos de assinaturas eletrônicas, é preciso entender o que é criptografia e certificado digital, porquanto inerentes à compreensão do tema. A Criptografia,

[19] Os processos judiciais que tramitam em meio eletrônico são regidos pela Lei nº 11.419, de 19 de dezembro de 2006. Conforme a lei, considera-se assinatura eletrônica a assinatura digital baseada em certificado digital emitido por Autoridade Certificadora, mediante cadastro do usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos (alíneas "a" e "b" do inciso III do §2º do art. 1º da Lei 11.419/2006).

[20] A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir (art. 107 do Código Civil de 2002).

[21] As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz (art. 369 do Código de Processo Civil de 2015).

em termos técnicos, é uma ferramenta de codificação de informações (PINHEIRO, 2016. p. 270). A origem da palavra é grega e, quando decomposta, nos revela os morfemas *kryptós* (escondido, oculto) e *graphía* (grifo, escrito) (KAZIENKO, 2013, p. 36). Ela serve para transformar informações inteligíveis em algo não cognoscível, utilizando um conjunto de técnicas algorítmicas.

As técnicas criptográficas podem ser classificadas, quanto ao número de chaves utilizadas no processo de cifrar e decifrar informações, em duas classes: simétrica e assimétrica. A simétrica usa uma única chave para cifrar e decifrar uma informação. Esta chave é de conhecimento do emissor e do receptor. A assimétrica, também denominada de criptografia de chave pública, utiliza um par de chaves para este processo: uma pública e uma privada. Neste caso, a chave utilizada para cifrar é de conhecimento público; no entanto, a informação só pode ser decifrada pela chave privada, a qual, em regra, deve ser de conhecimento restrito (KAZIENKO, 2013, p. 37).

Para cifrar um texto, é necessária uma chave com um número determinado de bits, de modo que, quanto maior o tamanho da chave, maior a quantidade de bits e, consequentemente, maior a segurança, uma vez que o espaço das chaves é aumentado (KAZIENKO, 2013, p. 36-37).

O objetivo principal da criptografia é a inviolabilidade da segurança da informação, a saber, confidencialidade, integridade e disponibilidade, conjugando aspectos como a autenticidade e autorização e responsabilidade, os quais serão objetos de estudo posterior. Aliás, importante mencionar que o fato de uma informação ser criptografada não necessariamente a torna inviolável, por mais extensos que sejam os bits, porquanto há certas metodologias específicas para violação de criptografia[22] .

2.1 Certificado digital

Apresentada a criptografia, passamos ao conceito de certificado digital, que é um arquivo assinado eletronicamente por

[22] Veja-se, a título introdutório, que há certos tipos de ataques específicos à tecnologia criptográfica, bastando o conhecimento de métodos de criptografia e descriptografia, tais como: ataque de texto cifrado (*cyphertext-only*), que consiste na dedução das chaves criptográficas a partir do texto cifrado; ataque de texto conhecido (*known-plaintext*), aqui o atacante possui conhecimento da mensagem criptografada e das originais sem a cifra, com as quais o intuito é descobrir a chave; e, por fim, o ataque de chave escolhida (*choosen-key*), no qual são testadas chaves

uma entidade confiável, denominada Autoridade Certificadora (AC). Os certificados digitais são utilizados com o fim principal de fazer a associação entre a chave pública e uma pessoa ou entidade, atribuindo confiabilidade à divulgação da chave pública.

Em outras palavras, o certificado permite identificar quem emitiu a chave pública por meio da atribuição privativa de chaves aos seus titulares. O papel da AC, portanto, é de emitir o certificado e garantir que determinado indivíduo ou empresa, e somente ele, detenha um certo par de chaves. Ele transporta a chave pública e confere segurança sobre quem é seu autor e emissor (KAZIENKO, 2013, p. 43-44).

Note-se que a certificação digital é utilizada e disseminada em países da Europa e também nos Estados Unidos, com o fim de conferir mais segurança, garantir a autenticidade e mitigar riscos de interceptação. No Brasil, o certificado digital já é utilizado junto a alguns órgãos de governo, como a Receita Federal, que aceita o e-CPF (PINHEIRO, 2016, p. 272). Feitos tais esclarecimentos, passa-se às classificações de assinaturas eletrônicas.

3 Assinaturas eletrônicas e suas espécies

A etimologia da palavra 'assinar' deriva do latim *assignare*, que significa "pôr sinal em". O ato de assinar um documento, seja ele eletrônico ou não, corresponde a assumir a autoria quanto ao seu conteúdo; declarar a vontade dirigida à produção dos efeitos jurídicos nele expostos. Seguindo os ensinamentos de Ricardo Lorenzetti, é possível inferir como elementos característicos de qualquer modalidade de assinatura o elemento objetivo (qualquer símbolo distintivo), e o subjetivo (identificação do autor e concordância com o ato) de monopólio exclusivo de seu titular (LORENZETTI, 2004, p. 123).

A diferença essencial da assinatura tradicional com a eletrônica reside em que o suporte desta é constituído por um conjunto de códigos (bits), ao passo que aquela é hológrafa - produzida por traços manuais (LORENZETTI, 2004, p. 116). Neste ínte-

pré-selecionadas, ou se induz o usuário legítimo do sistema a utilizar determinadas chaves de conhecimento do invasor. MAGALHÃES, Marcelo Vicente Vianna. Segurança de sistemas: ênfase em redes de computadores. **GTA – grupo de teleinformática e automação**: UFRJ, 2000. Não paginado. Disponível em: https://www.gta.ufrj.br/grad/02_1/seguranca/7.5.htm. Acesso em: 05 de maio de 2021.

rim, veja-se redação do art. 3º da Lei n º 14.063/20, a qual define assinatura eletrônica como sendo os dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos na legislação.

Vale salientar, em razão disso, que a assinatura não se confunde com a tecnologia utilizada para assinar, de modo que, em regra, a criptografia não é em si uma assinatura, muito embora possa ser utilizada como tal, quando então servirá de parâmetro de segurança e de sinal identificador[23]. Logo, esse raciocínio permite inferir ao menos duas proposições: (i) é possível que haja ato eletrônico criptografado sem assinatura, e (ii) a assinatura eletrônica não está adstrita às técnicas de criptografia.

Adiante, a legislação supracitada elenca as espécies de assinaturas eletrônicas, são elas: simples, avançada e qualificada[24]. A assinatura eletrônica simples, prevista no inciso I do art. 4º, é aquela que permite identificar o seu signatário e que anexa ou associa dados a outros dados em formato eletrônico do signatário. Como o próprio nome sugere, trata-se de assinatura 'vulgar', sem requisitos técnicos, admitida nas interações com ente público de menor impacto[25] e que não envolvam informações protegidas por grau de sigilo[26] (inciso I, §1º do art. 5º da 14063/2020).

Tome-se como exemplo de assinatura simples o nome do remetente apostado no corpo do texto de um e-mail, a imagem da assinatura de próprio punho inserida no documento eletrônico[27], o uso de *login* e senha, a biometria, o "aceite" nos termos de consentimento de plataformas digitais, entre outros. Neste tipo de assinatura, não há a implementação de um processo

---

23 É o caso das assinaturas eletrônicas avançadas que serão abordadas posteriormente.

24 A classificação das assinaturas eletrônicas, como colocada na lei em exame, muito se assemelha à existente na Diretiva 1999/93/CE, revogada pelo eIDAS (*eIectronic IDentification, Authentication and trust Services*) Regulamentação de Identificação Eletrônica e Serviços Confiáveis (eIDAS 910/2014/EC). A íntegra do documento está disponível em: https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eundeg9102014 Acesso em 13 de outubro de 2020.

25 Veja-se que a lei não caracteriza o que seria uma interação com ente público de menor impacto.

26 A lei também não classifica o grau de sigilo das informações.

27 MENKE, op cit.

criptográfico específico incidindo no conteúdo ou representação do ato eletrônico[28].

A assinatura eletrônica avançada, prevista no inciso II do art. 4º, a seu turno, é a que utiliza certificados *não* emitidos pela ICP-Brasil[29] ou por outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Este tipo de assinatura deve: i) estar associado ao signatário de maneira unívoca[30]; ii) utilizar dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo[31]; e iii) estar relacionada aos dados a ela associados de tal modo que qualquer modificação posterior seja detectável[32].

Por sua vez, a assinatura eletrônica qualificada, disposta no inciso III do art. 4º, é a que utiliza certificado digital ICP-Brasil, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2,

---

28 FORTNER, Carlos. Carlos Fortner, diretor-presidente do ITI, fala sobre a MP 983 e sua contextualização com assinatura digital e certificação digital. **CryptoID**, 2020. Disponível em: https://cryptoid.com.br/banco-de-noticias/carlos-fortner-diretor-presidente-do-iti-fala-sobre-a-mp-983-e-sua-contextualizacao-com-assinatura-digital-e-certificacao-digital/. Acesso em: 09 de outubro de 2020

29 Ou seja, por meio das infraestruturas de chaves públicas criadas em paralelo à regulamentação da ICP-Brasil. Tanto é assim que o artigo 3º da lei diferencia certificado digital de certificado digital ICP-Brasil. Certificado digital para a lei é o atestado eletrônico que associa os dados de validação da assinatura eletrônica a uma pessoa natural ou jurídica (inciso III do art. 3º da Lei 14063 de 2020). E certificado digital ICP-Brasil é o certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na forma da legislação vigente (inciso IV do art. 3º da Lei 14063 de 2020).

30 Significa dizer que a associação da assinatura ao seu titular não levanta dúvidas. Ou seja, a assinatura está vinculada ao seu titular de modo inequívoco. A lei não determinou quais são os procedimentos de associação inequívoca.

31 A operação de controle exclusivo remete ao acesso ao mecanismo de criação de assinatura. Isto é, à possibilidade de acessar, por exemplo, a chave privada para a criação de uma assinatura, por meio de um token.

32 Em muito se assemelha à legislação brasileira com a europeia, porquanto nesta a assinatura eletrônica avançada tem como elementos caracterizadores: i) estar associada inequivocamente ao signatário; ii) permitir identificar o signatário; iii) ser criada com meios que o signatário pode manter sob seu controle exclusivo; iv) estar ligada a dados a que diz respeito, de tal modo que qualquer alteração subsequente dos dados seja detectável. A íntegra da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de

de 24 de agosto de 2001[33]. Por ser a mais confiável e segura, nos termos da lei - tendo em vista as suas normas, seus padrões e seus procedimentos específicos -, ela será admitida em qualquer interação eletrônica com ente público, independentemente de cadastramento prévio, inclusive nos casos em que são aceitas as assinaturas simples ou avançadas (inciso II, §1º do art. 5º da Lei 14063/2020). Oportuno destacar, ainda, que a lei 14.063/20 estabelece quatro hipóteses, as quais o seu uso será obrigatório - art. 5º, § 2º, incisos I, III e IV; e art. 13 -, sem o qual o ato será inválido[34].

4 A tríade CIA nas assinaturas eletrônicas

Compulsando a lei das assinaturas eletrônicas, observa-se que o parâmetro básico para estigmatizar os diferentes tipos de assinaturas e, consequentemente, estabelecer reservas de validade a atos com maiores potenciais críticos e sensíveis à Administração Pública, é o nível de confiança das assinaturas. Para estudar esse parâmetro, inevitavelmente, há que se fazer referência aos pilares que sustentam a segurança da informação em todo seu ciclo de vida.

A segurança, no campo da Tecnologia da Informação, pode ser definida como o conjunto de regras de ordem técnica, administrativa e operacional cujo escopo tem por fim a garantia da confidencialidade, integridade e disponibilidade dos dados (KREMLING, 2017, p. 94). A pertinência temática é demonstrada a partir do aprofundamento no estudo da integridade, variável

1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas encontra-se disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31999L0093&from=PT Acesso em 13 de outubro de 2013.

33 Pela definição da lei, pressupõe-se que a assinatura eletrônica qualificada é aquela que utiliza certificado digital da MP nº 2.200-2/2001. Entretanto, temos uma previsão vaga. Isto é, a previsão *não* afirma de forma taxativa que só serão aceitas assinaturas qualificadas que utilizem certificados digitais ICP Brasil. A imprecisão faz surgir a seguinte dúvida: qualquer certificado, mesmo que não seja ICP Brasil, garantirá este *status* de assinatura qualificada? Esta resposta só é possível quando se conjugam os incisos II e III do art. 4º. Isso porque, da leitura destes dispositivos, chegamos à conclusão de que a assinatura eletrônica avançada dispensa certificados emitidos pela ICP.

34 Basta uma interpretação literal do texto para perceber que o legislador constantemente atrela a questão da assinatura ao plano de validade do ato jurídico, existindo 13 menções expressas ao termo 'validade' e suas derivações.

que pressupõe um conjunto de protocolos objetivos que permitem aferir quando determinada informação foi alterada de forma não autorizada pelos sujeitos do processo de comunicação, prejudicando a validade da manifestação de vontade exteriorizada nos atos eletrônicos.

Portanto, a assinatura eletrônica como objeto da CIA possui algumas peculiaridades, especialmente se considerado o fato de que elas conservam profundas distinções com as assinaturas tradicionais, já que, naquela, o autor é vinculado à mensagem por meio de códigos[35], em detrimento do uso das grafias. Assim, enquanto no modelo tradicional o exame de autenticidade pode ser verificado através de raciocínio falso e verdadeiro, nas assinaturas eletrônicas, os bits, por sua própria natureza, não são suscetíveis a este juízo de apreciação empírico, pois as cópias são exatamente iguais às originais (LORENZETTI, 2004, p. 102).

Outro ponto a ser trabalhado se refere à confidencialidade, abrangendo tanto a assinatura em si (o sinal distintivo) quanto aos algoritmos que componham sua proteção, de modo que, também, os mecanismos de segurança não devem ser expostos, a exemplo das chaves de criptografia. Mas não basta que à assinatura eletrônica seja atribuída a integridade e confidencialidade sem que o seu titular possa fazer o uso dela no momento oportuno, eis, então, a necessidade de garantia da disponibilidade.

Ausentes esses atributos, os níveis de confiabilidade baseados nos tipos de tecnologias de cada assinatura se tornam irrelevantes, porquanto se revestem de vulnerabilidades graves ao não atender aos elementos basilares da segurança da informação. Estudadas essas premissas, passa-se à análise do controle de acesso enquanto parâmetro de proteção.

5 Os três "As" da segurança da informação e os atos eletrônicos da administração pública

Ao tratar de atos do poder público, necessariamente há que se considerar os princípios que o regem, nomeadamente o da competência[36], bem como os elementos do ato administrativo. Lado outro, na esfera da *cybersecurity*, a análise das ações, seja de agentes públicos ou corporativos, deve conjugar não apenas a autoria

[35] Desta forma, o legislador julgou por bem estabelecer a flexibilidade na adoção das assinaturas em casos de vazamento de dados relativos à tecnologia de sua implementação, a depender se simples ou avançada, com vistas a evitar violações de segurança (§2º, art. 4º da lei 11.063/20).

(*authentication*) do ato, mas também a autorização (*Authorization*) e a responsabilidade (*Accountability/non repudiation*), compondo os três "A(s)" da segurança da informação[37]

A Constituição Brasileira, respectivamente, em seus artigos 21 a 30, estabelece uma série de regras de organização e prerrogativas a serem exercidas pelos entes federativos, de modo exclusivo ou concorrente. Logo, não é correto pensar a assinatura desassociada da autorização para determinada função pública, pois, ao mesmo tempo em que a lei habilita a atuação do agente, de igual modo limita essa prerrogativa tornando-a indelegável e irrenunciável, no caso, estabelecendo reservas de assinaturas a determinados atos.

O conceito de ato administrativo, como destaca José dos Santos Carvalho Filho, é controverso. Para o autor, todavia, três pontos são fundamentais para a caracterização do ato administrativo: i) ele precisa emanar de agente da Administração Pública ou dotado de prerrogativas desta; ii) seu conteúdo deve produzir efeitos que visem a um fim público; e iii) esta categoria deve ser regida pelo direito público[38].

A validade jurídica do ato administrativo não se confunde com a validade técnica. Destarte, verificada a autenticação e autorização ligada à requisição da execução do ato, uma vez acionada, fica a Administração Pública algoritmicamente associada aos efeitos do ato indissociavelmente, não podendo negá-los (*accountability)*[39]. Desta forma, ainda que uma assinatura careça de aptidão para produzir efeitos jurídicos que lhes são próprios, dada a ausência de pressupostos de validade, é possível que produza efeitos eletrônicos, a exemplo de vazamento de

---

36 Que é descrito por Celso Antônio Bandeira de Mello como o círculo compreensivo de um plexo de deveres públicos a serem satisfeitos mediante o exercício de correlatos e demarcados poderes instrumentais, legalmente conferidos para a satisfação de interesses públicos (MELLO, *op cit*., p. 148).

37 LV, Yilun; DU, Bing. Application of AAA security management in classified network. In: **2013 IEEE 4th International Conference on Software Engineering and Service Science**. IEEE, 2013. p. 660-663. Disponível em: https://ieeexplore.ieee.org/abstract/document/6615393/?casa_token=O2_Kc3UJubcAAAAA:-dTNoZ37HW5eJLz1m4Ufesy34sk8GjUa3Tce6hg5eU8-5QDdnVCnTB4OmtVeJ8HDI7L64knL2a8. Acesso em: 05 de Maio de 2021.

38 Ibid., p. 99.

39 AOUAD, SIHAM; MAIZATE, ABDERRAHIM; ZAKARI, A. Cyber Security and the Internet of Things: vulnerabilities and Security requirements. **Revue Méditerranéenne des Télécommunications**, v. 9, n. 2, 2019. p. 2. Disponível em: https://revues.imist.ma/index.php/RMT/article/view/17475/9646. Acesso em: 06 de Maio de 2020.

informações pessoais e sensíveis, quando a assinatura violada for utilizada como ferramenta de controle de acesso a sistemas informáticos.

Daí a importância da adoção de parâmetros de segurança técnicos e administrativos visando à segurança das assinaturas e seu uso exclusivo pelo titular.

6 Níveis de confiabilidade e segurança das assinaturas

Em tópico anterior, foi exposto o ciclo dos serviços de segurança e como eles se alinham aos requisitos e à validade dos atos administrativos. Paralelamente, estabelece a lei uma presunção de confiança a certos tipos de assinatura estruturados em níveis, aos quais são associadas algumas reservas de validade.

É possível subtrair que a lei trabalha com uma presunção de segurança das assinaturas, levando em conta o modo de implementação. Sob a perspectiva conceitual, é evidente a imprecisão do termo para nivelar o grau de segurança das assinaturas, vez que, para a garantia da inviolabilidade da tríade, são necessárias também ferramentas de controle não técnicas conjugadas a elementos subjetivos dos agentes. Logo, a premissa básica de confiança trabalhada, nos termos da lei, deve ser alinhada ao fato de que o vínculo mais frágil na cadeia de segurança da informação é o elemento humano.

Lado outro, a confiança, do ponto de vista científico, não detém precisão terminológica, malgrado sua constituição seja pautada em aspectos objetivos e subjetivos[40]. De fato, a forma com que as comunicações se dão "*on-line*" na velocidade e intensidade da internet não permite que os atos de vida em rede sejam cuidadosamente trabalhados, motivo pelo qual a confiança se demonstra indispensável na execução de ações intermediadas pelas tecnologias da informação e comunicação. Justamente nesta casuística, explica Rezende citando Schneier, é possível deduzir que, contemporaneamente, os indivíduos vivem um efetivo "teatro de segurança", porquanto*:*

> [...] alguém pode se sentir inseguro em relação a um sistema cujo uso contabiliza certas probabilidades de incidência de falhas, fraudes ou sabo-

[40] REZENDE, Pedro. A. D. **Modelos de Confiança para Segurança Informática**. (artigo). 2012. p. 3. Disponível em: https://cic.unb.br/~rezende/trabs/modelos_de_confianca.pdf. Acesso em: 20 de outubro de 2020. 2012.

> tagens, e se sentir seguro em relação a outro sistema com maiores probabilidades de incidentes com potencial de danos equivalentes.[41]

Nesta sintonia, a lei depõe sobre as assinaturas com suposições acerca de sua segurança em abstrato, desconsiderando o contexto de implementação que, para Huang, é essencial à análise da confiança empregada no sentido de consistência fática dos sistemas de informação[42], sendo que, v.g., uma assinatura eletrônica qualificada pode ser, a depender do caso concreto, mais segura que uma assinatura avançada, e vice-versa. Essa problemática ganha contornos emblemáticos a partir do pressuposto de que a "pessoa", enquanto elemento dos sistemas de dados, compreende também o complexo de gerenciamento de riscos.

Assim, Josang, Gray e Kinateder entendem que a confiança está intimamente associada à conceituação de risco, pois serve de parâmetro para avaliação e adoção de ações pelos indivíduos[43]. Deste modo, o intuito legislativo em nivelar os tipos de assinatura é, efetivamente, limitar a liberdade do poder público para deliberar sobre qual tipo de código será usado para validar o ato eletrônico.

Porém, o legislador falha na medida em que subordina a flexibilização à reserva de validade associada à assinatura nas hipóteses em que a segurança for comprometida ou houver vazamento de dados, isto é, subsequente ao fato danoso[44]. A se-

---

41 *ibid*.

42 HUANG, B. *et al*. **Probabilistic soft logic for trust analysis in social network**. Maryland: University of Maryland, 2012. *Apud*: SOUZA, Raul Carvalho. **Prevenção para ataques de engenharia social: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural, interdisciplinar utilizando fontes de dados abertos.** (Dissertação Mestrado). 2015. p.113. Disponível em: https://repositorio.unb.br/bitstream/10482/18863/1/2015_RaulCarvalhodeSouza.pdf. Acesso em: 20 de outubro de 2020.

43 JOSANG, A.; GRAY, E.; KINATEDER, M. Analysing Topologies of Transitive Trust. In: **Proceedings of the Workshop of Formal Aspects of Security and Trust (FAST)**. Apud: LÓPES, Victor Leonel Orozco. Análise de Riscos de Segurança de Informação: Quantificação de Confiança Como um Parâmetro de Redução de Desvios de Resultados Por Causas Humanas. (Dissertação Mestrado). 2014. p. 30. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/5424/LOPEZ%2c%20VICTOR%20LEONEL%20OROZCO.pdf?sequence=1&isAllowed=y. Acesso em: 20 de outubro de 2020.

44 BRASIL, lei da assinatura eletrônica 14.063/20. Art. 4, § 2°.

gurança da informação está diretamente relacionada à busca por impedir a ocorrência de incidentes e à diminuição de vulnerabilidades que possam ser exploradas por ataques cibernéticos, razão pela qual foca em prevenir sua exploração, bem como amenizar seus impactos caso venham a se concretizar.

Ao preestabelecer quais assinaturas devem seguir certos atos com base no potencial de criticidade, a lei também restringe a atuação do poder público no zelo dos pilares que sustentam a proteção dos sistemas informáticos exteriorizados em atos eletrônicos. Pensar segurança negligenciando a situação em que é aplicada, por meio de classificações estáticas, mesmo diante da diversidade dos fluxos de comunicação e sua dinâmica global, vai de encontro às metodologias por trás da proteção dos sistemas, sobretudo à adoção de políticas.

Neste ínterim, Coimbra (2018, p. 17) destaca:

> Uma política de segurança diz respeito ao conjunto de normas, indicações ou instruções a seguir, com objetivo de prevenir a ocorrência de incidentes (ameaças) relacionados com a segurança da informação, sendo a prevenção, a '[...] capacidade de proteger a informação e os sistemas que a processam da perda da Confidencialidade, Integridade e Disponibilidade.

Outrossim, Marciano e Marques (2006. p. 1) destacam que essas políticas, voltadas essencialmente ao agir antecedente, envolvem uma série de fatores variados que abarcam, de forma sistematizada, recursos técnicos e humanos contextualmente aplicados. A proteção dos sistemas é subordinada, pois amparada em condicionantes técnicas, sociais e culturais; de igual modo, é orientada, vez que sua personalização é elaborada analiticamente às exigências da organização, de forma que a interpretação rígida ao disposto no art. 4 da Lei 14.063/2020 não apenas torna menos eficazes as tentativas de proteção dos sistemas, como também limita o campo de sua segurança, aumentando a probabilidade de ocorrência de incidentes e, consequentemente, de danos, atraindo a responsabilidade objetiva do Estado.

Conclusão

À vista do discorrido, o presente trabalho, entendendo a preocupação do Legislador em estabelecer e adaptar as prerrogativas públicas às intermediações pelas TICs, buscou estudar as

formulações da lei de assinatura eletrônica considerando a *praxe* da segurança da informação. Decerto, objetivando explorar os conceitos e as classificações da legislação, foram realizadas duas análises sob diferentes ângulos de aplicação, a saber, a normativa e a prática, relacionada aos desafios originados pelo desenvolvimento dos novos modelos informáticos e sua aplicação no âmbito da Administração Pública.

Preliminarmente, a pesquisa foi voltada ao campo de abrangência jurídica da lei e aos requisitos imprescindíveis para validade dos atos administrativos à luz da doutrina e da legislação pátria. Posteriormente, buscou-se observar os conceitos propriamente ditos e as diferenças existentes entre cada tipo de assinatura, destacando seus aspectos fundamentais com análise comparativa de legislações estrangeiras e bibliografias pertinentes.

Ao final, foram dedicados alguns capítulos para desmembramento dos conceitos estudados e suas implicações no campo da segurança da informação, pelo que foram levantados alguns parâmetros para imputação objetiva de responsabilidade, especialmente a confiança, estruturada em níveis aos quais correspondem reservas de validade de atos eletrônicos, concluindo-se com os efeitos negativos que tal estipulação em abstrato pode causar à proteção dos sistemas informáticos do Poder Público.

Os objetivos da legislação são positivos e ela foi editada e aprovada em um momento adequado, tendo em vista a transformação digital que toda a sociedade passa, principalmente considerando o contexto pandêmico e a necessidade de isolamento e distanciamento social. É necessário que o Estado e a sociedade acompanhem o desenvolvimento tecnológico e utilizem as ferramentas tecnológicas para conferir maior agilidade e segurança aos trâmites burocráticos, de modo que não se deve recusar o uso das assinaturas eletrônicas que foram criadas pela lei, nas interações público-privadas.

Entretanto, é imprescindível realçar que a lei é vaga para um tema tão complexo, principalmente considerando as particularidades técnico-jurídicas relativas às nomenclaturas e classificações das assinaturas. A complexidade aumenta se for considerado que o Estado deverá implementar a estrutura tecnológica necessária para ampliar o acesso aos serviços públicos digitais de forma segura e confiável, tratar os dados das pessoas físicas conforme a nova Lei Geral de Proteção da Dados e assegurar a incolumidade e confiabilidade das comunicações, levando em

conta os apontamentos relativos à tríade CIA, os três Três "A(s)" da Segurança da Informação e os princípios da Administração Pública.

O âmbito de aplicação da lei é vasto e irá exigir da Administração Pública, em todos os seus níveis, um grande esforço para regulamentar a questão, adaptar-se, até julho de 2021, às novas exigências e capacitar o pessoal para evitar problemas de falhas de segurança como os decorrentes do "fator humano".

Por fim, entende-se que, em que pesem a existência do regime jurídico administrativo e as previsões de responsabilidade civil no ordenamento jurídico brasileiro, seria interessante que a lei tivesse disposto a respeito da responsabilização administrativa (sem desconsiderar a penal e civil) dos agentes públicos que, por uma eventualidade, venham a causar dano aos particulares ou utilizarem de forma indevida as assinaturas nas interações internas da Administração Pública, assim como fazem a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor, os quais trazem um regramento específico, considerando o âmbito de aplicação e as peculiaridades dos assuntos de cada lei.

Referências

BEHRENS, Fabiele. A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira. Dissertação (Mestrado) - Ciências Jurídicas e Sociais, Pontifícia Universidade Católica do Paraná, Curitiba, 2005, p. 37. Disponível em: http://www.biblioteca.pucpr.br/tede/tde_arquivos/1/TDE-2005-10-07T063157Z-206/Publico/FabieleDto.pdf. Acesso em: 10 de out. de 2020.

BRASIL. Lei nº 10.406, de 10 de Janeiro de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 9 de out. de 2020.

BRASIL. Lei nº 13.105, de 16 de Março de 2015. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 9 de out. de 2020.

BRASIL. Lei nº 14.063, de 23 de Setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: https://www.in.gov.br/web/dou/-/lei-n-14.063-de-23-de-setem-

bro-de-2020-279185931. Acesso em: 9 de out. de 2020.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. São Paulo: Atlas, 2017.

COIMBRA, Sara Alexandra Magalhães Pereira. Ameaças e Vulnerabilidades à Segurança da Informação dos Sistemas de Informação da Força Aérea. Política de Segurança e Prevenção. Instituto Universitário Militar, Pedrouços, 2018, p. 17. Disponível em: https://core.ac.uk/download/pdf/223219869.pdf. Acesso em: 20 de out. de 2020.

European Union. Regulation (Eu) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014. On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Disponível em: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf. Acesso em: 10 de out. de 2020

FORTNER, Carlos. Carlos Fortner, diretor-presidente do ITI, fala sobre a MP 983 e sua contextualização com assinatura digital e certificação digital. CryptoID, 2020. Disponível em: https://cryptoid.com.br/banco-de-noticias/carlos-fortner-diretor-presidente-do-iti-fala-sobre-a-mp-983-e-sua-contextualizacao-com-assinatura-digital-e-certificacao-digital/. Acesso em: 22 de out. de 2020.

GUELFI, Airton Roberto. Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela Infra-Estrutura de Chaves Públicas do Brasil - ICP-Brasil. Dissertação (Mestrado) Engenharia Elétrica, Universidade de São Paulo. São Paulo, 2007, p. 64-65. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3142/tde-26072007-164132/pt-br.php. Acesso em: 10 de out. de 2020.

HOLANDA FERREIRA, Aurélio Buarque de. **Dicionário Aurélio Escolar da Língua Portuguesa**. 1. ed. Rio de Janeiro: Nova Fronteira, 1988.

HUANG, B.; et al. Probabilistic soft logic for trust analysis in social network. Maryland: University of Maryland, 2012. APUD: SOUZA, Raul Carvalho. Prevenção para ataques de engenharia social: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural, interdisciplinar utilizando fontes de dados abertos. Dissertação (Mestrado) - Ciência da Informação, Universidade de Brasília, Brasília, 2015, p. 113. Disponível em: https://repositorio.unb.br/bitstream/10482/18863/1/2015_RaulCarvalhodeSouza.pdf. Acesso em: 10 de out. de 2020.

JOSANG, A.; GRAY, E.; KINATEDER, M. Analysing Topologies of Transitive Trust. In: DIMITRAKOS, T., MARTINELLI, F. (eds.) Proceedings of the First International Workshop on Formal Aspects in Security & Trust. Pisa, Italy, p. 9-22, 2003. APUD: LÓPES, Victor Leonel Orozco. Análise de Riscos

de Segurança de Informação: Quantificação de Confiança Como um Parâmetro de Redução de Desvios de Resultados Por Causas Humanas. Dissertação (Mestrado) - Ciência da computação, Universidade Federal de Santa Maria, Rio Grande do Sul, 2014, p. 30. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/5424/LOPEZ%2c%20VICTOR%20LEONEL%20OROZCO.pdf?sequence=1&isAllowed=y. Acesso em: 10 de out. de 2020.

KAZIENKO, Juliano Fontoura. A**ssinatura digital de documentos eletrônicos através de impressão digital**. Dissertação (Mestrado) - Ciência da Computação, Universidade Federal de Santa Catarina. Florianópolis, 2013, p. 36. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/86583/191996.pdf?sequence=1&isAllowed=y. Acesso em: 9 de out. de 2020.

LORENZETTI, Ricardo Luis. **Comércio eletrônico**. trad. MENKE, Fabiano. São Paulo: Revista dos Tribunais. 2004.

MARCIANO, João Luiz; MARQUES, Mamede Lima. **O Enfoque Social da Segurança da Informação**. Ciência da informação, Brasília, v. 35, n. 3, p. 89-98, 2006, p. 89. Disponível em: https://www.scielo.br/pdf/ci/v35n3/v35n3a09.pdf. Acesso em: 20 de out. de 2020.

MELLO, Celso Antônio Bandeira de. C**urso de Direito Administrativo.** 32. ed. São Paulo: Malheiros, 2015.

MENKE, Fabiano. **A MP 983 e a classificação das assinaturas eletrônicas:** comparação com a MP 2.200-2. CryptoID, 2020. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-mp-983-e-a-classificacao-das-assinaturas-eletronicas-comparacao-com-a-mp-2-200-2-por-fabiano-menke/. Acesso em: 9 de out. de 2020.

MENKE, Fabiano. **A MP 983 e a classificação das assinaturas eletrônicas:** comparação com a MP 2.200-2. CryptoID, 2020. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-mp-983-e-a-classificacao-das-assinaturas-eletronicas-comparacao-com-a-mp-2-200-2-por-fabiano-menke/. Acesso em: 10 de out. de 2020

MOURÃO, Licurgo; ELIAS, Gustavo Terra; FERREIRA, Diogo Ribeiro. A imprescindibilidade da assinatura eletrônica, da assinatura mecânica e da certificação digital para a administração pública brasileira. Revista do Tribunal de Contas do Estado de Minas Gerais, Belo Horizonte, v. 73, n. 4, p. 29-44, dez. 2009. Disponível em: https://revista1.tce.mg.gov.br/Content/Upload/Materia/635.pdf. Acesso em: 9 de out. de 2020.

PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. Pinheiros: Saraiva, 2016.

REZENDE, Pedro. A. D. **Modelos de Confiança para Segurança Informática**. Brasília, [S.I.]: Universidade de Brasília, 2012, p. 3. Disponível em: https://cic.unb.br/

~rezende/trabs/modelos_de_confianca.pdf. Acesso em: 10 de out. de 2020.