

UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CAMPUS DE ERECHIM
ÁREA DO CONHECIMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

NELSON GONÇALVES

CRIMES VIRTUAIS: FRAUDES EM ASSINATURAS ELETRÔNICAS

ERECHIM

2024

NELSON GONÇALVES

CRIMES VIRTUAIS: FRAUDES EM ASSINATURAS ELETRÔNICAS

**Trabalho de conclusão de curso
apresentado como requisito parcial à
obtenção do grau de Bacharel em Direito,
Departamento de Ciências Sociais
Aplicadas da Universidade Regional
Integrada do Alto Uruguai e das Missões –
Câmpus Erechim - RS.**

Orientador(a): Ma. Diana Casarin Zanatta

ERECHIM - RS

2024

NELSON GONÇALVES

CRIMES VIRTUAIS: FRAUDES EM ASSINATURAS ELETRÔNICAS

**Trabalho de conclusão de curso
apresentado como requisito parcial à
obtenção do grau de Bacharel em Direito,
Área do Conhecimento de Ciências Sociais
Aplicadas da Universidade Regional
Integrada do Alto Uruguai e das Missões –
Câmpus Erechim - RS.**

Erechim, 13 de Novembro de 2024.

BANCA EXAMINADORA

Profa. Ma. Diana Casarin Zanatta

Profa. Ma. Simone Gasperin de Albuquerque

Prof. Me. Gilmar Bianchi

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão a todos que contribuíram para a realização deste trabalho de conclusão de curso. Em primeiro lugar, agradeço à minha orientadora, Prof^a. Ma. Diana Casarin Zanatta, por sua orientação inestimável, paciência e apoio ao longo de todo o processo. Suas sugestões e críticas construtivas foram fundamentais para o aprimoramento deste trabalho.

Agradeço também aos meus familiares e amigos, especialmente minha esposa Rosemeri Demarco e meu filho Miguel Bento Gonçalves Demarco, que me ofereceram apoio emocional e incentivo incondicional durante todos os momentos desta jornada acadêmica, com sua compreensão pelas minhas ausências físicas e mesmo no ambiente familiar. A compreensão e motivação de vocês foram essenciais para que eu pudesse me dedicar plenamente ao estudo e à pesquisa.

Um agradecimento especial aos meus colegas de curso, que compartilharam comigo momentos de aprendizado e colaboração, tornando essa experiência ainda mais enriquecedora e significativa.

Por fim, sou grato a todas as instituições, profissionais e professores que disponibilizaram recursos e informações valiosas que contribuíram para a fundamentação teórica e prática deste estudo.

A todos, meu sincero muito obrigado, e que Deus lhes retribua grandemente.

RESUMO

A pesquisa estabelece uma abordagem acerca das possibilidades de cometimento de crimes virtuais utilizando as assinaturas e certificações digitais. O objetivo é apresentar os pontos sensíveis com foco no estabelecimento de diretrizes necessárias para segurança de dados pessoais, num tempo em que recrudescem os crimes relacionados à tecnologia e à internet. Para tanto, o estudo parte da verificação acerca da transformação digital, da migração da documentação física para a digital, dos elementos necessários para a assinatura e certificação digitais e, em seguida, verifica os requisitos necessários para a validação da assinatura digital. São analisados os tipos de crimes digitais relacionados à assinatura digital, antes e depois da implementação da Infraestrutura de Chaves Públicas Brasileira - ICP, em 2001. Também é apresentado um levantamento da jurisprudência no Estado do Rio Grande do Sul, sobre os crimes relacionados à assinatura e certificação digital. Busca-se, ao final, apresentar algumas sugestões de medidas de segurança para um emprego seguro dos certificados digitais. A metodologia empregada é a indutiva, a partir de pesquisa bibliográfica, consistente na busca por referencial teórico já construído, além de análise de documentos oficiais, oriundos de órgãos governamentais.

Palavras-chave: transformação digital; assinatura eletrônica; certificado digital; segurança de dados; crimes digitais.

ABSTRACT

The research establishes an approach regarding the possibilities of committing cybercrimes using digital signatures and certifications. The aim is to present sensitive points focusing on establishing necessary guidelines for personal data security at a time when technology and internet-related crimes are on the rise. To this end, the study begins with an examination of digital transformation, the migration from physical to digital documentation, the necessary elements for digital signatures and certifications, and then verifies the requirements needed for digital signature validation. It analyzes the types of digital crimes related to digital signatures, both before and after the implementation of the Brazilian Public Key Infrastructure (ICP) in 2001. A survey of case law in the State of Rio Grande do Sul concerning crimes related to digital signatures and certifications is also presented. Ultimately, the research seeks to offer some suggestions for security measures to ensure the safe use of digital certificates. The methodology employed is inductive, based on bibliographic research, consisting of a search for already established theoretical references, as well as an analysis of official documents from governmental bodies.

Keywords: digital transformation; electronic signature; digital certificate; data security; digital crimes.

SUMÁRIO

1	INTRODUÇÃO	5
2	TRANSFORMAÇÃO DIGITAL	7
2.1	BIG DATA	9
2.2	INTERNET DAS COISAS	10
2.3	INTELIGÊNCIA ARTIFICIAL	10
3	DOCUMENTO FÍSICO E DOCUMENTO DIGITAL	12
3.1	ELEMENTOS ESSENCIAIS PARA A VALIDADE DE UM DOCUMENTO DIGITAL	14
3.2	VALIDADE JURÍDICA DAS ASSINATURAS ELETRÔNICAS	15
3.4	ARCABOUÇO JURÍDICO DE ASSINATURAS ELETRÔNICAS	20
3.4.1	O RECONHECIMENTO DA VALIDADE DA CERTIFICAÇÃO DIGITAL PELA JURISPRUDÊNCIA GAÚCHA	21
4	SEGURANÇA DIGITAL E CRIMES VIRTUAIS	23
4.1	CRIMES VIRTUAIS E FRAUDES EM ASSINATURAS ELETRÔNICAS	25
4.2	CRIMES RELACIONADOS ÀS ASSINATURAS ELETRÔNICAS	27
4.2.1	CASOS DE FRAUDES EM ASSINATURAS ELETRÔNICAS	28
4.3	MEDIDAS PREVENTIVAS DE SEGURANÇA	30
4.3.1	O DESCONHECIMENTO COMO FATOR DE VULNERABILIDADE	30
4.3.2	CUIDADOS COM O <i>TOKEN</i> : CERTIFICADO DIGITAL	31
5	CONCLUSÃO	34
	REFERÊNCIAS	36

1 INTRODUÇÃO

A transformação digital trouxe um aumento significativo de crimes eletrônicos, também denominados digitais. Atualmente, observa-se uma crescente dependência das pessoas - físicas e jurídicas – com o mundo digital e suas facilidades. Assim, quanto maior o número de dados digitalizados, bem como processos online que levam estas informações para servidores distribuídos, qual seja, a nuvem de arquivos, mais sujeitos a invasões estarão os usuários e, conseqüentemente, maior o número de vítimas de crimes diversos, tais como o sequestro e uso indevido de dados.

Busca-se abordar o tema segurança digital no contexto da transformação digital, com foco nos desafios e riscos associados aos crimes cibernéticos. O problema abordado é o aumento dos crimes eletrônicos devido à crescente digitalização e dependência de tecnologias plugadas (conectadas à internet). Destaca-se como essa transformação demonstra a vulnerabilidade tanto de indivíduos quanto de empresas frente a riscos significativos, principalmente pela falta de conhecimento básico sobre segurança digital e a necessidade de medidas eficazes para proteger dados e informações sensíveis. Além disso, reforça a importância de estudar e compreender as fragilidades dos sistemas digitais para reduzir tais riscos.

De fato, a disseminação de equipamentos conectados à internet, como telefones celulares, computadores portáteis, *gadgets* (acessórios) inteligentes, entre outros, podem expor os indivíduos a riscos decorrentes de ações maliciosas perpetradas por *hackers* (criminosos digitais) e pela utilização de *malwares* (programas maliciosos). A ausência de consciência sobre comportamentos seguros na internet, como o emprego de senhas robustas e a não divulgação de dados pessoais, igualmente têm acarretado no aumento de delitos virtuais.

A modernização tecnológica apresenta novos obstáculos, em especial, à segurança virtual de empresas, que precisam garantir a segurança das informações de seus clientes e parceiros, bem como resguardar seus próprios ativos intelectuais. A digitalização de procedimentos amplia as chances de invasões a redes e sistemas empresariais, o que pode acarretar prejuízos econômicos e de reputação às organizações.

Uma das maiores comodidades surgidas com a tecnologia, recentemente, trata-se das assinaturas eletrônicas. Com elas, tornou-se possível efetivar contratos, mesmo diante das restrições impostas pela recente pandemia de Covid-19, ocorrida no ano de 2020, que restringiu reuniões e assinaturas presenciais. Contudo, junto com essa praticidade, surgiram os malfetores especializados em burlar a segurança desse método virtual de assinatura.

Diante desse cenário, é imprescindível estudar a temática, observando os diversos artifícios que podem acabar sendo utilizados para burlar a segurança dos sistemas, cuja maior vulnerabilidade tem sido a falta de conhecimento básico acerca de seu funcionamento. Justifica-se, portanto, a pesquisa, por ser fundamental que empresas, governo e indivíduos estejam cientes dos riscos, buscando implementar ações para se manterem informados, atualizados e, dessa forma, preservar suas informações e dados.

O método de pesquisa é o indutivo, sendo que a escolha por essa metodologia parte da observação de que o assunto é novo e, por estar sob construção, busca-se produções bibliográficas tradicional e principalmente no formato de *e-book* (livros eletrônicos), assim como documentos governamentais e de certificação digital oriundos de empresas privadas, disponíveis online.

Para que o estudo alcance seu objetivo, apresenta-se a evolução histórica das mídias, como meios utilizados para documentar as transações entre partes contratantes e os cuidados para manter e melhorar a confiabilidade destas. Explicam-se a assinatura e certificados digitais, seus elementos, verificando-se o que é necessário para a validade jurídica das assinaturas digitais. Verifica-se como a jurisprudência do Estado do Rio Grande do Sul tem analisado a matéria e parte-se para a observação da segurança de dados pessoais. Apresenta-se o tema crimes cibernéticos, bem como medidas de segurança que buscam deixar o usuário menos vulnerável.

2 TRANSFORMAÇÃO DIGITAL

A transformação digital tem se apresentado como uma tendência na vida das pessoas e, em especial, das organizações privadas e governamentais. O processo visa a adoção de tecnologias digitais para melhorar a eficiência das empresas, por meio da automação de processos, análise de dados, uso de inteligência artificial, entre outras formas.

Segundo Schwab (2016), a Quarta Revolução Industrial, iniciada em 2011, apresentou essa transformação do mundo em diversos aspectos, integrando tecnologias digitais, físicas e biológicas e está mudando a forma como as pessoas vivem, trabalham e se relacionam. Nesse contexto, é fundamental que governos, empresas e a sociedade em geral estejam atentos às mudanças e trabalhem juntos para aproveitar ao máximo as oportunidades e enfrentar os desafios. Há que se observar que não se trata de um caminho simples, monótono, mas sim, de algo muito turbulento. Em outras palavras:

Estamos à beira de uma revolução tecnológica que transformará fundamentalmente a forma como vivemos, trabalhamos, estudamos e nos relacionamos. Em sua escala, alcance e complexidade, a transformação será diferente de qualquer outra coisa que o ser humano já tenha experimentado antes (Schwab, 2016, p. 01).

A transformação digital é um processo complexo que requer mudanças em diversos aspectos das organizações. Ela não se limita apenas ao uso de tecnologias, mas também envolve mudanças na cultura organizacional e na forma como as empresas se relacionam com seus clientes e fornecedores. É também um processo de integração entre tecnologia e negócio, com o objetivo de criar valor para o cliente e melhorar a performance empresarial. Aceitá-la é essencial para que as empresas sobrevivam aos novos tempos, coisa que só conseguirão ao entenderem o processo. Conforme depreende-se:

[...] um processo contínuo pelo qual as organizações se adaptam a mudanças disruptivas ou criam essas mudanças no seu ecossistema externo por meio de competências digitais para inovar com novos modelos de negócios, produtos e serviços que integram o digital e o físico de maneira transparente, bem como as experiências de negócio e as dos clientes, ao mesmo tempo em que geram melhorias na eficiência operacional e organizacional. (IDC apud Veras, 2019, p. 72).

A apregoada personalização das experiências dos clientes é alcançada oferecendo-se soluções adaptadas às necessidades individuais. Isso pode resultar em uma maior satisfação do cliente e lealdade à marca. Todavia, a implementação da transformação digital não é uma tarefa fácil, e muitas empresas ainda enfrentam desafios nesse processo.

Um dos principais desafios é a resistência cultural, pois muitos colaboradores e gestores ainda não compreendem a importância da transformação digital para o sucesso da empresa. A falta de habilidades digitais e a dificuldade de encontrar profissionais capacitados também são dificuldades no caminho da transformação digital.

Apesar dos desafios, a transformação digital tem se mostrado uma estratégia importante para o sucesso das empresas brasileiras, haja visto que é natural que as empresas que investem em transformação digital tendem a ser mais inovadoras e tendem a obter melhores resultados financeiros.

A transformação digital pode contribuir para a inclusão social e a redução das desigualdades, permitindo o acesso a serviços digitais e oportunidades de trabalho remoto em regiões de difícil acesso. Entretanto, as empresas precisam exercitar um papel de pioneirismo, mas de forma autossustentável. Conforme destacado pela Confederação Nacional das Indústrias - CNI:

É fundamental que as empresas promovam uma cultura de inovação, invistam em capacitação e desenvolvimento de habilidades digitais, e estejam atentas às tendências e oportunidades do mercado para implementar a transformação digital de forma efetiva. É importante ressaltar que a transformação digital deve ser realizada de forma responsável e ética, considerando os impactos sociais e ambientais das tecnologias utilizadas (CNI, 2021).

Enfatiza-se a importância de as empresas adotarem um novo comportamento e promoverem inovação, capacitação e desenvolvimento de habilidades digitais. Para isso, precisam estar atentas às tendências e oportunidades do mercado, buscando empenhar-se na efetiva transformação digital. Além disso, destaca-se que essa transformação deve ser feita de maneira responsável e ética, levando em consideração os impactos sociais e ambientais das tecnologias utilizadas.

O esforço empregado pelas empresas deve lhes trazer muitos benefícios a médio e longo prazo. Tal conclusão depreende-se do estudo denominado Transformação Digital no Brasil: Oportunidades e Desafios, produzido pela Fundação Getúlio Vargas, que enfatiza o seguinte:

Em suma, a transformação digital é uma tendência global que está mudando a forma como as empresas e as pessoas se relacionam e se comunicam. No contexto brasileiro, ela representa uma oportunidade para as empresas inovarem, melhorarem sua performance e se prepararem para os desafios do futuro. Para isso, é fundamental que as empresas superem os desafios da resistência cultural e da falta de habilidades digitais, promovam uma cultura de inovação, invistam na melhoria

do seu desempenho no mundo virtual e estejam atentas às tendências do mercado (FGV, 2021).

A transformação digital no Brasil e no mundo está revolucionando a forma de interação entre empresas e pessoas, sendo que isso representa uma grande oportunidade para as empresas se anteciparem aos seus concorrentes. Porém, é necessário vencer a barreira do paradigma relacionado à estagnação tecnológica, arraigado no pensamento dos administradores mais tradicionais. Visar melhorias no desempenho online e acompanhar as tendências de mercado também são elementos-chave para o sucesso nessa transformação.

É nessa esteira que se encontram os meios eletrônicos de assinatura de documentos, os quais são estigmatizados e, quando isso acontece, as organizações acabam não acompanhando o movimento necessário imposto pelo atual ritmo global de transformação digital. Vencer tais paradigmas é obrigatório para a adoção em massa dessas ferramentas, bem como desenvolver maneiras de torná-las seguras.

2.1 BIG DATA

A transformação digital vem acompanhada de muitos termos novos, e entre eles cita-se o Big Data. Tal termo tornou-se popular em 2010, mas desde o nascimento da própria internet (www) em 1990, já se falava em Big Data, que significa dados em grande escala (Rogers, 2017). Tal termo provém do uso massivo de armazenamento de dados em função da própria rede mundial de computadores e sua voraz necessidade de acumulação de informações. Big Data, pode ser conceituado como sendo:

novos tipos de dados não estruturados – informações que são registradas mas não se encaixam com facilidade em fileiras e colunas bem organizadas. Uma empresa pode ter acesso a posts de textos agramaticais das mídias sociais, ao dilúvio de imagens geradas por smartphones, aos sinais de mapeamento e localização em tempo real, ou aos dados oriundos de sensores que se espalham rapidamente pelo nosso corpo e pelo mundo inteiro (Rogers, 2017, s/p).

Tratar grandes quantidades de dados exige energia em amplos sentidos. Energia elétrica, engenhosidade e tecnologias avançadas de armazenamento e mesmo criatividade no desenvolvimento de mecanismos de cópias de segurança de tais dados. Redes Sociais, tecnologias de geolocalização, programas de comunicação instantâneas, armazenamento de fotos, entre tantas novidades, são os responsáveis pela geração absurda de dados. Tudo isso precisa ser arquivado fisicamente, e mesmo que se fale em nuvem de armazenamento, o termo induz a erro, pois na ponta do processamento, os dados precisam estar gravados fisicamente

em algum meio palpável, mesmo que distribuído aleatoriamente em vários discos (Rogers, 2017).

2.2 INTERNET DAS COISAS

Pode-se falar da internet das coisas em separado do termo Big Data, pois o caminho de ambos, apesar de serem parecidos, precisam ser explanados em separado. Isso se deve ao fato de que a tendência de se integrar chips e microchips nos mais inusitados objetos do cotidiano são uma tendência irreversível. Convive-se atualmente com sensores, captadores de som e imagem e controladores em locais e coisas que muitos jamais imaginam estarem presentes, ou que se souber, ignora-se voluntariamente.

Sujeita-se a permitir a invasão de privacidade em favor de uma prometida preditividade que venha a beneficiar o usuário, antevendo suas necessidades e promovendo a antecipação de ações para suprir o mais brevemente possível o fornecimento do produto ou serviço faltante. A automatização de coisas é um caminhar de passos largos (Rogers, 2017). Em outras palavras:

Na medida que sensores e conectividade digital se tornam partes essenciais de cada vez mais objetos (automóveis, tratores, motores de jatos, aparelhos domésticos), a Internet das Coisas provavelmente redefinirá as fronteiras de muitos setores que até agora foram menos impactados pela internet que os negócios de mídia e informação (Rogers, 2017, s/p).

Como já mencionado, a Internet das Coisas e o Big Data se interligam, pois o primeiro fornece a matéria-prima para o segundo. O imenso volume de informações geradas pela coleta dos sensores, coletores e captadores, usados para compor as bases de dados formam os mecanismos da chamada Internet das Coisas segue uma tendência de aumento geométrico.

2.3 INTELIGÊNCIA ARTIFICIAL

É necessário abordar o tema Inteligência Artificial (I.A.). No entanto, é necessário reduzir a o ritmo e reavaliar a rota, pois, no caminho da transformação digital, prevalece uma tendência a entender a inteligência artificial como é vendida na ficção cinematográfica, ou seja, de forma desconectada da realidade (Armstrong, 2019). Dito de outra forma:

Se olharmos a história do cinema – Chappie; Ela; Eu, Robô; A.I. Inteligência Artificial; Matrix; Transcendence – A Revolução; Blade Runner, Ex Machina; e, evidentemente, o tremendo HAL, de 2001, Odisseia no Espaço -, as coisas não terminarão bem para os humanos, de acordo com Hollywood. (Armstrong, 2019, s/p).

A inteligência artificial, conforme descrita no texto, busca emular comportamentos humanos inteligentes, como a compreensão de conteúdos complexos, a participação em conversas naturais e a capacidade de aprender e tomar decisões próprias. As aplicações dessa tecnologia são vastas e variadas, abrangendo desde veículos autônomos e reconhecimento de voz até a detecção e gestão de riscos. Essa versatilidade destaca tanto o potencial quanto os desafios associados à Inteligência Artificial, que, apesar de suas promessas, ainda está longe de alcançar o nível de sofisticação frequentemente retratado nas telas de cinema.

São muitos os temas possíveis de serem abordados para exemplificar a tendência da transformação digital que se apresenta no atual momento histórico, sendo estes elencados de maneira breve e minimamente aprofundados, pois não é este o objetivo principal buscado. O foco atual é o caminho natural das tendências digitais relacionadas às assinaturas digitais e consequentemente as possíveis utilizações fraudulentas dos meios eletrônicos e digitais de assinatura, acerca das quais o estudo se debruça na sequência.

3 DOCUMENTO FÍSICO E DOCUMENTO DIGITAL

O documento físico manuscrito teve e ainda tem em seu bojo, por sua característica artesanal, traços únicos e passíveis de individualização por perícia técnica. Conforme Gomide *apud* Lawand (2001, p. 56), “tratando-se de registro gráfico resultante de gesto psicossomático, a escrita apresenta elementos técnicos personalíssimos, decorrentes do movimento comandado pelo cérebro do escritor”.

Para manter a confiabilidade de documentos digitais é necessário fazer um paralelo com estes mesmos documentos em meio físico. Com o avanço da tecnologia, tornou-se possível transformar documentos físicos em arquivos digitais, o que permite o exercício comparativo entre átomos e *bits*:

Pode-se dizer que experimentamos hoje um mundo virtual onde, no lugar de átomos, agora temos que nos acostumar com uma realidade de coisas formadas tanto por átomos como por bits. O documento tradicional, em nível microscópico, não é outra coisa senão uma infinidade de átomos que, juntos, formam uma coisa que, captada pelos nossos sentidos, nos transmite uma informação. O documento eletrônico, então, é uma das sequências de bits que, captada pelos nossos sentidos com o uso de um computador e um software específico, nos transmite uma informação (Negroponte *apud* Gandini, *et al*, 2001, p. 06).

Essa transformação do documento físico para digital foi o que possibilitou uma série de benefícios, entre elas destaca-se a facilidade de acesso. Documentos digitais podem ser acessados a partir de qualquer lugar do mundo, desde que se tenha uma conexão à internet, tornando mais fácil para as pessoas trabalharem em conjunto, independentemente de sua localização geográfica.

Nos trilhos da transformação digital, seguindo a locomotiva tecnológica, o vagão que interessa nesse momento refere-se aos métodos de digitalização de documentos e a manutenção de sua integridade. Como se percebe, a evolução do documento físico para o digital tem sido uma tendência cada vez mais crescente na era da informação. A evolução chegou e traz consigo um repensar do conceito daquilo que é chamado de documento. Como se observa:

O documento tradicional, apostado em papel, não mais se adequa à necessidade atual de dar agilidade à circulação de informações. São evidentes suas limitações, tanto em relação à conservação, como à transmissibilidade e segurança (Gandini, *et al*, 2001, p. 05).

Há mais de vinte anos já se alertava acerca das limitações do uso de documentos em papel - documentos fisicamente produzidos, questionando-se sobre a necessidade de se fomentar a busca por novas soluções (Gandini, 2001). Neste caminho, no entanto, também já se enfatizava a necessidade de se manter as informações seguras para que as questões jurídicas inerentes a tais documentos também permanecessem seguras, posto serem essenciais para o pleno valor dos negócios neles envolvidos. A ideia era a de que documentos digitais podem ser protegidos por senhas e criptografia, garantindo que apenas as pessoas autorizadas tenham acesso aos dados confidenciais (Gandini, 2001).

Um dos maiores benefícios que já se previa para a utilização de documentos digitais seria a economia de espaço, já que o armazenamento de documentos físicos requer espaço, ao contrário dos documentos digitais, que são armazenados em servidores locais ou distribuídos (*cloud computing*). Há que se considerar a evidente redução de custos que uma organização obtém convertendo documentos físicos para digitais, seja na impressão, armazenamento e transporte de documentos. Além disso, ainda há a questão da sustentabilidade, posto que o uso da documentação digital implica na redução do uso de papel, o que significa uma medida importante para a preservação do meio ambiente (Moraes, 2009).

Para assegurar a confiabilidade dos documentos digitais, bem como garantir a integridade e autenticidade das informações neles contidas, Gandini (2001) aponta algumas medidas fundamentais. Inicialmente, há que se utilizar *softwares* (programas de computador) e ferramentas de criptografia, a fim de se obter a proteção das informações digitais por meio de códigos para garantir a confidencialidade dos dados. Também é necessário que se assine digitalmente os documentos, para dar garantia da autenticidade dos documentos digitais, semelhante ao que ocorre com a assinatura em documentos físicos.

É necessário manter *backups* de segurança, que são cópias de segurança dos documentos digitais, evitando perdas ou corrupção de dados. Faz-se necessária a utilização de sistemas de gestão documental, ou seja, controle do acesso aos documentos apenas às pessoas autorizadas. Há que se verificar a validade dos documentos, ou seja, garantia da origem emissora e da integridade, utilizar sistemas de controle de versão, para garantia de que as informações contidas nos mesmos são consistentes e confiáveis. Por fim, aponta-se a necessidade de utilização de certificados digitais, para garantia da autenticidade das informações, bem como asseguradora da confiabilidade destas (Gandini, 2001).

Portanto, para que o documento digital seja adotado de forma mais ampla e irrestrita, é fundamental que demonstre cada vez maior solidez e transparência confiança àqueles que dele

se utilizam. Para isso, cabe aos usuários adotar medidas específicas e cultivar uma cultura voltada para a segurança da informação. Só assim é possível assegurar a integridade de documentos digitais, tornando-os uma opção segura e confiável em relação aos documentos físicos. Com esse norte, pode-se esperar uma maior abertura dos diversos agentes ao aceite dessas novas formas de assinatura, buscando tornar cada vez mais comum seu uso e divulgação, pois são inumeráveis os benefícios da circulação dos documentos digitais.

3.1 ELEMENTOS ESSENCIAIS PARA A VALIDADE DE UM DOCUMENTO DIGITAL

Para Guelfi (2007) e Gandini, *et al* (2001), os elementos essenciais para a validade de um documento digital são aqueles que garantem a autoria, autenticidade, integridade e confidencialidade das informações contidas no documento. Os autores ainda elencam uma série de características que o documento digital deve conter.

Essas características são as seguintes: informações que identifiquem claramente o emissor (contendo nome, endereço e e-mail); a data e hora de emissão, para garantir que as informações contidas no documento sejam relevantes e atualizadas; informações que identifiquem claramente o destinatário; a assinatura digital, que é um elemento fundamental para a validade do documento digital; a criptografia, visto que elemento fundamental para a confidencialidade do documento digital; o certificado digital, documento eletrônico que garante a autenticidade do documento digital; controle de versão, importante para garantir a integridade do documento digital, permitindo acompanhar as alterações realizadas no documento ao longo do tempo (Gandini, *et al*, 2001). Acerca de um dos componentes da segurança dos documentos digitais:

A chave codificadora permite mais do que privacidade. Ela pode também garantir a autenticidade de um documento, porque a chave privada pode ser usada para codificar uma mensagem que só a chave pública pode decodificar. Funciona assim: se eu tenho uma informação que quero assinar antes de mandar para você, meu computador usa minha chave privada para codificá-la. Agora a mensagem só pode ser lida se minha chave pública – que você e todo mundo conhece – for usada para decifrá-la. Essa mensagem é com certeza minha, pois ninguém mais tem a chave privada capaz de codificá-la dessa forma (Gates *apud* Gandini, *et al*, 2001, p. 11).

Note-se que a utilização simultânea desses componentes (chave privada e chave pública) é imprescindível para a preservação da autenticidade e segurança de documentos digitais, de modo que a integridade, confidencialidade e autenticidade das informações

presentes no documento sejam garantidas. A garantia da integridade e privacidade da mensagem é dessa forma preservada, pois são duas etapas fundamentais e intrinsecamente dependentes para essa finalidade.

No contexto brasileiro, a Medida Provisória nº 2.200-2, que estabelece a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), desempenha um papel fundamental na conferência de validade técnica e jurídica aos documentos eletrônicos (Brasil, 2001). Através desse sistema de certificação digital, é possível utilizar assinaturas digitais qualificadas, garantindo a autenticidade e a integridade dos documentos, fortalecendo a confiança nas transações eletrônicas e impulsionando a adoção da digitalização em diversos setores.

São vários e essenciais os mecanismos que compõem o documento digital, sendo que, neste sentido, podem ser agregados rotineiramente novos elementos. Não se trata de rol taxativo, mas tão somente exemplificativo o arcabouço atual de travas de segurança, podendo surgir novos mecanismos sempre que houver necessidades. Neste sentido, apresentam-se alguns destes, objetivando demonstrar tão somente que a confiabilidade já seria suficiente para sua adoção em grande escala.

3.2 VALIDADE JURÍDICA DAS ASSINATURAS ELETRÔNICAS

A crescente tendência de digitalização de processos e documentos exige que tais processos e documentos, mesmo no ambiente virtual, tragam em seu bojo as mesmas características de segurança jurídica exigidas no mundo físico. Dessa forma, para que os documentos eletrônicos sejam cada vez mais aceitos por pessoas físicas e jurídicas, devem possuir mecanismos que lhes proporcionem a devida integridade e autenticidade inquestionáveis.

3.2.1 CRIPTOGRAFIA E CERTIFICADO DIGITAL

São elementos essenciais para a integridade e autenticidade das assinaturas eletrônicas a criptografia e o certificado digital. Segundo Matte *apud* Lawand (2021, p. 120), a criptografia “caracteriza-se por ser um sistema que codifica uma informação, utilizando-se de cálculos matemáticos realizados com senha(s) chave(s) por meio de programas, aplicando-os (codificando) à informação”.

A criptografia utiliza cálculos matemáticos realizados com senhas ou chaves por meio de programas para codificar informações. Esse processo de codificação transforma a informação original em uma forma ilegível para pessoas não autorizadas, garantindo a segurança e confidencialidade dos dados. Ao aplicar os cálculos matemáticos com as senhas ou chaves aos dados, é possível proteger a informação contra acessos não autorizados. Esse sistema é implementado por meio de programas de software especializados, que executam os cálculos necessários para a codificação dos dados (Matte *apud* Lawand, 2021).

A criptografia pode ser simétrica e assimétrica, sendo dois métodos fundamentais de criptografia utilizados para proteger informações. Segundo Matte *apud* Lawand (2021, p. 120), a criptografia simétrica utiliza uma única chave para criptografar e descriptografar dados, o que significa que ambas as partes envolvidas na comunicação devem possuir a mesma chave secreta. Esse método é geralmente mais rápido e eficiente para processar grandes volumes de dados, mas apresenta o desafio de distribuição segura da chave. Por outro lado, a criptografia assimétrica utiliza um par de chaves: uma chave pública, que pode ser compartilhada abertamente, e uma chave privada, que é mantida em segredo pelo proprietário. A chave pública é usada para criptografar dados, enquanto a chave privada correspondente é usada para descriptografá-los.

Por outro lado, o certificado digital é uma tecnologia que permite a identificação e autenticação de pessoas físicas e jurídicas no ambiente digital. Trata-se de um arquivo eletrônico que contém informações como nome, CPF ou CNPJ, além de uma chave privada que permite a realização de transações seguras na internet (Guelfi, 2007). O certificado digital tem grande importância no contexto atual, em que cada vez mais atividades são realizadas em meio eletrônico.

No Brasil, a utilização do certificado digital é regulamentada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), criada pela Medida Provisória nº 2.200-2/2001, como já apontado (Brasil, 2001). A ICP-Brasil é responsável por emitir e gerenciar os certificados digitais no país, além de estabelecer os padrões de segurança necessários para garantir a autenticidade e integridade das transações realizadas, estabelecendo padrões e políticas para a utilização de certificados digitais e definindo os requisitos para softwares de assinatura digital. A utilização de certificados digitais emitidos por ACs credenciadas, a implementação de medidas de segurança adequadas para o armazenamento da chave privada e a utilização de softwares de assinatura digital em conformidade com as normas estabelecidas

pela ICP-Brasil são fundamentais para garantir a autenticidade e a integridade dos documentos assinados digitalmente.

O certificado digital é uma tecnologia fundamental para a realização de atividades seguras no ambiente digital. A sua regulamentação no Brasil, conforme informado pela ICP-Brasil e a sua crescente utilização em diferentes áreas são indicativos da importância que a tecnologia tem para a sociedade. No entanto, apesar dos benefícios que a tecnologia proporciona, ainda existem desafios a serem superados, como a falta de conhecimento da população sobre o tema e a necessidade de maior investimento em infraestrutura para a sua utilização em larga escala (Guelfi, 2007).

3.3 ASSINATURA ELETRÔNICA: CLASSIFICAÇÃO

Atualmente, com a adoção da expressiva digitalização de processos e documentos, a assinatura eletrônica evoluiu para acompanhar a crescente demanda e a consequente segurança exigida para a validação destes procedimentos. A assinatura eletrônica *latu sensu*, representa uma categoria de assinaturas ditas não autorais. Essa é definida como qualquer instrumento eletrônico que possibilita a atribuição de uma assinatura a um documento, com o intuito de validar a autenticidade do signatário e a integridade do documento em questão (Guelfi, 2007). Essa modalidade de assinatura é representada por assinaturas que não tenham uso de criptografia ou chaves de segurança, tanto públicas quanto privadas. Devido a essa característica, ela é comumente aplicada em documentos que não demandam um elevado nível de segurança e autenticidade. Mais simples, mas não ausente de confiança:

Assinar um documento eletronicamente significa executar função tecnológica que lhe confira marca específica e torne impossível de ser dissociada sem alterar seu conteúdo – consistente não apenas da mensagem que é exibida na tela, mas também em bytes em linguagem hexadecimal (Pinheiro *et al*, 2019, p. 42).

Assinar um documento eletronicamente é possível mesmo sem um certificado digital, utilizando-se somente alguns mecanismos, como, por exemplo, um e-mail e um código enviado por *sms* (mensagem de texto). Esse tipo de assinatura, segundo Pinheiro *et al* (2019) ainda pode conter o grafismo digitalizado da assinatura física do emissor, o qual representa de maneira eletrônica sua assinatura manuscrita, ou ter anexado ao documento uma *selfie* (fotografia) do emissor. A assinatura eletrônica é utilizada em diversas áreas, como em contratos de serviço, autorizações de trabalho e certificações de cursos online.

A assinatura digital *strictu sensu*, é uma espécie de assinatura eletrônica, que utiliza certificado digital e criptografia assimétrica, ou seja, utiliza-se uma chave pública para a assinatura e uma chave privada para a verificação (Guelfi, 2007). É um método mais seguro e confiável, pois garante a integridade e autenticidade do documento. Ela é utilizada para documentos que exigem segurança e autenticidade, como contratos, transações financeiras e documentos legais. Segundo Pinheiro *et al* (2019, p. 44) “A assinatura digital utiliza um par de chaves distintas (chave privada e chave pública) que consiste na geração de códigos pareados com certa quantidade de símbolos (1024 ou 2048 bits) e que funcionam somente se associados”.

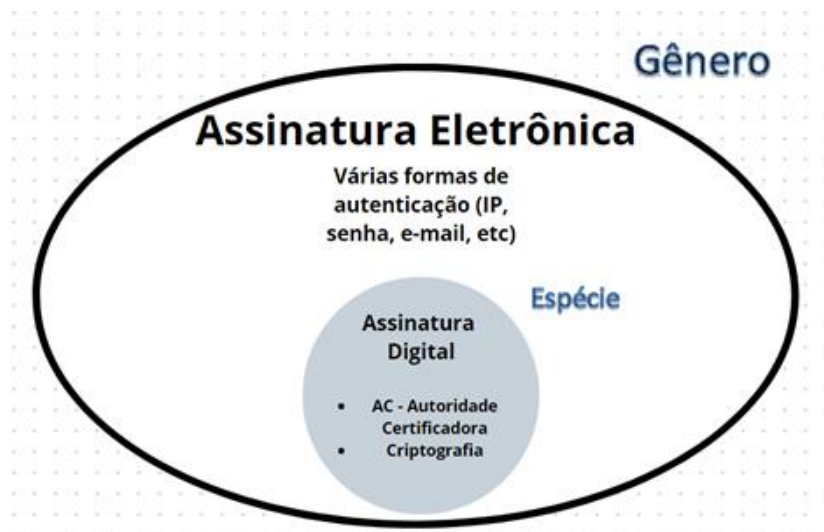
A assinatura digital é provida de um nível maior de segurança, por contar com a proteção dos certificados digitais, os quais fornecem uma maior proteção contra a ação de hackers e outros agentes mal-intencionados. Uma das características de segurança é garantida pela metodologia do uso de chaves (privada e pública).

A chave privada é gerada através da atribuição de uma chave disponível e individual pela autoridade certificadora (empresa responsável pela geração e controle de validade de chaves) e, simultaneamente, é gerada uma chave pública associada à privada, mas que a partir da chave pública não se pode deduzir ou descobrir a privada. Por isso, recebem o nome de assimétricas. A assinatura digital utiliza um par de chaves distintas (chave privada e chave pública) que consiste na geração de códigos pareados com certa quantidade de símbolos (1024 ou 2048 bits) e que funcionam somente se associados (Pinheiro *et al*, 2019, p. 44).

Além de garantir a autenticidade dos documentos, as assinaturas eletrônicas também oferecem outras vantagens, como a redução de custos com impressão e armazenamento de documentos em papel, a diminuição do tempo necessário para a assinatura de contratos e documentos, e a eliminação de erros humanos na assinatura de documentos. A assinatura digital permite a autenticação de documentos eletrônicos de forma segura e confiável. Essa tecnologia tem ganhado cada vez mais importância no contexto empresarial e governamental, uma vez que permite reduzir custos e agilizar processos que envolvem a assinatura de documentos.

A principal diferença entre a assinatura eletrônica e a assinatura digital é que a última é mais segura e confiável, utilizando certificado digital e criptografia assimétrica para garantir a autenticidade e integridade do documento. A assinatura eletrônica, por outro lado, é uma forma mais simples e menos segura de assinatura, adequada para documentos que não exigem um alto nível de segurança.

Pode-se ilustrar as diferenças entre assinaturas eletrônicas e digitais da seguinte forma:



Fonte: elaborado pelo autor

Em linhas gerais, considera-se Assinatura Digital uma espécie do gênero Assinatura Eletrônica, sendo que a primeira é composta de todas as características da segunda, e adicionada de mais camadas de segurança e validade jurídica.

Como visto, as assinaturas eletrônicas são tecnologias em evolução, e recentemente passaram a ser classificadas, de acordo com o disposto na Lei nº 14.063/2020, em três novas categorias: assinatura eletrônica simples, avançada e qualificada. Veja-se o texto legal:

Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

I - assinatura eletrônica simples:

- a) a que permite identificar o seu signatário;
- b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou 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, com as seguintes características:

- a) está associada ao signatário de maneira unívoca;
- b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;
- c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;

III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

§ 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos.

§ 2º Devem ser asseguradas formas de revogação ou de cancelamento definitivo do meio utilizado para as assinaturas previstas nesta Lei, sobretudo em casos de comprometimento de sua segurança ou de vazamento de dados (Brasil, 2020).

Como se depreende do texto legal, as assinaturas eletrônicas simples são as assinaturas que não estão vinculadas à certificados digitais. Essas assinaturas podem ser representadas, por exemplo, pelo nome do assinador digitado ao final de um texto ou mesmo um clique de aceite em um botão de um site, compreendendo a forma mais simples e menos segura de assinatura eletrônica. Já as assinaturas eletrônicas avançadas possuem vinculação exclusiva ao seu signatário, utilizando biometria - facial, iris, digital - *pin* e permitem identificar alterações de dados nos documentos, no entanto, são passíveis de contestação judicial. Por fim, a assinatura eletrônica qualificada é baseada no Certificado Digital ICP-Brasil, sendo a mais segura das três, gozando de presunção legal de veracidade, ou seja, validade jurídica presumida.

Apesar dos benefícios oferecidos pelas assinaturas eletrônicas, ainda há desafios a serem superados, como a falta de infraestrutura tecnológica adequada em algumas regiões do país e a necessidade de investimentos em treinamento e capacitação para o uso da tecnologia. No entanto, a tendência é que a utilização da assinatura eletrônica/digital cresça nos próximos anos, impulsionada pelo aumento da digitalização de processos e pela busca por maior eficiência e segurança nas transações eletrônicas.

3.4 ARCABOUÇO JURÍDICO DE ASSINATURAS ELETRÔNICAS

A validade jurídica das assinaturas digitais é um tema de extrema importância para a segurança jurídica das transações virtuais. A assinatura digital é uma técnica criptográfica que permite a autenticação e identificação de pessoas e empresas, além de conferir integridade aos documentos virtuais. A sua regulamentação no Brasil é realizada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que estabelece os padrões de segurança e emite os certificados digitais necessários para a realização de atividades online.

A assinatura digital hoje no Brasil é regulamentada por um arcabouço legislativo, uma série de normas, quais sejam: Medida Provisória nº 2.200-2, de 24 de agosto de 2001, Lei do Processo Civil Eletrônico (Lei nº 11.419/2006), Código Civil, Código de Processo Civil, Marco Civil da Internet (Lei Nº 12.965/2014), MP da Liberdade Econômica (Lei 13.874/2019), Decreto nº 10.278/2020, Medida Provisória 983/2020, convertida na Lei da Assinatura Eletrônica (Lei nº 14.063/ Set 2020).

A Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Ela estabelece a validade jurídica da assinatura digital, desde que ela

seja realizada por meio de um certificado digital emitido por uma Autoridade Certificadora credenciada pela ICP-Brasil (Brasil, Medida Provisória 2.200-2/2001).

No Brasil, a Lei nº 14.063/2020, regulamentou o uso da assinatura eletrônica e da assinatura digital em diferentes contextos, reconhecendo a sua validade jurídica. Além disso, o próprio Supremo Tribunal Federal - STF, já se rendeu à era digital, corroborando a validade jurídica das assinaturas digitais, entendendo que elas possuem o mesmo valor que as assinaturas manuscritas, validando essa tecnologia, com a ampliação da AC-JUS - Autoridade Certificadora da Justiça (STF, 2005).

A jurisprudência dos tribunais brasileiros tem se mostrado favorável ao reconhecimento da validade jurídica das assinaturas digitais, em diversos contextos, como na celebração de contratos, na emissão de notas fiscais eletrônicas, na realização de assembleias de acionistas, entre outros, como se verá em detalhes na apresentação de julgados do Rio Grande do Sul, no próximo tópico do estudo. Além disso, a utilização de assinaturas digitais tem se mostrado vantajosa para as empresas, uma vez que permite a realização de transações de forma mais rápida e eficiente.

No entanto, é importante ressaltar que a validade jurídica das assinaturas digitais está condicionada à observância dos requisitos legais estabelecidos pela ICP-Brasil, como a utilização de certificados digitais válidos e a adoção de medidas de segurança adequadas, nos termos da Medida Provisória nº 2.200-2/2001 (Brasil, 2001). Dessa forma, é fundamental que as empresas estejam atentas às normas e regulamentos vigentes, a fim de garantir a validade jurídica das assinaturas digitais utilizadas em suas transações eletrônicas.

3.4.1 O RECONHECIMENTO DA VALIDADE DA CERTIFICAÇÃO DIGITAL PELA JURISPRUDÊNCIA GAÚCHA

No Estado do Rio Grande do Sul, a jurisprudência do Tribunal de Justiça - TJRS reconhece a validade dos contratos e outros documentos assinados com certificado digital. Em 2022, o TJRS confirmou a validade da assinatura eletrônica realizada pelas partes, que seguiu todos os passos exigidos pela Autoridade Certificadora, inclusive com a identificação dos envolvidos, com fotos e a apresentação dos documentos pessoais. A decisão entende que devem ser reconhecidas as assinaturas eletrônicas, mesmo sem certificado digital emitido pela ICP-Brasil, porquanto garantida a devida identidade dos signatários (Rio Grande Do Sul, 2022).

Em 2018, o TJRS já havia destacado não ser necessária a assinatura física para validação do negócio jurídico, sendo plenamente viável a assinatura eletrônica em contratos de mútuo (Rio Grande Do Sul, 2018). Em 2021, o TJRS considerou que os documentos produzidos em forma eletrônica com a utilização de processo de certificação disponibilizada pela ICP-Brasil presumem-se verdadeiros em relação aos signatários (Rio Grande Do Sul, 2021).

Até mesmo contratos de compra e venda de imóveis, cujos valores são expressivos, ao serem assinados com certificado digital possuem validade jurídica plena, desde que atendam aos requisitos legais e o procedimento seja realizado em conformidade com a legislação aplicável. Assim, é possível afirmar que a jurisprudência do TJRS, em consonância com outros tribunais nacionais e mesmo internacionais, tem reconhecido a validade jurídica de contratos assinados com certificado digital, desde que sejam respeitados os procedimentos legais para o uso da assinatura eletrônica.

4 SEGURANÇA DIGITAL E CRIMES VIRTUAIS

A segurança de dados pessoais é um tema cada vez mais relevante na sociedade atual, com o crescente uso da tecnologia e a coleta e compartilhamento de informações pessoais por empresas e governos. A proteção desses dados é fundamental para a privacidade e segurança dos indivíduos, mas também para a prevenção de crimes cibernéticos e a proteção de informações confidenciais. No entanto, essas informações têm valor comercial, e como tal, estão sujeitas aos mesmos destinos de outros tipos de bens de valor.

A Informação é um dos bens mais preciosos da humanidade; aquele que a detém também detém o poder. Dessa forma, os homens sempre irão à busca das informações, infelizmente perdendo, em muitos casos, o escrúpulo e a ética para consegui-las (Cassanti, 2014, p. 12).

A informação é um recurso de valor inestimável para a humanidade, sendo que aqueles que possuem acesso a ela também possuem o poder que ela proporciona. No entanto, em muitos casos, a busca por informações leva as pessoas a abandonarem seus princípios éticos e escrúpulos, colocando em segundo plano a importância de obter informações de maneira responsável e ética. Essas ações questionáveis podem levar a consequências negativas para a sociedade, enfraquecendo a confiança e minando os fundamentos éticos necessários para um mundo equitativo e justo.

As políticas de proteção de dados variam de país para país, e o Brasil conta com a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais - LGPD, que entrou em vigor no ano de 2020 e estabelece regras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais (Brasil, 2018). A lei prevê multas e sanções para empresas que não cumprirem as normas de proteção de dados, buscando garantir a privacidade e segurança dos indivíduos. Diz a lei, já em seu Art. 1º:

Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

A proteção de dados é fundamental para garantir a privacidade e a segurança dos usuários da internet. Além das medidas legais, é importante que as empresas e indivíduos adotem medidas de segurança para proteger seus dados pessoais. De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 2020, é responsabilidade das

empresas garantir a segurança dos dados que coletam (Brasil, 2018). Para isso, é recomendado o uso de senhas fortes e a verificação de configurações de privacidade em redes sociais e sites, além da utilização de softwares de segurança, como antivírus e firewalls. Segundo o Instituto Nacional de Tecnologia da Informação - ITI, é importante também adotar medidas de autenticação forte, como o uso de certificados digitais, para garantir a identidade dos usuários (ITI, 2021).

Mesmo com as medidas de segurança adotadas, a coleta e uso de dados pessoais por empresas e governo pode apresentar riscos à privacidade e segurança dos indivíduos. É importante estar ciente das informações que estão sendo compartilhadas e coletadas, e a conscientização sobre a proteção de dados pessoais é fundamental para manter a confiabilidade nos sistemas de informação online. A Cartilha de Segurança para Internet, publicada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2021), apresenta diversas recomendações de segurança para usuários da internet, incluindo a importância de manter softwares atualizados e evitar o compartilhamento de senhas.

Apesar das medidas de segurança e da conscientização sobre a importância da proteção de dados pessoais, ainda há riscos de crimes cibernéticos. É importante lembrar que os criminosos estão sempre em busca de maneiras de burlar os sistemas de segurança e subtrair dados pessoais e bancários dos usuários. Por isso, é fundamental estar sempre atento e adotar as medidas de segurança recomendadas. O Comitê Gestor da Internet no Brasil - CGI.br e a Sociedade Brasileira de Computação -SBC, promovem discussões e eventos sobre segurança da informação, com o objetivo de conscientizar a população sobre os riscos e as medidas de proteção necessárias (CGI.br, 2021; SBC, 2021).

Em resumo, a proteção de dados pessoais é um tema de extrema importância na era da informação. É responsabilidade das empresas garantir a segurança dos dados que coletam, mas também é fundamental que os usuários adotem medidas de segurança e estejam cientes dos riscos envolvidos na coleta e uso de dados pessoais. A conscientização e a adoção de medidas de segurança recomendadas por entidades como a CERT.br, o ITI, o CGI.br e a SBC são fundamentais para prevenir crimes cibernéticos e garantir a privacidade e a segurança dos usuários da internet no Brasil.

4.1 CRIMES VIRTUAIS E FRAUDES EM ASSINATURAS ELETRÔNICAS

O aumento do uso das ferramentas tecnológicas via internet fez com que os crimes praticados no meio digital também se tornassem cada vez mais frequentes. De acordo com o Relatório de Crimes Cibernéticos do *Federal Bureau of Investigation* (Departamento de Investigação Federal) - FBI - dos Estados Unidos da América (2020, p. 02), "os crimes cibernéticos se tornaram um grande problema para empresas, organizações governamentais e indivíduos. Esses crimes podem ter impactos financeiros significativos e podem prejudicar seriamente a reputação das vítimas". No Brasil, o país ocupa a 2ª posição no ranking mundial de ataques cibernéticos (CERT.br, 2021).

Pois bem, o Código Penal - CP - brasileiro, que entrou em vigor na década de 1940, foi sendo adaptado e alterado ao longo dos anos, para que pudesse abranger os crimes praticados pelo meio virtual, sequer imagináveis na época em que o CP entrou em vigor. Assim, atualmente, o CP dispõe sobre alguns tipos de crimes digitais, tais como, invasão de dispositivos eletrônicos, divulgação de informações privadas e fraudes eletrônicas, previstos nos artigos 154-A, 153 e 171, §2º, respectivamente (Brasil, 1940).

Em 2012 foi aprovada e entrou em vigor a Lei nº 12.737/2012, denominada Lei Carolina Dieckmann, tipificando o crime de invasão de dispositivo informático, que passou a estar previsto no artigo 154-A do CP e foi alterado em 2021, pela Lei nº 14.155. De acordo com a redação atual do dispositivo penal:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Brasil, 2021).

A jurisprudência brasileira tem acompanhado as mudanças no mundo digital, e tem julgado casos relacionados aos crimes digitais, como o uso indevido de informações de cartão de crédito, o acesso indevido a contas bancárias online, e a disseminação de informações falsas na internet. Com o avanço tecnológico, surgem novos desafios para a legislação e a jurisprudência no que diz respeito aos crimes digitais. Entre esses desafios, destaca-se a utilização da inteligência artificial para a criação de imagens e vídeos falsos, conhecidos como *deepfakes*, que podem ser usados para difamação e extorsão.

No entanto, a legislação brasileira ainda não prevê, especificamente, um tipo penal para tal conduta, o que pode dificultar a punição dos responsáveis. De acordo com a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, “os *deepfakes* apresentam novos desafios para a segurança e para a privacidade na era digital, e podem ser utilizados para a difamação, para o assédio, extorsão, fraude e até mesmo na interferência em processos eleitorais” (CERT.br, 2021, p. 26).

A ausência de uma legislação específica para esse tipo de crime pode dificultar a punição de seus autores, como destaca a Sociedade Brasileira de Computação (SBC), SBC (2021). Além disso, a globalização e a transnacionalidade da internet têm gerado problemas em relação à competência e cooperação entre as autoridades de diferentes países. Como se afirma:

Uma das características da Internet é a desterritorialização das relações nela havidas, ou seja, estas não são localizáveis tão facilmente do ponto de vista geográfico. Nesse ambiente são comuns contratações envolvendo diversos elementos de estraneidade, denotando a característica da desterritorialização (Strenger *apud* Piffer e Schonin, 2021, p. 9).

O Brasil tem firmado acordos internacionais para o combate aos crimes digitais, mas ainda enfrenta desafios em relação à aplicação desses acordos na prática. A Lei Geral de Proteção de Dados - LGPD - também é uma importante ferramenta no combate aos crimes digitais, já que estabelece regras para o tratamento de dados pessoais, o que pode ajudar a prevenir o uso indevido dessas informações.

Os crimes digitais são uma realidade crescente no mundo digital, e o Brasil tem enfrentado desafios em relação à legislação e jurisprudência para lidar com essa questão. É importante que a legislação acompanhe as evoluções tecnológicas para que os crimes digitais

possam ser punidos de forma efetiva, e que haja uma cooperação internacional para combater esses crimes.

4.2 CRIMES RELACIONADOS ÀS ASSINATURAS ELETRÔNICAS

A implementação do ICP-Brasil trouxe maior segurança às transações e comunicações eletrônicas realizadas no país, pois antes disso os certificados digitais eram emitidos por diversas autoridades certificadoras privadas, sem regulamentação e sem garantia de que suas práticas de segurança e emissão de certificados fossem adequadas. Além disso, a validação dos certificados era feita por softwares de terceiros que também não eram regulamentados e podiam apresentar falhas de segurança. Segundo o site oficial do Instituto Nacional de Tecnologia da Informação - ITI, responsável pela implementação e gestão da ICP-Brasil:

A Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação de pessoas físicas e jurídicas, provedores de serviços e equipamentos no âmbito do Governo Eletrônico, com o objetivo de 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 (ITI, 2021).

A implementação do ICP-Brasil trouxe maior segurança às transações e comunicações eletrônicas realizadas no país, pois antes disso os certificados digitais eram emitidos por diversas autoridades certificadoras privadas, sem regulamentação e sem garantia de que suas práticas de segurança e emissão de certificados fossem adequadas. Além disso, a validação dos certificados era feita por softwares de terceiros que também não eram regulamentados e podiam apresentar falhas de segurança.

Essa situação tornava as assinaturas digitais pouco confiáveis e sujeitas a fraudes, já que era relativamente fácil falsificar certificados digitais e usá-los para assinar documentos fraudulentos ou se passar por outra pessoa. A falta de padronização e regulamentação na emissão e validação dos certificados digitais também dificultava a interoperabilidade entre diferentes sistemas e aplicativos.

A implementação do ICP-Brasil em 2001 foi um marco importante na história da segurança digital no Brasil, pois estabeleceu uma infraestrutura pública confiável para emissão e validação de certificados digitais. Com a criação do ICP-Brasil, o país passou a ter uma autoridade certificadora raiz governamental e um conjunto de normas e procedimentos para a emissão e validação de certificados digitais. Isso tornou as assinaturas digitais mais

seguras e confiáveis, incentivando o uso da tecnologia em transações eletrônicas e ajudando a garantir a autenticidade, integridade e confidencialidade dos documentos eletrônicos.

4.2.1 CASOS DE FRAUDES EM ASSINATURAS ELETRÔNICAS

Com a crescente utilização de assinaturas digitais em transações eletrônicas, também tem ocorrido um aumento nos crimes relacionados a esse tipo de assinatura. De acordo com o Relatório de Crimes Cibernéticos da Internet - *Crime Complaint Center* (IC3) do FBI, em 2020, foram recebidas mais de 791.790 reclamações de crimes cibernéticos, com perdas estimadas em mais de US\$ 4,1 bilhões (IC3 FBI, 2020).

A assinatura digital é um meio de autenticação que possui validade jurídica, mas como qualquer meio tecnológico, pode ser alvo de fraudes. Nesse sentido, é importante conhecer os tipos de crimes digitais relacionados às assinaturas digitais e como eles são tratados pela legislação brasileira.

Um dos crimes relacionados a assinaturas digitais é a falsidade ideológica, que ocorre quando alguém utiliza uma assinatura digital falsa para se passar por outra pessoa e obter vantagens indevidas. A legislação brasileira prevê pena de reclusão de um a cinco anos para quem pratica esse crime:

Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:

Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular (Brasil, 1940).

Outro crime é a falsificação de documento particular, que também pode ser cometido com o uso de assinatura digital. Esse crime ocorre quando alguém falsifica um documento particular, como um contrato, por exemplo, e utiliza uma assinatura digital falsa para dar aparência de autenticidade. O artigo 298 do Código Penal prevê pena de reclusão de um a cinco anos para quem pratica esse crime. No rastro desse crime, de acordo com o tipo de documento falsificado, as consequências podem ser geometricamente danosas. Por exemplo, nos casos de falsificação de receituários médicos, cujas assinaturas digitais são válidas legalmente. Neste último caso, as consequências são financeiras e contra a saúde pública, tendo consequências até mesmo com a morte de pacientes.

Também é possível que ocorram crimes de invasão de sistemas e roubo de informações para obter acesso às assinaturas digitais de terceiros. Essas práticas configuram crimes cibernéticos previstos na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que prevê pena de reclusão de três meses a um ano, além de multa, para quem pratica crimes dessa natureza (Brasil, 2012).

Caracteriza o crime de estelionato o uso de assinaturas digitais falsas ou indevidas em documentos eletrônicos com a finalidade de obter vantagem ilícita, previsto no artigo 171 do Código Penal (Brasil, 1940). No entanto, é importante destacar que a utilização de assinaturas digitais, quando realizada de forma correta e dentro dos padrões estabelecidos pela legislação, é segura e tem validade jurídica. As fraudes ocorrem quando há falhas nos sistemas de segurança ou quando há má-fé por parte de um ou mais envolvidos na transação.

Para a prevenção de crimes relacionados a assinaturas digitais, é fundamental que sejam adotadas medidas de segurança no processo de autenticação, como a utilização de certificados digitais e a adoção de protocolos criptográficos seguros. É muito importante que as empresas que prestam serviços de autenticação digital sigam as normas estabelecidas pelos órgãos reguladores e estejam em conformidade com a legislação brasileira (ITI, 2021).

Já foram documentados alguns casos envolvendo a fraude em assinaturas digitais e certificados digitais no Brasil. Cumpre destacar um caso referente à suspensão do pagamento de alvarás da Justiça do Trabalho no Rio de Janeiro, após uma suspeita de fraude. O Tribunal Regional do Trabalho da 1ª Região (TRT-1) recebeu uma denúncia de que uma pessoa teria se passado por outra para receber o pagamento de um alvará. A partir dessa denúncia, o TRT-1 decidiu suspender todos os pagamentos de alvarás até que fossem adotadas medidas para garantir a segurança do processo (O Globo, 2022).

Outro caso tornado público referiu-se à descoberta de um trojan (vírus da classe cavalo de troia) brasileiro que possuía um certificado digital falso. Esse trojan, chamado de *SpyEyes*, permitia que os criminosos roubassem informações bancárias das vítimas. A descoberta foi feita pela *Kaspersky Lab*, que identificou que o certificado digital usado pelo *SpyEyes* era falso e havia sido emitido por uma autoridade certificadora brasileira. A *Kaspersky Lab* informou a autoridade certificadora sobre o certificado digital falso e alertou as instituições financeiras brasileiras sobre a ameaça (Tecnoblog, 2012).

4.3 MEDIDAS PREVENTIVAS DE SEGURANÇA

A assinatura digital é um recurso cada vez mais utilizado para validar transações, contratos e outros documentos no ambiente digital. Ela é uma ferramenta segura e eficiente, mas sua efetividade depende do conhecimento e da habilidade dos usuários em utilizar esse recurso de forma correta e principalmente de forma segura.

4.3.1 O DESCONHECIMENTO COMO FATOR DE VULNERABILIDADE

O desconhecimento dos procedimentos e dos meios de confirmação da autenticidade das assinaturas digitais pode ser um fator que leva as pessoas a se tornarem vítimas de crimes dessa natureza. Isso ocorre porque os criminosos podem se aproveitar dessa falta de conhecimento para cometer fraudes e falsificações, uma vez que muitas pessoas não sabem como verificar a validade de uma assinatura digital.

Por exemplo, um indivíduo pode receber um e-mail aparentemente legítimo solicitando que ele clique em um link e faça login em uma plataforma de assinatura digital. Se ele não tiver conhecimento suficiente para identificar possíveis fraudes ou *phishing*, termo que pode ser traduzida em pescaria de dados, pode acabar inserindo suas informações em um site falso e ter suas assinaturas digitais roubadas. A reação retardada aos ataques é decisiva para o sucesso dos criminosos. Veja-se:

No entanto, as ameaças no mundo virtual tendem a ser mais rápidas e sofisticadas que as do mundo real, o que gera um tempo menor de reação por parte do alvo a ser atingido. Por isso, ações de inteligência, baseadas em mecanismos específicos de hardware e software, aliados ao conhecimento humano, podem ser fundamentais à perfeita defesa e à melhor reação, fazendo com que países, organizações públicas e privadas, posicionem-se ou não adequadamente em relação à sua segurança na rede (*cyber security*). (Wendt, 2011, p. 26).

Depreende-se do texto, a fragilidade da vítima das ameaças virtuais (*latu sensu*), por não conseguir acompanhar a galopante velocidade das técnicas avançadas utilizadas para a prática de crimes cibernéticos. Além disso, muitas pessoas não conhecem, ou tratam com desídia os mecanismos de segurança que devem ser adotados para garantir a autenticidade das assinaturas digitais, como a utilização de certificados digitais e senhas seguras. Isso pode levar a situações em que a assinatura digital é facilmente falsificada e usada em transações fraudulentas e criminosas.

Outro problema relacionado ao desconhecimento é a falta de cuidado com o armazenamento de senhas e informações pessoais. Quando esses dados são armazenados em dispositivos inseguros ou compartilhados de forma inadequada, eles podem ser acessados por pessoas mal-intencionadas, e daí para a prática do ilícito.

A falta de conhecimento também pode levar as pessoas a não saberem como agir caso sejam vítimas de crimes envolvendo assinaturas digitais. A falta de informações sobre os procedimentos necessários para denunciar e resolver esses casos pode tornar o processo mais difícil e prolongado. Muitas pessoas podem confundir a assinatura eletrônica com a assinatura digital, que são duas engrenagens diferentes do mesmo mecanismo. A assinatura eletrônica é uma opção mais simples e não requer certificados digitais ou outros recursos adicionais, mas é menos completa do que a assinatura digital, o que pode levar a situações em que a validade da assinatura seja questionada.

O desconhecimento dos procedimentos e dos meios de confirmação da autenticidade das assinaturas digitais é um fator que pode levar as pessoas a se tornarem vítimas de crimes dessa natureza. Por isso, é fundamental que as pessoas busquem informações e conhecimentos sobre essas tecnologias para utilizá-las de forma segura e consciente, evitando maiores problemas financeiros e jurídicos.

4.3.2 CUIDADOS COM O *TOKEN*: CERTIFICADO DIGITAL

O *token* é o dispositivo físico que contém o certificado digital, usado para autenticar as assinaturas digitais (Guelfi, 2007). Se alguém utilizar o *token* de terceiro, de forma criminosa, para assinar um documento digital, sem a autorização ou conhecimento do responsável pelo *token*, evidentemente que este não sofrerá responsabilização penal. No entanto, caso o responsável pelo *token* tenha agido com negligência na proteção do objeto ou tenha compartilhado suas senhas com terceiros, pode ser responsabilizado pelo uso indevido do dispositivo (Compare Certificado Digital, 2020).

De acordo com o site Compare Certificado Digital (2020), é importante que sejam tomadas todas as medidas de segurança necessárias para proteção do *token*. Em caso de perda ou suspeita de uso indevido, deve-se notificar imediatamente a autoridade competente e a instituição que emitiu o certificado digital. A AC (Autoridade Certificadora) pode revogar o certificado digital, para evitar o uso indevido do dispositivo. Recomenda-se que o indivíduo responsável pelo *token* utilizado indevidamente, registre um boletim de ocorrência em uma Delegacia de Polícia Civil ou mesmo através da Delegacia de Polícia Online (a exemplo do

RS), para documentar o extravio do *token* e evitar responsabilização por eventuais crimes cometidos com o dispositivo. Recomenda-se trocar todas as senhas associadas ao *token* de certificado digital, incluindo a senha do próprio dispositivo, caso exista essa possibilidade (Compare Certificado Digital, 2020).

Caso o *token* seja utilizado para acessar sistemas de empresas ou organizações, estas deverão ser notificadas sobre o extravio do dispositivo, para que possam fornecer ao usuário as orientações de segurança recomendadas. O usuário lesado deverá adquirir um novo *token* e certificado digital, a fim de manter sua segurança digital e continuar realizando transações eletrônicas de forma segura (Guelfi, 2007).

Seguindo tais orientações, o usuário do *token* pode evitar que o objeto seja utilizado indevidamente por terceiros e se proteger de possíveis responsabilidades criminais. É importante sempre tomar as medidas de segurança necessárias para proteção do certificado digital, incluindo o armazenamento seguro do *token* e a não divulgação de senhas ou outras informações de segurança.

Veja-se que o *token* é um dos componentes de segurança relacionados à segurança dos documentos digitais e, nesse sentido, considera-se serem vários os cuidados a serem tomados para evitar ser vítima de crimes relacionados à segurança dos documentos eletrônicos, sendo esse um alerta específico ao *hardware* de armazenamento do certificado digital. O comportamento consciente e seguro em relação a todos os componentes é um hábito que deverá ser agregado e absorvido pelos usuários dos sistemas, os quais, com o passar do tempo, perceberão de forma tranquila, dado o costume adquirido (Compare Certificado Digital, 2020).

Os advogados, assim como muitos profissionais, utilizam o *token* como uma ferramenta essencial para garantir a autenticidade e a segurança das suas assinaturas digitais em documentos jurídicos. O *token* permite que os advogados assinem petições, contratos e outros documentos eletrônicos com validade jurídica, assegurando que a identidade do signatário seja verificada de forma confiável. Este dispositivo é especialmente importante no contexto do processo eletrônico, que se tornou padrão em muitos tribunais, facilitando o envio e recebimento de documentos de maneira ágil e segura. Portanto, o uso do *token* é uma prática indispensável para advogados que buscam eficiência e segurança em suas atividades profissionais.

Além de garantir a segurança das assinaturas digitais, o *token* também oferece aos advogados a conveniência de acessar sistemas judiciais e plataformas de forma segura, como

o e-proc e o PJE. Isso é crucial para a proteção das informações confidenciais dos clientes e para evitar fraudes e acessos não autorizados. Os advogados devem estar cientes da importância de proteger seu *token*, adotando medidas como o armazenamento seguro e a mudança regular de senhas. Em caso de perda ou suspeita de uso indevido, é fundamental que os advogados notifiquem imediatamente a autoridade certificadora e tomem as providências necessárias para revogar o certificado digital, evitando assim qualquer responsabilidade por ações realizadas indevidamente com o dispositivo (Compare Certificado Digital, 2020).

5 CONCLUSÃO

A transformação digital é uma realidade cada vez mais presente na sociedade e tem sido amplamente utilizada em diversas áreas, incluindo nas assinaturas eletrônicas e digitais. Essas tecnologias oferecem muitas vantagens, como a agilidade nos processos, a redução de custos e o aumento da segurança. No entanto, assim como qualquer outra tecnologia, elas também podem ser utilizadas para cometer crimes, neste caso, crimes digitais, como fraudes e falsificações.

Os crimes digitais envolvendo assinaturas eletrônicas e digitais representam um grande desafio para as autoridades, uma vez que muitas vezes eles são difíceis de serem identificados e rastreados. É importante destacar que a tecnologia em si não é a responsável pelos crimes, mas sim as pessoas que a utilizam de forma inadequada e mal-intencionada.

Fato a ser combatido é o desconhecimento do cidadão médio a respeito do uso correto das assinaturas digitais. Muitas pessoas não sabem como utilizar essas tecnologias de forma segura e eficiente, o que pode levar a prejuízos financeiros e jurídicos. É fundamental que a população seja educada e informada sobre os riscos e cuidados necessários no uso dessas tecnologias.

A adoção em larga escala das assinaturas eletrônicas e digitais também representa um desafio para o sistema jurídico. É preciso que haja atualização das leis e regulamentações a respeito dessas tecnologias, para que elas sejam cada vez mais reconhecidas como meio legal de autenticação e validação em todos os setores, garantindo assim a obrigatória segurança jurídica entre os negócios entabulados entre as partes envolvidas.

Premente é a necessidade de investimento em tecnologias e infraestrutura que possibilitem o uso seguro e eficiente das assinaturas eletrônicas e digitais. Isso inclui sistemas de segurança robustos, mecanismos de autenticação e identificação confiáveis, e treinamento adequado para o uso dessas tecnologias. É preciso garantir que as assinaturas eletrônicas e digitais sejam usadas de forma responsável e ética, para que os benefícios superem os riscos.

A pandemia da COVID-19, ocorrida no ano de 2020, acelerou ainda mais a transformação digital em diversos setores da sociedade, incluindo as relações jurídicas e os processos empresariais. Com as restrições de distanciamento social, as pessoas passaram a fazer negociações, contratos e transações financeiras de forma remota, o que reforça a importância das assinaturas eletrônicas e digitais como mecanismos de validação jurídica dessas operações.

A pesquisa não exaure a problemática, sugerindo-se que o estudo tenha sequência, com novas abordagens, sendo fundamental que a sociedade, empresas, governos e órgãos regulatórios trabalhem juntos para buscar maneiras de trazer ao público usuário todas as informações necessárias, no intuito de garantir a efetividade e a segurança no uso das assinaturas eletrônicas e digitais. Somente assim será possível aproveitar plenamente os benefícios da transformação digital, sem comprometer a segurança e a privacidade dos usuários. A transformação digital e a adoção de assinaturas eletrônicas e digitais são tendências irreversíveis na sociedade, cabendo a cada um e a todos trabalhar para garantir que essas tecnologias sejam utilizadas de forma segura e responsável.

REFERÊNCIAS

ARMSTRONG, PAUL. **Dominando as tecnologias disruptivas**. Autêntica Business. Edição Kindle. 2019.

BRASIL. Código Penal. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 11/08/2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Lei Carolina Dieckmann. Brasília, DF, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 07 abr. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 07 abr. 2023.

BRASIL, **Lei nº 14.063/2020**. Dispõe sobre o uso de assinatura eletrônica. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 26/05/2023.

BRASIL. **MEDIDA PROVISÓRIA 2.200-2/2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm. Acesso em: 26/05/2023.

BRASIL. Supremo Tribunal Federal. **Tribunais superiores entram na era da assinatura digital**, disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=65821&ori=1>, Acesso em: 26/05/2023.

BRASIL, Supremo Tribunal Federal. **Plenário define que assinatura eletrônica em processo judicial tem validade jurídica**. Notícias STF, Brasília, DF, 08 jun. 2017. Disponível em: <https://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=348424>. Acesso em: 26 mar. 2023.

CASSANTI, Moisés de Oliveira, **Crimes virtuais, vítimas reais**. São Paulo. Editora Brasport, 2014.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para Internet**. São Paulo: NIC.br, 2021. Disponível em: <https://cartilha.cert.br/>. Acesso em: 07 abr. 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Segurança**. São Paulo: NIC.br, 2021. Disponível em: <https://cgi.br/seguranca/>. Acesso em: 07 abr. 2023.

COMPARE CERTIFICADO DIGITAL. **Perdi o token USB com certificado digital, saiba o que fazer**. Compare Certificado Digital, [S.l.], 10 jun. 2020. Disponível em: <https://comparecertificadodigital.com/perdi-o-token-usb-com-certificado-digital-saiba-o-que-fazer/>. Acesso em: 08 abr. 2023.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (CNI). **Transformação digital na indústria: desafios e oportunidades**. Brasília: CNI, 2021.

ROGERS, DAVID L. **Transformação digital: Repensando o seu negócio para a era digital**. Autêntica Business. Edição Kindle. 2017.

FGV. **Transformação Digital no Brasil: Oportunidades e Desafios**. São Paulo: FGV, 2021.

GANDINI, J. A. D., SALOMÃO, D. P. S., JACOB, C., **A Segurança dos Documentos Digitais**. 2001. Disponível em: <https://egov.ufsc.br/portal/conteudo/seguran%C3%A7a-dos-documentos-digitais-0>. Acesso em: 25/02/2023.

GUELFÍ, Airton R. **Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela infra-estrutura de chaves públicas do Brasil - ICP-Brasil**. 2007. Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica da Universidade de São Paulo. São Paulo, 2007.

IC3 FBI. **Internet Crime Report 2020**. Disponível em: https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf. Acesso em 07/10/2023

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Autenticação forte**. Brasília, DF, 2021. Disponível em: <https://www.iti.gov.br/areas-de-atuacao/seguranca-da-informacao/autenticacao-forte>. Acesso em: 07 abr. 2023.

LAWAND, Jorge José. **O Testamento Digital e a Questão de sua Validade**. Belo Horizonte. Editora Dialética, 2021.

MORAES, RAFAEL LUIS. **O Uso da Assinatura Digital em Contratos de Câmbio: Estudo de Caso no Sicredi**. Monografia (Curso de Especialização do Programa de Pós-Graduação Lato Sensu Gestão em Arquivos) - Universidade Federal de Santa Maria/RS. Santa Maria, 2009.

O GLOBO. **Pagamentos de Alvarás da Justiça do Trabalho são Suspensos Após Suspeita de Fraude de Pelo Menos R\$ 4 milhões**. Disponível em: <https://oglobo.globo.com/rio/noticia/2022/11/pagamento-de-alvaras-da-justica-do-trabalho-sao-suspensos-apos-suspeita-de-fraude.ghtml>, Acesso em: 26/05/2023.

PIFFER, Carla e SCHONING, Raquel. **Contratos na Internet e a Transnacionalização dos Consumidores**. Revista Ponto de Vista Jurídico, v. 10, n. 2, p. 25-44, jul./dez. 2021. Disponível em: <https://periodicos.uniarp.edu.br/index.php/juridico/article/view/2649/1355>. Acesso em: 08 abr. 2023.

PINHEIRO, Patrícia Peck, WEBER, Sandra Tomazi, NETO, Antonio Alves de Oliveira. **Fundamento dos Negócios e Contratos Digitais**. Thomson Reuters Brasil, 2019.

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível n. 70078458387**. Apelação Cível. Direito Privado Não Especificado [...]. Apelante: Fundos de Investimentos em Direitos Creditórios da Ind. Exodus I. Apelada: ACF Industria de Plásticos Ltda. Relator: Des. Eduardo João Lima Costa. Porto Alegre, 25 de Outubro de 2018. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa Acesso em: 11/08/2023

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível n. 5002556-84.2021.8.21.0003**. Apelação Cível. Negócios Jurídicos Bancários [...]. Apelante: Luz, V. S. Apelada: Banco Cetelem S.A. Relator: Des. Marco Antonio Angelo. Porto Alegre, 22 de Outubro de 2021. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa Acesso em: 11/08/2023

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível n. 5009243-86.2022.8.21.0021**. Apelação Cível. Locação. Ação de Despejo por Falta de Pagamento [...]. Apelante: de Lima, V. D. Apelada: Verzeletti, G. E. Relator: Desa. Carmem Maria Azambuja Farias. Porto Alegre, 08 de Novembro de 2022. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa Acesso em: 11/08/2023

SCHWAB, Klaus. **A Quarta Revolução Industrial**, São Paulo: Edipro, 2016.

TECNOBLOG. **Surge o Primeiro Trojan Brasileiro com Certificado Digital**. Disponível em: <https://tecnoblog.net/noticias/2012/09/03/trojan-brasileiro-certificado-digital/>. Acesso em: 28/05/2023.

VERAS, Manoel. **Gestão da Tecnologia da Informação**. Rio de Janeiro. Brasport. 2019.

WENDT, Emerson. **Inteligência Cibernética: A (In)segurança Virtual no Brasil**. São Paulo. Delfos, 2011.