FACULDADE PARA O DESENVOLVIMENTO SUSTENTAVEL DA AMAZÔNIA
COORDENAÇÃO DO CURSO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

MADSON DA SILVA SOUSA

CRIPTOGRAFIA E AUTENTICAÇÃO DE DOCUMENTOS PÚBLICOS COMO FORMA DE REDUÇÃO DA BUROCRACIA E AUMENTO NA SEGURANÇA DE DADOS.

PARAUAPEBAS
2022

MADSON DA SILVA SOUSA

CRIPTOGRAFIA E AUTENTICAÇÃO DE DOCUMENTOS PÚBLICOS COMO FORMA DE REDUÇÃO DA BUROCRACIA E AUMENTO NA SEGURANÇA DE DADOS.

Trabalho de conclusão de Curso (TCC) apresentado a Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do programa do curso de Análise e Desenvolvimento de Sistemas para obtenção do título de Analista.

Orientador: Prof. Kenedy Miné

PARAUAPEBAS
2022

MADSON DA SILVA SOUSA

CRIPTOGRAFIA E AUTENTICAÇÃO DE DOCUMENTOS PÚBLICOS COMO FORMA DE REDUÇÃO DA BUROCRACIA E AUMENTO NA SEGURANÇA DE DADOS.

Trabalho de conclusão de Curso (TCC) apresentado a Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do programa do curso de Análise e Desenvolvimento de Sistemas para obtenção do título de Analista.

APROVADO: ___ de junho de 2022.

Prof. Esp. Lucimara Fonseca de Jesus Almeida
(Avaliadora – FADESA)

Prof. Me. Manuel Martins Pino Estrada
(Avaliador – FADESA)

Prof. Esp. Jefferson Cardoso Van de Graaf
(Avaliador – FADESA)

Dedico este trabalho a Deus, pois sem ele eu nada seria, aos meus pais e a meu irmão Mateus da Silva Sousa, pois sempre me apoiaram nesta caminhada e nos momentos mais difíceis me mostraram que todo esforço seria recompensado.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado sabedoria e saúde para vencer todas as adversidades, aos meus pais Marusan Vieira e Joelma da Silva pelo amor incondicional, e aos meus amigos de sala, em especial o Rhafael Krüger, Thailson e Gyancarlo que de certa forma contribuíram grandemente para que vários processos importantes acontecessem durante o curso.

Agradeço também aos docentes, Glorisnaldo Rosa, Almir Hiriu e Kenedy Miné, pelos ensinamentos apresentados no decorrer do curso e pelos conselhos que contribuíram no meu processo de aprendizado e ao meu orientador Kenedy Miné por seu empenho ao me aconselhar no desenvolvimento do presente trabalho.

“Desde que você não desista, vai sempre existir salvação.”

(Hatake Kakashi)

RESUMO

Na emergência das novas Tecnologias de Informação e Comunicação (TIC), os governos de todo o mundo, bem como as empresas, passam por uma transição, tentando se adaptar às demandas da Sociedade do Conhecimento. As tecnologias podem auxiliar no combate a um problema recorrente na gestão pública, que é a burocracia. Ela é caracterizada por uma grande quantidade de papelada, muitas mesas, certa cultura de escritório e comunicação burocrática lenta devido às suas muitas camadas hierárquicas. Destarte, o presente trabalho tem como objetivo geral abordar a criptografia e autenticação de documentos públicos como forma de redução da burocracia e aumento na segurança de dados. Como objetivos específicos, tem-se: 1. Percorrer o processo evolutivo das reformas administrativas, da burocracia e suas disfunções. 2. Tratar do contexto atual com relação a desburocratização, proteção e segurança dos dados no Brasil, e, por fim 3. Expor a temática da criptografia e autenticação de documentos via Blockchain. Sera, por tanto, nessa ordem que organizar-se-á os capítulos vindouros da presente pesquisa. Quanto a metodologia utilizada, a pesquisa requer contato com a realidade a qual nos dispomos a investigar. Pensando nessa afirmativa, procuramos fazer uma pesquisa hipotético dedutiva, mediante uma revisão bibliográfica e legislacional em obras físicas e digitais adequada aos temas estudados. Como conclusão, a assinatura e autenticação por padrão Blockchain se mostrou útil, segura e bastante maximizadora da gestão desburocratizada, vez que permite a autenticação e análise de documentos assinados sob seu rito de modo prático, sem necessidade, por exemplo, de o administrador ou administrado se locomover a repartições, pegar longas filas e desperdiçar tempo, tudo de maneira rápida, prática e segura.

Palavras-chave: Assinatura. Autenticação. Blockchain. Gestão desburocratizada.

ABSTRACT

In the emergence of new Information and Communication Technologies (ICT), governments around the world, as well as companies, undergo a transition, trying to adapt to the demands of the Knowledge Society. Technologies can help combat a recurring problem in public management, which is bureaucracy. It is characterized by a lot of paperwork, many desks, a certain office culture and slow bureaucratic communication due to its many hierarchical layers. Thus, the present work has the general objective of approaching the encryption and authentication of public documents as a way of reducing bureaucracy and increasing data security. As specific objectives, there are: 1. Go through the evolutionary process of administrative reforms, bureaucracy and its dysfunctions. 2. Address the current context in relation to the reduction of bureaucracy, data protection and security in Brazil, and, finally, 3. Expose the topic of encryption and authentication of documents via Blockchain. Therefore, the following chapters of this research will be organized in this order. As for the methodology used, the research requires contact with the reality that we are willing to investigate. Thinking about this statement, we seek to make a hypothetical deductive research, through a bibliographic and legislative review in physical and digital works appropriate to the themes studied. In conclusion, the signature and authentication by Blockchain standard proved to be useful, safe and very maximizing of the debureaucratized management, since it allows the authentication and analysis of documents signed under its rite in a practical way, without the need, for example, of the administrator or administrator. moving to offices, taking long lines and wasting time, all quickly, conveniently and safely

Keywords: Signature. Authentication. Blockchain. Unbureaucratic management.

LISTA DE ABREVIATURAS E SÍMBOLOS

ABIN	Agência Brasileira de Inteligência
ANATEL	Agência Nacional de Comunicações
ANPD	Agencia nacional de proteção de dados
ANVISA	Agência Nacional de Saúde
CF/88	Constituição federal de 1988
COTEC	Criação da comissão técnica executiva
COVID-19	Corona vírus 2019
Dra.	Doutora
ECD	Escrituração contábil digital
ECF	Escrituração contábil fiscal
GSI.	Gabinete de Segurança Institucional
ICP.	Infraestrutura de chaves públicas
ITI	Instituto Nacional de Tecnologia da Informação
LGPD	Lei geral de proteção de dados
MP	Medida provisória
NSA	Sigla em inglês para “Agência de Segurança Nacional”
PEC	Projeto de emenda à constituição
Prof.	Professor
Profª.	Professora
p.	Página
ROI	Retorno sobre o investimento

SUMÁRIO

1. INTRODUÇÃO

Com o advento das novas Tecnologias de Informação e Comunicação (TIC), os governos de todo o mundo, bem como as empresas, passam por uma transição, na tentativa de se adaptar às demandas da Sociedade do Conhecimento. Tais tecnologias inovadoras permitem a melhoria das relações entre a sociedade, governos, empresas e parceiros, proporcionando melhorias na qualidade e eficiência dos setores públicos e privados.

A gestão pública utiliza as tecnologias como ferramenta para amenizar os impactos causados pela burocratização, caracterizada pela quantidade de papelada, mesas, cultura organizacional e comunicação lenta devido às camadas hierárquicas, sendo a maior desvantagem do sistema burocrático. Assim como, influenciam negativamente a motivação na execução das atribuições dos funcionários que permaneçam distantes uns dos outros e da organização.

As tecnologias estão atreladas aos documentos digitais e as autenticidades dos dados. Entretanto, se faz necessário a proteção das informações eletrônicas a fim de garantir a segurança das transações e a privacidade dos usuários. Diante disso, observou-se a evolução e a presença da criptografia em diversas atividades diárias, sejam elas simples ou complexas.

O advento dos computadores e a criptografia incorporou algoritmos intrincados da Matemática com dígitos binários em seus processos, promovendo maior velocidade no processo e no nível de complexidade. Já nas técnicas tradicionais remete se ao embaralhar e substituir letras do alfabeto Para Ferreira (2020) O ato de cifrar, criptografar e codificar correspondem ao processo de transformação de dados ou informações para uma forma ininteligível usando um algoritmo criptográfico e uma chave criptográfica.

Os dados não podem ser recuperados sem usar o processo inverso de decifrar “ou” o processo de conversação de dados de código ilegível para evitar pessoas não autorizadas acessar às informações. Entretanto, essas interfaces oferecem oportunidades sem precedentes. O crescimento do universo digital revela ameaças relacionadas à vulnerabilidade da informação eletrônica. A assinatura digital via blockchain viabiliza a solução para os governos e as empresas operarem nesse ambiente de incerteza. Diante desses questionamentos surgiu a necessidade

de analisar a tecnologia de criptografia e seus impactos para possíveis reduções da burocracia e aumento da segurança de dados.

Destarte, o presente trabalho tem como objetivo geral analisar a criptografia e autenticação de documentos digitais públicos como forma de redução da burocracia e aumento na segurança de dados. Já os objetivos específicos,1. pretendem verificar. o processo evolutivo das reformas administrativas, da burocracia e suas disfunções. 2. Identificar contexto atual com relação a desburocratização, proteção e segurança dos dados no Brasil, e, por fim 3. Expor a temática da criptografia e autenticação de documentos via Blockchain.

O presente trabalho justifica-se por contribuir para o meio tecnológico, mostrando que a criptografia e autenticação de dados públicos via blockchain seria uma opção eficaz como forma de redução da burocracia, esta pode ser um diferencial enorme na gestão do setor público, passível de ser fator diferencial entre o sucesso e o fracasso. Ainda como contribuição para ao meio tecnológico, busca quebrar paradigmas que estão enraizados na cultura dos gestores quando, de maneira equivocada, tratam a criptografia como algo não necessário.

A pesquisa tem fundamental relevância no âmbito acadêmico, pois proporciona um estudo aprofundado sobre a criptografia e autenticação de documentos públicos com forma de redução da burocracia e aumento na segurança de dados, podendo trazer um olhar crítico sobre a temática entre professor e aluno, e isso possibilita outros dissentes a desenvolverem outras pesquisas e se aprofundado ao tema.

Importante destacar que para o meio social, a pesquisa contribui para abordar a criptografia e autenticação de documentos públicos com forma de redução da burocracia e aumento na segurança de dados como um vetor para fortalecer as empresas e órgãos públicos fazendo com que elas forneçam um serviço mais seguro e eficaz, gerando menos transtornos para seus usuários.

Quanto a metodologia utilizada, a pesquisa requer contato com a realidade a qual nos dispomos a investigar. Pensando nessa afirmativa, procuramos fazer uma pesquisa hipotético dedutiva, mediante uma revisão bibliográfica e legislacional em obras físicas e digitais adequada aos temas estudados.

2. REFORMAS ADMINISTRATIVAS AO LONGO DO TEMPO

As reformas administrativas surgem como necessidade de alterar o modelo de gerenciamento da coisa pública. Sem dúvidas elas influenciaram no desenvolvimento das regras burocráticas documentais. Para Martins (1997), no Brasil, três foram as fases que a administração pública vivenciou: o patrimonialismo, a burocracia, e o gerencialismo. Ressalta-se, conforme o autor, nenhuma delas acabaram por completo, pois sempre havia traços do antepassado no substituto. Assim de certa forma, patrimonialismo, burocracia e gerencialismo convivem em nossa administração contemporânea, embora uma ou outra exerça mais poder.

O conceito de "patrimonialismo" como conhecemos hoje foi desenvolvido por Weber (1998) e se remetia à uma forma de dominação baseada nas tradições, se legitimando, portanto, a partir dela. Assim, toda dominação tradicional tende ao patrimonialismo. No Modelo Patrimonialista, o aparelho do Estado era centralizado e funciona como uma extensão do poder do soberano e seus servidores tem status de nobreza real. Não havia compromisso em servir a população, pelo contrário. Os únicos serviços que haviam era o de justiça e o de segurança (do território e não do povo). O soberano era tratado como se fosse um deus, logo, isento de punições. Os bens públicos (*res publica*) e privados (*res principis*) se misturavam, pois, tudo era do rei (se originou nas monarquias absolutistas). (SILVA, 2019)

A prebenda era o nome dado a ocupação rendosa (subsídio), pelo particular de um cargo estatal e com pouco trabalho e sinecura um “emprego” cujas funções nem são exercidas. Essas espécies de ocupação eram para auxiliar o nepotismo e corrupção, pois não haviam carreiras administrativas. no o advento do capitalismo, o patrimonialismo tornou-se, inaceitável. Assim, com fortes críticas ao modelo, como o autoritarismo, a corrupção e o nepotismo, esse acabou por ser substituído pelo modelo burocrático, na década de 1930, no Brasil. (BURGOS; BELLATO, 2019)

O modelo burocrático, conforme Weber (1998) constituída como segunda fase da administração pública, foi o primeiro modelo estruturado efetivo de administração que tivemos em nosso país. surgiu na segunda metade do século XIX como forma de acabar com nepotismo e corrupção. (SILVA, 2019)

No Brasil, tivemos duas fases. A primeira, iniciada no Governo de Getúlio Vargas com um funcionalismo mais profissional para o plano de industrialização do

país (1930 a 1945). A segunda etapa começou em 1945 e foi até a reforma Gerencial. Com as organizações burocráticas ganhando corpo o problema é que passaram a ser cada vez mais independentes e se autocontrolar/organizar/administrar. (SOUZA, 2019)

Foi pautada na “organização por excelência”. E cujo poder se tornou baseado na impessoalidade, na lei, controles por procedimentos e na organização racional da divisão de trabalho formal, com possibilidade de meritocracia. o controle administrativo é feito sempre a Priore de modo a garantir previsibilidade. Outra classificação é a de que o processo burocrático é estável e busca equilíbrio, havendo vários tipos, configurando Excesso de Burocratização (muitas normas e regulamentos) até a escassez de burocracia (falta de normas e regulamentos, com foco na pessoa, e não no cargo). (SOUZA, 2019)

As principais características do modelo são: caráter legal das normas; caráter formal das comunicações; caráter racional e divisão do trabalho (horizontal) (se apegar ao que manda a norma); hierarquia (vertical) da autoridade (ainda sim os comandos são definidos por regras pré-estabelecidas); rotinas e procedimentos padronizados; impessoalidade nas relações; competência técnica e meritocracia (concurso); especialização da administração (distinção entre o bem público e o privado); profissionalização dos funcionários; previsibilidade de funcionamento. O Brasil nunca teve uma burocracia weberiana pura porque as normas legais deixavam lacunas contrárias à burocracia racional-legal. (SILVA, 2019)

As disfunções da burocracia, ou seja, características as quais não eram para ocorrer, mas ocorreram são, basicamente: criar imprevisibilidade e considerar mais importante os seus procedimentos do que o atendimento e melhoria na prestação do serviço. É como se a organização fosse o fim e não o meio para a consecução dos objetivos. A incapacidade de dirigir seus serviços para os cidadãos, irrelevância do cidadão, resistência a mudanças, rigidez e falta de flexibilidade, Decisões distantes da realidade, Desconsideração ao servidor (como pessoa), apego exagerado às regras e regulamentos e a autorreferência. (SOUZA, 2019).

Com se observou, a burocracia já não atendia mais os anseios sociais, passou perceber que se a burocracia “se tornar rígida demais, causaria ineficiência” (o que foi correto, conforme apareceram as disfunções). Não podia descartar tudo da burocracia, pois muito se aproveitava, mas necessitava de um aperfeiçoamento, assim no Brasil, surgiu o paradigma pós-burocrático ou o gerencialismo, fase que

consistia na busca do controle por resultados. No final do século XX começa a fazer um movimento em direção ao gerencialismo, mas os mecanismos institucionais de governança, ainda se baseiam essencialmente na teoria burocrática weberiana. (BURGOS; BELLATO, 2019)

O Gerencialismo ou *managerialism* (gerencialismo puro), em tese, substituiria o modelo burocrático, introduzindo a redução de custos e aumento da eficiência e qualidade (produtividade) e flexibilidade na burocracia, bem como o *modus operandi* do setor privado ao setor público. As características são a descentralização e redução dos níveis hierárquicos, a competição administrativa no interior do próprio Estado e a terceirização de atividades auxiliares ou de apoio. (BURGOS; BELLATO, 2019)

A opinião pública acreditava que o modelo privado era melhor para gerir os recursos e serviços públicos. O gerencialismo prega que a melhor forma de combater o clientelismo é dar autonomia ao administrador público, valorizando-o por sua capacidade de tomar decisões em que o critério de êxito seja sempre o melhor atendimento ao cidadão-cliente. Abriu caminho para as privatizações, redução de pessoal e redução da dívida pública que impedia novos investimentos estatais.

2.1. VISÃO DE MAX WEBER QUANTO A BUROCRACIA

Atualmente, termos como “burocracia” e “autoridade” têm conotações principalmente negativas. Não era assim no início do século XX. De fato, quando o sociólogo Max Weber desenvolveu suas teorias de gestão detalhando as “características da burocracia”, elas foram consideradas inovadoras e inovadoras entre acadêmicos e gerentes de negócios. (SOUZA, 2019)

No final do século XIX, foi o sociólogo alemão e autor de A Ética Protestante e o Espírito do Capitalismo (1905), Max Weber, o primeiro a usar e descrever o termo burocracia. Isso também é conhecido como a teoria burocrática da gestão, a teoria da gestão burocrática ou a teoria de Max Weber. (SILVA, 2019)

Ele acreditava que a burocracia era a maneira mais eficiente de configurar uma organização, administração e organizações. Max Weber acreditava que a burocracia era melhor do que as estruturas tradicionais. Em uma organização burocrática, todos são tratados iguais e a divisão do trabalho é claramente descrita para cada funcionário. (SILVA, 2019)

A burocracia é uma estrutura organizacional caracterizada por muitas regras, processos padronizados, procedimentos e requisitos, número de mesas, divisão meticulosa de trabalho e responsabilidade, hierarquias claras e interações profissionais, quase impessoais entre os funcionários. (SOUZA, 2019)

Para o Weber (1998), a burocracia é um método de controle social, desde que seja legitimada por aqueles que se subordinam a ela, contudo apesar de uma certa conotação negativa, Weber classificou-a como um instrumento administrativo capaz de aperfeiçoar as atividades administrativas, organizando o bom funcionamento dos serviços públicos e alcançando o máximo desempenho da máquina pública na prestação de serviços.

2.2. DISTORÇÃO DA BUROCRACIA

A burocracia é definida como uma divisão hierárquica de funcionários que atuam em atribuições formais. A definição seguinte sugere que cinco dimensões específicas da burocracia, a saber: estrutura hierárquica, tomada de decisão, dispositivos procedimentais, natureza do trabalho e gargalos processuais, foram medidos para compreender o funcionamento da burocracia (SILVA, 2019).

Esses fatores são predominantemente apropriados para a compreensão do funcionamento burocrático, conforme indicado por estudos anteriores que a magnitude desses atributos difere de uma organização para outra. As complexidades funcionais de qualquer sistema burocrático dependem em grande parte da mistura desses atributos (SOUZA, 2019).

Atributos como estrutura hierárquica, divisão de trabalho e o tipo de tomada de decisão estão intimamente relacionados entre si. A escolha de objetivos e meios apropriados estão geralmente entrelaçados. Uma boa política pode ser formulada quando os tomadores de decisão descobrem que estão de acordo (SILVA, 2019).

Vários estudos observaram que a complexidade das regras e procedimentos afetam fortemente a eficiência burocrática (SILVA, 2019). A burocracia também é extremamente dependente da conformidade regulatória e política. Isso restringe os funcionários a terem ideias inovadoras, fazendo com que se sintam apenas um número em vez de um indivíduo. Pesquisas posteriores (a teoria das relações humanas) demonstraram que os funcionários apreciam a atenção e querem ter voz na tomada de decisões. (SOUZA, 2019).

Embora tenha sido criada com o intuito de facilitar e maximizar o desempenho administrativo, nele incluso a gestão de projetos, a burocracia contemporânea é sinônimo de ineficiência e lentidão. Com a quantidade de protocolos, inflexíveis, normas rígidas e prazos razoáveis, a grande parte dos serviços que se alcançam através da burocracia tendem a ser difíceis de se conseguir. (SILVA, 2019)

> As disfunções como irregularidades ou anormalidades que se confundem nos processos administrativos das organizações, ocasionando confrontos até mesmo no comportamento do indivíduo no ambiente de trabalho, faz com que os objetivos pretendidos pela organização deixem de ser atendidos e a qualidade de vida dos indivíduos da organização se torne insatisfatória (OLIVEIRA, 2006, p. 291-292).

Com a falta do alinhamento de ideias e objetivos de processos, acabam ocasionando falta de confiança e podendo conter atrasos em processos de documentações fazendo que transtornos sejam causados aos utilizadores dos serviços, e com a falta de confiança entre funcionários ações de corrupção podem ser tomadas como adulteração de documentos por suborno.

Como os funcionários de uma organização burocrática não têm oportunidade de expressar sua opinião ou influenciar a tomada de decisões, a burocracia pode desmotivar os funcionários a longo prazo. (SILVA, 2019). Além disso, com o passar do tempo, os funcionários podem começar a se incomodar com as diversas regras e exigências, com o risco de começarem a boicotar e/ou abusar dessas regras e fazer frente à ordem estabelecida. (SILVA, 2019)

Portanto, é muito importante que as organizações burocráticas informem adequadamente os funcionários com antecedência sobre sua abordagem de trabalho e exija que eles aceitem isso. Somente os funcionários que concordam com essa abordagem são adequados para trabalhar em uma organização burocrática. (SILVA, 2019)

Weber (1998) e Campos (1976), acreditam que o problema dessa nova visão negativa burocrática seria o apego incessante e inflexível as normas que regem a execução da prestação dos serviços submetidos a burocracia e o esquecimento do real papel desse instrumento que é, na verdade, proporcionar a efetiva prestação do serviço. Decerto, está claro, que a manutenção da rigidez dos meios se tornou mais importantes do que o alcance dos próprios objetivos.

3. CONTEXTO ATUAL: MEDIDAS TECNOLÓGICAS GERAIS E

ANTIBUROCRÁTICAS JÁ VERIFICADAS NO GOVERNO BRASILEIRO

Assinaturas eletrônicas e digitais são regulamentadas por lei no Brasil. Medida Provisória n. 2.200, de 24 de agosto de 2001, criou a Infraestrutura de Chaves Públicas Brasileira – PKI Brasil. (KRELL; DANTAS; LINS JÚNIOR, 2021)

Presume-se que 'assinatura eletrônica' é um termo que se refere a qualquer método técnico de identificação legal das partes no mundo on-line, e o termo assinatura digital se refere a um tipo de assinatura eletrônica que é gerada através do software de criptografia assimétrica. A MP 2.200 regulamenta ambas as formas de assinatura. (ALVES, 2020).

O conceito de assinatura digital pode ser extraído da lei ou do trabalho de juristas. Assinaturas digitais são definidas como um selo afixado em um documento eletrônico que é gerado por um algoritmo de hash, que usa como entrada o documento eletrônico original e a chave de assinatura privada do signatário. O uso da chave é capaz de afirmar que a pessoa de quem foi a chave é a pessoa que fez com que a assinatura digital fosse afixada no documento eletrônico. As assinaturas digitais são capazes de garantir a integridade dos dados. (ALVES, 2020).

O método usado para gerar assinaturas digitais é relativamente simples. O remetente criptografa o e-mail com sua chave privada. Um selo criptografado é gerado e adicionado à mensagem, que é então enviada ao destinatário. O destinatário descriptografa a mensagem com a chave pública do remetente. Se o processo de descriptografia for executado perfeitamente, então pode-se dizer com certeza que uma pessoa que usou a chave privada assinou a mensagem. usuário final. (KRELL; DANTAS; LINS JÚNIOR, 2021)

A MP 2.200 também criou as autoridades de registro – RAs que são responsáveis por identificar o usuário final. As RA estão operacionalmente associadas às AC, nos termos do artigo 6.º da MP Para vincular o nome do remetente à sua chave privada, o sistema conta com um certificado emitido por um terceiro confiável, uma Autoridade de Certificação - AC. Quando o destinatário recebe a mensagem e o certificado emitido pela Autoridade de Certificação, o destinatário pode ter certeza de que o documento eletrônico é juridicamente vinculativo se o proprietário da chave privada fizer com que a chave seja usada para assinar o documento. (KRELL; DANTAS; LINS JÚNIOR, 2021)

Em outras palavras, no Brasil, uma assinatura digital com certificado digital emitido por uma AC pertencente à PKI Brasil (que tem o ITI brasileiro como autoridade certificadora raiz) produz os mesmos efeitos de uma assinatura civil. (KRELL; DANTAS; LINS JÚNIOR, 2021)

A Medida Provisória nº 951/2020 (“MP nº 951/2020”), publicada em 15 de abril de 2020, alterou o procedimento de emissão de certificados digitais no âmbito da ICP-Brasil, autorizando a emissão de certificados digitais à distância, sem a necessidade de o requerente estar presente nos estabelecimentos credenciados para emitir tais certificados (Entidades de Registo). (KRELL; DANTAS; LINS JÚNIOR, 2021)

A MP 951/2020 revogou o artigo 7º da MP 2.200-2, que obrigava as Autoridades de Registro a atuarem presencialmente com os requerentes para validar sua identidade. Com a MP 951/2020, as Autoridades Registradoras podem emitir certificados eletrônicos remotamente, desde que adotem outros meios de verificação que garantam um nível de segurança equivalente à verificação presencial, observadas as normas técnicas da ICP-Brasil aplicáveis. (KRELL; DANTAS; LINS JÚNIOR, 2021)

A alteração segue as alterações legislativas decorrentes da pandemia de COVID-19, que levou ao distanciamento social e à determinação de encerramento de estabelecimentos em diversas localidades do país, de forma a evitar interações presenciais. Essa mudança é fundamental para facilitar a emissão de certificados ICP-Brasil remotamente, permitindo que as empresas migrem para assinaturas eletrônicas lastreadas em ICP-Brasil para continuar realizando transações comerciais mais complexas. (ALVES, 2020).

No entanto, espera-se mais regulamentação para definir os procedimentos para permitir que as Autoridades de Registro realizem a verificação remota de identidade para garantir a emissão segura e confiável de certificados digitais da ICP-Brasil. (ALVES, 2020).

É importante consignar ainda que a União já preza pela desburocratização, tanto que instituiu o Decreto 6932/09 recentemente revogado pelo decreto nº 9.094, de 17 de julho de 2017, cuja redação ratifica e desnecessidade de amontoados de documentos, e a simplificação do processo de atendimento prestado aos usuários dos serviços públicos. O art. 1º da norma mais recente supracitada salienta que:

> Art. 1º Os órgãos e as entidades do Poder Executivo federal observarão as seguintes diretrizes nas relações entre si e com os usuários dos serviços públicos”
> I- Compartilhamento de informações, nos termos da lei;
> II- Racionalização de métodos e procedimentos de controle;
> III - Aplicação de soluções tecnológicas que visem a simplificar projetos e procedimentos de atendimento aos usuários dos serviços públicos e a propiciar melhores condições para o compartilhamento das informações;
> IV- Articulação com os Estados, o Distrito Federal, os Municípios e os outros Poderes para a integração, racionalização, disponibilização e simplificação de serviços públicos. (BRASIL, 2017.)

Com base, nesse artigo, pode-se observar que diversas melhorias podem ser implantadas. Como uma ainda maior informatização, minimizando ao máximo a necessidade de deslocamento até a sede de qualquer órgão público, além de aprimorar os projetos de gestão dos projetos advindos da pratica administrativa no setor público.

Ademais, recentemente o governo federal instituiu o que se chama de “Login Único do Governo Federal” cujo cadastro é feito para através do site “acesso.gov.br”. Tal feito fez algo simples, mas de grande impacto no gerenciamento de projetos. Isto porque o governo criou um banco de dados único, capaz de armazenar uma infinidade de dados de uma pessoa em um único sistema que antes, era dividida em dezenas de outros bancos de dados de maneira esparsa. No mesmo sistema, se vislumbra os dados do FGTS; PIS/PASEP; INSS, Seguro Desemprego; Bolsa Família; FIES; SUS; dentre outros. O desenvolvimento de um sistema uno propicia uma maior facilidade na verificação de incongruências cadastrais e, por consequência, aprimora a gestão de projetos.

3.1. A PROTEÇÃO LEGAL DOS DADOS

Após várias discussões e adiamentos, a Lei Geral de Proteção de Dados (LGPD), Lei Federal n. 13.709/2018, entrou em vigor em 18 de setembro de 2020. A LGPD é o primeiro regulamento abrangente de proteção de dados do Brasil e está amplamente alinhado com a Lei Geral de Proteção de Dados da UE (RGPD). (MELO, 2018). A Lei Geral de Proteção de Dados (LGPD) pode ser resumida como uma nova lei que exige que organizações públicas e privadas cumpram normas de segurança para evitar roubos, vazamentos e vendas ilegais de informações digitais e eletrônicas.

O artigo 6º da LGPD prevê que quaisquer atividades de tratamento de dados

pessoais devem ser realizadas observando os seguintes princípios (artigo 6º da LGPD) (MELO, 2018):

- boa-fé: não bastar pensar em respeitar a lei, mas transparecer
- finalidade: processamento para fins legítimos, específicos e explícitos informados ao titular dos dados, sem qualquer possibilidade de processamento posterior incompatível com esses fins;
- Adequação: no âmbito do tratamento, a compatibilidade do tratamento com a finalidade para qual o titular dos dados foi informado
- Necessidade: limitar o tratamento ao mínimo necessário para atingir as suas finalidades, abrangendo dados que sejam relevantes, proporcionais e não excessivos para efeitos de tratamento de dados;
- Livre acesso: garante a consulta cômoda e gratuita aos titulares dos dados sobre a forma e duração do tratamento e a integridade dos seus dados pessoais;
- Qualidade dos dados: garantir a exatidão, clareza, relevância e atualização dos dados sujeitos as necessidades e finalidades do tratamento;
- Transparência: garante informação clara, precisa e de fácil acesso aos titulares dos dados sobre a execução do tratamento e respetivos agentes de tratamento, sujeito ao sigilo comercial e industrial;
- Segurança: utilização de medidas técnicas e administrativas capazes de proteger os dados pessoais de acesso não autorizado e destruição, perda, alteração, comunicação ou divulgação acidental ou ilícita;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais;
- Não discriminação: impossibilidade de tratamento de dados para fins discriminatórios, ilícitos ou abusivos;
- Responsabilização Demonstração pelo controlador ou processador de que medidas eficazes foram tomadas para demonstrar a conformidade com as regras de proteção de dados pessoais e a eficácia dessas medidas.

Embora a lei esteja em vigor a partir de 2020, as penalidades emitidas pela LGPD só entrarão em vigor em 1º de agosto de 2021. No entanto, autoridades públicas (como agências de defesa do consumidor e ministérios públicos) e titulares de dados podem cumprir o GDPR de 18 de setembro de 2020. (SIMÕES, 2020). A

LGPD se aplica a qualquer pessoa física ou jurídica de direito público ou privado, que processe dados pessoais (como coleta, produção, recepção, classificação, processamento, etc.) no território brasileiro, nos casos: (i) o tratamento tem por finalidade a oferta ou fornecimento de bens ou serviços; (ii) os dados pessoais processados são de pessoas físicas localizadas no território brasileiro; ou (iii) os dados pessoais processados foram coletados em território brasileiro. Nesse sentido, é perceptível que os termos de aplicação da lei são de fato próximos aos previstos no RGPD. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020)

Ela abrange o tratamento de dados pessoais, inclusive meios digitais, por pessoas físicas e jurídicas de direito público ou privado. Foi criado principalmente para proteger os direitos fundamentais de liberdade e privacidade. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020) Estes são os direitos concedidos aos usuários e clientes de empresas pela LGPD conforme determina o artigo 18 da LGPD (FUCCI, 2022):

1. Confirmação da existência de tratamento.
2. Acesso aos dados.
3. Correção de dados incompletos, imprecisos ou desatualizados.
4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desacordo com o previsto na lei.
5. Portabilidade de dados para outro prestador de serviço ou produto, mediante solicitação expressa e observância de segredos comerciais e industriais, conforme regulamentação do órgão controlador.
6. Portabilidade dos dados para outro fornecedor de serviço ou produto, mediante solicitação expressa, de acordo com as normas da autoridade nacional, observados os segredos comerciais e industriais.
7. Eliminação dos dados pessoais tratados com o consentimento do titular, salvo nos casos previstos no artigo 16.º da lei.
8. Informações de quaisquer entidades públicas e privadas com as quais o controlador tenha feito uso compartilhado de dados.
9. Informação sobre a possibilidade de não dar o consentimento e sobre as consequências da recusa.
10. Revogação do consentimento, nos termos do n.º 5 do artigo 8.º da lei.

A LGPD não é aplicável, no entanto, nos casos em que o tratamento de dados pessoais seja feito (FUCCI, 2022):

(i) por uma pessoa singular para fins exclusivamente privados e não económicos;

(ii) exclusivamente para fins jornalísticos, artísticos e acadêmicos;

(iii) pelo Poder Público, nas hipóteses de utilização para a promoção da segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou

(iv) quando os dados tenham origem fora do território nacional e não sejam objeto de comunicação, uso compartilhado de dados com agentes brasileiros de tratamento ou objeto de transferência internacional de dados com outro país que não seja o país de origem (desde que já que o país de origem oferece um nível de proteção de dados pessoais adequado ao estabelecido na LGPD).

A LGPD estabeleceu casos específicos em que o consentimento exigirá maior cautela quanto à sua obtenção, sendo necessário, portanto, que além de livre, informado e inequívoco, seja expresso de forma específica e destacada em relação a outras operações. Estas condições adicionais serão necessárias caso o consentimento seja necessário para fins de processamento (i) de dados pessoais sensíveis; ou (ii) dados de crianças; ou, para (iii) autorizar a transferência internacional de dados pessoais. (CARVALHO; PEDRINI, 2019)

Em relação ao tratamento de dados pessoais de crianças, algumas peculiaridades estão presentes, pois essas operações devem ser realizadas no melhor interesse da criança. Por esse motivo, o consentimento específico e destacado não é apenas a única base legal aplicável a essas operações, como também é necessário que seja fornecido por pelo menos um dos responsáveis legais da criança. (CARVALHO; PEDRINI, 2019)

Nesse cenário, o controlador também deve manter informações públicas sobre os tipos de dados coletados, bem como a forma de seu uso e o exercício dos direitos que a LGPD confere ao titular dos dados. A lei também impõe aos controladores o dever de exigir apenas as informações mínimas necessárias para a participação de crianças em jogos, aplicativos de internet e outras atividades. (BASTOS; PANTOJA; SANTOS, 2021)

O titular tem o direito de receber uma confirmação sobre o tratamento ou não dos seus dados pessoais e, se for o caso, de consultar esses dados e informações adicionais relacionadas com o seu tratamento (como, por exemplo, a partilha de informação com entidades públicas e privadas). (BASTOS; PANTOJA; SANTOS,

2021). Caso o titular o solicite, o Controlador tem a obrigação de corrigir os dados pessoais incompletos, incorretos ou desatualizados. (BASTOS; PANTOJA; SANTOS, 2021)

O titular tem o direito de solicitar que o Controlador torne seus dados pessoais anônimos, ou seja, impossíveis de associar ao titular. Além disso, pode restringir o tratamento dos seus dados e solicitar a eliminação dos mesmos se (i) não for necessário ou adequado para a finalidade para a qual foram fornecidos ou (ii) quando o tratamento não seguir as disposições da LGPD. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020)

O direito à portabilidade de dados permite que os titulares solicitem a transferência de seus dados pessoais para outro Controlador, mas esse direito ainda depende de regulamentação adicional por parte da Autoridade Nacional. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020). Quando o tratamento depender de consentimento, o titular pode, mediante pedido expresso, exigir a destruição dos dados objeto do tratamento.

Os titulares têm o direito de recusar o consentimento, quando necessário para o tratamento dos dados, bem como de serem informados sobre as consequências dessa decisão. Além disso, podem lamentar o consentimento anteriormente dado e, a qualquer momento, revogar a autorização por expressão expressa. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020)

Os titulares têm o direito de se opor ao processamento de seus dados pessoais a qualquer momento, mesmo em situações que não dependam de seu consentimento, caso verifiquem que está sendo realizado em violação à LGPD. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020). Em linhas gerais, eis o que a LGPD proporciona aos cidadãos brasileiros (FUCCI, 2022):

- Direito à privacidade: proteção de dados pessoais de cidadãos brasileiros; assegurar maior controle sobre as informações, por meio de práticas transparentes e seguras, para garantir direitos e liberdades fundamentais;
- Regras claras para empresas: a coleta, armazenamento, processamento e compartilhamento de dados pessoais para empresas é seguido por normas legais;
- Promoção do desenvolvimento: a partir de uma base legal para o desenvolvimento econômico e tecnológico da sociedade, cada vez mais movida por dados (na transformação digital, no caso das empresas);

- Direito do consumidor: garantia da livre iniciativa, livre concorrência e proteção do consumidor/usuário;
- Fortalecimento da confiança: aumentar a confiança da sociedade na coleta e uso de seus dados – o que impacta, por exemplo, a compra e venda de produtos e serviços na web (e-commerce);
- Segurança jurídica: aumentar a segurança jurídica como um todo na utilização e tratamento de dados pessoais.

Até a promulgação dessa lei, os códigos legais brasileiros eram um tanto vagos em relação à proteção de dados pessoais e privacidade, especialmente online. (SIMÕES, 2020). As empresas do mercado de Telecom, por exemplo, não tinham uma legislação sólida para sustentar seus modelos de negócios; atuaram seguindo códigos internacionais, conforme jurisprudência nacional. (FUCCI, 2022)

Da mesma forma, o próprio estado brasileiro tratou milhões de dados pessoais e corporativos de forma muito não divulgada, sem mostrar claramente como as informações foram tratadas. Agora, por meio da LGPD, há diretrizes claras na forma da lei. (SIMÕES, 2020). Também é importante observar que além de regulamentar a Lei Geral de Proteção de Dados Pessoais, o texto cria a Autoridade Nacional de Proteção de Dados (ANPD). O novo órgão deve regular, interpretar e fiscalizar o cumprimento da lei geral e punir quem descumprir. (SIMÕES, 2020). O que também precisa ser destacado é que a LGPD faz parte de um movimento internacional pela regulamentação da manipulação de dados. (SIMÕES, 2020)

Talvez a legislação mais marcante dos últimos anos seja o Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor recentemente na União Europeia (UE). (SIMÕES, 2020). Assim como a LGPL, a RGPD é um conjunto de regras projetadas para dar aos cidadãos da UE mais controle sobre seus dados; simplificar o quadro regulamentar para que os cidadãos e as empresas possam beneficiar plenamente da economia digital. (BASTOS; PANTOJA; SANTOS, 2021)

Olhando para o mundo corporativo, com o RGPD em vigor, as organizações não apenas terão que garantir que os dados pessoais sejam coletados legalmente e sob condições estritas, mas também gerenciá-los de maneira a protegê-los do uso indevido. (BASTOS; PANTOJA; SANTOS, 2021). O RGPD se aplica a qualquer empresa que opere na UE, bem como a qualquer organização fora da UE que ofereça bens ou serviços a clientes ou empresas na região. (BASTOS; PANTOJA; SANTOS, 2021)

Existem muitas semelhanças nessa regulamentação com a LGPD, embora seja 100% voltada para cidadãos brasileiros, residentes e empresas que ali trabalham. (BASTOS; PANTOJA; SANTOS, 2021). Assim como no RGPD, as organizações que não são brasileiras, mas que atuam no Brasil (presencial e ou virtualmente) devem se adequar à LGDP. (BASTOS; PANTOJA; SANTOS, 2021)

A LGPD é bastante ampla. Inclui dados de todos os formatos que identificam ou tornam uma pessoa identificável. Além disso, todas as empresas que tratam dados pessoais no território brasileiro ou de pessoas nele localizadas, com poucas exceções específicas, devem cumprir as novas regras. (BASTOS; PANTOJA; SANTOS, 2021)

Da LGPD, para uma empresa tratar os dados de um usuário, é preciso que haja uma base legal. O consentimento da pessoa precisa ser bem documentado. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020). Os titulares dos dados, também chamados de usuários, têm maior controle sobre suas informações – a finalidade da coleta e com quem são compartilhadas, por exemplo. (PEDROSO SOARES; BARDEMAKER ANHAIA; CADORE TOLFO, 2020)

As violações da lei de proteção de dados podem levar a inquéritos administrativos conduzidos pela ANPD, que concederá o direito de apresentar defesa e recurso, podendo resultar em sanções administrativas. As violações da lei de proteção de dados normalmente não levam a penalidades ou responsabilidades criminais. As sanções que podem ser aplicadas pela ANPD são as seguintes (SIMÕES, 2020):

- advertências, que incluirão prazo para adoção de medidas corretivas;
- multa única de até 2% do faturamento líquido do conglomerado da entidade infratora no Brasil em seu exercício fiscal anterior, excluindo impostos, até 50 milhões de reais por violação;
- multa diária, que também está sujeita aos limites anteriormente estabelecidos;
- divulgações da violação depois de verificada e confirmada sua ocorrência;
- o bloqueio dos dados pessoais correspondentes à violação até que as operações de processamento do controlador estejam em conformidade;
- eliminação dos dados pessoais correspondentes à violação;

- a suspensão parcial da base de dados a que se refere a infração por seis meses, prorrogável por mais seis meses;
- a suspensão da atividade de tratamento de dados a que se refere a infração por seis meses, prorrogável por mais seis meses; e
- uma proibição parcial ou total de quaisquer atividades de processamento de dados.

3.2. SEGURANÇA DE DADOS

A criptografia tornou-se uma questão importante no Brasil devido aos debates sobre o uso de criptografia de ponta a ponta por provedores de aplicativos; a expansão do mercado de criptomoedas; e legislação recente sobre uso da internet, proteção de dados e privacidade. Este resumo explorará essas questões, apresentará políticas relacionadas e examinará o futuro da criptografia no país. Até agora, nem a legislação nem as decisões judiciais traçaram uma linha definitiva sobre o acesso a dados criptografados. (ABREU, 2018). O debate sobre criptografia no Brasil concentra-se em equilibrar as necessidades de aplicação da lei e a promoção de sistemas de criptografia seguros. Um dos principais problemas é o uso de criptografia de ponta a ponta por aplicativos de comunicação (apps). (VIEIRA, et al. 2019).

Algumas empresas adotaram arquiteturas tecnológicas que inibem a capacidade do governo de obter acesso a dados de comunicações que possam ser úteis a funcionários que investigam e processam atividades criminosas. Juízes brasileiros ordenaram repetidamente que provedores de serviços bloqueiem o aplicativo de comunicação WhatsApp em resposta ao descumprimento da empresa (que é de propriedade do Facebook) de decisões judiciais que exigem que ela forneça informações relacionadas a investigações em andamento. Dois casos importantes ainda não foram resolvidos. (VIEIRA, et al. 2019).

Uma das principais instituições envolvidas nas dimensões técnicas da criptografia é a Equipe Brasileira de Resposta a Emergências em Computadores (CERT), responsável por promover a adoção da criptografia para aprimorar a segurança cibernética. (ABREU, 2018)

Além disso, a Agência Nacional de Comunicações (ANATEL) emitiu uma resolução que exige que as empresas de telecomunicações incorporem a criptografia em seus serviços. Outro ator de destaque é o Instituto Nacional de

Tecnologia da Informação, que coordena o desenvolvimento e gerenciamento de certificados de chave criptográfica – especificamente o ICP-Brasil, um software para certificação de assinaturas digitais. (ABREU, 2018)

Enquanto isso, o Gabinete de Segurança Institucional (GSI), sob o controle do presidente, tem a tarefa de criptografar documentos confidenciais, proteger sistemas criptográficos estatais e fornecer inteligência criptografada para serviços de comunicação de ponta a ponta. Por fim, o Banco Central do Brasil adotou uma política de segurança cibernética por meio de uma resolução de 2018, o que reforça a exigência de que a criptografia seja utilizada para o compartilhamento de dados financeiros. Nenhuma das autoridades listadas tem um mandato específico para ordenar a violação de um serviço criptografado de terceiros. Essa questão depende de como o Supremo Tribunal Federal se pronuncie sobre os dois importantes processos em andamento relativos a essa questão. (VIEIRA, et al. 2019).

O debate sobre criptografia no Brasil ainda é incipiente, e poucos especialistas fora do governo estão engajados publicamente nesta questão. Mesmo em campos que normalmente tratam de criptografia, como matemática, as implicações de política não são um tópico proeminente de conversa; o debate que está acontecendo está sendo conduzido principalmente por especialistas técnicos, especialistas em políticas e organizações – incluindo professores universitários, grupos de pesquisa acadêmica e representantes da sociedade civil – que discutem a tecnologia e os desafios que ela levanta. (ABREU, 2018)

Embora a criptografia seja obviamente legal no Brasil (apesar das proibições judiciais temporárias do WhatsApp), não há direito à criptografia consagrado no código legal do país. As disposições legais sobre privacidade e sigilo em informática datam da década de 1980 e, na década de 1990, a criptografia de ponta a ponta foi enquadrada principalmente como uma medida de segurança para indivíduos e organizações estabelecerem confiança (para bancos ou provedores de serviços de e-mail, por exemplo).

O uso de criptografia como medida de segurança no setor público é bem regulamentado e é um elemento-chave do ecossistema de identidade digital supervisionado pelo governo. O Comitê Gestor da Internet no Brasil também promove o uso da criptografia como essencial para a proteção da privacidade, liberdade de expressão e direitos humanos. (VIEIRA, et al. 2019).

Ações legislativas diretamente relacionadas à criptografia não são típicas,

pois poucos projetos de lei tratam da tecnologia. Duas leis tratam da modernização dos sistemas de saúde e estabelecem a exigência de que os registros eletrônicos de saúde sejam protegidos por criptografia. Outro ato semelhante diz respeito aos meios de pagamento e assinaturas digitais no comércio eletrônico, utilizando criptografia para garantir que as transações sejam realizadas com segurança. Por fim, outro projeto de lei prevê o uso de criptografia em petições judiciais eletrônicas. (VIEIRA, et al. 2019).

É difícil dizer quais stakeholders, questões e tecnologias serão os motores mais importantes do debate sobre criptografia, visto que o debate ainda é incipiente. No entanto, os desenvolvimentos recentes em criptografia podem ser vistos em termos de dois fatores: criptografia usada pelo governo para proteger a privacidade de suas próprias comunicações e segurança nacional e preocupações com a privacidade dos cidadãos e proteção de dados. (ABREU, 2018)

Em termos de como o governo usa a criptografia, houve uma mudança de paradigma em 2014. Após o escândalo de vigilância da NSA, o governo brasileiro aumentou sua preocupação com o sigilo das comunicações de funcionários de alto nível. Abandonou um dos padrões criptográficos para certificados digitais do Sistema de Chave Pública ICP-Brasil (V3), emitido pelo Instituto Nacional de Tecnologia da Informação, e adotou novos sistemas criptográficos, incluindo CriptoGOV e cGOV. Ambos os padrões foram desenvolvidos pela Agência Brasileira de Inteligência (Abin) e utilizam uma plataforma criptográfica portátil (PCPv2). (ABREU, 2018)

Além disso, o mercado de criptomoedas pode ser um importante impulsionador do debate sobre criptografia, uma vez que vem crescendo e expandindo seus serviços e tecnologias no Brasil. Em 2017, o Brasil se tornou um dos mercados de Bitcoin mais significativos do mundo. O valor da moeda digital disparou em 2017 e atraiu a atenção de uma ampla gama de investidores antes de cair substancialmente depois disso. (ABREU, 2018)

Pelo menos uma empresa pública, o Banco Nacional de Desenvolvimento Econômico e Social, anunciou em 2018 que emitiria um token próprio para atividades financeiras. Por sua vez, a Receita Federal também editou norma em 2018 autorizando o compartilhamento de dados da administração pública usando blockchain. Esse desenvolvimento é relevante para o debate sobre criptografia na medida em que a tecnologia blockchain depende da criptografia, que está sendo gradualmente incorporada para usos públicos e privados. (VIEIRA, et al. 2019).

4. CRIPTOGRAFIA E AUTENTICAÇÃO DE DOCUMENTOS PÚBLICOS COMO FORMA DE REDUÇÃO DA BUROCRACIA E AUMENTO NA SEGURANÇA DE DADOS

A Lei 14.063/2020, originada da Medida Provisória 983/2020 (“MP”), foi sancionada pelo presidente Jair Bolsonaro e publicada em 24 de setembro. Certificado, nas operações que envolvam a administração pública. Essas novas formas de assinatura eletrônica têm o mesmo valor jurídico das assinaturas em papel e visam simplificar e desburocratizar a relação entre os cidadãos e o governo. (DOURADO, 2020)

A Lei aplicar-se-á (i) à comunicação interna entre os órgãos e entidades da administração direta, autárquica e fundacional do Governo e os órgãos autônomos dos órgãos da federação; (ii) a comunicação entre pessoas físicas ou jurídicas e as entidades públicas indicadas no item (i) acima; e (iii) a comunicação entre as entidades públicas indicadas no item (i) acima. (BRASIL, 2020)

As assinaturas eletrônicas serão classificadas de acordo com os níveis de risco dos documentos a serem assinados, em três tipos: (i) simples , que (a) permite a identificação do signatário, e (b) anexa ou associa dados a outros dados no formato eletrônico do signatário; (ii) avançado , que (a) está associado ao signatário de forma inequívoca, (b) utiliza dados para sua criação permitindo que o signatário, com alto grau de segurança, opere sob seu controle exclusivo, e (c) permita a detecção de qualquer modificação após a assinatura no documento; e (iii) habilitado , que utiliza o certificado digital, nos termos da Medida Provisória nº 2.200/2001. (BRASIL, 2020)

A Lei estabelece que cada ente do Poder Público ou órgão autônomo de cada ente federativo definirá o tipo de assinatura que será aceita, observadas as seguintes diretrizes (DOURADO, 2020):

- As assinaturas eletrônicas simples podem ser utilizadas em qualquer interação com entidade pública que não envolva informações protegidas por sigilo.
- As assinaturas eletrônicas avançadas serão aceitas sempre que forem aceitas assinaturas eletrônicas simples e também nas interações com entidade pública que envolva informações protegidas pelo sigilo, e no registro de atos junto à junta comercial.

- Assinaturas eletrônicas qualificadas serão exigidas nos atos relativos à transmissão e registro de imóveis; em atos normativos assinados por chefes de Governo, Ministros de Estado ou por órgãos autônomos de entidade federal; e nos demais casos previstos em lei.

A exigência original de assinatura eletrônica avançada (para pessoas físicas e microempreendedores individuais) ou qualificada (para outras disciplinas) no contexto de interações com entidades públicas envolvendo informações protegidas de forma confidencial foi rejeitada sob o argumento de que a exigência tornada pública Muitas das medidas da administração não são viáveis. A exigência de assinaturas eletrônicas qualificadas para transferências de veículos automotores também foi rejeitada. (DOURADO, 2020)

Importante observar que, durante o período de pandemia do COVID-19, poderão ser aceitos atos do Poder Público ou de qualquer órgão autônomo quanto ao uso de assinaturas eletrônicas com níveis de segurança incompatíveis com as diretrizes definidas pela Lei. Tal disposição visa reduzir os contatos presenciais e permitir a prática de atos que de outra forma não seriam possíveis de ocorrer. (DOURADO, 2020)

Além disso, a Lei determina que as novas formas de assinatura não se aplicam a: (i) ações judiciais; (ii) nas comunicações (a) entre pessoas físicas e jurídicas; (b) em que o anonimato é permitido; e (c) dispensada a identificação das pessoas físicas; (iii) sistemas de ouvidoria das entidades públicas; (iv) programas de assistência às vítimas e testemunhas ameaçadas; e (v) nos demais casos em que seja necessário garantir o sigilo da identidade da pessoa física ao atuar perante o ente público. (BRASIL, 2020)

Em relação a documentos médicos, como atestados e outros, serão aceitas assinaturas eletrônicas avançadas e qualificadas. As hipóteses e critérios para validação de documentos médicos serão especificados por ato do Ministro da Saúde ou da Diretoria Colegiada da Agência Nacional de Saúde (“Anvisa”), conforme suas competências. (DOURADO, 2020)

A alteração mais relevante na área da saúde diz respeito aos critérios de emissão de prescrições médicas, em que a obrigatoriedade de escrever a tinta foi substituída pela necessidade de incluir a assinatura eletrônica do profissional na prescrição emitida por via eletrônica. Tal formato de prescrição também deverá observar os requisitos definidos pela Diretoria Colegiada da Anvisa ou pelo Ministro

da Saúde (DOURADO, 2020).

A Lei também dispõe sobre o código-fonte dos softwares desenvolvidos pela administração pública, definindo que todos serão regidos por uma licença de código aberto, permitindo seu compartilhamento com órgãos e entidades públicas. Exceções à regra se aplicam a sistemas cujo código-fonte tenha acesso restrito às informações; dados armazenados por sistemas de informação e comunicação; componentes de propriedade de terceiros; e contratos de desenvolvimento de sistemas assinados antes da entrada em vigor da Lei e que contenham cláusula que não permite licença de código aberto. (DOURADO, 2020)

Outras disposições rejeitadas incluem exigir que os livros fiscais e contábeis registrados em entidades públicas tenham assinatura eletrônica qualificada de um profissional contábil, uma obrigação em nível federal que se aplica apenas à escrituração digital (ECD) e escrituração fiscal (ECF); estabelecendo tecnologia executiva

A Comissão (Cotec), que estabelece as diretrizes e normas para emissão de assinatura eletrônica qualificada, o que a equipe econômica do governo vê como burocratização desnecessária do setor; e o estabelecimento da capacidade e atribuição do Instituto Nacional de Tecnologia da Informação (ITI), segundo Bolsonaro disse que isso foi definido pela Medida Provisória nº 2.200/2001. (DOURADO, 2020)

As assinaturas físicas continuam válidas e os órgãos públicos não são obrigados a adotar os novos meios de assinatura eletrônica estabelecidos pela Lei. Os sistemas que já utilizam assinaturas digitais devem estar em conformidade com as novas regras até 1º de julho de 2021. Os serviços estaduais que não estabelecerem regras próprias seguirão as regras gerais a serem definidas pelo governo federal.

4.1. BLOCKCHAIN

Blockchain é definido como um registro descentralizado de dados compartilhado com segurança. A tecnologia Blockchain permite que um grupo selecionado de participantes compartilhe dados. Com os serviços de nuvem blockchain, os dados de várias fontes podem ser facilmente coletados, integrados e compartilhados. Os dados são divididos em blocos compartilhados que são

vinculados a um identificador exclusivo na forma de um hash criptográfico. Blockchain fornece integridade de dados por meio de uma única fonte de verdade, eliminando a duplicação de dados e melhorando a segurança. (DOURADO, 2020)

Essas transações mostram a movimentação de ativos que podem ser tangíveis (produto) ou intangíveis (intelecto). Os blocos de dados podem registrar informações que você escolher: quem, o quê, quando, onde, quanto e até mesmo a temperatura da comida que está sendo enviada. (LEITÃO; FERREIRA, 2021)

Cada bloco está conectado aos blocos anteriores e seguintes. Esses blocos formam uma cadeia de dados quando os ativos são transferidos de um lugar para outro ou a propriedade muda de mãos. Os blocos confirmam o momento exato e a ordem das transações, e os blocos são conectados com segurança para evitar que quaisquer blocos sejam alterados ou inseridos entre dois blocos existentes. (PATRÍCIO; FERREIRA, 2020). Cada bloco adicional fortalece a verificação do bloco anterior, que por sua vez fortalece a verificação de todo o blockchain. Isso torna o blockchain à prova de adulteração, fornecendo a principal vantagem da imutabilidade. Isso elimina a possibilidade de adulteração de agentes maliciosos — e cria um registro de transações em que todos os membros da rede podem confiar. (LEITÃO; FERREIRA, 2021)

Em um sistema blockchain, a fraude e a adulteração de dados são evitadas porque os dados não podem ser alterados sem a permissão de um quórum das partes. Um ledger blockchain pode ser compartilhado, mas não alterado. Se alguém tentar alterar os dados, todos os participantes serão alertados e saberão quem fez a tentativa (PATRÍCIO; FERREIRA, 2020)

Pense em um blockchain como um registro histórico de transações. Cada bloco é “encadeado” ao bloco anterior em uma sequência e é gravado imutavelmente em uma rede ponto a ponto. A tecnologia de confiança e garantia criptográfica aplica um identificador exclusivo — ou impressão digital — a cada transação.

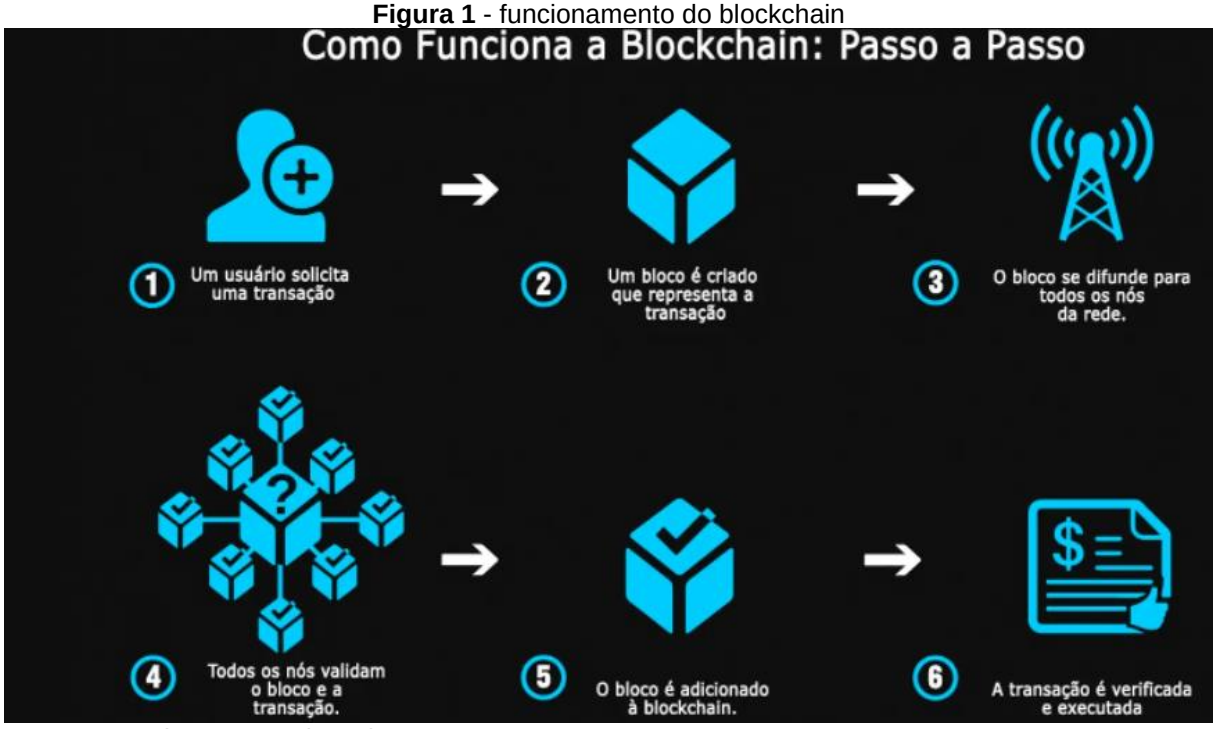
Confiança, responsabilidade, transparência e segurança são forjados na cadeia. Isso permite que muitos tipos de organizações e parceiros comerciais acessem e compartilhem dados, um fenômeno conhecido como confiança baseada em consenso de terceiros. (LEITÃO; FERREIRA, 2021)

Todos os participantes mantêm um registro criptografado de cada transação dentro de um mecanismo de gravação descentralizado, altamente escalável e

resiliente que não pode ser repudiado. Blockchain não requer nenhuma sobrecarga ou intermediários adicionais. Ter uma fonte de verdade única e descentralizada reduz o custo de execução de interações comerciais confiáveis entre partes que podem não confiar totalmente umas nas outras. Em um blockchain autorizado, usado pela maioria das empresas, os participantes são autorizados a participar da rede e cada participante mantém um registro criptografado de cada transação. (LEITÃO; FERREIRA, 2021)

Qualquer empresa ou grupo de empresas que precise de um registro de transações seguro, em tempo real e compartilhável pode se beneficiar dessa tecnologia exclusiva. Não existe um único local onde tudo é armazenado, levando a uma melhor segurança e disponibilidade, sem ponto central de vulnerabilidade. (PATRÍCIO; FERREIRA, 2020)

Figura 1 - funcionamento do blockchain



Fonte: Google Imagens (2022)

A figura acima demonstra o processo de funcionamento do blockchain desde sua transação ao certificado digital emitido e verificado, onde o bloco com as informações é criado, e as informações são descentralizadas e distribuídas entre vários nós de informações onde os dados são sincronizados e atualizados, após isso o bloco é adicionado ao blockchain e é verificada e validada, são processos eficazes e seguros pois a todo momento as informações do bloco são consultadas para

serem validadas sem alterações.

Blocos de blockchain:

O nome do blockchain vem do fato de que os dados são armazenados em blocos, e cada bloco é conectado ao bloco anterior para formar uma estrutura em cadeia. Com a tecnologia blockchain, você só pode adicionar (anexar) novos blocos ao blockchain. Você não pode modificar ou excluir nenhum bloco depois de adicionado ao blockchain. (PATRÍCIO; FERREIRA, 2020)

Algoritmos de consenso:

Algoritmos que impõem regras em um sistema blockchain. Depois que as partes definem as regras para o blockchain, o algoritmo de consenso garante que essas regras sejam seguidas. (PATRÍCIO; FERREIRA, 2020)

Nós de blockchain:

Os blocos de dados Blockchain são armazenados em nós - unidades de armazenamento que mantêm os dados sincronizados ou atualizados. Qualquer nó pode determinar rapidamente se algum bloco foi alterado desde que foi adicionado. Quando um novo nó completo se junta à rede blockchain, ele baixa cópias de todos os blocos atualmente na cadeia. Depois que o novo nó é sincronizado com outros nós e tem a versão mais recente do blockchain, ele pode receber novos blocos, assim como outros nós. (PATRÍCIO; FERREIRA, 2020)

Existem dois tipos principais de nós blockchain (PATRÍCIO; FERREIRA, 2020):

- Os nós completos armazenam uma cópia completa do blockchain.
- Nós leves armazenam apenas os blocos mais recentes e podem solicitar blocos mais antigos quando os usuários precisarem deles.

Três tipos de blockchain (PATRÍCIO; FERREIRA, 2020):

- Blockchain público.

Uma rede blockchain pública ou sem permissão é aquela em que qualquer pessoa pode participar sem restrições.

- Blockchain permitido ou privado.

Um blockchain privado ou com permissão permite que as organizações definam controles sobre quem pode acessar os dados do blockchain. Somente os usuários que recebem permissões podem acessar conjuntos específicos de dados.

Blockchain federado ou de consórcio.

Uma rede blockchain onde o processo de consenso é controlado de perto por

um conjunto pré-selecionado de nós ou por um número pré-selecionado de partes interessadas.

4.2. ASSINATURA E AUTENTICAÇÃO DE DOCUMENTOS VIA BLOCKCHAIN

O mundo tornou-se tecnologicamente avançado e agora a necessidade de tecnologia está em demanda mais do que nunca, pois o mundo digital está se multiplicando mais do que nunca. As inovações tecnológicas, como a assinatura digital, tiveram um aumento em relação aos métodos tradicionais de assinatura. (LEITÃO; FERREIRA, 2021)

As assinaturas digitais tornaram-se mais seguras ao combinar as novas tecnologias, como Blockchain. A assinatura digital em Blockchain ajuda a proteger sua identidade digital pela internet e a torna válida e autenticada. Os documentos Blockchain são protegidos em código digital e, em seguida, salvos em bancos de dados transparentes e distribuídos, protegidos contra adulteração, alteração e exclusão. (PATRÍCIO; FERREIRA, 2020). Com isso, agora, indivíduos e organizações podem fazer transações e interagir livremente. Agora, indivíduos e organizações utilizarão o imenso potencial da tecnologia Blockchain para assinaturas digitais. (DOURADO, 2020)

A possível utilização da descentralização de conteúdo, bem como da distribuição, é vasta. Com a assinatura de documentos Blockchain, não haverá mais certificados, diplomas e assinaturas com photoshop falsos. (PATRÍCIO; FERREIRA, 2020). As pessoas serão proprietárias de sua identidade digital e registros criando um armazenamento de registros único, verificável e imutável. A Assinatura Digital será aplicada a todos os documentos, como registros médicos, educacionais, residenciais e licenças. Todos esses certificados e seus metadados podem ser emitidos e assinados utilizando assinaturas digitais baseadas em Blockchain. (LEITÃO; FERREIRA, 2021)

Mesmo em transações financeiras, as assinaturas digitais são usadas para realizar assinaturas eletrônicas. Blockchain produz um hash dos dados. Hash pode ser denominado como os códigos numéricos usados para identificar pedaços de informação. (PATRÍCIO; FERREIRA, 2020). Esses códigos de hash podem ser verificados com o número de hash atual em outro documento. Se os códigos corresponderem, isso indica que o documento é idêntico e se pode prosseguir com a

transação com segurança. O código hash é atribuído exclusivamente a cada informação. (PATRÍCIO; FERREIRA, 2020)

Uma vez que o código hash é gerado, ele envia os dados e a assinatura digital para a pessoa designada. Quando o receptor recebe a informação e a assinatura, o receptor insere a chave pública do remetente e a assinatura digital é enviada para o algoritmo. Esse processo cria o código do número de hash. (PATRÍCIO; FERREIRA, 2020)

E como explicado acima, para verificar a validade do documento, o receptor verifica o código de hash do documento original e o compara com seu código de hash. Se ambos os códigos de número de hash forem iguais, então é uma assinatura válida; caso contrário, é considerada uma assinatura falsa ou inválida. (DOURADO, 2020)

Assinaturas digitais armazenadas em um blockchain vivem independentemente do objeto ao qual a assinatura se refere. Não há necessidade de uma autoridade de certificação central ou servidor central de registro de data e hora, que são as dependências típicas dos sistemas de assinatura eletrônica existentes. (PATRÍCIO; FERREIRA, 2020)

Assinaturas digitais são a maneira mais segura de alcançar o mais alto nível de segurança de dados devido à criptografia. Além do valor de hash, o destinatário confirma a autenticação da mensagem aprovando a assinatura digital com a chave pública gerada do remetente, que verifica a identidade da pessoa com quem está se comunicando. (PATRÍCIO; FERREIRA, 2020)

Além disso, oferece a vantagem crítica de salvar e transferir informações em Blockchain, o que garante integridade. Sem Blockchain, os dados podem ser modificados sem serem totalmente hackeados. Embora isso aconteça em uma assinatura digital baseada em Blockchain, a assinatura se tornará inválida por padrão. Assim, a assinatura digital, que é criptografada, é segura e não pode ser adulterada, pois revelará que os dados foram modificados, cimentando sua corruptibilidade. (LEITÃO; FERREIRA, 2021)

Além de fornecer autenticação de mensagens e integridade de dados, as assinaturas digitais também oferecem mensagens de não repúdio. Como se considera que o remetente se associa à chave de assinatura, o destinatário também pode apresentar os dados e a assinatura digital como prova caso ocorra alguma disputa. (PATRÍCIO; FERREIRA, 2020)

A intenção do Blockchain é substituir um terceiro externo e confiável (incluindo a necessidade de autoridades de certificação) e também impedir que qualquer pessoa possa voltar atrás e cobrir seus rastros se corromper uma entrada. A tecnologia funciona nas seguintes propriedades (DOURADO, 2020):

- Replicação de log – Para criar resiliência, a replicação baseada em log é cada vez mais usada para sistemas distribuídos para replicar logs para todos os pares na rede.
- Cadeia de valor comprovada – Os valores armazenados no blockchain podem ser moeda digital, dados, documentos e outros ativos. As cadeias de hash são mantidas para cada bloco, fornecendo um histórico de alterações, o que ajuda a proteger a integridade dos dados do ativo do bloco.
- Criptografia de chave pública – Blockchain usa diferentes tipos de criptografia, incluindo ECDSA e curva elíptica para autenticar transações.
- Livro- razão de transações descentralizado – O livro-razão é blockchain e é mantido sem uma autoridade central e atua como um sistema de reconciliação descentralizado.

Senso assim, resta indubitável os benefícios trazidos por assinatura ou autenticação, na seara pública, de documentos, arquivos e outros itens intangíveis necessários ao bom andamento do serviço público, por meio do sistema Blockchain. Se não bastasse a praticidade, de modo que reduz enormemente a burocracia, tais sistemas são bastante seguros e confiáveis.

5. METODOLOGIA DA PESQUISA

A presente pesquisa é qualitativa e bibliográfica, tendo utilizado revistas, livros e sites que abordavam o mesmo tema ou similar. Uma pesquisa qualitativa, de acordo com Veal (2011), envolve a coleta de uma grande quantidade de informações, no entanto, sobre um pequeno número de pessoas. As informações coletadas geralmente não são apresentadas em formato numérico.

A análise tem um foco exploratório, que, segundo Dencker (1998), busca enaltecer ideias. Também se caracteriza por ter um planejamento volúvel, geralmente envolvendo vasta bibliografia. Uma pesquisa bibliográfica, por seu turno, desenvolve-se a partir de materiais já produzidos, como livros, artigos, periódicos, etc. (GIL, 2009). Sobre isso, Dencker (1998) afirma que essa pesquisa consiste no

uso de estudos já preparados, como livros e artigos científicos.

Gil (2008), por outro lado, mostra que sua principal vantagem ao consultar tais materiais, é a possibilidade de verificar, ao mesmo tempo, uma rica quantidade de situações já verificadas, compara-las, ou mesmo, garantir seu próprio ponto de vista. A pesquisa teve cunho exploratório e ocorreu durante o primeiro semestre de 2022, por meio de busca nas bases de dados do google acadêmicos e Livros físicos, com prioridade em artigos e livros recentes (últimos 10 anos) e, excepcionalmente, fora desse intervalo que se fazer de suma necessidade.

Além disso, a revisão narrativa tem o objetivo fazer uma revisão atualizada do conhecimento estudado, visto que é adequada para a fundamentação teórica de artigos, dissertações, teses, trabalhos de conclusão de cursos (TYBEL, 2018).Foram utilizados artigos direito com pertinência temática, isto é, que tratem de aspectos mais importantes relacionados a burocracia, criptografia, blockchain e assinatura digital/virtual/eletrônica

Como critério de exclusão adorar-se-á para aqueles artigos que não tratam do assunto de interesse deste estudo; artigos com clara superação de entendimento (devido a mudanças na lei, por exemplo); artigos de fontes não consolidadas e/ou de cunho não acadêmico e artigos muito antigos que não sejam meramente conceituais.

6. CONSIDERAÇÕES FINAIS

Pelo até então exposto, é claro que, pelos projetos históricos, o modelo de burocratização imaginado por Weber, possuía e ainda possui grande importância para a garantia de efetividade da prestação de serviços públicos através do seguimento de ritos previstos em lei. Contudo, com o passar do tempo, a visão burocrática em sua essência foi distorcida, tornando-se um motivo de nomear a prestação de serviços públicos de um desserviço.

Para a recuperação da essência do papel da burocracia e o abandono do estigma que a faz sofrer hoje, faz-se necessário um trabalho árduo, a priori de conscientização por parte do gestores para com aqueles prestadores desses serviços sob seu poder, para usarem normas adjetivas voltadas ao rito de execução apenas como norte e com teor meramente declaratório para o alcance do objetivo principal, que é a prestação do serviço, e não como requisito constitutivo do direito,

pois se assim for, o requisito de validade do papel do serviço público está em cheque.

Quanto ao uso das TIC's como um todo para fins de aprimoramento do setor público, embora já se tenha ações no sentido de minimizar os projetos burocráticos registre-se, por força de lei - cabe lembrar que estas podem ser um diferencial enorme na gestão do setor público, passível de ser fator diferencial entre o sucesso e o fracasso.

No tocante ao uso de assinatura e autenticação por padrão Blockchain, restou possível concluir que atualmente, as assinaturas digitais estão em alta na Internet, pois todos as aceitam. Blockchain aqui vem como um suporte para o futuro da assinatura digital, permitindo que ela (assinatura e autenticação) se torne segura e protegida, pois o Hashing fornece um código ou uma chave no Blockchain, que é único e o torna seguro, e por outro lado, uma assinatura digital garante que o proprietário faça todas as transações sem qualquer adulteração.

A assinatura e autenticação por padrão Blockchain se mostrou útil, segura e bastante maximizadora da gestão menos burocrática, vez que permite a autenticação e análise de documentos assinados sob seu rito de modo prático, sem necessidade, por exemplo, de o administrador ou administrado se locomover a repartições, pegar longas filas e desperdiçar tempo, tudo de maneira rápida, prática e segura.

Nesses termos, conclui-se que o Estado latu sensu (União, Estados, DF e Municípios), devem assegurar medidas efetivas afim de aprimorar os processos de gestão de projetos, bem como da prestação de serviços, o que, sem dúvidas, pode ser facilitado com o uso de todas a ferramentas à dispor dos gestores, tal qual as de informação e de comunicação (TIC's) por meio, por exemplo, das assinaturas digitais via blockchain.

Como sugestão de pesquisas futuras, é possível indicar com a análise das principais diferenças entre as assinaturas digitais/eletrônicas existentes, considerando também as que utilizam de tecnologia blockchain, expondo as vantagens e desvantagens de cada uma delas bem como o custo benefício de curto, médio e longo prazo. Por fim, o cenário jurisdicional atual demonstrou que se requer dos já atuantes e futuros operadores de sistemas, não somente a vontade de participar desse mundo tão repleto de informações, mas requer, também, o conhecimento necessário para tal fim, que somente é adquirido através do estudo.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline De Souza. **PASSADO, PRESENTE E FUTURO DA CRIPTOGRAFIA FORTE: DESENVOLVIMENTO TECNOLÓGICO E REGULAÇÃO.** Revista Brasileira de Políticas Públicas, v. 7, n. 3, 2018. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4869>. Acesso em: 10 maio 2022.

ALVES, Clécio Frank Silva **A certificação digital para o governo e para a sociedade mineira: estudo das principais contribuições na perspectiva da Autoridade Certificado e de Registro do Estado de Minas Gerais** – Prodemge. 54f. TCC (Especialização em Administração Pública) Fundação João Pinheiro/Escola de Governo Professor Paulo Neves de Carvalho, Belo Horizonte, MG, 2020.

BASTOS, E. A. V.; PANTOJA, T. L. S.; SANTOS, S. H. C. S. DOS**. Os impactos das novas tecnologias da informação e comunicação no direito fundamental à privacidade.** Brazilian Journal of Development**,** v. 7, n. 3, p. 29247–29267, 2021.

BRASIL. **Constituição da República Federativa de 1988**. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em: 15 mar. 2022

BRASIL. **Decreto nº 9.094, de 17 de julho de 2017**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9094.htm#art25 acesso em 15 mar. 2022

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**: **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 15 abr. 2022

BRASIL. **Lei 14.063, de 23 de setembro de 2020**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm Acesso em: Acesso em: 15 abr. 2022

BURGOS, Marcelo Tadeu Baumann ; BELLATO, Caíque Cunha. **GERENCIALISMO E PÓS-GERENCIALISMO**: **EM BUSCA DE UMA NOVA IMAGINAÇÃO PARA AS POLÍTICAS EDUCACIONAIS NO BRASIL.** Sociologia & Antropologia, v. 9, n. 3, p. 919–943, 2019. Disponível em: <https://www.scielo.br/j/sant/a/hzHGhpwGMxYvzhvqwzPP7vs/?format=html&lang=pt>. Acesso em: 10 maio 2022.

CAMPOS, E. **Sociologia da burocracia**. Rio de Janeiro: Zahar Editores, 1976.

CARVALHO, G. P.; PEDRINI, T. F. **DIREITO À PRIVACIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.** Revista da ESMESC, v. 26, n. 32, p. 363–382, 16 dez. 2019.

DENCKER, A. F. M. **Pesquisa em turismo: planejamento, métodos e técnicas**. São Paulo: Futura, 1998.

DOURADO, Dourado, Letícia Berlese Mello. **A tecnologia de blockchain como facilitadora dos serviços cartorários brasileiros**. 58f. Trabalho de Conclusão de Curso (Graduação em direito) -Universidade Federal Do Rio Grande Do Sul, UFRS, Porto Alegre, 2020. Disponível em: <https://www.lume.ufrgs.br/handle/10183/222259>. Acesso em: 10 maio 2022.

FUCCI, Caio Machado Botelho. **A LGPD como ferramenta para garantir o direito à privacidade dos brasileiros diante do cenário tecnológico atual**. 2022. 45f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Produção) - Universidade Federal Fluminense, Escola de Engenharia, Niterói, 2022.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4 ed. São Paulo: Atlas, 2002.

KRELL, Andreas Joachim; DANTAS, Juliana de Oliveira Jota; LINS JÚNIOR, George Sarmento (org**). A pandemia do coronavírus sob a ótica do Direito:** desafios e transformações em pauta. Maceió: Edufal, 2021. E-book (104 p.). ISBN 978-65-5624-034-3

LEITÃO, Andre Studart ; FERREIRA, Hélio Rios. **AS NOVAS TECNOLOGIAS A SERVIÇO DA NOVA ADMINISTRAÇÃO: A BLOCKCHAIN, OS SMART CONTRACTS E A NOVA LEI DE LICITAÇÕES E CONTRATOS** (LEI Nº 14.133/2021). Revista de Direito Brasileira, v. 29, n. 11, p. 71–91, 2021. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/7493>. Acesso em: 10 maio 2022.

MELO, Jonas Santos de. **O direito à privacidade, autodeterminação informativa e proteção de dados pessoais: o contexto da Lei 13709/2018**. 47f. TCC - Graduação em Direito - Bacharelado - Universidade do Estado do Amazonas, Manaus, 2018.

OLIVEIRA, Silvio Luiz de. **Sociologia das Organizações: Uma Análise do Homem e das Empresas no Ambiente Competitivo**. São Paulo: Thomson Learning, 2006.

PATRÍCIO, Lurdes D; FERREIRA João J. **Blockchain security research:** theorizing through bibliographic-coupling analysis | Emerald Insight. Journal of Advances in Management Research**,** v. 18, n. 1, p. 1–35, 2020. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/JAMR-04-2020-0051/full/html?casa_token=M-Ry_ScmLsQAAAAA:Y-Y3dGG2J3xf62d3W05k-I461BM0fMSxmxTa__0kXjjacFSMif9X5o_i32G-

sVDQwdFZTLWFrGvxz6vlITDpszqkk3D-u4OIxf9PtI_BYS9sXKXGtDi8LA>. Acesso em: 10 maio 2022.

PEDROSO SOARES, N.; BARDEMAKER ANHAIA, V.; CADORE TOLFO, A. **O DIREITO À PRIVACIDADE E SUA PROTEÇÃO NA ERA DIGITAL.** Anais do Salão Internacional de Ensino, Pesquisa e Extensão, v. 12, n. 2, 4 dez. 2020.

SILVA, Diego Holtz. **Os modelos de administração pública na secretaria de administração da Prefeitura municipal de Santana do Livramento/RS**. 20f. Trabalho de conclusão apresentado ao curso de Gestão Pública. Santana do Livramento: Unipampa, 2019.

SOUZA, Vanessa Gonçalves Ribeiro. **A evolução da administração pública brasileira: reforma gerencial, a nova gestão pública**. 2019. 20 f. Trabalho de Conclusão de Curso (Especialização em Gestão Pública Municipal)—Universidade de Brasília, Anápolis - GO, 2019.

TYBEL, Douglas. **Tipos de Revisão de Literatura**. Disponível em: https://guiadamonografia.com.br/tipos-de-revisao-de-literatura/. Acesso em 23 abr. 2022.

VEAL, A.K. **Metodologia de pesquisa em lazer e turismo**. São Paulo: Aleph, 2011.

VIEIRA, Carolina Coimbra; *et al*. **O Paradoxo da Viralização de Informação Criptografada no WhatsApp.** Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2019)**,** 2019. Disponível em: <https://sol.sbc.org.br/index.php/sbrc/article/view/7375>. Acesso em: 10 maio 2022.

WEBER, Max. **Economia e sociedade**. Brasília: UNB, 1998.