IURI FERREIRA BITTENCOURT

DISRUPÇÃO TECNOLÓGICA NOS REGISTROS PÚBLICOS

Londrina – PR

2022

IURI FERREIRA BITTENCOURT

DISRUPÇÃO TECNOLÓGICA NOS REGISTROS PÚBLICOS

Trabalho de conclusão de curso apresentado à Escola de Direito das Faculdades Londrina, submetido ao Programa de Mestrado Profissional em “Direito, Sociedade e Tecnologias”, como requisito parcial para obtenção do título de Mestre em Direito, Sociedade e Tecnologias.

Orientador: Prof. Dr. Fábio Fernandes Neves Benfatti.

Londrina – PR

2022

Dados Internacionais de Catalogação-na-Publicação (CIP)

B624d Bittencourt, Iuri Ferreira.

Disrupção tecnológica nos registros públicos. / Iuri Ferreira Bittencourt. – Londrina: s.n., 2022.

105 f. : il.

Orientador: Prof. Dr. Fábio Fernandes Neves Benfatti.

Trabalho Final [apresentado ao] Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias, 2022.

1. Direito - Sociedade - Tecnologia. 2. Registros Públicos. 3. Certificado Digital. 4. Segurança Jurídica. 5. Blockchain. I. Benfatti, Fábio Fernandes Neves. II. Faculdades Londrina. III. Direito, Sociedade e Tecnologias. IV. Título.

CDD 341.182
CDU 005.591.6

IURI FERREIRA BITTENCOURT

DISRUPÇÃO TECNOLÓGICA NOS REGISTROS PÚBLICOS

Trabalho de Conclusão de Curso, apresentada à Escola de Direito das Faculdades Londrina, submetido ao Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias, como requisito parcial para obtenção do título de Mestre em Direito, Sociedade e Tecnologias, avaliado pela Banca Examinadora formada pelos professores:

_____

Prof. Dr. Fábio Fernandes Neves Benfatti.
Faculdades Londrina
Orientador

_____

Prof. Dr. José Carlos Francisco dos Santos
Faculdades Londrina

_____

Prof. Dr. Jônatas Luiz Moreira de Paula
Universidade Paranaense - UNIPAR

Londrina, 01 de Agosto de 2022.

DISRUPÇÃO TECNOLÓGICA NOS REGISTROS PÚBLICOS

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

_____

Prof. Dr. Fábio Fernandes Neves Benfatti.
Faculdades Londrina
Orientador

_____

Prof. Dr. José Carlos Francisco dos Santos
Faculdades Londrina

_____

Prof. Dr. Jônatas Luiz Moreira de Paula
Universidade Paranaense - UNIPAR

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em nome do título obtido pelo Programa de Mestrado Profissional em Direito, Sociedades e Tecnologias.

_____

Coordenação do Programa de Pós-Graduação

_____

Prof. Dr. Fábio Fernandes Neves Benfatti
Orientador

LONDRINA, 2022.

Este trabalho é dedicado aos meus queridos pais Abner de Lima Bittencourt Ferreira e Maria Sueli Bavia, a minha esposa e meus amados filhos Sophia Palácio Bittencourt e Vicente

(Palácio Bittencourt)

AGRADECIMENTOS

Dedicado a Deus todo-poderoso que me deu a vida e a condição de escrever este trabalho;

Ao meu pai que me incentivou desde o início da minha vida profissional a optar pelo direito, bem como sempre demonstrando a importância do estudo constante para conseguir atingir um objetivo;

Por fim, a minha esposa e meus dois filhos que acompanharam essa trajetória com incentivos constantes para não me deixando desistir.

BITTENCOURT, Iuri Ferreira. **Disrupção tecnológica nos registros públicos**. 2022. 105 f. Trabalho de Conclusão de Curso (Mestrado Profissional em Direito, Sociedade e Tecnologias) - Faculdades Londrina, Londrina – PR, 2022.

RESUMO

Este trabalho decorre da conclusão do mestrado profissional em direito, sociedade e tecnologia das faculdades Londrina, Estado do Paraná, da linha 2, sistema jurídico e desenvolvimento e tecnologias, projeto de pesquisa 1, direito, inovação, tecnologias e desenvolvimentos. Desde os primórdios dos tempos foi possível encontrar vestígios da atividade dos notários, bem como procedimentos embrionários que estavam sendo formado os Registros Públicos. Eles agem na tradução e da vontade da pessoa ao ordenamento jurídico local, prevenindo litígios, armazenando atos jurídicos e conservando-os das intempéries da vida e do tempo, de modo a oferecer segurança jurídica à sociedade. Ocorre que, com advento do avanço tecnológico, vários métodos e protocolos analógicos foram sendo substituídos pelo digital. Sendo assim, também apareceram efeitos colaterais. Destaca-se como um desses métodos e protocolo a jovem tecnologia Blockchain, a qual é uma rede descentralizada que promete também oferecer garantia de integridade e segurança no armazenamento das informações ali inseridas. Além disso, proporciona rapidez no processamento de seus dados no acervo digital. Deste modo, frisa-se o certificado digital que cada dia mais disseminado nas sociedades em todo o mundo. Diante disso, o presente estudo, traça, com singeleza, algumas funções individuais de cada instituto, reflexões e críticas, interessar-se proporcionar ao leitor elementos substanciais sobre cada assunto. Por fim, identificam linhas de convergências e divergências que podem ser melhor explorada pela sociedade, antes dela, sob o efeito do “conto das sereias” tomar direção sem volta e comprometer a segurança jurídica à sociedade.

Palavras-chave: Blockchain. Certificado Digital. Registros Públicos. Segurança Jurídica. Tecnologia - vulnerabilidade.

BITTENCOURT, Iuri Ferreira. **Technological disruption in public records**. 2022. 105 f. Trabalho de Conclusão de Curso (Mestrado Profissional em Direito, Sociedade e Tecnologias) - Faculdades Londrina, Londrina – PR, 2022.

ABSTRACT

This work stems from the conclusion of the professional master's degree in law, society and technology of the faculties Londrina, State of Paraná, line 2, legal system and development and technologies, research project 1, law, innovation, technologies and developments. Since the dawn of time, it was possible to find traces of the activity of notaries, as well as embryonic procedures that were being formed the Public Records. They act in the translation and the will of the person to the local legal system, preventing disputes, storing legal acts and conserving them from the storms of life and time, in order to offer legal security to society. It so happens that, with the advent of technological advances, several analog methods and protocols were being replaced by digital ones. So there were also side effects. The young Blockchain technology stands out as one of these methods and protocol, which is a decentralized network that also promises to offer a guarantee of integrity and security in the storage of the information entered there. In addition, it provides speed in the processing of your data in the digital collection. In addition to this, the digital certificate that is increasingly disseminated in societies around the world is highlighted. Therefore, the present study traces, with simplicity, some individual functions of each institute, reflections and criticisms, in order to provide the reader with substantial elements on each subject. Finally, they identify lines of convergences and divergences that can be better explored by society, before it, under the effect of the "mermaids' tale" taking direction without return and compromising legal security to society.

Keywords: Blockchain. Digital certificate. Public Records. Legal Security. Technology - vulnerability.

SUMÁRIO

1 INTRODUÇÃO

Propõe-se abordar temas inerentes as facetas de algumas novas tecnologias, a cujo impacto nos registros públicos, tanto para melhorar, quanto para pôr em dúvida certas questões relevantes. Estas decorrem do aumento exponencial das relações jurídicas formadas no ambiente digital, aliada a hiper conectividade da sociedade presente. Assim, a preocupação é justamente saber se a ela será bem atendida pelas novas modalidades realizar negócios. Pois, as tecnologias vieram para melhorar a vida das pessoas.

De início, a pesquisa estudará as tecnologias utilizadas para certificação dos negócios jurídicos formalizados na sociedade, tendo como protagonista a atuação dos notários e/ou escribas até os dias atuais. Logo, será abordado breve relato sobre a origem dos Registros Públicos, o qual foi possível percorrer épocas primárias até esbarrar na era da quarta revolução industrial — tecnologia e sociedade da informação. Além disso, de modo a facilitar o entendimento, detalhou-se como é formado o ambiente digital — tanto na esfera física — *hardware,* como também na linguagem binária — *software* — suas, eficiências, fragilidades e obsolescências.

Nelas foram incluídas análises de segurança do ambiente digital e formas para invadir e proteger os softwares — vírus, malwares e protocolos de segurança. Por oportuno, houve também, aprofundamento sobre o tema — Certificado Digital — atingindo sobretudo a figura da autoridade de registro e sua forma de sua atuação, as quais de difícil pesquisa na literatura brasileira.

Com intuito de deixar o presente trabalho mais robusto quanto às inovações tecnológicas, foi possível realizar estudo crítico sobre a arquitetura tecnológica *blockchain*, visando, oportunamente, tecer pontos de confluências e divergências com o instituto dos Registros Públicos.

Por fim, forçoso se fez demonstrar alguns impactos perigosos que as novas tecnologias podem atingir a sociedade se ela as olhar com ceticismo. Com isso, transitou-se sobre os assuntos acima mencionados, proporcionando ao leitor, fortes subsídios para com que ele possa abrir sua mente e refletir sobre os temas deste estudo que, atualmente, está sendo palco de calorosos debates pela comunidade jurídica e tecnológica contemporânea.

Ademais, importante ressaltar que a pretendida pesquisa visa estudar

tecnologias disruptivas que atingem os registros públicos. Será demonstrado que a tecnologia não é somente o que se constrói no mundo digital, mas tudo que abarca modelos e utilidades que possam realizar tarefa ou cumprir obrigações de maneira diferente.

Também abordará se essas novas tecnologias oferecem segurança jurídica à sociedade, bem como se elas são compatíveis e/ou substitutivas aos modelos outrora utilizados. Ademais, ressalta-se alertar à sociedade no que tange a importância de ela ser protegida frente as opiniões disseminadas pelos pseudos especialistas em tecnologias.

Para trilhar o caminho do presente, será analisado desde os primórdios até os dias atuais, de como são certificados determinados negócios jurídicos perante a sociedade, tendo como maestro a atuação dos notários e/ou escribas. Além disso, será demonstrado quais tecnologias eram usadas; como o sistema jurídico brasileiro, atual, é entendido sob este prisma; avaliar como era realizada as solenidades nos negócios jurídicos.

Nesse prisma, não ficarão de fora o certificado digital, *blockchai*n, a preservação dos documentos, a hostilidade do ambiente digital em face ao instituto dos Registros Públicos, além de demonstrar a origem da internet, como ela funciona e como é formada a base de uma sociedade digital contemporânea.

Por fim, serão retratados o que é ciberespaço, desmistificado certificado digital, apontando detalhadamente seu funcionamento, a legislação que o autoriza, bem como suas vulnerabilidades frente ao que ele promete oferecer à sociedade. Além disso, será estudado a figura da autoridade de registro como a do Tabelião de Notas. Assim, traçando, breves comparativos entre ambas funções, de modo a proporcionar subsídios para com que o leitor possa refletir sobre se as tecnologias apresentadas podem conseguir substituir os Registros Públicos ou se aliar a elas.

2 PAPEL DOS REGISTROS PÚBLICOS PARA SEGURANÇA DAS RELAÇÕES JURÍDICAS NA SOCIEDADE CONTEMPORÂNEA

2.1 SURGIMENTO E DESENVOLVIMENTODOS REGISTROS PÚBLICOS

Para saber o que são os Registros Públicos, mister se faz transcrever alguns relatos históricos da atividade notarial (FUJITA; MATHEUS, 2021):

> O conhecimento humano, transmitido inicialmente pela oralidade, atingiu o seu ápice após o descobrimento da escrita, concedendo ao homem a oportunidade de registrar, na história antiga, atual e porquê não dizer na futura, o seu próprio desenvolvimento, permitindo-lhe perpetuar valores, tradições e descobertas, mas também provocar mudanças significativas que certamente farão por alterar o próprio curso da história.
> Sabemos que a linguagem é o meio que utilizamos para transmitir nossas ideias, conceitos, emoções e é classificada de várias formas, pois são expressões puras do próprio homem e, com o tempo, essa comunicação foi adquirindo formas mais complexas, como a fala e, ao seu lado, uma das mais importantes de que temos conhecimento, a escrita, traduzida inicialmente por desenhos descobertos nas cavernas há mais de oito mil anos.
> A história nos remete ao povo sumério, que ocupou os territórios entre os rios Tigres e Eufrates na Mesopotâmia, no quarto milênio antes de Cristo, como sendo aquele que criou a chamada escrita cuneiforme, pois este sistema de comunicação usava a impressão de caracteres sobre uma base de argila, exposta primeiramente ao sol e posteriormente ao fogo, produzindo essa civilização grande atividade literária como poemas, fábulas e códigos com leis, sendo atribuída a eles, portanto, a criação da advocacia.

Nota-se a evolução tecnológica da forma com que o ser humano iniciou a se comunicar. Segue os relatos:

> Quanto ao alfabeto, acredita-se que se iniciou com a escrita semítica, originária da região da Síria e da Palestina nos anos de 1.700 antes de Cristo, e os passos para o alfabeto ocidental tiveram origem no sistema Romano, por volta de 700 anos antes de Cristo, servindo de base aos caracteres gregos que deram origem ao atual alfabeto ocidental, tal como hoje conhecemos, estabelecendo-se, inclusive, a leitura da escrita da esquerda para a direita. Esses eventos da humanidade, dentre outras influências sociais, foram fundamentais para o surgimento da função notarial.
> A atividade notarial, nos dizeres de BRANDELLI (2011, p. 26), é uma criação social, nascida no seio da sociedade com o fim de atender às necessidades e o desenvolvimento das normas jurídicas. O mesmo autor aponta como sendo o mais remoto antepassado do notário, na civilização egípcia, a figura dos escribas, que eram responsáveis pela

> redação e formalização dos atos jurídicos da monarquia e acontecimentos privados. Os escribas, inclusive, são mais conhecidos e relatados na bíblia como homens de cultura diferenciada, que registravam as leis e acontecimentos da vida dos hebreus.
> Já na Grécia, muito próximo da atividade notarial, havia a figura dos mnemons, ou seja, técnicos das memórias, com função de lavrar os negócios jurídicos particulares. Aristóteles, no livro A Política, faz referência a um oficial público, considerando personagem essencial em povos civilizados e bem organizados, mas, é na Roma antiga, o verdadeiro predecessor do notário que conhecemos hoje, chamados de tabeliones, com atividade de lavrar negócios jurídicos, assessorar as partes, guardar e conservar os documentos produzidos e realizados.

Com o surgimento da escrita, interessante notar a mudança da maneira com que o ser humano se comunicava. Os métodos foram se alterando. Isso é inovação tecnológica. Ou seja, maneira de apresentar alternativas diferente e inovadora de realizar uma tarefa. Conforme texto acima nota-se que a sociedade evolui com a presença de soluções inéditas para realizações de ações. Logo, a tecnologia não é somente aquilo que conhecemos no âmbito digital, mas diversas formas de se resolver uma questão. Ademais, segue a continuação da citação acima mencionada:

> Em tempos remotos, a autenticidade dos documentos se dava pela utilização do sinete ou selo real, utilizados pela autoridade para dar veracidade ao documento por ela emitido. O sinete ou selo real, criado também na Grécia antiga, no terceiro milênio antes de Cristo, foi muito usado por reis, imperadores, príncipes e autoridades eclesiásticas para, junto com a sua assinatura, dar autenticidade aos seus decretos, ordens ou mesmo à execução de pena de morte, como ocorreu com Tiradentes, condenado à morte pelo crime chamado, naquela época, de lesa-majestade (traição), por sentença de D. Maria I, com formas e condições a serem aplicadas, como vem descrita na certidão de enforcamento, datada de 21 de abril de 1792, escrita pelo Desembargador Escrivão da Comissão, Francisco Luiz Álvares da Rocha, que certificou e autenticou o estrito cumprimento da sentença dada por Joaquim José da Silva Xavier, o qual deveria ser conduzido pelas ruas públicas, ao lugar da forca levantada na cidade de Vila Rica, no Campo de São Domingos, e nela morreria de morte natural e, depois de morto, lhe fosse cortada a cabeça e o corpo dividido em quatro quartos, de acordo com a narrativa contida no livro O Processo de Tiradentes (TOSTO; LOPES, 2007, p. 240).

Interessante destacar que o anel de sinete era usado pelas autoridades intelectuais para certificar e autenticar determinados documentos, fazendo uma analogia na atualidade com assinatura do Tabelião e o certificado digital.

Segue trecho final da citação:

> Não se pode deixar de mencionar que a autenticidade, contida nos atos jurídicos antigos, praticamente aqueles escritos nos documentos notariais latino-portugueses, não estavam atados apenas na lavra do escrivão, pois tinham formas rígidas a seguir, independentemente da veracidade lançada nos documentos pelos escrivães, sendo uma delas, a oralidade, uma vez que, somente eram considerados totalmente válidos após a leitura destes perante testemunhas, pois, a leitura em voz alta deste tipo de documento ou texto, na presença de pessoas ignorantes ou analfabetas, pressupunha a compreensão de todo o seu conteúdo pelas partes interessadas, dando-lhe, portanto, a chamada autenticidade (DIP; JACOMINO, 2011, p. 51).
> Ainda, na história em Portugal, as Ordenações Afonsinas (1446), Manuelinas (1521) e Filipinas (1603) continham regras embrionárias acerca da atividade notarial. No Brasil, essa atividade é bem evidente ainda no período de seu descobrimento e colonização pelos irmãos Portugueses, e o primeiro ato notarial de que se tem notícia, praticado em solo pátrio, é a carta de Pero Vaz de Caminha endereçada ao Rei de Portugal, narrando com detalhes a chegada em terras brasileiras:
> [...] Senhor:
> Posto que o Capitão-mor desta vossa frota, e assim os outros capitães escrevam a Vossa Alteza a nova do achamento desta vossa terra nova, que ora nesta navegação se achou, não deixarei também de dar disso minha conta a Vossa Alteza, assim como eu melhor puder, ainda que — para o bem contar e falar — o saiba pior que todos fazer. Tome Vossa Alteza, porém, minha ignorância por boa vontade, e creia bem por certo que, para aformosear nem afear, não porei aqui mais do que aquilo que vi e me pareceu. Da marinhagem e singraduras do caminho não darei aqui conta a Vossa Alteza, porque o não saberei fazer, e os pilotos devem ter esse cuidado. Por- tanto, Senhor, do que hei de falar começo e digo: [...]1.
> No período do Brasil-Colônia, como se sabe, a legislação portuguesa era a fonte normativa do Direito Brasileiro, logo, a atividade notarial era regulamentada e obedecia às Ordenações Portuguesas, onde tabeliães eram nomeados pelos reis e investidos de um direito vitalício, o que, em larga medida, contribuiu para o descrédito da atividade, diante das críticas por falta de comprometimento da atividade e alienação das transformações e avanços da sociedade (FUJITA; MATHEUS, 2021, p. 4-5).

De lá para cá, verifica-se que o instituto dos registros públicos é uma inovação tecnológica. Tanto é que o ordenamento jurídico brasileiro o regulamentou pela Constituição Brasileira de 1988, conforme o artigo 236, Caput, da Constituição Federal dispõe que: “Os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público” (CONSTITUIÇÃO, 1988, Online).

Essa delegação vem após aprovação em concurso público, para que, assim, o particular possa exercer função dotada de fé pública. O delegatário intervirá no negócio jurídico e dará vazão à vontade privada, transformando-a em instrumento

jurídico público, autêntico e legal, nos termos da Lei 8.935/1994, art.6, I e II (BRASIL, 1994).

Eles que exercem essa função pública desenvolve seu ofício em um ambiente popularmente chamado “cartórios”. Neste local é construído e armazenado o acervo que compõe os Registros Públicos. Atualmente, com a evolução da sociedade, houve exponencial crescimento do volume das relações negociais decorrentes das instrumentalizações das vontades privadas.

Ocorre que, parcela significante desta fatia é realizada pelos Registros Públicos, tais como: Tabelião de Notas, Protestos, registrador civil das pessoas naturais, imobiliário, registrador de Pessoas Jurídicas e de títulos e documentos.

Os cartórios estão presente em quase todas as fases do ciclo da vida de uma pessoa Brasileira. Pois, nota-se que, desde o nascimento da pessoa natural, casamento e óbito (registro civil das pessoas naturais); aquisição e alienação de bens imóveis (tabelião de Notas com registro imobiliário) separação, divórcio (Tabelião de Notas com Registro Civil); constituição de pessoa jurídica para exercer atividade intelectual (Registro das Pessoas Jurídicas), inventário (Tabelião de Notas, registro civil e imobiliário), dentre outros.

Destarte, certamente, o ambiente digital já é responsável para a construção da história de uma sociedade, pois, além de armazenar dados sensíveis, também oferecem elementos que contém vastas informações que contribuem para definir as características de determinados grupos políticos e sociais.

Para preservar este tesouro histórico construído e armazenado pelos registros Públicos, a Lei impõe que eles devam ser realizados e ancorados no princípio da segurança jurídica, organização técnica, publicidade, autenticidade e eficácia dos atos jurídicos, conforme art. 1º da Lei 8.935/94, sob a custódia do notário e/ou registrador.

Ressalta-se que os registros públicos deverão proporcionar plena segurança para o arquivamento de livros e documentos, nos termos do art. 4º da Lei 8.935/94:

> Art. 4º Os serviços notariais e de registro serão prestados, de modo eficiente e adequado, em dias e horários estabelecidos pelo juízo competente, atendidas as peculiaridades locais, em local de fácil acesso ao público e que ofereça segurança para o arquivamento de livros e documentos (BRASIL, 94, p. 1).

Neste sentido, oportuno trazer considerações reveladas por Rufino Larraud comentadas por Leonardo Brandelli (2007):

> As formas notariais entre nós são sempre documentais, isto é, perpetuam-se no tempo, o que aliás é uma de suas principais características, geradora de segurança e certeza jurídica. (...) têm a importante função de perpetuar no tempo a informação a respeito do ato jurídico celebrado, com o intuito de constituir prova segura dos fatos, propiciando segurança jurídica e fomentando a paz social ao evitar conflitos, ou torna-los mais facilmente resolúveis (LARRAUD apud BRANDELLI, 2007, Online).

Portanto, salutar conhecer o ambiente dos Registros Públicos. Sendo que, atualmente — no ano de 2022 — estão sendo construídos e armazenados por meio físico (instrumentalizado pelo papel), por meio misto(digitalizado) e/ou inteiramente digital(nato-digital).

2.1.1 Reflexões sobre crescimento tecnológico, aumento das informações, preservação dos documentos no âmbito digital dos Registros Públicos

O propósito deste capítulo é trazer breves reflexões sobre a realidade tecnológica, o crescimento do ambiente digital, algumas vantagens e vulnerabilidades, notadamente a luz do armazenamento dos documentos digitais produzidos no âmbito dos registros públicos.

Este fenômeno é real, advém da quantidade de informações processadas diariamente pelas pessoas. Isto é reflexo do crescimento da sociedade, bem como o aumento exponencial das relações jurídicas e informações que o ser humano é submetido diariamente.

Com advento do crescimento populacional e a evolução da sociedade, mister se faz ressaltar o desenvolvimento da tecnologia, de modo a servir como aliada à sua necessidade.

Neste sentido a expansão do ambiente digital está presente em todo o ramo do direito, inclusive nos registros públicos. Por isto, soa importante estudar

alguns de seus reflexos à sociedade. Ela está cada dia mais dependente da tecnologia, como, por exemplo: estudar remotamente, efetuar compras pela internet, conversar com amigos, clientes e família por videoconferência, dentre outros.

Com advento da covid-19, acelerou-se o investimento e o uso tecnológico. A cuja foi responsável em acelerar o investimento e o uso tecnológico tanto para o fomento de pesquisas científicas para descoberta da cura dessa doença, quanto na ampliação de ambientes digitais. Assim como nas execuções de trabalhos e no relacionamento social, interessar-se possibilitar o distanciamento físico das pessoas e evitar a proliferação do vírus.

Neste cenário, dentre várias medidas, o governo brasileiro instituiu por decreto nº 10.497/2020 (referência desta lei) visando inspirar a família, sobretudo as crianças e os jovens, a participarem de atividades, programas e palestras sobre Ciência, Tecnologia e Inovação.

> Institui o Mês Nacional da Ciência, Tecnologia e Inovações.
> O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84,caput, inciso VI, alínea "a", da Constituição,
> D E C R E T A :
> Art. 1º Fica instituído o Mês Nacional da Ciência, Tecnologia e Inovações, comemorado no mês de outubro de cada ano.
> Parágrafo único. Caberá ao Ministério da Ciência, Tecnologia e Inovações a coordenação das comemorações relativas ao Mês Nacional da Ciência, Tecnologia e Inovações, que contará com a colaboração de órgãos e entidades públicos e privados atuantes na área de ciência, tecnologia ou inovação.
> Art. 2º O Mês Nacional da Ciência, Tecnologia e Inovações terá, notadamente, como finalidades:
> I - mobilizar a população, em especial as crianças e os jovens, em torno de temas e atividades relacionados com ciência, tecnologia e inovações, com o intuito de valorizar a criatividade, o desenvolvimento científico e a inovação; e
> II - apresentar a produção de conhecimento e de riqueza, relacionada com a melhoria da qualidade de vida da população, de modo a permitir o debate dos resultados, da relevância e dos impactos das pesquisas científico-tecnológicas, especialmente as realizadas no País, e de suas aplicações.
> Art. 3º Este Decreto entra em vigor na data de sua publicação. (BRASIL - decreto nº10.497, 2020, p. 1).

A transformação digital é presente. Está agindo em todos os lados, inclusive no relacionamento como observamos o mundo. No entanto, não podemos tapar os olhos para seus efeitos colaterais. A sociedade não pode agir pela emoção, mas deverá ser serena, enfrentar e aprender com pós pandemia. Efetuadas essas

considerações, a partir de agora será explorado o ambiente digital e como ele atinge os registros público.

3 TECNOLOGIA NA SOCIEDADE DIGITAL

3.1 AMBIENTE DIGITAL, MANEJAM DOCUMENTOS FÍSICOS E DIGITAIS

Este tema tem forte ligação com os registros públicos, pois o delegatário além de utilizar essas ferramentas para seu labor, também deverá proporcionar segurança jurídica à sociedade.

Por ocasião do exercício da atividade delegada, os notários e registradores manejam documentos físicos e digitais. Aqueles é definido por Maria Helena Diniz, Curso de direito civil brasileiro: teoria das obrigações contratuais e extracontratuais. São Paulo: Saraiva, como sendo: "*representa um fato, destinando-se a conservá-lo para futuramente prová-lo sendo esses documentos particulares os efeitos mediante atividade privada, como por exemplos as cartas, telegrama, fotografias, fonografia"* (DINIZ, 2002, p.192-193).

Os documentos digitais (nato-digital) diferem dos físicos, pois são registrados em uma base de dados inteiramente eletrônica. Eles são compreensíveis por um sistema de informação que interpreta os comandos binários (0/1), ou seja, para a máquina computacional entender um comando é necessário intermediário para ler as informações: leitor.

Além desses dois modelos, também haverá os mistos, ou seja, os construídos de maneira analógica, porém transportados para um ambiente digital por intermédio da digitalização, escaneamento. Esse documento físico é replicado para o ambiente eletrônico e/ou digital, tendo seu original conservado no modo físico.

Diferentemente do documento físico (papel), o digital é construído em um ambiente que compõe hardware e software, este é a parte lógica do computador, ou seja, os sistemas operacionais, aquele é a parte mecânica, ou seja, são peças, periféricos e equipamentos físicos que fazem o computador funcionar: processadores, dentre outros.

No que tange esse ambiente, o ramo da ciência que estuda esta matéria é o da tecnologia e segurança da informação. Assim, com intuito de trazer breves considerações sobre este assunto, sem esgotar o tema e nem a pretensão de aprofundar, exploraremos separadamente o que é *hardware* em seguida *software.*

3.2 PARTE FÍSICA - OBSOLECÊNCIA E OXIDAÇÃO

Composto pelas peças físicas do computador: processador, HD, memória RAM, placa-mãe, placa de Vídeo, periféricos, etc. Eles contêm forte uso da nanotecnologia, pois, basta notar os lançamentos dos novos modelos de hardware (cada vez menores e mais rápidos) sendo ofertados ao mercado.

É inegável que a inovação tecnológica facilita a vida das pessoas. Ela traz rapidez e agilidade em diversas operações negociais, médicas, educacionais, científicas, etc. O avanço da tecnologia também traz longevidade vital ao ser humano, quesito importante para considerá-la indispensável à vida das pessoas.

ão se pode ignorar que a tecnologia utilizada indiscriminadamente pode gerar sérios prejuízos à sociedade. O hardware é considerado por diversos autores como cérebro do computador CPU (central de processamento de dados), vejamos segundo Norton (1996):

> A unidade central de processamento, ou CPU (Central *Processing Unit*) é o local onde os dados são manipulados. Ela pode ser imaginada como o cérebro do computador. Em um microcomputador, toda a CPU está contida em um minúsculo chip chamado microprocessador, que não é maior do que uma unha. (NORTON, 1996, p. 113).

Esta peça física chamada “microprocessador” é integrante do hardware. Ele passa por constantes transformações ao longo dos anos, conduzido pela evolução tecnológica da computação. Novos chips são lançados nos mercados, substituindo os antigos com mudanças robustas de tecnologias. Como exemplo trago o citado por Null (2006, p. 173): “dentro de poucos anos, chips AMD e Intel Core 2 Duo estarão fora do contexto. Isso porque a tecnologia multicore (vários núcleos) está apenas dando seus primeiros passos”.

No ano de 2006 a tecnologia *multicore* era novidade, conforme se depreende na pesquisa abaixo:

> Conforme a tecnologia dos processadores foi progredindo, o tamanho de seus transistores foi diminuindo de forma significativa. Contudo, após o lançamento do Pentium 4, eles já estavam tão pequenos (0,13 micrômetros) e numerosos (120 milhões) que se tornou muito difícil aumentar o clock por limitações físicas, principalmente pelo superaquecimento gerado. A principal solução para esse problema veio com o uso de mais de um núcleo ao mesmo tempo, através da tecnologia multicore. Assim, cada núcleo não precisa trabalhar numa frequência tão alta. Se o esquema de escalonamento de tarefas funcionasse de maneira eficiente, seria possível trabalhar com quase o dobro do clock. (...). Portanto, com o advento do processador multicore. Intel Core. Em 2006, a Intel inicia a sua linha Core, para consumidores que precisam de mais poder de processamento. Faz parte dessa linha o modelo Core 2 Duo, que demonstra uma capacidade incrível se comparado com os dual-core anteriores da empresa (ARRUDA, 2011, p. 1).

Ocorre que, já no ano de 2020, dificilmente encontra-se alguém utilizando-a. Ademais, destacam-se que eles são construídos por materiais frágeis de plásticos e metais. Embora sejam eficientes, não se pode negar que sofram o efeito do tempo: oxidação.

Os documentos digitais se forem construídos e/ou conservados em um hardware deverão ser tratados com muito cuidado, pois haverá diversas intempéries que poderão depreciá-los e desatualizados, como exemplo o tempo, oxidação e a obsolescência.

Neste contexto, acentua-se a obsolescência, pois com a velocidade da transformação tecnológica as máquinas que compõe os computadores são rapidamente substituídas em um pequeno espaço de tempo por novas tecnologias, deixando-as, outrora utilizadas, obsoletas. Sendo que, por exemplo, uma máquina que produziu um documento digital há 5(cinco) anos, hoje pode ser ultrapassada, entretanto, ela ainda pode estar ativa e produzindo documentos, ocasionando risco à sua preservação.

Assim, não ocorrendo a substituição permanente do hardware haverá incompatibilidade de tecnologia, impossibilitando a transição dos dados de maneira segura à nova tecnologia. Este fenômeno poderá ocasionar graves riscos à conservação do documento digital produzido pela tecnologia ultrapassada.

Não é novidade dizer que quanto mais se usa uma máquina eletrônica e por um longo tempo, mais se desgastará. Também será considerado os problemas decorrentes de sua manipulação constante, frequência de uso e os próprios defeitos de fabricação, diminuindo a vida útil do suporte. Por conseguinte, tudo que estiver

eventualmente armazenado poderá ser danificado ou perdido.

3.3 PARTE DIGITAL - LINGUAGEM BINÁRIA

Este elemento faz parte do ambiente digital. Ele será responsável pela leitura do conteúdo processado pelo hardware. Observemos o que diz a literatura da informática, (WAZLAWICK (2015, p.15): "*Software: são compiladores, drives e componentes do sistema operacional. São constituídos pelos programas que lhe permitem atender as necessidades dos usuários no processamento e armazenamento da informação".*

Ademais, salutar definir sistema operacional, segundo Fernando Castro Velloso (2017, p. 21): "é o conjunto de rotinas que oferece serviços aos usuários; programa de grande complexidade responsável por todo funcionamento de uma máquina desde o software até o hardware instalado, Ex: Windows, Linux"

Além desses conceitos transcreve-se o disposto na Lei do Software em seu artigo 1º da Lei 9.609/98:

> **Art. 1º** Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados (BRASIL - Lei 9.609/98, 1998, p. 1).

Isso permitirá que se obtenha breve noção de como é desenvolvida para proteger e invadir as informações construídas e armazenadas no ambiente digital.

No período pré-internet, os computadores se comunicavam em rede por intermédio de cabeamento. Com avanço da tecnologia, surgiu a internet permitindo que os computadores pudessem se comunicar por servidores centrais, os quais fazem as conexões entre diversos computadores.

Os servidores são espalhados pelo mundo de modo a armazenar o tráfego das informações captadas pelos computadores. Desse modo, os dados circulam na internet sem grande controle.

Os programas de computadores são desenvolvidos pelos programadores a fim de atender a necessidade do usuário. Eles são construídos por intermédio de várias linguagens de programação.

Migrou-se da máquina de escrever para os primeiros computadores do varejo com acesso às impressoras. Ocorre que, essa tecnologia era onerosa. Poucas serventias extrajudiciais utilizavam sistemas de informática próprios. No entanto, com advento do aumento das normas estaduais relacionadas aos cartórios extrajudiciais, não sobrou espaço para ignorar a necessidade de a serventia utilizar sistemas de programação com intuito de agilizar o serviço e atender as orientações das corregedorias, decorrente poder fiscalizatório insculpido no art. 236 da Constituição Federal.

Há época, gerou-se a necessidade de as serventias contratarem programas — sistema software — construído pela linguagem *"clipper"*, a qual operacionalizada pelo sistema *DOS*. Na ocasião, esta linguagem — *clipper* — era a mais evoluída e utilizada. Assim, a maioria dos sistemas oferecidos no mercado possuía a sua arquitetura, pois atendia as necessidades do usuário.

Com o avanço da internet, surgi o sistema operacional *Windows* substituindo o *MS-DOS,* sendo, portanto, o principal sistema da *Microsoft*, pois sua interface se adaptou melhor a outras linguagens e compiladores como *Delphi*, *Visual Basic* e *Powerbuilder.* Embora parte do código *MS-DOS*, por conseguinte, do *Clipper*, eram os que dominavam o mercado na década de 90, na de 2000 já não eram mais, pois se tornaram obsoleta.

A problemática foi em substituir o acervo das serventias extrajudiciais construídos na linguagem antiga para as em novas que foram surgindo. Com crescimento no ambiente da internet o sistema operacional *Windows* foi se tornando base para o desenvolvimento de novos softwares. Assim, serventias que utilizavam o sistema *clipper,* foram obrigadas a migrar para outra linguagem com arquitetura mais avançada (*Delphi)*. Em decorrência disto, houve a necessidade da transição entre o banco de dados construído em uma linguagem para outra. Isso geraria um alto risco em danificar os dados outrora armazenados.

Como, por exemplo, demandaria perícia do programador para implantar o novo sistema diante de incompatibilidades de linguagem, ocasionando, portanto, um alto custo operacional e o risco de perder parte das informações. Assim, nessa operação, para não correr esse risco, muitas serventias, eventualmente, poderiam construir seu acervo documental também em ambiente físico, ou seja, compreendendo a forma híbrida de materializar seus documentos impressos — livros físicos e mídias digitais.

Assim, mesmo se não fosse possível fazer o transporte do banco de dados entre os sistemas, as informações não se perdiam, pois, havia cópias redundantes tanto em documentos físicos, quanto em digital. Ambos documentos poderiam ser usados simultaneamente, possibilitando, portanto, emissões de certidões no acervo antigo e operação do trabalho contemporâneo no sistema novo.

Isso demonstra a importância do formato híbrido para construção de documentos. A depender dos documentos a serem construídos, não soa prudente a sociedade se tornar refém de uma única tecnologia, exemplo: as puras digitais — nato-digital. Ademais, a realidade é que haverá modificações nas realizações das tarefas em decorrência da inovação tecnológica, sendo assim, a sociedade deveria se ater a métodos preventivos, como o sistema híbrido nas construções de documentos e/ou de redundância.

Os sistemas de programação — *software* — possuem diversas modalidades de linguagem. Elas surgem e se modificam na mesma velocidade da evolução tecnológica, assim como o *hardware*. Cada época é apresentada nova linguagem com a promessa de ser mais eficiente. No entanto, nem sempre serão compatíveis entre si, o que pode gerar insegurança à preservação da documentação por ela construída.

Por esse motivo surgiu a política mundial para fomentar a interoperabilidade entre os softwares. Neste sentido, Santos (2011), trata muito bem do assunto em seu artigo científico ao definir o que é interoperabilidade:

> **Define-se interoperabilidade** como sendo a capacidade de sistemas computacionais operarem e cooperarem mesmo na presença de diferentes representações de dados e protocolos de comunicação (CAFEZEIRO, 2008). Segundo Lichun Wang (2005), interoperabilidade determina se dois componentes de um sistema, desenvolvidos com ferramentas diferentes, de fornecedores diferentes, podem ou não atuar em conjunto. Para BISHR (1997), interoperabilidade é a capacidade que um sistema possui de compartilhar e trocar informações em aplicações. Segundo Lichun Wang (2008), interoperabilidade é a habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, software e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados.

Essa categoria de instituto é como se fosse um incentivo às nações adotarem um idioma universal, em que, ao menos, sejam compreensíveis entre si, a

fim de fomentar a maior intercomunicação entre os povos de diferentes línguas.

> A interoperabilidade de tecnologia, processos, informação e dados é condição vital para o provimento de serviços de qualidade. A interoperabilidade entre os mais variados sistemas autônomos permite operar em colaboração, aumentando a produtividade e reunindo esforços, rumo ao objetivo da qualidade total nas organizações. Além disso, ela oferece condições de racionalizar investimentos em Tecnologia da Informação, por meio do compartilhamento, reuso e intercâmbio de recursos tecnológicos (CUNHA, 2005). A interoperabilidade, que já chamava atenção dos profissionais da computação, passou a representar um ponto crucial após o advento da internet, que acelerou o intercâmbio de informações e eliminou fronteiras antes intransponíveis (CAFEZEIRO, 2008). Os problemas atuais da informática e do uso da Internet são muito mais uma consequência de uma evolução extremamente rápida, e por isso não ordenada, do que de uma falta de tecnologia para resolvê-los.

Por conseguinte, depreende-se a importância da interoperabilidade dos sistemas de software. Isso irá possibilitar as diversas linguagens binárias conversarem entre si, trazendo, portanto, agilidade e democratizando-as à sociedade. Nesse sentido:

> Diante destas evoluções, o desenvolvimento de sistemas se tornou uma encruzilhada tecnológica. Dispomos de uma infraestrutura nunca antes imaginada, mas ainda não dispomos de sistemas que utilizem todo este potencial. Sistemas que se possa integrar com outros que já foram desenvolvidos utilizando produtos tecnológicos distintos, plataformas e arquiteturas até então incompatíveis (CAMPOS, 2006). Interoperabilidade não é somente integração de sistemas nem somente integração de redes. Não referencia unicamente troca de dados entre sistemas e não contempla simplesmente definição de tecnologia. É, na verdade, a soma de todos esses fatores, considerando também a existência de um legado de sistemas e plataformas de hardware e software instalados. Parte de princípios que tratam da diversidade de componentes, com a utilização de produtos diversos de fornecedores distintos. Tem por meta a consideração de todos os fatores para que os sistemas possam atuar cooperativamente, fixando as normas, as políticas e os padrões necessários para consecução desses objetivos (SILVA, 2005) (SANTOS, 2011, p. 40-41).

Nota-se que ela é crucial para o desenvolvimento tecnológico e inovador, pois proporcionará com que o produto — software — possa ser reaproveitado por outro produto tecnológico inovador, ocasionado, dessa maneira, grande economia de tempo e dinheiro. Justamente, por esse motivo que a legislação brasileira incorporou essa tendência mundial em nosso sistema jurídico, destacando-

a como objetivo a ser seguido, conforme o Marco Civil da internet, Lei n.º 12.965, de 23 de abril de 2014, em seu artigo Art. 4º:

> Art.4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e **a interoperabilidade** entre aplicações e bases de dados (BRASIL, 2014, p. 1).

Assim, o sistema jurídico brasileiro está sendo ajustado para regulamentar esta importante missão com objetivo de construir um ambiente digital no âmbito do Poder Judiciário e extrajudicial que possam conversam entre si.

3.4 PROTEÇÃO DAS INFORMAÇÕES – CRIPTOGRAFIA

Na ciência da criptografia há protocolos que contribuem para proteger documentos no tráfego digital, dentre eles, citam-se os elencados pelo Dr. Marcos. A. Simplício Junior, da Univesp (2019, Online).

> Há diversas formas de proteger os conteúdos produzidos no ambiente digital. Dentre elas, faz se necessário dividir em algumas facetas:
> a) Disponibilidade: controle de acesso físico e redundância;
> b) Confidencialidade: acesso à informação (criptografia)
> c) integridade: detectar se houve alteração na informação;
> d) autenticidade: detectar a autoria da mensagem; e) irretratabilidade: o agente, após emitir uma mensagem, não pode negar que emitiu (assinatura digital) como se fosse um carimbo digital.

Essas são algumas facetas, dentre várias, que servem para evitar ataques, intrusos, queda do sistema, modificação em sua base, ou danificação onde são armazenadas as informações. É importante ressaltar, que a maioria dos estudiosos enxerga que o sistema computacional é seguro, entretanto, não é protegido das ações humanas.

O alvo será o próprio ser humano. Ex: um sistema protegido por criptografia, sendo quase impossível acessá-lo, no entanto, o ser humano consegue capturar a criptografia de alguém, logo terá acesso a todo banco de dados.

A propósito criptografia é definida por Tanenbau (1994) citado na obra de Zaniolo (2021):

> [...] criptografia é originário das palavras gregas que significam *escrita secreta.* No estudo da criptografia, é comum distinguir *cifra* e *código. Cifra* é uma transformação de caracteres por caracteres ou de *bit* por *bit*, sem levar em conta a estrutura linguística da mensagem. O *código*, por sua vez, substitui uma palavra por outra palavra ou símbolo, todavia não é mais usado, muito embora tenha um passado glorioso, a exemplo da utilização, pelas Forças Armadas dos estados Unidos na Segunda Guerra Mundial, por meio de índios navajos, que se comunicavam uns com os outros usando palavras navajos específicas para termos militares [...]. (ZANIOLO, 2021, p. 534).

Essa ciência da escrita permite com que ela circule e impeça que terceiros, ou o público, leiam mensagens secretas.

Além do quesito “ser humano”, as criptografias também são quebradas por sistemas — software — desenvolvidos especificadamente para este fim.

Um evento histórico interessante é a Cifra de Cesar. Nas guerras da Gália, Júlio César enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem criptografada e incompreensível para o inimigo.

Muito embora à época essa modalidade era eficiente, não se pode ignorar que em pouco tempo foi descoberto a chave para decifrá-la. Em seguida, foram sendo aprimorado novos códigos de criptografia, mas também, em paralelo, novas técnicas para quebrar suas cifras, ou seja, o ciclo de vida que oferece rigidez às criptografias é curto e dinâmico.

A criptografia está presente nos registros públicos, pois, atualmente, contamos com as famosas chaves públicas, as quais foram instituídas pela MP 2200/2001 (BRASIL, 2001). Neste sentido, ela é conceituada segundo Stallings (2008):

> A criptografia assimétrica, mais conhecida como criptografia de chave pública, utiliza um par de chaves denominadas chave privada e chave pública. Qualquer uma das chaves pode ser usada para criptografar os dados, porém a mesma não pode ser usada para, decifra-lo, ou seja, se a criptografia for realizada com chave púbica, somente a respectiva chave privada poderá decifrar, ou vice-versa. Para que este tipo de criptografia obtenha sucesso é fundamental que a chave privada seja mantida em segredo, enquanto a chave púbica pode, e deve ser divulgada a outros usuários, que desejam se comunicar. (STALLINGS, 2008, Online).

Na prática, ela funciona no ambiente dos registros públicos da seguinte forma: primeiramente, para adquirir o certificado privado, o delegatário deverá entrar em contato físico e/ou virtual com representante de alguma unidade certificadora AC e entregar seus documentos pessoais para autoridade de registro (AR). Ela fará seu cadastro e entregará seu certificado com validade entre 1 a 3 anos.

De posse de seu certificado, o delegatário no exercício de sua profissão poderá produzir documentos digitais. Logo, assim com que o delegatário produzir o documento, submeterá à autoridade certificadora — ICP-Brasil — infraestrutura de Chaves Públicas que assina e lacra o documento com criptografia, a fim de possibilitar seu trânsito com segurança pela internet.

Este preparo do documento confeccionado pelo delegatário, consiste em disponibilizar uma chave privada personalíssima ao notário. Ela será usada para decifrar o algoritmo criptografado pela chave pública que transitou pela internet.

A partir desse procedimento, a rigor, o documento adquiri confidencialidade, integridade, autenticidade e irretratabilidade. Nota-se que este processo é realizado no ambiente digital por intermédio de um computador.

Na ocasião do documento transitar pela internet, em tese, estará seguro por criptografia, o qual somente poderá ser aberto pela chave privada do delegatário — certificado digital.

Este Certificado que contém a chave privada é logado ao computador de seu proprietário, combinado com uma senha pessoal tornando possível a abertura do cadeado que protege o documento ora recebido.

Quanto a vulnerabilidade da autenticidade da autoria do documento produzido, indaga-se: curioso é que a autoridade certificadora somente realiza avaliação da autoria no período de 1 a 3 anos — quando vence o certificado. Ou seja, presumem-se que a autoria dos documentos fora assinada pelo delegatário.

Durante este período, outra pessoa poderá assinar o documento

público se passando pelo delegatário. Um funcionário mal-intencionado pode facilmente copiar a senha pessoal, o leitor do Token e realizar os atos que quiser.

Imaginem hipoteticamente o delegatário pluga seu certificado — *Token* — em seu computador e anota sua senha pessoal no monitor, em seguida entra em coma. Após três (03) anos, um dia antes de vencer o certificado, ele volta do coma e se apresenta a uma autoridade certificadora para renovar seu certificado. Assim, presumem-se que todos os atos realizados por esse período foram praticados pelo delegatário. Portanto, nota-se falha na autenticidade da autoria.

Por outro lado, é salutar ressaltar que a chave-pública é responsável pela transformação do documento em código. Este é figurado por um cadeado que contém criptografia para retornar seu estado de documento. Assim, será transformado em um código secreto, o qual é somente decifrado pela chave-privada que detém a cifra criptográfica de posse do delegatário (certificado digital). Logo, em tese, o documento se torna seguro apenas para trafegar pela internet.

Constatemos o que diz Diego Aranha (2018), sobre esse a criptografia e a inviolabilidade das urnas eletrônicas:

> A segurança depende diretamente da qualidade do software de votação e de sua resistência contra manipulação por agentes internos e externos. A principal crítica da comunidade científica é que essas variáveis tornam praticamente impossível estabelecer o nível de segurança — ou de insegurança. Portanto, deveria haver um mecanismo adicional, um registro físico conferível pelo eleitor, para eliminar a dependência dessas variáveis. O que sabemos é que, em todos os testes públicos de segurança realizados pelo TSE até hoje, foram encontradas vulnerabilidades graves, que afetavam tanto o sigilo do voto quanto a integridade dos resultados. Isso ocorreu mesmo com obstáculos e restrições burocráticas impostos aos investigadores e mesmo sem que os investigadores tivessem conhecimento completo do funcionamento do sistema de votação em seus mínimos detalhes, conhecimento esse que acreditamos ser do domínio apenas de alguns técnicos da Justiça Eleitoral, mesmo porque o código é gigantesco — mais de 24 milhões de linhas. (ARANHA, 2018, p. 1).

Evidencia-se, pois, mesmo sendo adotada a criptografia ainda é possível a discussão sobre a autenticidade e autoria dos documentos, sendo, inclusive, sugerido pelo autor mencionado acima, por precaução, cópia redundante física.

3.5 RISCOS, INTRUSOS, VÍRUS, MALWARES

São programas que circulam nos ambientes digitais, Ulbrich (2009), citado por Zanioli (2021):

> Vírus de computador é um software malicioso que se aloja em determinado sistema, infectando-o: são microscópios, reproduzem-se sozinho, consomem recursos computacionais que não lhes pertencem e têm alta capacidade de infecção por contágio (...). Um vírus de computador possui objetivos muitos claros: infectar o máximo possível de sistemas, reproduzir-se rapidamente e opcionalmente consumir recursos e danificar os sistemas invadidos. (ULBRICH apud ZANIOLI, 2021, p. 555):

É muito comum sua circulação pela internet. Quase que diariamente há notícias que determinado sistema invadido por algum vírus, causando prejuízos à sociedade de grande monta, vejamos:

> **a) Vírus**: é um programa que é anexado a um outro programa, a fim de alterá-lo conforme sua configuração;
> **b) Worm**: ele também tem as características de vírus, mas ele se propaga a diversos outros computadores;
> c**) Cavalo de Tróia**: Programa que faz algo útil, porém esconde malícias. Ele é fácil de ser instalado nos computadores, pois podem ser representados por algum antivírus e/ou versão pirata de algum software, etc;
> **d) Backdoor(trapdoor**): o próprio construtor do software permite acesso não autorizado a alguma funcionalidade possibilitando roubo de senhas; Na própria programação é deixada uma lacuna misteriosa para esse fim. Ex: NSA – caso SNOWDEN – A NSA (National Security Agency) construiu sistema vulnerável de propósito a fim de espionar seus usuários;
> **e) Rootkit**: grave – ele tem acesso e controle até de seu antivírus;
> **f) Keylogger**: ele rouba senhas nos toques registrados nos teclados;
> **g) Ransomware**(sequestrador de dados) – ganhou notoriedade em 2017. Ex: ele cifra os dados e extorque a pessoa pedindo dinheiro para decifrá-los**;**
> **h) Exploração do dia zero**: exploram vulnerabilidades recém descobertas, ainda não inclusas em antivírus (SIMPLÍCIO JUNIOR, 2018, Online).

Esses exemplos são algumas das modalidades de malware. Eles podem invadir sua máquina e causar sérios danos. Conquanto existem esses vírus, não se pode ignorar as metodologias preventivas para evitar que eles atinjam os computadores. Para essa proteção, há antivirus, firewall, proxy, honeypots, backup, dentre outros. Essa metodologia decorre dos protocolos de segurança elencados nas

normas da família ISO (organização internacional de normatização) 27000 — ABNT NBR ISO/IEC27701:2019.

Em relação às reflexões sobre a preservação dos documentos no ambiente digital e registros públicos, concluem-se que por muitos anos os registros públicos eram construídos pelo método analógico. Ou seja, os delegatários praticavam seus atos por intermédio do ambiente físico: papel. Com avanço da tecnologia iniciou-se a utilização do ambiente digital no labor de seus ofícios.

Neste novo formato, os delegatários tiveram que se adaptar, ressaltando a importância de que todos os atos por eles construídos estarão sob suas custódias, visando construir segurança jurídica à sociedade.

Esse ambiente de trabalho digital compõe-se por dois principais elementos: hardware e Software. Aquele, trata-se de componentes físicos e periféricos que integram o computador. São erigidos por peças metálicas e plásticas, as quais sofrem os efeitos da oxidação, desgaste natural do uso, bem como eventuais defeitos de fábrica.

Esses efeitos podem repercutir negativamente à produção e ao armazenamento dos atos praticados pelos delegatários. Portanto, imprescindível serem tratados com muito cuidado.

Quanto ao Software, destaca-se que fará a parte lógica do computador. Ele realiza a leitura do conteúdo processado pelo Hardware. É como se fosse uma pessoa que detém perícia da linguagem adequada para traduzir a informação ali veiculada.

Esse elemento é produzido por programadores, os quais utilizam-se de vários formatos de linguagem. Elas podem ser compatíveis ou incompatíveis entre si. Além disso, salientam-se que tanto o Hardware, quanto o Software, ambos sofrem os efeitos da obsolescência, os quais decorrem da velocidade da evolução tecnológica. Esse efeito mostra-se danoso e também pode comprometer os atos e as informações armazenadas nos registros públicos.

Ademais, a fim de minimizar os riscos produzidos pelo ambiente digital, importante conhecer alguns dos Malware. Eles são programas maliciosos feitos para invadir sistemas, visando os mais diversos objetivos. Segue alguns exemplos: Vírus, *Worm*, Cavalo de Tróia, *Backdoor, Hootkit, Keylogger, Hansonware* e, o pior de todos, Explorador do dia Zero.

Para isso, soa salutar o operador do ambiente digital saber a

necessidade de seguir rigorosos protocolos de segurança, tais como: antivirus, firewall, proxy, honeypots, backup e demais arrolados nas normas ISO da família 27000 que compõem padrões técnicos de um sistema de segurança da informação.

Notabiliza-se que, embora os delegatários fossem profissionais do direito, não se podem ignorar que suas atividades estão submetidas a novidades tecnológicas. Na prática de seu ofício, custodiam-se os atos por eles elaborados. Logo, indispensável saber o terreno que estão trilhando. Sendo assim, poderão garantir a preservação dos documentos originais para com que suas respectivas interpretações sejam fidedignas.

4 CERTIFICADO DIGITAL E BLOCKCHAIN

4.1 CERTIFICADO DIGITAL: ASPECTOS HISTÓRICOS

Este estudo traz ao leitor informações relevantes sobre Certificado Digital, o qual está sendo utilizado em larga escala no mundo e no Brasil. Sobretudo, será abordado seu conceito, objetivo, finalidade e demais para melhor compreensão.

Para tal, além da ciência jurídica, importante se fez sobrevoar o campo da ciência da informação e tecnologia, para que ambas possam contribuir com subsídios sobre o assunto.

Ademais, foi possível encontrar alguns elementos no direito comparado elencados no decorrer. Assim, para não ficar de fora, é importante analisar como a sociedade era servida sem os certificados digitais, traçando, oportunamente, um paralelo com certificação promovida pelos Registros Públicos pela figura do Tabelião de Notas e as empresas privadas.

O certificado digital é apresentado por dois modelos de certificações — Certificado Digital Privado e o Certificado Digital Notarial Público. Para facilitar o entendimento, ambos serão analisados. No entanto, antes de adentrarmos propriamente sobre o assunto, mister se faz considerar sobre o prisma do negócio jurídico, bem como a possibilidade de identificar seus agentes envolvidos.

4.1.1 Certificação no Contexto do Negócio Jurídico

Conveniente estabelecer divisão em dois períodos — analógico e digital — sendo que o primeiro será antes do certificado digital e o segundo após. No período analógico foi marcado pelo formalismo decorrente de uma sociedade menor, orientada pelo Direito Romano, deixando, inclusive essa herança em nosso ordenamento jurídico brasileiro. Ademais, ressalta-se que, desde os tempos mais remotos — direito romano — sempre foi possível ouvir vozes de jurisconsultos na defesa da mitigação ao formalismo.

Entretanto, vigoravam rituais solenes para certificação dos negócios jurídicos visando preservar a segurança. Pois, era desse modo a maneira adequada aos romanos para estabelecer autenticidade, publicidade eficiência e proporcionar segurança jurídica à sociedade. Exemplo interessante é o da transferência de

propriedade no império Romano, o qual foi bem elucidada pelos ensinamentos de Cretella (1978):

> Mancipação: (“mancipatio”) é o modo convencional e solene de transferência da propriedade que, na época clássica, consiste em uma venda simbólica por meio do bronze e da balança (“per aes et libram”) (…) como uma venda fictícia ("imaginaria venditio”), imaginando-se a pesagem da quantia paga, surgindo o conjunto como um ato de transferência formal e simbólico (CRETELLA JÚNIOR, 1978, p. 209).

Além desse relato, também foi possível encontrar em outra obra, escrita e compilada por Dárcio:

> A mancipatio, (…) e ela se dá do seguinte modo: na presença de não menos do que cinco testemunhas, que sejam cidadãos romanos púberes, e, além disso, de mais de um indivíduo da mesma condição, que segure uma balança de bronze - o qual é chamado de libripens - o adquirente, segurando uma moeda de bronze, diz o seguinte: “afirmo que este escravo é meu pelo direito quiritário, e seja ele por mim comprado por meio desta moeda e desta balança com a moeda e a entrega àquele de quem faz a aquisição, como se à guisa de pagamento do preço” (…) deste modo tanto escravos quanto pessoas livres são transferidos por mancipatio. Também os animais que sejam passíveis de mancipatio - entre os quais se incluem os bois, os cavalos, as mulas, e igualmente os prédios, tanto urbanos quanto rústicos (RODRIGUES, 2020, p. 72).

Logo, nota-se que a solenidade arcaica era uma característica fundamental para a certificação dos negócios, regra para com que as partes interessadas pudessem realizar um determinado negócio jurídico. Essa metodologia, apesar de, aparentemente, exagerada, contribuiu anos a fio para a lisura e a segurança jurídica das relações do povo daquela época.

Com evolução da sociedade romana, surgiu o direito Justinianeu, abolindo o formalismo da mancipatio, o qual simplificou o problema reunindo somente um tipo de propriedade e o modo único de transferi-la como sendo a simples tradição.

Este modo, atualmente, ainda se faz presente em nosso ordenamento jurídico conforme se depreende nos artigos 1.245 e 1.267 do NCC. Sendo que, sua instrumentalização, em muitos casos, é realizada pelos Registros Públicos. Estes, no que lhe concerne, são encarregados por cumprir as formalidades legais, a fim de certificar, garantir a autenticidade, eficácia, segurança jurídica dentre outros.

O instituto dos registros públicos conta com particulares profissionais do direito que atuam exercendo função pública, após serem aprovados por um

rigoroso concurso público, artigo 236 Parágrafo Terceiro da CF/88 e artigo 3º da Lei 8.935/1994. Esses particulares são Notários e Registradores. Além disso, estão espalhados em todo território nacional, ao menos um deles em cada município para atender a população, conforme art. 44 § 2º da Lei 8.935/1994, portanto, presente sua capilaridade.

A importância de os notários e registradores estarem espalhados em todo território nacional é para atender melhor as pessoas em um país continental como o Brasil, proporcionando, portanto, à população realizar negócios jurídicos locais ou à distância. Por exemplo: uma pessoa precisa assinar um contrato qualquer e certificar ao destinatário que aquela assinatura aposta no documento é autêntica.

Para tal, o signatário irá assinar o documento na presença do Tabelião de Notas ou seu preposto, após elaborar uma ficha-padrão — cadastro — no cartório; agora o Tabelião efetuará a qualificação notarial do ato — captando fisicamente a vontade do agente; na sequência, serão efetuados: o cadastro da pessoa, análises dos documentos a ser assinado, identificação das partes, a capacidade da autonomia da vontade e, somente, por fim, chancelar a assinatura aposta no documento.

Vale ressaltar, que todo esse procedimento faz parte de protocolos a serem seguidos — herança do direito romano — conforme Lei Federal, bem como as normas de serviços da Corregedoria Geral da Justiça do Tribunal do Estado da Federação.

Neste sentido, oportuno transcrever trechos em que Gonçalves (2014) demonstra rigor no momento do cadastro na qualificação notarial:

> Num primeiro momento, confecciona-se o cartão de autógrafos do usuário, para que fique arquivado na serventia seus padrões de assinatura. Aqui ocorre a primeira qualificação notarial que se consubstancia na análise do documento de identificação apresentado pela parte, bem como da sua capacidade natural. Os documentos de identificação que podem ser aceitos estão em regra previstos em lei e incluem a cédula de identidade, as carteiras expedidas por órgãos controladores do exercício profissional (Art. 1º Lei 6206/75), a carteira de habilitação (Art. 159 da Lei 9503/97), a carteira de trabalho (Art. 40 CLT) e Passaporte. Ressalta-se que em alguns estados há disposição normativa expressa vedando o uso da carteira de trabalho e do passaporte para a abertura do cartão de autógrafos.

Nota-se, na ocasião da qualificação notarial, no primeiro momento de atendimento, o Tabelião avaliará a capacidade natural da parte, ou seja, análise não será resumida somente pelo aspecto formal, como as linguagens binárias oferecem.

Ele adentrará no campo subjetivo da parte. Ademais, segue:

> A higidez do documento apresentado deve ser analisada pelo Tabelião de Notas, podendo recusá-los quando contiver caracteres morfológicos geradores de insegurança, ou seja, quando estiverem replastificados, com foto muito antiga ou quando de qualquer forma não servirem para identificar o seu portador. Estando hígido o documento de identificação, o notário deve proceder a análise da capacidade natural do usuário. Aqui a qualificação notarial incide somente sobre a vontade de entender e querer o reconhecimento de firma sem adentrar na manifestação de vontade constante do documento sobre o qual incidirá a assinatura reconhecida. (…) Reconhecer significa admitir como certo, legítimo ou verdadeiro. Por seu turno, assinatura é o sinal gráfico produzido por uma pessoa para representar seu nome num documento, sendo em acepção notarial, sinônimo de firma. (GONÇALVES, 2014, p. 1).

A fim de corroborar com essa linha de explicação, ensina Jacomino (2016):

> A base de todo o argumento ali desenvolvido é a ideia de que o cidadão não necessita mais se deslocar a um cartório para ter a sua firma reconhecida num determinado contrato. Bastaria enviá-lo ao notário, que o "examinará" e o depositará num repositório qualquer na nuvem. Voltando ao notário digital, o que se perde aqui? Justamente o contato entre seres humanos. É desse encontro que o notário haverá de aferir a capacidade das partes, a licitude do negócio, evitando, tanto quanto possível – e os órgãos de sua percepção sensória permitirem – a eventual ocorrência de erro, dolo, fraude, simulação. Depois, o documento público faz prova não só da sua formação, mas também dos fatos que o tabelião declarar que ocorreram em sua presença (art. 405 do CPC).
>
> Para alguns casos – especialmente naqueles em que a escritura pública é da substância do ato – nada substitui a audiência notarial.
>
> A cerimônia legal se realiza perante um Oficial Público, que identifica as partes, inquire-as, colhe a sua vontade e a reduz no instrumento, dando forma jurídica e eficácia ao negócio. Por fim, registra em suas notas o ato notarial com todas as formalidades e minudências que a lei impõe. Trata-se do fenômeno do unitas actus, tão desprezado hoje em dia como um arcaísmo formalista, ultrapassado, que não pode sobreviver no ambiente das transações eletrônicas.
>
> O grande desafio posto aos notários e registradores é promover a modernização de seus serviços, sem cair na tentação de emular os simulacros da fé pública (JACOMINO, 2016, Online).

Além de todo protocolo seguido pelo Tabelião, ele irá utilizar seus órgãos sensoriais para conferir fisicamente se a pessoa é quem ela diz ser — insubstituível pela máquina. Portanto, um documento assinado e reconhecido firma será considerado autêntico e poderá circular em todo o Brasil sem precisar da

presença do signatário. Isso possibilita a desnecessidade de o cadastrado ter que repetir e confirmar sua verdadeira identidade e dizer que ele é quem ele diz ser. Pois, o sistema dos Registros Públicos permite com que as pessoas utilizem os documentos e possam confiar nele após a sua atuação e certificação.

Portanto, o fato de existirem Tabeliães em todo território nacional possibilita com que as pessoas utilizem seus serviços de forma dinâmica e sincronizada. Ocasionando, contudo, que à sociedade possa ter garantido a certificação em âmbito nacional, independentemente do local com que o ato foi praticado. Assim, mesmo de forma analógica é possível o trafego e a interconexão dos documentos rompendo com as fronteiras da unidade da federação.

O exemplo acima foi extraído de uma sistemática presente no período analógico, onde a atuação do instituto oferece proximidade entre as pessoas envolvidas, a fim de que estejam mais presentes à realidade dos fatos, além de proporcionar acompanhamento por um profissional do direito qualificado para atuar na operação.

Contudo, perceba-se a proximidade dos agentes delegados na construção de atos e negócios jurídicos, além da tutela do Poder Judiciário que exerce sobre eles. Pois, fiscalizam a atividade nos termos do art.236, §1º da CF. Desse modo, mais um elemento constitucional que contribui à lisura e segurança do Instituto.

Porquanto, resultado diferente não seria, senão os raros casos de vícios — anulação ou nulidade — de atos e negócios jurídicos quando construídos com a chancela dos Registros Públicos.

Destacam-se, em vista disso, dados estatísticos que confirmam o mencionado considerando a propriedade imobiliária, pois dependem de forte atuação dos Registros Públicos, artigos 108 e 1.245 CCB, conforme interessante matéria citada na obra de Melo (2016):

> Informação objetiva adquirida em 23 de setembro de 2015, da SECRETARIA DE PLANEJAMENTO ESTRATÉGICO (SEPLAN 1.2 - Coordenadoria de Análise Estatística), sob a responsabilidade de Emerson Ryuji Takase: Nos últimos cinco anos, a média das ações distribuídas no TJSP tendo por objeto o defeito, a nulidade ou anulação de negócios jurídicos representou 0,504% do total das ações cíveis do período; já as ações de evicção ou vício redibitório são menores ainda, totalizando a média de 0,073%. Para uma compreensão estatística mais próxima da realidade, seria necessário, ainda filtrar tão somente as ações que têm como base a propriedade imobiliária e as improcedentes, o que ainda reduziria drasticamente a representação percentual. (MELO, 2016, p. 199).

Logo, denotam-se que os negócios jurídicos construídos pelo crivo do instituto dos Registros Públicos são sinônimo de estabilidade e segurança, forte aliado para a paz social.

4.1.2 Certificação e a Transição do Período Analógico para o Digital

Importante tecer breves comentários sobre a transição do período analógico para o digital onde a sociedade está enfrentando. Trata-se de uma realidade pós internet. Esta é formada por cabos de fibras ópticas transatlânticos espalhadas pelo mundo que interconectam entre si através de diversos computadores ao redor do planeta.

A questão é que esses cabos formam o caminho com que as informações são trafegadas pela rede. É como se fossem vários túneis que ligam pontos espalhados pelo globo. Estes, no que lhe concerne, em cada uma de suas extremidades são conectados por computadores. Além disso, também há caminhos ligando aos servidores, dentre outros. Enfim, tudo isso forma uma gigantesca “teia de aranha”.

Com advento da popularização da internet e o contingenciamento do fluxo na rede, na década de 90 criou-se WWW (Word Wide Web). Assim, a rede teve alcance mundial e, permitiu com que qualquer pessoa pudesse conectar seu computador para transitar documentos de forma de vídeos, sons, hipertextos e figuras. Assim, formaram-se milhares de caminhos públicos e abertos para tráfego, proporcionando, um crescimento exponencial do digital.

Por conseguinte, houve condições para um grande fluxo de arquivos digitais circulando em simultâneo, possibilitando, assim, aumento expressivo dos usuários no ambiente digital, os quais migraram do analógico para o digital. Nesta

seara, transcrevo trecho de Nalini (2021) para melhor esclarecimento:

> O desenvolvimento tecnológico é capaz de introduzir profundas transformações socioculturais, alterando a forma como as pessoas se relacionam entre si e com ambiente. Foi o domínio do conhecimento agrícola que permitiu às sociedades caçadoras-coletoras se estabelecerem em cidades. A primeira e a segunda revolução industriais organizaram novas formas de relações interpessoais, fomentando o acúmulo de riquezas e o investimento em novas pesquisas. O avanço da tecnologia da informação e o aumento da capacidade computacional tornaram a cada dia mais complexas as ligações entre pessoas e máquinas. Vivemos agora a chamada Quarta Revolução Industrial, caracterizada pela disseminação da microeletrônica, programação algorítmica e inteligência artificial. É necessário reconhecer o elevado estágio tecnológico alcançado pela humanidade. Equipamentos portáteis, como smartphones, se comunicam com satélites que navegam pela órbita terrestre. Estes aparelhos que gravitam em torno da Terra transmitem comandos que poderão ser executados por outras máquinas em quaisquer partes do globo. (…) Há, contudo, o risco de que essa enorme dependência das máquinas aniquile a já abalada conexão e a confiança entre os próprios humanos. (NALINI, 2021, p. 313).

De fato, a sociedade está passando por transições, sendo que a tecnologia também traz consigo efeitos colaterais, tais como o risco de documentos serem interceptados por algum malicioso, alteração de seu conteúdo ou mesmo sumir com eles por completo, além de fomentar o distanciamento social, dentre outros.

Nesta direção a sociedade está experimentando em maior escala a realidade de recorrer a aparelhos eletrônicos, inclusive com a chegada dos smartfones. Assim, foi possível realizar diversos negócios jurídicos de forma eletrônicos. Ou seja, chegamos a era sem papel — paperless, como bem esclarece Peck (2019):

> A tecnologia tem sido muitas vezes o fator motivador para a mudança na arena do direito comercial. Com o advento de novas tecnologias, surgem métodos empresariais que exigem uma reavaliação do quadro jurídico do comércio. Estruturas jurídicas tradicionais presumem que as transações são baseadas em papel com assinaturas de acompanhamento. No entanto, ofertas ou aceitações transmitidas através de meios eletrônicos não apresentam tais assinaturas. Tal constatação é cada vez mais verdadeira para o cotidiano e, por isso, a ciência do Direito precisou encontrar soluções que garantisse a segurança jurídica das transações no contexto da sociedade paperless. (…) Conforme apontam Thomas Ehrlinch e Ernestine Fu os benefícios óbvios são o “acesso onipresente para qualquer pessoa com um computador e entrega praticamente instantânea” (..) Mas é inegável que a possibilidade de acúmulo quase ilimitado de

> informação traz problemas de gestão de dados e documentos, assim como certa insegurança acerca da autenticidade das informações fornecidas. (PECK, 2019, p. 19).

Neste contexto, a população pôde notar ser possível realizar diversos negócios jurídicos totalmente digitais, pois basta usar um dispositivo eletrônico como seu computador pessoal ou smartphone, conforme Peck: "*Assim, qualquer contrato que possa ser celebrado verbalmente também o pode por via eletrônica em qualquer modalidade, desde um simples "clique ok*" (PECK, 2019, p. 79).

Surgiu a necessidade de incorporar os negócios analógicos ao novo formato digital. Assim, aqueles que até então eram responsáveis pela construção de boa parcela dos negócios jurídicos — o instituto dos Registros Públicos e a iniciativa privada — puderam ter a chance de apresentar solução a esta nova problemática — à corrida tecnológica.

Exige com que os competidores tenham condições ancorados em inovação, pois caso contrário estarão fadados ao fracasso. Que a propósito, pertinente transcrever o pensamento de Schumpeter sobre a inovação, extraída da rica obra de Benfatti (2021), que recomendo a leitura:

> Schumpeter foi provavelmente o primeiro economista a desenvolver teorias sobre o empresário. As inovações e mudanças tecnológicas advêm da ação dos empresários, com os seus espíritos animais. Ou então, como Schumpeter passou a destacar depois, os agentes da inovação são as grandes companhias que têm os recursos e o capital para investir em pesquisa e desenvolvimento. A realidade capitalista, assim, favorece a máxima produção, que gera, por sua vez, máximo desempenho produtivo, o que faz com que se elimine a concorrência, retroalimentando a própria produção e criando ondas de novas melhorias, as quais, em determinado momento, fazem a disrupção da produção, levando a produção a outro patamar, ou mesmo criando novas demandas ou produtos. (BENFATTI, 2021, p. 68).

Frente a esta problemática, empresas privadas de tecnologia chegaram à frente. Desenvolveram um produto com que prometessem viabilizar o transporte de documentos — pela internet — com proteção criptográfica e condição de identificar seu usuário, proporcionando, portanto, maior segurança pela rede.

Neste cenário, lobistas de empresas de tecnologia formaram uma forte frente perante o Congresso Nacional e conseguiram editar a MP 2.200-002 de 2001 que Instituiu a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil, a qual, estranhamente, tangenciou o Tabelião de Notas em não incluí-lo com autoridade de

registro (AR), responsável para cadastrar e identificar o usuário do certificado digital.

Isso decorreu de nítido reflexo de investimento em tecnologia e inovação no âmbito da iniciativa privada, bem como uma interlocução afinada perante os congressistas brasileiros. Por outro lado, o Instituto dos Registros Públicos permanecerá inerte até o advento do provimento 100 do CNJ/2021, ou seja, um *Delay de* mais de 20 anos, o qual será abordado mais adiante.

4.1.3 A criação do Internet Protocol Address (Endereço de Protocolo da Internet)

Essa inovação tecnológica apresentou, em tese, condições para identificar o usuário pela internet. Para isso, criaram protocolos de segurança e de identificações: Certificado Digital, ID (identity), IP (internet protocol) domínio e geolocalização.

O IP é um conjunto de protocolos que tornou possível o intercâmbio de dados. Todo computador, roteador, impressoras e dispositivos, deverão cadastrar seu endereçamento: endereço do IP. Caracterizado pela unicidade seu formato é representado por um número de 32 bits ou mais, permitindo assim a localização do seu computador na rede global, ex: IP: 111.28.99.3. Sendo que o gestor do IP é a ICANN(internet Corporation for Assigned Names and Numbers), entidade sem fins lucrativos e de âmbito internacional, responsável pela distribuição de endereço de IP e pelo controle de sistema de domínio e administração central de servidores é como se fosse um Registro Civil das máquinas computacionais com sede nos EUA.

Com advento do crescimento da quantidade de usuários pela rede, o número IP foi aumentado para poder garantir a unicidade de cada usuário. Ocorre que, mesmo mantendo a unicidade de identificação, chegou-se ao ponto que dificultou localizar o endereço das máquinas ligadas na rede.

Assim, surgiu o “Domínio” com seu conceito citado na obra de Zaniolo (2021):

> É um nome que serve para localizar e identificar conjuntos de computadores e serviços na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização desses endereços, pois sem ele, teríamos que memorizar uma sequência grande de números, e dar flexibilidade para que o operador desses serviços altere sua infraestrutura com maior agilidade. (ZANIOLO, 2021, p. 174).

Desta maneira, tanto o IP quanto o domínio são protocolos capazes de nominar a máquina, e identificar o usuário do computador e/ou dispositivo que está logado na rede, permitindo, portanto, descobrir o caminho percorrido entre o remetente e o destinatário dos dados trafegados.

Neste prisma, oportuno mencionar quem são os usuários da Rede Internet conforme Zaniolo (2021):

> Provedores de serviços Internet; usuários individuais e usuários Institucionais: provedores como exemplo: promovem acesso ä Internet para terceiros, a partir de suas instalações - shopping center, restaurantes, bares etc - wirelles ou outro tipo de acesso físico", também aqueles que oferecem o acesso por meio de serviços, como os sítios na web, porém não proporciona a conexão física dos computadores dos usuários à rede - STJ, STF, Google etc. Já os usuários individuais são pessoas físicas que se conectam à Internet com diversos objetivos, desde a simples utilização do correio eletrônico e comunicadores instantâneos (whatsApp) até divulgação de serviços pessoais, lazer, leitura de jornais e compras(…) acesso em computador, tablet ou smartphone. Por fim, usuários institucionais são aqueles que conectam suas redes corporativas à Internet, de forma parcial ou total, proporcionando acesso à grande rede a seus usuários (ZANIOLO, 2021, p. 205-206).

Assim, qualquer modalidade de usuários será necessária preencher o cadastro do protocolo IP, para identificar-se. Pois, a conexão à internet é estabelecida através de um dispositivo informático chamado modem. Ele permite com que o computador possa transmitir dados pela rede. Além disso, no próprio modem também pode estar presente o roteador, dispositivo para ligar diversas redes de computador entre si.

Quando um computador faz uma requisição para acessar um website, primeiro a informação passa pelo roteador, em seguida converte-se o IP privado para acessar à internet por meio do IP público. Assim, quando a requisição retornar as informações para o modem, o roteador saberá para qual computador enviará os pacotes de dados.

Esses endereços ficam geralmente registrados em um arquivo chamado log de dados, arquivo de texto gerado por um software para descrever eventos sobre seu funcionamento, utilização por usuários ou integração com outros sistemas.

Muito bem, já sabemos que a internet detém protocolos de segurança que servem para identificar e rastrear dispositivo logado à rede. Sendo que, o que

realmente interessa é poder identificar com fidedignidade o verdadeiro operador da rede, ou seja, o dono do dispositivo ou o usuário.

Para isso, é importância a fase de cadastro do usuário, dado que, atualmente, há muitas possibilidades do uso de ferramentas que possibilitam ações de golpistas, fraudadores e criminosos. O ponto crucial é a confirmação de que o usuário/cliente é mesmo quem diz ser.

Neste diapasão, mesmo com os criativos modelos de protocolos de segurança da rede, conforme acima estudados, é bem verdade que o que se verifica é vulnerabilidade quando se trata de usuários ao se conectarem sem alguma modalidade de certificação, vejamos:

O usuário do varejo ou atacado realiza diretamente o cadastro no sistema operacional — WINDOWS e/ou MAC. Também será possível o usuário cadastrar-se em uma conta de e-mail — gmail. Por fim, poderá realizar o cadastro diretamente a alguma operadora de internet que for eventualmente contratada, como OI, CLARO, TIM, dentre outras.

Ocorre que todas as modalidades de cadastro são realizadas sem a fiscalização de um terceiro imparcial qualificado para detectar eventuais irregularidades ou vícios na declaração da vontade, ou fraude nos documentos pessoas de identificação. Os cadastros são realizados diretamente pelo usuário na página da web. Sendo que, circunstancialmente, o cadastro será realizado com maior atenção quando envolver contratação com alguma operadora, a qual requisitará documentos pessoais e contrato assinado pelo usuário.

Notam-se que não há rigor na conferência dos dados pessoais do navegador, nem mesmo, uma qualificação que possa identificar a lisura na capacidade civil, física, intelectual, bem como qualquer vício na autonomia da vontade. Em resumo é efetuado um cadastro simples, possibilitando qualquer pessoa se passar por outra e realizar o cadastro na rede.

Advém que, por intermédio deste cadastro é que será possível nomear o proprietário e/ou usuário do computador, ou dispositivo na rede, pois o sistema irá buscar o nome do usuário que preencheu o cadastro e que o mesmo foi associado ao IP de sua máquina. Portanto, estabelecer-se-ia sua identidade digital — usuário da rede.

Ademais, importante ressaltar mais uma novidade de protocolo de segurança que se junta ao contexto — a geolocalização do usuário, entretanto, não

se pode negar que mesmo ela se mostrando uma ótima opção, ainda serve apenas para localizar a máquina que acessou a rede e não localizar o usuário, salvo quando a sociedade adentrar na era do cyborg — homem máquina.

A geolocalização é nada mais nada menos que a identificação ou estimativa da localização geográfica real de um objeto, como uma fonte de radar, que por um dispositivo com conexão à internet consegue gerar um conjunto de coordenadas geográficas, identificando a localização solicitada. Também conhecido como posicionamento, a geolocalização utiliza, geralmente, métodos de rádio frequência, Wi-fi e o GPS. Veja abaixo como funciona cada um deles separadamente: GPS: processo ligado a circunstâncias do tempo, possui localização realizada por satélite, captando no mínimo o sinal de três satélites. GSM ou Radiofrequência: Tem a localização executada por ondas de rádio e utiliza as informações fornecidas pelas operadoras móveis. Nesse processo, mesmo com o GPS desativado é possível localizar o dispositivo, desde que ele esteja ligado e com sinal. Wi-fi: A técnica permite com que o usuário encontre sua localização em um ambiente fechado através do Wi-fi em que você está conectado, mesmo o sinal de GPS desativado. (CANGUÇU, 2017, p. 1).

Destarte, atualmente, esses mecanismos de localizar nominalmente o usuário da rede — por intermédio do cadastro IP — permitirão, localizar fisicamente o dispositivo eletrônico encontrado pela geolocalização. Isto posto, agora falta alguma tecnologia que pudesse proteger os documentos em trânsito pela rede! Eis que surgi o certificado digital.

No que tange o certificado digital é conceituado pela doutrina nas palavras de Zaniolo (2021):

> Certificado digital é um produto intangível, pois eletrônico: um software personalíssimo (…) funciona como uma identidade virtual, permitindo a identificação segura e inequívoca do autor de uma mensagem ou transação realizada em meios eletrônicos, como a Internet. (..) deste modo o certificado digital é um arquivo de computador que identifica o usuário. (ZANIOLO, 2021, p. 542).

Conforme dito anteriormente, ele é como se fosse uma chave eletrônica — personalíssima — para com que cada usuário dos computadores possa acessar a rede com privacidade e segurança. Pois, agrupam vários protocolos de segurança como: identidade digital para cada máquina (IP) + (Geolocalização)

identidade física da máquina e, por fim, chave de acesso ao usuário da máquina = (certificado digital).

Em suma, o IP é uma sequência numérica separada por pontos que atribui uma identidade ao seu computador, o qual é ligado ao usuário mediante o seu cadastro. Contudo, o Certificado digital será vinculado ao IP de determinada máquina. Logo, ambos deverão ser utilizados em conjunto, não sendo possível a utilização do certificado sem a informação de algum IP.

4.1.4 Certificado Digital no Contexto da Legislação Brasileira

Sabendo que o certificado digital é conectado em alguma máquina e este, no que lhe concerne, detêm numeração como se fosse sua identidade. Ademais, ressalta-se que o certificado é um produto de computação personalíssimo que liga seu usuário autorizado ao empacotamento do arquivo a ser veiculado pela rede. Este empacotamento é como se o usuário estivesse camuflando sua encomenda que será transitada pela rede.

Para esclarecer, imaginem que o usuário acaba de produzir um texto de 100 páginas pelo Word Office, no Brasil. Este texto, no que lhe concerne, é um documento confidencial que deverá ser enviado a um destinatário localizado nos EUA.

Para ele percorrer esse trânsito sem ser atacado ou copiado é utilizado o Certificado Digital, o qual acionará comando para transformar o documento em código criptografado, como, por exemplo: uma combinação numérica complexa e/ou até em uma imagem aleatória.

Assim, quando o documento chegar ao seu destino somente o portador de outro certificado digital poderá decifrá-lo. Hipoteticamente, imaginem a seguinte situação: o usuário de uma ponta cria uma “banana” a ser enviada pela rede com segurança, sendo que ela não poderá ser vista, extraviada ou danificada, pois se sabem que o mundo quer banana pelo fato de ser valiosa. Logo, o certificado digital irá transformá-la em “maça” no momento do envio e, na ocasião de ela chegar ao destino, o destinatário, possuidor de outro Certificado digital, transformará de volta em “banana”.

Portanto, isso permite com que ela circule pela rede camufladamente como se fosse uma “maça” deixando-a longe dos holofotes dos interessados. Esta tecnologia, em tese, protege a integridade do documento, além de oferecer

pessoalidade do remetente ao destinatário.

Para isso, haverá duas chaves com códigos diferentes que serão usadas em cada ponta da rede. Somente o usuário logado a máquina terá condições de acessar o documento protegido. É como se fosse uma porta de acesso ao túnel que irá ligar os demais computadores.

Assim, o usuário poderá, em tese, controlar os envios e os recebimentos dos arquivos eletrônicos de sua máquina computacional. Uma porta de envio será aberta pelo remetente e outra porta de recebimento será aberta pelo destinatário, ambas utilizarão os certificados digitais com criptografia diferente. Ou melhor, um não consegue abrir a porta do outro, mas somente a sua.

Essa criptografia é crucial, pois no túnel com que as informações circulam, são congestionados de documentos e usuários, possibilitando, portanto, alto risco de serem interceptado por outros, daí a necessidade de camuflar em criptografia (transformar banana em maçã) utilizando o Certificado Digital.

Portanto, ele irá identificar os usuários das duas pontas da rede, bem como empacotar o documento a ser transportado pela internet. Oferecendo, por conseguinte, integridade de que os documentos não serão atacados, bem como conferir autenticidade de autoria dos agentes envolvidos — remetente/ destinatários.

Essa tecnologia foi inovadora e vista com bons olhos em todo o mundo, inclusive pelos governos, os quais visualizaram condições favoráveis a implantá-la em toda estrutura da administração pública, oferecendo maior agilidade e segurança ao tráfego de documentos no ambiente digital.

No Brasil foi regulamentado pela MP 2.200-002 de 2001, em vigor até agora, que Institui a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil. Sendo que, definiu como autêntico a autoria e o documento quando veiculados utilizando Certificado Digital, (BRASIL, 2001):

> Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (BRASIL - MP 2.200-2/2001, 2001, p. 1).

Assim, instituiu-se a ICP-Brasil que permanecerá no topo da cadeia hierárquica da arquitetura tecnológica criada para garantir a criação dos Certificados

Digitais, seu controle e distribuição pelo Brasil.

Ademais, frisa-se que a mesma medida provisória também trouxe nos seus dispositivos a definição da presunção de veracidade aos documentos utilizados com processo de certificação digital, abaixo:

> Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória. § 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil (Medida provisória que teve sua vigência arrastada até a lei em 2020/ Lei 14.063, permitindo o uso de assinaturas digitais e definindo as diferenças entre as assinaturas avançadas e qualificadas). (BRASIL - MP 2.200-2/2001, 2001, p. 1).

Com advento da Lei 14.063/2020, a mesma medida atribuiu poderes e permitiu a qualquer pessoa interessada que se filie à ICP-Brasil, a fim de comercializar os certificados, bem como chancelar validade de autoria e documental aos documentos por ela produzido:

> Art. 7º Compete às AR, entidades operacionalmente vinculadas a determinada AC, identificar e cadastrar usuários, encaminhar solicitações de certificados às AC e manter registros de suas operações. (Redação dada pela Lei nº 14.063, de 2020). (BRASIL, 2020, p. 1).

Nota-se que as autoridades de registros quem serão responsáveis para cadastrar e identificar pessoalmente os usuários. Mas para isso, ela deverá se apresentar somente no momento do cadastro à ICP-Brasil:

> Parágrafo Único. A identificação a que se refere o caput deste artigo será feita presencialmente, mediante comparecimento pessoal do usuário, ou por outra forma que garanta nível de segurança equivalente, observadas as normas técnicas da ICP-Brasil. (Incluído pela Lei nº 14.063, de 2020. (BRASIL, 2020, p. 1).

A citação acima refere-se a medida provisória que teve sua vigência arrastada até agora, sendo, portanto, complementada pela lei em Lei 14.063/2020, permitindo no decorrer dos anos, o uso de assinaturas digitais e definindo diferenças entre as assinaturas avançadas e qualificadas.

Nesse parágrafo, determina que o cadastro do usuário será efetuado

mediante comparecimento presencial perante à Autoridade de Registro, permitindo, portanto, com que ela possa fazer a identificação do usuário. Todavia, a verificação presencial será feita somente uma vez no prazo de vigência do Certificado. Logo, será repetida por ocasião de sua renovação, após expirar a validade (1 a 3 anos).

Verificam-se, que esta nova tecnologia foi tratada com tamanho ceticismo, incentivando, por consequência, a edição de uma lei que estabeleceu a possibilidade de qualquer pessoa se cadastrar para emitir certificado digital.

Para isso, basta o interessado se credenciar a ICP-Brasil que a mesma lhe transformará em uma autoridade de registro (AR). Sabendo que, a partir de então, o novo credenciado poderá qualificar e cadastrar qualquer pessoa civil e/ou jurídica em todo território brasileiro para certificar sua autoria em diversas modalidades de negócios jurídicos. Assim, a autoridade de registro (AR) certificará que o possuidor do certificado digital é quem diz ser, e ainda irá conferir autenticidade na autoria do agente envolvido na produção do documento.

No que tange o certificado digital, que o responsável pelo cadastramento do usuário será feito pela AR (Autoridade de Registro).

> As ARs são entidades públicas ou pessoas jurídicas de direito privado credenciadas pela AC Raiz e que sempre serão vinculadas operacionalmente à determinada Autoridade Certificadora. É o elo entre o usuário e a Autoridade Certificadora - AC e tem por objetivo receber e encaminhar as solicitações de emissão ou revogação de certificados digitais às AC, além de identificar os solicitantes, na forma e condição regulamentada pelo DOC-ICP-05. (BRASIL – INTI, 2021, p. 1).

Verifica-se que as ARs são pessoas jurídicas de direito privado credenciadas a autoridade ICP-Brasil, as quais fazem parte da iniciativa privada que buscam obter lucros para se manter no mercado.

Outrossim, é responsável em qualificar o usuário e remeter o envio de dados coletados à AC, conforme abaixo:

> INSTRUÇÃO NORMATIVA ITI No 11, DE 23 DE OUTUBRO DE 2020.
> Aprova a revisão e a consolidação do Cadastro de Agente de Registro da ICP-Brasil.
> Art. 3º O envio do conjunto de dados que compõem o CAR será realizado pelas Autoridades Certificadoras ou seus respectivos Prestadores de Serviços de Suporte credenciados no âmbito da ICP-Brasil.

> § 2º O serviço de Cadastro de Agente de Registro da ICP-Brasil é permitido somente para pessoas jurídicas e o acesso é realizado com certificado digital ICP-Brasil, conforme definido no Manual de Instruções, anexo desta Instrução Normativa.
> Art. 4º O ITI disponibilizará semanalmente a relação dos agentes de registro cadastrados no CAR no endereço. (BRASIL – INTI, 2022, p. 1).

Então, qualquer pessoa jurídica interessada em auferir lucro poderá se cadastrar à ICP-Brasil habilitando-se para emitirem certificados e comercializá-los em todo território nacional. Pois, basta buscar no Google que será possível acessar as pessoas jurídicas ora credenciadas.

O interessado chama-se autoridade de registro (AR) sendo vinculada a ICP-Brasil, o qual está ligado à arquitetura tecnológica para apenas identificar a máquina eletrônica que irá ser utilizada pelo certificado, bem como controlar sua confecção e distribuição pelo Brasil, isso quer dizer que, a autoridade de registro se tornou uma interface entre o usuário e o estado.

A lei determina que as máquinas envolvidas na construção e tráfego do documento serão vinculadas ao número de seu IP, o qual poderá ser rastreado pela certificadora — ICP-Brasil e que, portanto, possibilita ao sistema identificar o suposto usuário do referido IP e ligá-lo a qualquer movimentação operada pelo seu dispositivo eletrônico, considerando autêntico a autoria do documento.

Notam-se que a base da informação é justamente o cadastro do IP — efetuado de forma simples — sem certificado digital, ou pelo cadastro na ICP-Brasil com certificado digital. Deste modo, ambas disponibilizam condições de rastrear a máquina e não a pessoa real que utilizou o certificado digital. Assim, somente tentam oferecer condições para supor, por intermédio de senha pessoal, quem possa estar por trás de um determinado IP.

Essa engenharia tecnológica com o fito de identificar o usuário da rede, criou cadastro ligando-o ao número do IP. Nesse sentido, transcreve-se o voto do ministro Nefi Cordeiro que, por ocasião de um julgado enfrentado pelo STJ, teceu valiosas considerações sobre o tema (STJ, 2019):

> Documento: 95282320 - EMENTA, RELATÓRIO E VOTO - Site certificado Página 6 de 12 Superior Tribunal de Justiça informações de conexão à internet feitas a partir da rede móvel 3G até o dia 30/11/2009, especialmente porque o número IP requerido pela recorrida era utilizado de forma dinâmica, sendo alocado a diversos usuários conforme a necessidade. Assim, o início do armazenamento

> teria início 23 (vinte e três) dias após os fatos narrados na petição inicial, o que tornaria impossível o cumprimento da ordem judicial.

Interessante notar que os provedores de internet inventaram o IP dinâmico, ou seja, um IP rotativo que possibilita maior número de usuários. Ocorre que, isso dificulta o arquivamento dos seus logs de registros, bem como a identificação dos usuários, sendo, portanto, um argumento utilizado pelos operadores para se esquivarem de pedidos judiciais de identificação dos usuários, como segue:

> Sobre o tema de guarda e armazenamento de informações cadastrais dos usuários, a doutrina afirma o seguinte: Entre nós, como cediço, não há norma específica, opinando Marcel Leonardi que é dever dos provedores de internet, no momento de fazer a contratação com um usuário, colher todos os seus dados, principalmente nome, endereço e números de documentos pessoais válidos, e em alguns casos, os números de IP atribuídos e utilizados pelo usuário, os números de telefone utilizados para estabelecer a conexão e o endereço físico de instalação dos equipamentos informáticos utilizados para conexões de alta velocidade. A hipótese de os dados fornecidos pelo usuário não corresponde à realidade, não permitindo a sua identificação ou localização, para https://www.msn.com/pt-br/feedMarcel Leonardi sujeita os provedores a responder de forma solidária pelo ato ilícito cometido pelo terceiro que não puder ser identificado ou localizado. A proposta do autor, na verdade corresponde ao modelo pretendido e superado em sede de Direito Comparado, que configuraria o provedor de internet como solidariamente responsável por eventuais danos causados por usuários anônimos ou sem recursos para custear eventual condenação em uma demanda por danos. E deve ser enfatizado que o fato de a arquitetura da internet permitir o acesso anônimo e não identificável é uma realidade intransponível, ao menos por ora, valendo mencionar o brocardo jurídico *impossibilium nulla obligatio est* (não há obrigação de coisas impossíveis). Para aceder à internet e obter uma conta de correio eletrônico (e-mail), basta dirigir-se a um cybercafé, ou até mesmo a outros locais, como as redes abertas em aeroportos e centros comerciais, apenas munido de um computador portátil, sem qualquer possibilidade efetiva de um provedor host ter controle sobre a real identidade do usuário em geral.

Esse trecho do julgado, deixa claro uma das maneiras de tentar anonimizar a conexão com a rede pelos mal-intencionados, oportunizando, portanto, a prática de ilícitos. Ademais, continua o julgado:

> Obviamente, em muitos casos o usuário perpetrador de uma difamação, por exemplo, não terá como ser identificado ou alcançado. Para que esse ônus existisse, o formato atual da rede deveria ser reformulado (o que parece ser impensável ou impraticável) ou as cautelas exigidas de um provedor de conteúdo de terceiros seriam tantas que tornariam o serviço lento e excessivamente oneroso. A

> internet e seus serviços tiveram sua grande expansão em função da interatividade e da possibilidade de transações eletrônicas, não podendo ser aceitável a imputação de um ônus demasiado para os provedores, como o de garantir a real identidade de seus usuários. Contudo, cabe ao provedor de acesso conservar os dados existentes de seus usuários, apenas fornecendo-os por ordem judicial específica, sempre com um olhar em face de não poder ser exigido um dado impossível de ser informados. (PAULO ROBERTO BINICHESKI. Responsabilidade civil dos provedores de internet: direito comparado e perspectivas de regulamentação no direito brasileiro. Curitiba: Juruá, 2011, p. 236).

A tendência é cada vez mais aumentar o congestionamento pela rede, entretanto, isso não pode ser usado como argumento para anonimizar os seus usuários. O bônus dos provedores e das operadoras também deverão ser equacionados com ônus. Segue continuação do julgado:

> De todo modo, esta Corte Superior firmou entendimento de que as prestadoras de serviço de internet, como as demais empresas, estariam sujeitas a um dever legal de escrituração e registro de suas atividades durante o prazo prescricional de eventual ação de reparação civil, dever que tem origem no art. 10 do Código Comercial de 1850, e atualmente encontra-se previsto no art. 1.194 do Código Civil, abaixo transcrito:
> Art. 1.194. O empresário e a sociedade empresária são obrigados a conservar em boa guarda toda a escrituração, correspondência e mais papéis concernentes à sua atividade, enquanto não ocorrer prescrição ou
> decadência no tocante aos atos neles consignados.
> Conjugando esse dever de escrituração e registro com a vedação constitucional ao anonimato, nos termos do art. 5º, IV, da CF/88, os provedores de acesso à internet devem armazenar dados suficientes para a identificação do usuário, conforme os seguintes julgados desta Corte:
> (...) 2. Reconhecimento pela jurisprudência de um dever jurídico dos provedores de acesso de armazenar dados cadastrais de seus usuários
> durante o prazo de prescrição de eventual ação de reparação civil. Julgados
> desta Corte Superior.
> 3. Descabimento da alegação de impossibilidade fática ou jurídica do fornecimento de dados cadastrais a partir da identificação do IP. Julgados
> desta Corte Superior. 4. Considerações específicas acerca da aplicabilidade dessa orientação ao IP dinâmico consistente naquele não atribuído privativamente a um único dispositivo (IP fixo), mas compartilhado por diversos usuários do provedor de acesso. (...) (REsp 1622483/SP, Terceira Turma, DJe 18/05/2018) (...) 5. Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um

> desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada.

Nesta seara, é importante lembrar que a Constituição Brasileira veda o anonimato, conforme artigo 5º, IV, inclusive, considerando-o como direito fundamental. Segue o julgado:

> Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa *in omittendo*. 6. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço. (...) (REsp 1398985/MG, Terceira Turma, DJe 26/11/2013) (...) 5.- É juridicamente possível o pedido à empresa de telefonia de exibição do nome do usuário de seus serviços que, utiliza-se da internet para causar danos a outrem, até por ser o único modo de o autor ter conhecimento acerca daqueles que entende ter ferido a sua reputação. (...) (REsp 879.181/MA, Terceira Turma, DJe 01/07/2010) Dessa forma, com base nesses fundamentos, pode-se concluir que o provedor de acesso já possuía o dever de armazenar os dados cadastrais e os respectivos logs de seus usuários, para que estes pudessem ser identificados posteriormente, mesmo antes da publicação da Lei 12.965/2014, que instituiu o Marco Civil da Internet. Sobre a alegação segundo a qual, por utilizar método de alocação de números IP de forma dinâmica, seria impossível determinar qual o usuário do serviço de conexão à internet em um determinado espaço e tempo, esta Corte Superior já se pronunciou sobre esse tema, no julgamento do REsp 1622483/SP (Terceira Turma, DJe 18/05/2018) citado acima. Naquela oportunidade, o relator Min. Sanseverino afirmou o que segue: Quanto a esse aspecto, o provedor recorrente sustentou que o IP seria dinâmico, ou seja, que não haveria um número único para cada usuário. **Sustentou, também, que o armazenamento dos 'logs' dos usuários seria inviável (demasiadamente oneroso), em função do grande número de conexões que são continuamente realizadas**. O Tribunal de origem superou essas questões técnicas sob o fundamento de que o armazenamento de tais dados seria "providência inerente ao risco do próprio negócio desenvolvido pelo provedor" (fl. 658).

Como se não bastassem os pontos cegos que o acesso à rede proporciona para o anonimato as operadoras também dificultam o fornecimento de informações requerida pela justiça como no caso do IP dinâmico, o qual é explicado na continuação do julgado:

> Quanto a esse ponto, o recurso especial encontra óbice na Súmula 7/STJ. Cabe esclarecer, contudo, que o IP dinâmico é aquele não atribuído privativamente a um único dispositivo (IP fixo), mas compartilhado por diversos usuários do provedor de acesso. No IP dinâmico, o usuário recebe um número de IP diferente a cada conexão. Com essa medida, otimiza-se a utilização dos números de IP, pois o IP que ficaria ocioso é aproveitado por outro usuário. De todo modo, seja dinâmico, seja fixo, o número de IP é projetado para ser unívoco, de modo que, num dado momento, a cada IP corresponde um único dispositivo conectado à rede.

Por fim, não menos importante é o arquivo dos *logs* de registros, que estão sendo tratado como tamanho descaso pelas operadoras, conforme parte final do julgado:

> De outra parte, quanto aos custos do armazenamento dos logs dos usuários, correto o entendimento do Tribunal no sentido de que se trata de "providência inerente ao risco do próprio negócio", devendo a empresa suportar esse custo. A alegação de impossibilidade fática, portanto, não obsta o pedido de identificação do usuário. (Grifou-se) Assim, mesmo com a utilização do IP dinâmico, ao se determinar o local e a hora de acesso, é possível a identificação do usuário. Inclusive, naquela oportunidade mencionou-se um julgado em que foi permitida a identificação do usuário, in verbis: PENAL. PROCESSUAL PENAL. HABEAS CORPUS SUBSTITUTIVO DE RECURSO ESPECIAL, ORDINÁRIO OU DE REVISÃO CRIMINAL. NÃO CABIMENTO. DIVULGAÇÃO DE PORNOGRAFIA INFANTIL. INTERCEPTAÇÃO TELEMÁTICA. INCOMPETÊNCIA DO JUIZ QUE DECRETOU A MEDIDA CAUTELAR. NÃO RECONHECIMENTO. 1. Ressalvado pessoal compreensão diversa, uniformizou o Superior Tribunal de Justiça ser inadequado o writ em substituição a recursos especial e ordinário, ou de revisão criminal, admitindo-se, de ofício, a concessão da ordem ante a constatação de ilegalidade flagrante, abuso de poder ou teratologia. 2. Nos termos de precedente da Excelsa Corte, Quando a interceptação telefônica constituir medida cautelar preventiva, ainda no curso das investigações criminais, a mesma norma de competência há de ser entendida e aplicada com temperamentos, para não resultar em absurdos patentes. (HC 81260, Relator(a): Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 14/11/2001, DJ 19-04-2002 PP-00048 EMENT VOL-02065-03 PP-00570). 3. Na espécie, a operação deflagrada pela Polícia Federal visava identificar, em todo o território nacional, os indivíduos que estavam publicando material pedófilo na internet, motivo pelo qual entendeu-se que o Juízo da Capital Federal era o competente para a quebra do sigilo telemático. Em decorrência da referida medida foram descobertos os dados cadastrais dos usuários dos IP's investigados e a partir de então é que foram instaurados inquéritos policiais e as consequentes ações penais nos respectivos Estados.4. Habeas corpus não conhecido. (HC 263.311/SP, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 16/06/2016, DJe 28/06/2016 (STF, 2019, p. 1).

Destaca-se à importância do armazenamento dos *logs* de registros. Ele possibilita chegar ao número do cadastro IP do usuário, pois permite percorrer o rastro de sua navegação, caso contrário, dificilmente será possível localizar seu IP.

Também é possível extrair desse voto que as empresas de tecnologia não têm interesse em manter o arquivo dos *logs*, pois incide alto custo financeiro em razão da quantidade de acessos dado pela rede.

Outrossim, salutar esclarecer com mais detalhes o que é *log* de registro e, para isso, destaca-se trecho de um artigo científico escrito por Tebaldi e Guardia (2015):

> Com a expansão do acesso à Internet, foi criada no Brasil a lei considerada o marco civil da Internet, a lei de n° 12.965 de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no país. Por outro lado, essa lei indica também que é preciso **armazenar registros de acessos de seus utilizadores por meio do registro do IP (Endereço de Internet) pelos provedores de acesso (ISP) e pelos administradores de rede**. Como atestado no capítulo VI "- registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;" (BRASIL, 2014). Para atender os requisitos da lei, os provedores de acesso à Internet gravam informações dos endereços IPs utilizados pelos dispositivos dos seus clientes. Esse endereço IP atribuído ao usuário é um IP chamado de endereço público, atribuído a apenas um dispositivo de usuário de cada vez. Usando a versão 4 do protocolo IP, há ainda os chamados endereços privados. O endereço IPv4 é um endereço de identificação composto por 32bits escrito com quatro octetos. Entre os valores possíveis, os números privados são algumas faixas de números utilizadas para o uso de redes locais, para os quais não há rotas disponíveis na internet, 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16. Excluindo mais algumas faixas que são reservadas, o restante dos números é distribuído pela IANA (Internet Assigned Numbers Authority) para os provedores de Internet atribuírem a seus usuários. Assim, mesmo que contássemos o valor total de endereços possíveis, haveria 4 294 967 296 endereços, que não seriam suficientes para todos os dispositivos conectados. Assim, é comum que provedores de acesso à Internet entregam apenas um número IP para cada conexão de usuário (IETF, 1996). Se o local do ponto de acesso já oferecer um conjunto de endereços IP públicos disponíveis a todos os usuários, isso já atenderia a lei do marco civil, pois esse registro já garantiria a identificação do usuário, e o administrador da rede não precisaria armazenar mais nenhum tipo de registro.

Neste ponto, destaca-se a importância do armazenamento deles. Contudo, no modelo atual, a sociedade está nas mãos das iniciativas privadas (provedores e operadores de internet). Devido tamanha importância, em oportuno,

interessante reflexão para possibilidade dos registros públicos custodiarem os armazenamentos dos *logs*.

> Porém, como a maioria dos locais públicos são de pequeno porte, tais como cafés e bares, e têm apenas um endereço de IP disponibilizado pelos provedores de Internet, o acesso à Internet para vários usuários ao mesmo tempo é comumente feito com o método chamado de NAT, disponível em quase todos os roteadores ou modems de borda. O NAT (Network Address Translation) consiste em traduzir os endereços IP da rede local para o único IP público da rede. Isso é possível por meio da substituição de endereços e controle dos números de portas, nas conexões TCP e UDP iniciadas na rede local. Para resolver esse problema e atender ao marco civil, administradores de rede devem criar mais um sistema de registro, o log de acesso, que faz o registro de acesso de todas as conexões de cada usuário, para todos os endereços conectados, mas não das URLs e nem do conteúdo enviado ou compartilhado, evitando invadir a privacidade dos usuários (IETF, 2001). (TEBALDI; GUARDIA, 2015, Online).

Considerando a importância de as empresas de tecnologia manterem arquivas dos *logs* de registros, bem como o alto custo disso, por ocasião do Marco civil da Internet, nota-se que o legislador brasileiro foi complacente em face das empresas de tecnologia, pois determinou um prazo máximo de 6 (seis) meses para com que elas mantenham os registros, conforme art. 15º da Lei Nº 12.965, de 23 de abril de 2014:

> **Art. 15**. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo **prazo de 6 (seis) meses**, nos termos do regulamento (BRASIL, 2014, p. 1).

Diante do exposto, importante tecer um comparativo no que tange ao período de arquivo com que o Instituto dos Registros Públicos deve respeitar quanto a escrituração dos atos no seu acervo, art. 26 da Lei 6015/1973: "**Art. 26.** Os livros e papéis pertencentes ao arquivo do cartório ali permanecerão indefinidamente" (BRASIL, 1973, p. 1).

Assim, de um lado temos os provedores de internet que devem manter seus arquivos no máximo por 6(seis) meses, por outro lado, hipoteticamente, se o instituto dos Registros Públicos fizesse parte da integração da ICP-Brasil, a regra seria de manter arquivados os registros dos *logs* nos livros notariais, indefinitivamente.

Logo, se houvesse a necessidade de apurar a ocorrência de um fato realizado no ambiente da internet há mais de 6(seis) meses ou mais de 10(dez) anos, a sociedade não teria a quem recorrer.

Há eventual fragilidade na confiança em provedores da internet, além de, também apresentar vulnerabilidade quanto ao cadastro do usuário perante o oceano azul da rede. Surgindo, oportunamente, a figura do certificado digital a fim de oferecer mais segurança, entretanto, a lei delega, neste contexto, a um particular comum a importante tarefa de identificar o usuário uma vez, ou seja, somente no momento do pedido do certificado, podendo assim, navegar livremente ao longo de toda sua validade (1 a 3 anos).

Ocorre que mesmo com a utilização do certificado digital há relatos de eventos fraudulentos decorrentes de seu uso, embora pouco divulgado pelo governo e pela mídia, mas, felizmente possível encontrar, em pesquisa, o belo trabalho de Julia Baldissera, e Raphael Schwinden da Silveira (2017), intitulado "**Proposta De Um Modelo Para Detecção De Fraudes Na Emissão De Certificados Digitais Na ICP-Brasil**", este no que lhe concerne, apresentou pontos da fragilidade da arquitetura ICP-Brasil, a seguir:

> O mercado de certificação tem uma clara tendência de crescimento, e os dados gerados sobre as emissões podem revelar irregularidades, que muitas vezes passam despercebidas pelos indivíduos. Já existe um processo de comunicação de irregularidades dentro da ICP-Brasil, mas este mostra-se demorado e mais suscetível a erros, já que considera a intuição dos indivíduos e não leva em conta o conhecimento incorporado nesses dados. Com um estudo mais detalhado sobre a emissão de certificados digitais, foi possível identificar dois tipos de fraudadores: **o fraudador interno**, que foi corrompido e deixa a fraude acontecer, e o **fraudador externo** se passando por solicitante do certificado(...) O resultado desta simulação foi a detecção das atividades de um possível fraudador externo, que obteve alta pontuação para fraude, e de um fraudador interno, que aceitou emitir um certificado para um possível solicitante fraudador (BALDISSERA; SILVEIRA, 2017, p.).

Os dois tipos de fraudadores definidos pelos autores da pesquisa: **fraudador interno**, pode ser a autoridade de registro que, eventualmente, corrompida pode realizar um cadastro fraudulento, pois, poderá haver corrupção entre elas. Importante ressaltar que ela é uma pessoa jurídica e/ou física de direito privado com permanência transitória e/ou precária junto ao ICP-Brasil, com vínculo trabalhista conforme as regras da CLT (Consolidação das Leis do Trabalho), além disso, o salário

dela não tem características de conseguir manter o funcionário muitos anos no cargo, pois nota-se os valores a seguir:

Figura 1 – Pesquisa Salários de Agentes de Registro.

Fonte: https://bit.ly/35PZsZw acesso dia 01/04/2022 às 10h41min

Foi possível encontrar algumas opções de salários em torno de:

a) salário de R$ 1.180,00 (hum mil, cento e oitenta reais) por mês (https://bit.ly/3jhJHO4)
b) salários de R$ 1.666,00 (Hum mil e seiscentos e sessenta e seis reais) por mês (https://bit.ly/3jhonIx)

Portanto, o salário de uma Autoridade de Registro gira entre R$ 1.000,00(mil reais) a 1.666,00 (Hum mil e seiscentos e sessenta e seis reais). Logo, terá um vínculo de trabalho conforme a CLT com salário próximo ao mínimo nacional. Assim, a impressão que se têm é que dificilmente esse cargo proporcionará com que a pessoa siga carreira, tenha estabilidade financeira e expectativa de ascensão profissional.

Por outro lado, oportuno comparar com a função do notário, o qual é exercido por profissional do direito após ser aprovado em um dos mais difíceis concursos públicos do país para o cargo que garante vitaliciedade e remuneração que proporciona ascensão profissional, conforme as regras de provimento e remoção.

Logo, após essa comparação entre a Autoridade de Registro e o Notário, a resposta para a indagação acima deverá ser respondida pelo leitor deste

estudo, o qual terá, certamente, elementos para reflexão.

Quanto ao **fraudador externo** será aquele que engana a Autoridade de Registro se fazendo passar por uma pessoa que ele não é, como, por exemplo: uma pessoa faz o cadastro utilizando documento falso.

Além dessas modalidades de fraude, também ocorre diversas outras, como, por exemplo o fraudador capturar a senha do Certificado Digital. Para isso, há inúmeras formas, sendo uma das mais utilizadas é por intermédio de malware:

Figura 2 – Tipo de fraude por intermédio de malware:

Novo golpe do saque do FGTS fez mais de 10 mil vítimas; veja que cuidados tomar

Criminosos utilizam aplicativos de mensagens para enganar vítimas e roubar dados pessoais

Foto: Reprodução/CNN

Tatiana Paiva, colaboração para o CNN Brasil Business

02/06/2021 às 14:17 Compartilhe:

Fonte: https://bit.ly/3xcG58j Acesso em Jun. 2022.

> Depois da divulgação do calendário de saques do FGTS (Fundo de Garantia do Tempo de Serviço), um golpe já conhecido fez mais de 10 mil vítimas no Brasil. No golpe, os bandidos enviam links maliciosos via aplicativo de mensagens, direcionando as vítimas a um falso cadastro. Com as informações fornecidas, é possível sacar indevidamente o dinheiro do FGTS, assim como fazer assinatura de serviços online ou abrir contas em bancos (CNN BRASIL, 2022, p. 1).

Em vista disso, nota-se que as vítimas são em projeções exponenciais, pois em apenas um comando (envio de links maliciosos) foi possível espalhar pela rede e atingir mais de 10(Dez mil vítimas), realidade completamente diferente se a liberação do dinheiro do FGTS exigisse reconhecimento de firma realizada por um Tabelião de Notas. Assim, dificilmente esse golpe teria sido concretizado nas proporções ocorrida. Ademais, desde a constituição da república

brasileira de 1988, nunca se ouviu dizer uma fraude de mais de 10 mil vítimas de uma só vez envolvendo reconhecimento de firmas fraudulentos.

Aliás, observamos o que diz o órgão público federal máximo que regulamenta as assinaturas digitais, denominado ITI (O Instituto Nacional de Tecnologia da Informação – ITI autarquia federal. Vinculado a Casa Civil da Presidência da República, tem por missão manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Ao ITI compete ainda ser a primeira autoridade da cadeia de certificação digital – AC Raiz) (ITI, 2018, p. 1). Entre as atribuições descritas no site oficial (ITI, 2017c), o ITI deve executar as normas técnicas e operacionais, e Políticas de Certificados definidas pelo Comitê Gestor.

> Segundo o diretor do ITI, a prática do compartilhamento da chave privada com terceiros, a popular senha, ocorre em larga escala e poderia muito bem explicar casos como os relatados pela seccional. Recentemente, instaurou-se processo administrativo disciplinar contra um juiz de Santos por causa desta prática. Outra possibilidade seria a emissão fraudulenta do certificado, quando determinada pessoa se identifica com documentos falsos e consegue obter o certificado digita (ITI, 2018, p. 1).

Assim, não se sustenta o argumento de que as pessoas usuárias devem custodiar suas senhas pessoais, pois, a arquitetura da ICP-Brasil aliada as empresas privadas de tecnologia deveriam antever o caos e os litígios — trabalhar pela prevenção — e não pela repressão.

A arquitetura ICP-Brasil, embora em evidência e franco crescimento, emite uma falsa impressão de autenticidade na autoria nos documentos por ela certificada:

a) a pessoa responsável pelo cadastro do cidadão — AR — embora tenha autorização legal para operar, carece de qualificação técnico-intelectual para o fim sobredito;
b) conforme se depreende no artigo 7º Parágrafo único da MP 2.200-2/2001, o cidadão — usuário — comparecerá apenas uma vez presencialmente perante a AR (autoridade de Registro) para realizar seu cadastro, devendo retornar somente quando expirado prazo do seu certificado — validade mínima de 12(doze) meses — ou seja, durante os doze meses futuros ele será considerado plenamente capaz, independentemente das circunstâncias e intempéries da vida — incapacidade civil momentânea, definitiva e/ou se alguém fingir se passar pelo proprietário do certificado, podendo inclusive compartilhar sua

senha com quem quiser;

c) a finalidade do certificado é permitir rastrear a máquina ou dispositivo eletrônico utilizando, assim, será possível localizar com certeza somente o IP da máquina — identidade digital — utilizado, e por suposição, presumir-se-á presença de um ser humano — outrora cadastrado — que, em tese operou o computador, carecendo de garantias robustas.

Sobre o assunto, ensina Peck (2019) uma das maiores autoridades do direito digital no Brasil:

> O certificado digital, assim como uma senha, pode ser emprestado, enquanto que as características biométricas, não. Logo, mesmo o certificado tendo toda tecnologia de criptografia assimétrica, ele não dá a certeza que a pessoa é realmente quem ela diz ser. (PECK, 2019, p. 50).

Situação similar é imaginar que o possuidor de determinado Certificado Digital, acesse sua máquina e deixa-o logado direto 24 horas e 7 dias por semana e meses, ou compartilha sua senha com terceiros. Em todo esse período, qualquer pessoa poderá utilizar sua máquina emitindo documentos e assinando-os se fazendo passar pelo verdadeiro proprietário.

Neste contexto, avançando um pouco nas hipóteses, de maneira muito fácil é uma terceira pessoa coagir o detentor do certificado e utilizá-lo para os mais variados fins, sem que o destinatário do documento, nem a certificadora, muito menos a autoridade de registro possa ter conhecimento. Também é possível, o usuário estar sob efeito de álcool e/ou drogas praticar negócios jurídicos sem que ninguém saiba o seu real estado mental, dentre inúmeras hipóteses. Casos em que dificilmente ocorreria no balcão de um cartório.

Interessante mencionar que no ano de 2021 e 2022 houve aumento expressivos nos crimes digitais, como exemplo: O usuário de certificado digital recebe um e-mail ou telefonema, o qual é informado de que seu certificado expirou, devendo, portanto, passar a sua senha para atualização, em seguida o usuário passa sua senha, pronto o golpe está concluído. Esse tipo de *modus operandi* é comum, embora o usuário saiba que a senha não pode ser compartilhada e deverá estar sob sua responsabilidade, ele é facilmente persuadido passá-la a terceiros, causando, portanto, insegurança jurídica a todo sistema.

Notam-se que o fato de a senha dever ser mantido em sigilo e sob

custódia do próprio usuário, isso não foi suficiente para impedir a atuação dos criminosos, ocasionando, por conseguinte, aumento exponencial dos crimes digitais e a migração maciça dos problemas para o Poder Judiciário resolver.

Em suma, tamanha arquitetura tecnológica, para que ao fim e ao cabo embasa a autenticidade de autoria à análise de que qualquer pessoa jurídica de direito privado — autoridade de registro — sirva de elo entre o usuário e a certificadora, fomentando, portanto, o crescimento de crimes cibernéticos.

Sendo que, neste contexto a base da estrutura que oferecerá segurança jurídica é justamente a Autoridade de Registro (AR) que irá comercializar os certificados em todo Brasil com intuito unicamente de aferir lucros — pois basta realizar uma consulta rápida no Google para descobrir o mercantilismo que virou a emissão de certificados digitais.

De outra banda, neste universo, vale acentuar como paradigma o Tabelião de Notas na ocasião em que é efetuado a qualificação notarial para reconhecer firma — cadastro — cartão de autógrafo — que após ser preenchido pessoalmente, bem como análise acurada dos documentos de identificação das partes, para que, em seguida, o Tabelião possa ser o elo — interface — entre o usuário e o direito posto, conforme ensina Dalledone (2016):

> No mais, uma grande parcela das relações jurídicas envolvendo a vida cotidiana a ser regida pelo direito popular: “costumes locais, alguns reduzidos a escrito, posturas locais e as praxes dos julgados, o chamado estilo do tribunal. Nessa ordem de coisas, os tabeliães serviam como um elo entre o direito oficial e o direito popular (…) a instituição notarial era também moldada pelo meio social e pelas contingências históricas, daí ressaltar Pedro Clamote que se tratou de uma instituição gerada pela própria realidade social (e não por decreto). (DALLEDONE, 2016, p. 31).

Além do mais, não se pode realizar o presente estudo e deixar de fora os elementos presentes na verdadeira autenticidade que se extrai dos atos elaborados pelos notários, conforme ministrado por Nunez Lagos (apud FALBO; CASTELNUOVO, 2019):

> O documento notarial resultante das referidas tarefas, opus que deixa o notário e corolário da função notarial, é então a expressão do pensamento humano (não apenas uma representação dele), um facto jurídico e ao mesmo tempo um acto jurídico, cujo autor é o notário e que é dotado de autenticidade ou fé pública, que se irradia em três níveis: autenticidade subjetiva ou autoria, autenticidade corporal ou do documento como coisa e autenticidade ideológica (esta última refere-se ao pensamento documentado, atos próprios do notários, os factos que o notário percebe pelos seus sentidos, as sentenças do notário e o conteúdo das declarações). Para que essa autenticidade seja possível e duradoura, é necessário que o notário, cuidando da forma, penetre no conteúdo, enfim, realize todas as tarefas essenciais da função notarial, explicadas acima. (...) Assim, ambas as presunções se baseiam na autoria do documento. O documento notarial é autêntico e presume-se válido e legítimo porque o seu autor é um notário que ajustou o negócio quanto à sua substância e forma à legislação em vigor. (NUNEZ LAGOS apud FALBO; CASTELNUOVO, 2019, p. 38).[1]

Logo, os elementos extraídos pela autenticidade, tais como:

> a) autenticidade subjetiva ou de autoria, refere-se a verdadeira identidade física da pessoa que construiu o documento, e não uma identidade digital — IP — de uma máquina utilizada em que, no máximo, pode oferecer uma suposição a uma pessoa que, em tese, tenha operando-a;
> b) autenticidade corporal do documento ou da coisa;
> c) autenticidade ideológica, que se refere ao pensamento, a sensibilidade, aos sentidos e ao juízo de valor na análise dos documentos onde a certificadora deveria oferecer, sendo que, humanamente impossível encarregar à máquina computacional cumprir essas funções, restando, portanto, competência típica para o notário.

Neste contexto, mister se faz mencionar trecho da doutrina peruana em que destaca o cuidado do Tabelião em identificar os envolvidos e avaliar a verdadeira manifestação das partes no negócio jurídico, agindo, portanto, como interface entre o usuário e o estado, resultando em captura de amplos elementos de identificações dos envolvidos, inclusive na ordem subjetiva, abaixo:

---

[1] El documento notarial fruto de las tareas dichas tareas, opus que deja el notário y corolario de la función notarial, es entonces la expresión del pensamiento humano(no solo una representación del mesmo), un hecho jurídico y al mismo Tiempo un acto jurídico, cujo autor es el notario y que se encuentra dotado de autenticidade o fe publica, la que irradia sobre tres planos: la autenticidad subjetiva o de autoría, la autenticidad corporal o del documento como cosa y la autenticidad ideológica (esta última atiene al pensamiento documentado, los actos proprios del notarios, los hechos que el notario percibe por seus sentidos, los juicios del notario y el contenidos de la declaraciones). Para que esa autenticidad Sea posible y perdurable es necessario que el Notario, cuidando de la forma, penetre en el contenido, en cuento lleve a cabo todas las tares esenciales de la función notarial, arriba explicadas. (…) De aquí pues, que ambas presunciones encuentren fundamento en la autoría del documento. El documento notarial es autêntico y se presume válido y legítimo porque su autor es un notário que ha ajustado el negocio en cuanto a su fondo y forma a la legalidad vigente. (NUNEZ LAGOS apud FALBO; CASTELNUOVO, 2019, p. 38).

Julgamento de capacidade, liberdade e conhecimento

A introdução deve expressar a capacidade, a liberdade e o conhecimento a que estão vinculados os que aparecem (art. S4-h LN). Trata-se de uma manifestação do notário, em consequência da sua capacidade jurídica, e cristaliza-se numa sentença que, enquanto tal, e não a verificação de um facto, só adquire o valor de afirmação proferida por pessoa especialmente habilitada. De fato, a capacidade (de entender e querer as próprias ações) não pode ser considerada um fato que se verifica diretamente de forma sensorial, por isso não é protegida pela fé pública. Por outro lado, a presunção de verdade imposta pelo julgamento notarial -sendo igualmente considerada verdadeira no trânsito-, produz menor eficácia, quando contrariada. Em alguns casos, pela gravidade da doença sofrida pelo comparecente ou pela idade avançada, o notário exige a intervenção de médicos, psicólogos ou psiquiatras, embora a sua presença não seja regulamentada por lei. Os médicos verificam a saúde física da pessoa, enquanto os psiquiatras o fazem em relação à saúde mental. A perícia médica ou psiquiátrica não exime o tabelião de sua obrigação profissional de proferir sentença de capacidade em relação aos comparecimentos, mas pode exonerá-lo da responsabilidade se for utilizada a diligência prévia (presença de médico especialmente habilitado), que não teria sido capaz de perceber a deficiência, que o sujeito sofre. Nesse caso, não há culpa profissional, portanto, também não há responsabilidade.

Pelo contrário, no domínio da liberdade (agir sem pressão interna ou externa) ou do conhecimento (consentimento informado dos efeitos do acto praticado) de quem compareça, o notário não pode recorrer a qualquer perito, uma vez que a liberdade é avaliada no seu contacto directo com as partes, enquanto o conhecimento decorre de sua própria ação quando ele executa seu dever de conselho ou informação em alerta para os efeitos jurídicos do instrumento que autoriza (art. 27 LN).[2]

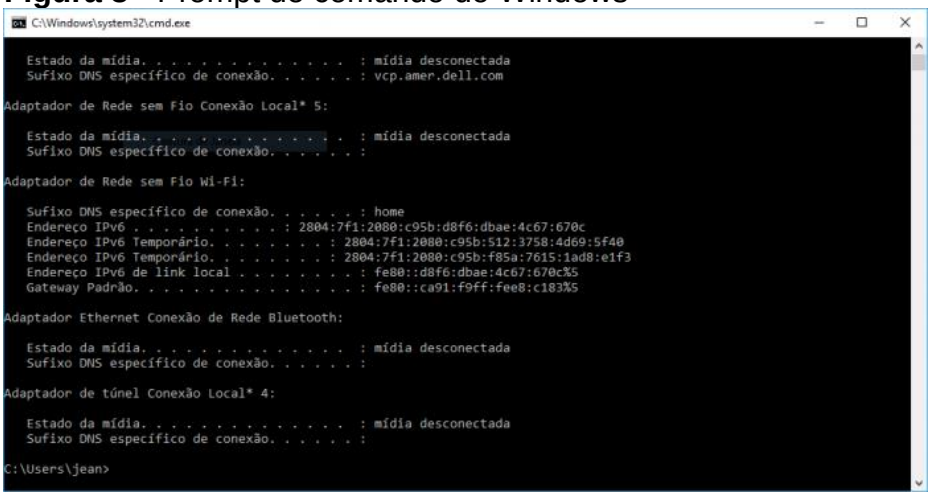
[2] Juicio de capacidad, libertad y conocimiento. La introducción deberá expresar la capacidad, libertad y conocimiento con que se obligan los comparecientes (art. S4-h LN). Esta es una manifestación del notario, consecuencia de su calidad de jurista, y cristaliza en un juicio que, por ser tal, y no la comprobación de un hecho, solo llega a adquirir el valor de una afirmación proveniente de persona especialmente cualificada. En efecto, la capacidad (de entender y querer los actos propios) no puede afirmarse que sea un hecho que directamente se constate en forma sensorial, por lo que no tiene amparo de fe pública. En cambio, la presunción de verdad impuesta por el juicio notarial -siendo igualmente considerada como cierta en el tráfico-, produce una eficacia menor, cuando se le contradice. En algunos casos, por la gravedad de la dolencia que padece el compareciente o por su avanzada edad, el notario requiere la intervención de médicos, psicólogos o psiquiatras, aunque su presencia no está regulada por la ley. Los médicos constatan la salud física de la persona, mientras los psiquiatras lo hacen respecto de la salud mental. La pericia médica o psiquiátrica no libera al notario de su obligación profesional de emitir el juicio de capacidad en relación con los comparecientes, sin embargo, podría liberarlo de responsabilidad si es se utilizó la diligencia debida (concurrencia de un facultativo especialmente cualificado), quien no habría podido advertir la discapacidad, que sufre el sujeto. En tal caso no hay culpa profesional, por lo que tampoco existe responsabilidad. Por el contrario, en el ámbito de la libertad (actuación sin presiones internas o externas) o el conocimiento (consentimiento informado de los efectos dei acto celebrado) de los comparecientes, el notario no puede auxiliarse en ningún experto, pues la libertad se evalúa en su contacto directo con las partes, mientras el conocimiento surge de su propia actuación cuando ejecuta su deber de consejo o información en advertir los efectos legales del instrumento que autoriza (art. 27 LN).

Assim, o notário não se resume simplesmente à análise superficial e objetiva dos elementos de identificações do usuário, mas, mais que isso, pois sua função primária é pavimentar um caminho seguro para construção da verdadeira autenticidade na ordem objetiva, bem como na subjetiva.

Por outro lado, além de todo o exposto, é importante apontar que, o usuário do computador logado a rede da internet, poderá, facilmente, navegar por ela ocultando ou modificando seu IP. Para ocultá-lo basta fazer uma simples pesquisa no Google com o seguinte tema: como navegar ocultando o IP? Em resposta, a primeira opção que apareceu na lista foi um navegador chamado “torproject” (https://www.torproject.org/pt-BR/download/languages/), que permitirá sua navegação anônima pela internet.

Já para modificar seu IP basta também fazer a mesma consulta no Google e/ou YouTube, os quais lhes entregarão algumas opções, dentre elas: Prompt de comando do Windows e via proxy.

Figura 3 - Prompt de comando do Windows

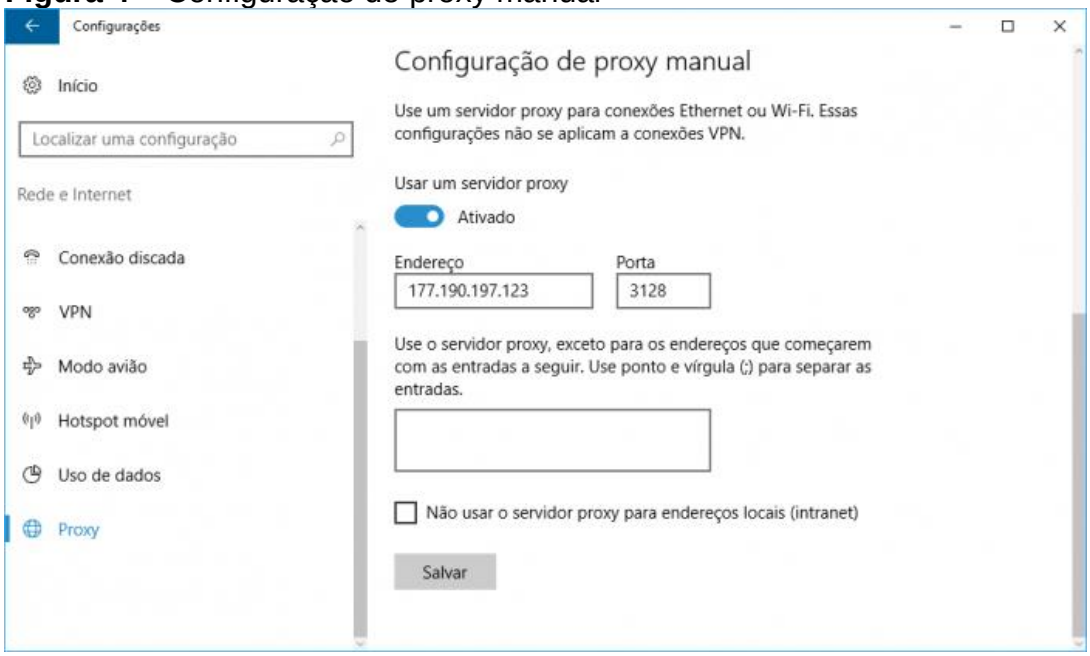


Fonte: (TECNOBLOG.NET, 2017, p. 1).

> Aperte a tecla Windows e digite “cmd” ou Prompt de Comando;
> No Prompt de Comando, digite ipconfig /release. Sua conexão vai cair;
> Espere um pouco até tudo ficar offline e digite ipconfig /renew;
> Isso deve renovar o seu IP, junto com a conexão (TECNOBLOG.NET, 2017, p. 1).

> Como mudar o IP do PC via Proxy. Se o método acima não funcionou, seja bem-vindo. O segundo método é um pouco mais complicado, mas certamente vai fazer com que você fique com um novo IP. Ele consiste em definir um proxy (intermediador entre você e o servidor) para traduzir a sua conexão. (TECNOBLOG.NET, 2017, p. 1).

Figura 4 – Configuração de proxy manual



Fonte: (TECNOBLOG.NET, 2017, p. 1).

> No Windows 7 ou anterior, entre no Painel de Controle > Opções da Internet;
> Entre na aba de Conexões e depois em Configurações da LAN;
> Ative a opção de usar um servidor de proxy para a rede local;
> No Windows 10, entre nas Configurações > Rede e Internet > Proxy;
> Depois, ative a opção Usar um servidor de proxy embaixo de "Configuração de proxy manual";
> Em ambas as versões do Windows, coloque o endereço de IP e a porta do Proxy e depois clique em Salvar ou OK. (TECNOBLOG.NET, 2017, p. 1).

Existem diversos *proxies* gratuitos para você usar. Recomendamos este site, que lista vários servidores e as portas para configurar no *Windows*, separando por *uptime*, velocidade e região. Basta copiar o **Proxy** IP e a *Proxy Port* e colocar nos respectivos campos de configuração.

Ademais, atualmente, no mercado, há diversos comandos criados para bloquear e apagar seus rastros, também desativar a sua geolocalização, enfim, tudo que for possível para garantir uma navegação mais oculta possível, impedindo, por conseguinte, a identificação do IP utilizado.

Neste sentido, a Medida Provisória 2.200-2/2001 (em vigor até hoje) que regulamenta a assinatura digital com ou sem uso de certificados digitais, estabelece como âncora de segurança a identificação do IP bem como a

geolocalização do dispositivo eletrônico que foi logado à rede, considerando como presunção de veracidade e autenticidade na autoria do documento desde que utilizado a arquitetura da ICP-Brasil. Assim, equivale, por óbvio, que qualquer pessoa — Autoridade de Registro — poderá ser dotada de fé pública, independentemente de sua qualificação técnico-intelectual, percorrendo, portanto, pela contramão da qualificação notarial.

Em contrapartida, é importante ressaltar que a fé pública é um dos mais antigos princípios do direito, o qual revestem as autoridades de condições jurídicas para autenticar fatos ou atos por ela presenciadas. Neste prisma, segue o que a doutrina diz sobre o assunto por intermédio do ensinamento de Loureiro (2017):

> A fé pública pode ser definida como a autoridade legítima atribuída aos notários — e a outros agentes públicos como juiz, o registrador e os cônsules, dentre outros — para que os documentos que autorizam em devida forma sejam considerados autênticos e verdadeiros, até prova em contrário (LOUREIRO, 2017, p. 1022).

Neste sentido, registra-se o entendimento de Santos (2004): “A fé pública notarial não provém do Estado, mas de um atributo da qualidade profissional do notário. O artigo 3º da Lei 8.935, diz expressamente que o notário é profissional do direito, dotado de fé pública”. (SANTOS, 2004, p. 36).

Para corroborar com a importância do Notário como portador da fé pública e interlocutor entre o mundo físico real para o mundo digital, o qual detém o poder certificante nas relações jurídicas do usuário, mister se faz trazer à pauta o ensinamento de Jacomino que, por ocasião de seu artigo publicado, citou um precedente do STF importante ao estudo; tema: *NFT´s* – a *tokenização* imobiliária e o *metaverso* registral.

> Os oficiais registradores são “órgãos da fé pública instituídos pelo Estado e que desempenham atividade essencialmente revestida de estatalidade – dependem, para efeito de ingresso na atividade notarial e de registro, de prévia aprovação em concurso público de provas e títulos”, consoante MOREIRA ALVES. A eles cabe “velar pela segurança, registro, publicidade e autenticidade dos atos jurídicos, além de investidos na relevantíssima função inerente à tutela administrativa dos interesses”. Os cartórios são instituições de direito público, “organizadas pelo Estado, em ordem a preservar a segurança das situações jurídicas individuais”. E remata o ilustre ministro no mesmo precedente do STF:
> “Os tabeliães e os oficiais registradores, nesse contexto – e no desempenho de seu ofício público –, dispõem de uma prerrogativa

> singular, ínsita à própria e suprema autoridade do Estado**, consistente no exercício do poder certificante, destinado a atestar a veracidade e a legitimidade de determinados fatos e atos jurídicos**. Essa circunstância só faz acentuar a estatalidade que qualifica as atribuições dos serventuários extrajudiciais, como enfatizou JOÃO MENDES JÚNIOR, em obra clássica (Órgãos da Fé Pública, 2ª ed., 1963, Saraiva)”38. (JACOMINO; UNGER, 2022, Online).

Assim, embora ela adviesse da lei, até a edição da famigerada MP, não se tinha notícias que o legislador escolhesse, aleatoriamente, o agente a ser revestido de fé pública. Ora, a base da fé pública é justamente a intelectualidade do agente, e não, isoladamente, um comando legal autorizando a qualquer pessoa jurídica de direito privado se cadastrar para tal.

O agente deverá ter condições para exercer esse princípio, que sejam pessoas altamente qualificadas que, na maioria das vezes, são profissionais do direito, além de serem submetidas pelo crivo do concurso público. Desse modo, aquele quem detém fé pública é porque se preparou para isso.

Pelo exposto, no Brasil, conforme a MP 2.200-2/2001 estabeleceu que qualquer interessado pode ser AR (autoridade de Registro) e, realizar o cadastro e a validação do cidadão que tenha interesse em adquirir Certificado Digital.

Diferente é a realidade na Argentina em que, determinou com que a AR (Autoridade de Registro) será somente exercida por Notários, pois estes sim, são o elo entre o usuário e a certificadora, conforme mencionado na obra dos professores Santiago Falbo e Franco Di Castelnuovo (2019):

> Em seguida, o processo de validação da assinatura consiste, primeiramente, em aplicar a chave pública do assinante ao hash do documento, criptografado com sua chave privada. O resultado desta operação será recuperar o hash original. Um segundo hash do documento assinado é gerado e comparado ao hash original recuperado. A partir da comparação destes dois hashes irá emergir se houve modificações no documento leigo de assinatura. (...) processos informáticos que se desenvolvem na aplicação de uma assinatura digital. Uma Autoridade Certificadora de assinatura digital (CA) é a entidade que presta serviços de certificação, gerando certificados de assinatura para requerentes e assinantes. Por sua vez, as entidades certificadoras dispõem de uma estrutura de Autoridade de Registo (AR) que (...) exerce as funções de validação e demais dados dos requerentes e assinantes certificados, registando as apresentações e procedimentos que por elas são formulados. Por sua vez, o Colégio de Notários da Província de Buenos Aires foi constituído como Autoridade de Registro de Assinaturas Digitais da certificadora ONTI, estabelecendo que os assinantes de certidões serão pessoas físicas que sejam notários da Província de Buenos Aires em pleno exercício da profissão". Da política de certificação única da Autoridade Certificadora ONTI (Escritório Nacional de Tecnologia da Informação) em http://pki.jgm.gov.ar/cps/cps.pdf (SANTIAGO FALBO; FRANCO DI CASTELNUOVO, 2019, p. 72).[3]

Desse modo, verifica-se que na Argentina reconheceu a importância de escolher, acertadamente, quem deveria figurar como elo entre o usuário e a certificadora, determinando, portanto, que somente os notários pudessem exercer a função de Autoridade de Registro (AR).

Além da República da Argentina, após acurado estudo, foi possível encontrar que no Peru também delega ao Notário a função de qualificar a identidade do interessado em se cadastrar, a fim de adquirir Certificado digital, conforme abaixo:

[3] Luego, el proceso de validación de la firma consiste en, primero, aplicar la clave pública del firmante al hash del documento, encriptado com su clave privada. El resultado de esta operación será recuperar el hash original. A continuación, se general un segundo hash del documento firmado, y se compara com aquela hash original recuperado. Del cotejo de estos dos hash surgirá si ha habido modificaciones en el documento lego de la firma. (…) procesos informáticos que se desarrolhan en la aplicación de una firma digital. Una Autoridade Certificante (AC) de firma digital es la entidad que presta los servicios de certificación, generando los certificados de firmas de los solicitantes y suscriptores. A Su vez, las autoridades certificantes cuentam com una estructura de Autoridade de Registro (AR) que (…) efetuan la funciones de validacion y de otros dados de los solicitantes y suscriptores certificados, registrando las presentaciones y trâmites que eles Sean formulados por éstos. Por su parte, el Colegio de escribanos de la Provincia de Buenos Aires se ja constituído como Autoridade de Registro de firma Digital del certificador ONTI, estabeleciendo que los suscriptores de certificados será las personas físicas que sean notários de la Provincia de Buenos Aires en pleno ejercicio de la profesión". De la política única de certificación de la Autoridad Certificante ONTI (Oficina Nacional de Tecnologia de información).

> De acordo com a lei peruana, os instrumentos extraprotocolares podem ser atas ou certificações. Os primeiros são instrumentos lavrados pelo notário público, nos quais atestam a consumação de um facto e, excepcionalmente, uma declaração de vontade. A segunda são atestados em documento particular lavrado por sujeitos particulares, onde o notário verifica, extrinsecamente, aquele fato específico que lhe é conhecido.
> São atos (art, 94 LN):
> a) autorização de viagem de menores;
> b) destruição de propriedade;
> c) entrega;
> d) conselhos, diretorias, assembleias, comitês e demais atos societários;
> e) verificação de identidade, para fins de prestação de serviços de certificação digital;
> f) transmissão por meio eletrônico de manifestação de vontade de terceiros; g) Verificação de documentos e comunicações eletrônicas em geral. (página 1038/1039 DIREITO DE REGISTRO E NOTARIAL Volume II Günther Gonzales Barrón - Jurista Editores E.I.R.L, 2022 - Quinta Edição - janeiro de 2022)[4]

Logo, nota-se que essa modalidade funcional exercida pelo notário peruano é chamada atos extraprotocolares, os quais fazem parte de uma extensa gama de possibilidades, inclusive a análise da identificação do usuário, para efeitos de serviços de certificação digital, conforme letra “e” acima mencionada.

Voltando ao tema sobre a corrida tecnológica citada no início desse estudo, o notariado brasileiro, somente no ano de 2021, após do advento do provimento 100 do CNJ inovou apresentando o Certificado Notarial “E-notariado”:

[4] Según la ley peruana, los instrumentos extraprotocolares pueden ser actas o certificaciones. Las primeras son instrumentos redactados por el notario, en el que otorga fe de la realización de un hecho y, excepcionalmente, de alguna declaración de voluntad. Los segundos son atestaciones en documento privado redactado por sujetos particulares, en donde el notario comprueba, de forma extrínseca, aquel hecho específico que le consta.
Son actas (art, 94 LN):
a) de autorización para viaje de menores
b) de destrucción de bienes
c) de entrega
d) de juntas, directorios, asambleas, comités y demás actuaciones corporativas
e) de constatación de identidad, para efectos de la prestación de servicios de certificación digital
f) de transmisión por medios electrónicos de la manifestación de voluntad de terceros
g) de verificación de documentos y comunicaciones electrónicas en general. (página 1038/1039 DERECHO REGISTRA! Y NOTARIAL Tomo II Günther Gonzales Barrón - Jurista Editores E.I.R.L, 2022 - Quinta Edición - Enero 2022).

> Plataforma e-Notariado. O e-Notariado é a plataforma digital gerida pelo Colégio Notarial do Brasil – Conselho Federal, que conecta os usuários aos serviços oferecidos pelos cartórios de notas em todo o Brasil. O que é um ato notarial online. A partir da publicação do Provimento nº 100/2020, cidadãos de todo o País podem realizar atos notariais de forma online, por meio da plataforma e-Notariado, que oferece segurança jurídica e os mesmos efeitos de um ato realizado de forma presencial no cartório de notas. Todo ato notarial online contará com videoconferência entre o requerente e o tabelião, e a assinatura da parte por meio de certificado digital (BRASIL – e-Notariado, 2022, p. 1).

Para isso, criou-se um produto para competir com o Certificado Digital Privado. Este produto é o Certificado Notarial Público, o qual pode ser adquirido facilmente por qualquer cidadão, pois basta com que o usuário acesse a plataforma para buscar um cartório credenciado, em seguida emitir gratuitamente seu certificado digital. Embora esta iniciativa viesse após o instituto notarial já ter perdido diversas atribuições (reconhecimentos de firmas digital) pela iniciativa privada, resultado da disseminação dos Certificados Digitais privados pelo Brasil, é salutar considerá-la como necessário suspiro de sobrevida ao instituto, caso contrário, certamente, será eliminado do sistema.

O Certificado digital notarizado é gratuito. Além disso, ele adota protocolos de segurança vinculados a arquitetura da ICP-Brasil com criptografia assimétrica somada à qualificação notarial exercida por um profissional do direito dotado da genuína fé pública.

Ocorre que na ocasião da edição da MP 2.200-2 no ano de 2001 estabeleceu-se que qualquer interessado pudesse ser AR (Autoridade de Registro) substituindo, portanto, a figura do Tabelião no exercício dos reconhecimentos de firmas, os quais foram realizados eletronicamente por intermédio da arquitetura vinculada a ICP-Brasil. Ou seja, se no ano de 2001 o colégio Notarial já tivesse a tecnologia e-Notariado, jamais o instituto notarial passaria de protagonista à coadjuvante neste quesito.

Não para por aí, pois, o fato de o Instituto Notarial à época não ter acesso à tecnologia das assinaturas eletrônicas, não o impediria de trabalhar perante o Congresso Nacional a fim de demonstrar a importância do Tabelião para figurar como interface do usuário e o estado. Ou seja, a Autoridade de Registro deveria ser, por óbvio, o Tabelião de notas.

Pelo exposto, foi elencada várias perspectivas sobre o certificado

digital. Abordou-se seu significado, sua formação, como é comercializado e qual sua finalidade. Também, foi possível traçar um paralelo do período analógico e do digital sob o enfoque da construção dos atos e negócios jurídicos.

Seguimos analisando se realmente o Certificado Digital pode entregar autenticidade de autoria como prometido pela lei, bem como a integridade dos documentos assinados por ele. Também citamos como é enfrentado o Certificado Digital na República da Argentina e Peruana.

Além disso, apresentaram-se algumas vulnerabilidades dessa tecnologia e sugestões para torná-la realmente mais assertiva. Destacamos, principalmente a questão da disseminação e o mercantilismo do certificado digital privado e o aumento dos crimes digitais, permitindo, portanto, abertura para a uberização do Notariado Brasileiro.

Respeitando posições adversas, conforme estudo, resta demonstrado que a MP 2.200-2/2001 deveria sofrer pequenos ajustes, sendo como principal, seguir o modelo argentino, a cuja autoridade de registro deverá ser exclusivamente representada por um notário. Por conseguinte, a emissão do Certificado deverá ser feita pela plataforma e-Notarial e gratuita para toda população brasileira.

Neste padrão, a milenar fé pública será respeitada ao oferecer verdadeira autenticação para a construção, validade e integridade dos negócios e atos jurídicos, a fim de fomentar a segurança jurídica e prevenir de litígios**.**

4.2 OS REGISTROS PÚBLICOS NA ERA DA TECNOLOGIA BLOCKCHAIN

4.2.1 Surgimento e Desenvolvimento do *Blockchain*

Com a explosão da crise imobiliária de 2008 nos Estados Unidos, o mercado financeiro sentiu fortemente seu impacto. Isso gerou boatos de que os bancos americanos entrariam em estado de insolvência. O que de fato, não foi só boato, pois realmente levou a falência o Lehman Brothers um dos mais tradicionais bancos dos Estado Unidos. No entanto, não parou por aí, pois, em seguida, vários outros anunciaram perdas bilionárias.

Essa situação fez com que um grupo de anônimos de programadores (*cypherpunks*) construíssem uma moeda digital que pudesse ser estruturada e transacionada sem a intermediação do sistema financeiro tradicional(bancos), a fim

de blindá-la de crises semelhantes à de 2008.

Por outro lado, há especulações que diz que a moeda digital, bem como a *Blockchain*, foi criada para possibilitar com que os hackers pudessem receber e movimentarem *criptoativos* sem ser identificados e/ou rastreados.

Então surgiu a bitcoin, a fatídica moeda virtual. Entretanto, para ela poder ser usada foi necessário ser projetada com base em uma arquitetura de consenso por blocos interligados, ou seja, *blockchain*.

Há três componentes que compõe a *blockchain*: nós, transações e blocos. Os nós são representados pelos computadores espalhados pela rede que atuam armazenando os blocos, por intermédio de um software que armazena e distribui cópias das informações em tempo real.

Os blocos são os registros das informações que advém das transações confirmadas e adicionadas na rede *blockchain* formando uma cadeia de blocos interligados. Logo, só se altera o conteúdo de um bloco se houver o consenso dos demais. Portanto, se houver alteração ilícita de um bloco, os demais garantem a integridade das réplicas originais.

A transação é o comando que recepciona a vontade particular e autoriza a movimentação e/ou inserção da informação na rede. A rigor é uma assinatura digital particular de alguém que encaminha a informação aos blocos, por intermédio dos nós. É a porta de entrada.

Trazendo para os Registros Públicos, suponha, por exemplo, que os blocos são os livros e arquivos dos registradores civil e imobiliário, os quais irão armazenar as informações trazidas pela transação representada pelo Tabelião de Notas. Percebam que, este recebeu e tratou a vontade particular, em seguida, encaminhou-a a rede *Blockchain* para ser registradas aos blocos.

Ademais, para melhor esclarecimento, ressalta-se a obra *Blockchain*, *tokens* e *criptomoedas* (UHDRE, 2021):

> Descentralização da arquitetura de rede, de modo a se ter vários computadores conectados de forma distribuída ao redor do globo. Ainda, distribui-se o registro dos dados, de forma que cada um desses computadores detenha a contabilidade atualizada das operações realizadas. (É como se todos os computadores são chamados de nós, nodes ou legder) da rede e que cada um deles atualizaria quase simultaneamente o registro das informações recebidas. Essa estrutura descentralizada de rede e registro é o que chamamos de Distributed Ledger Tecnology (DLT) = blockchain. A ligação entre os blocos é

> iniciada por meio dos chamados hash do bloco anterior, o qual faz a conexão entre ele e o bloco anterior, e ao final terá um hash unívoco seu, que simultaneamente iniciará o bloco seguinte (UHDRE, 2021, p. 33).

Em suma, é uma arquitetura tecnológica de registros descentralizadas de informações capturadas e interligadas entre diversos computadores no globo. E para que suas informações sejam inseridas e/ou alteradas deverá haver um consenso com validação dos códigos *hash* (ou seja, desde que resolvido as operações dos problemas matemáticos).

Neste sentido, então, como ocorrerá a garantia da integridade das informações constantes nos blocos? Pois bem, será necessária validação e/ou certificação de suas informações constantes nos *nós*.

Assim, conforme mencionado anteriormente, é necessário garantir a integridade das informações armazenadas nos *nós*. Para tanto, elas são replicadas e criptografadas resultando em um código *hash*, o qual é muito difícil de gerar.

Este código consiste em resolver complexos problemas matemáticos até encontrar a cifra chave da criptografia ou criar um código inédito para fechar o bloco. No entanto, não é tarefa fácil. Pois, para isso ser possível, os computadores ficam ligados diretos, ou seja, 24 horas por dia e sete (07) dias na semana e todos os dias do ano, demandando alto consumo de energia elétrica.

Além do que, deverá haver o consenso de 50% mais 1% de todos os nós da rede para validar e/ou alterar a informação do bloco. Ocorre que, não para por aqui, pois, além delas serem criptografadas, também deverão se submeterem ao consenso na forma mencionada.

Nessa arquitetura, as informações, para serem alterada, os *nós* interligados deverão decifrar e/ou criar códigos inéditos por intermédio de uma metodologia de segurança: prova de trabalho, prova de estaca e prova de autoridade.

A prova de trabalho(*proof-of-work*) é conhecida por sua alta segurança no que tange a integridade das informações constante nos blocos. Pois, esta metodologia contém o maior número de nós espalhados pelo globo. E, quanto maior o número de nós, mais seguro é a rede. Por outro lado, esta quantidade de nós trabalhando nas operações matemáticas para gerar seus códigos *hashs*, demandará enorme consumo de energia.

Quem adota esta metodologia de segurança é a conhecida moeda

virtual Bitcoin e, também Litecoin, Namecoin, dentre outras. Neste sentido, oportuno mencionar uma pesquisa citada e publicada como trabalho científico de Mereles:

> O custo computacional de geração desse hashes é alto, o que se traduz em uma grande quantidade de energia que deve ser consumida para sua energia. Em 2015, a quantidade de energia elétrica usada para gerar uma transação de Bitcoin foi estimada em 1,75 vezes o consumo diário de energia elétrica de uma casa média nos Estados Unidos. Um estudo mais recente realizado em 2018 estima que o custo para realizar uma transação em Bitcoin é de 851 quilowatts/hora, enquanto para realizar 100.000 transações em VISA são utilizados 169 quillowatts/hora. (MERELES apud TECMUNDO- ONLINE, 2019).

Ademais, cumpre ressaltar, em 12/05/2021, em seu Twiter, o fundador da TESLA, Elon Musk, teceu o seguinte comentário:

> Nos preocupa o uso cada vez maior de combustíveis fósseis na mineração (ndr: emissão monetária) e transações de bitcoins, especialmente o carvão, que tem emissões piores do que qualquer combustível. A criptomoeda é uma boa ideia em muitos níveis e achamos que tem um futuro promissor, mas isto não pode ter um grande custo para o meio ambiente. (MUSK, 12/05/2021, @elonmusk).

Assim, nota-se que o consumo de energia está ligado diretamente a quantidade de *nós* existente na rede, a cuja tem reflexo direto na segurança e integridade das informações. Assim, se uma rede tem uma quantidade menor de *nós*, para economizar energia, consequentemente sua segurança será menor e o sistema torna-se mais vulnerável ao ataque dos 51%.

A Prova de aposta (*Proof of stake*) é outra metodologia de segurança criada como alternativa à Prova de Trabalho e, é usada pela *Ethereum, Credits*, dentre outras. Este método de segurança difere da prova de trabalho, pois neste é ilimitado a criações de blocos, e aquela é limitado e será representado por criptomoedas, dificultando o ataque dos 51%.

Por fim, há também a Prova de autoridade (*Proof of authority*), é usada com quantidade reduzidas de *nós* a fim de reduzir a carga computacional e energia. Entretanto, mais vulnerável ao ataque dos 51%.

Ademais, no que tange a imutabilidade das informações armazenadas e a segurança da rede, Uhdre (2021) menciona:

> Blockchain pública, se um número suficiente de participantes decidir agir contra as regras, não há como detê-los. Ou seja, sempre há a possibilidade, ainda que teórica, de um ataque de 50%+1(cinquenta por cento mais um), o que significa que um grupo que controla a maioria da energia (ou pontos) de mineração da rede poderia assumir o controle de toda a rede. Apesar de isso parecer extremamente improvável – sobretudo ante o custo energético que precisa ser gasto, no caso do consenso – proof-of-work -, é de se perceber que os principais pools de mineração atualmente controlam mais de 50% de todo o poder de computação da rede Bitcoin, o que torna a ameaça de um ataque de 50%+1 ainda mais real. (UHDRE, 2021, Online).

Logo, verifica-se que a tecnologia *Blockchain* é segura, entretanto, não incorruptível como é vendido pela mídia e pseudos “especialistas”. Pois, o exemplo citado acima é somente uma das maneiras de corrompê-la.

Ainda, ressalta-se o gasto presente de energia elétrica para sua operação e também as taxas das transações que, a médio e longo prazo, a tendência é elevar os valores. Pois, além da eletricidade despendida, também deverá contar com a atividade dos participantes donos dos computadores — *nós* — que resolvem os problemas matemáticos.

Essa atividade consiste em apontar um vencedor que descobre a cifra e/ou cria nova criptografia inédita, para, em seguida, validar e inserir o novo bloco de informação. Ou seja, são os mineradores proprietários dos computadores *(nós).* Estes participantes receberão como contraprestação uma quantia em Bitcoin além das taxas de transações “*fees*”.

Ademais, sobre o contexto, mister se faz trazer informações sobre a escassez da contraprestação (Bitcoin e as taxas de transações) oferecidas aos mineradores. Pois, elas são finitas e, com o tempo, poderão se tornar muito onerosas UHDRE, 2021:

> Convém esclarecer ainda que, consoante a programação do protocolo Bitcoin, apenas 21 milhões de unidades de bitcoins serão criadas (emissão essa que tem previsão de se encerrar em 2040). Após isso, a remuneração dos validadores dar-se-á apenas com as taxas transacionais “fees” que tendem, obviamente, a serem mais custosas (UHDRE, 2021, Online).

Muito bem, após descrever sobre a maneira como os mineradores atuam, agora é o momento de continuar desvendando como as informações cifradas nos *nós* podem ser alteradas.

Caro leitor, imagina uma teia de aranha onde cada ponto de ligação

do fio é um computador/nó e toda a teia é representada pela arquitetura *blockchain*. Logo, para alterar qualquer informação armazenada em cada bloco do nó será necessário o consenso da maioria dos nós. Por esta razão que se denomina cadeia descentralizada.

Neste protocolo de consenso somando todos os nós da cadeia, será necessário o consenso de 50% mais 1% de todos, para autorizar a alteração de qualquer conteúdo constante no bloco. Esta metodologia, em tese, traz segurança, pois é muito difícil conseguir o consenso desta porcentagem de blocos. Em um exemplo prático, uma invasão hacker deverá invadir e acessar no mínimo 51% da cadeia total da rede, o que se torna uma tarefa difícil, porém, não impossível como já mencionado neste estudo. Nada difícil para força computacional das *Big Tech's*.

Por outro lado, o uso da tecnologia *Blockchain* traz dúvidas quanto a soberania de uma nação. Pois, como se estudou, para ela poder funcionar serão necessários a descentralização de vários pontos de minerações compostos pela força computacional e alto consumo de energia espalhados pelo mundo. Nesse sentido, os locais ideais para minerar os códigos são países frios, pois proporcionam refrigeração adequada aos computadores, bem como aqueles que oferecem energia com baixo custo, em razão do alto consumo de energia elétrica. Portanto, os países sedes dos mineradores são poucos, atualmente, podendo ser citado como China, Rússia, EUA, Paraguai, dentre outros — menos o Brasil.

Assim, quando uma nação utiliza essa arquitetura tecnológica, certo será que ela ficará dependente dos países sede dos mineradores, ocasionando, portanto, vulnerabilidade aos documentos processados por ela. De modo que, por óbvio, haverá vulnerabilidade tanto do conteúdo das informações, como também do sistema na totalidade, ocasionado uma, eventual, fissura na soberania dos países usuários.

Neste prisma, segue a seguinte reportagem:

> CAZAQUISTÃO - Governo desativou o serviço e prejudicou o poder computacional da rede de criptoativos; o país asiático é o segundo maior minerador do mundo, atrás dos EUA. Pouco antes de oficializar a renúncia, o gabinete do presidente Kassym - Jomart Tokayev ordenou a suspensão dos serviços de internet no país. Com isso, a segunda maior rede de mineração de Bitcoin do mundo. (VEJA-ABRIL, 2022, p . 1).

Embora, houvesse o fator da descentralização do local dos

mineradores, não se pode negar que se um pool de mineradores corresponder a mais de 51% da rede estiver localizado em algum país que possa gerar esse tipo de incidente, haverá sério risco a rede.

Diante disso, soa elementar a existência de vulnerabilidade, pois basta o país sede de o pool de mineração interromper o sinal da internet ou o acesso à energia para desestabilizar a *blockchain*. Causando, por conseguinte, eventuais, prejuízos, ao país usuário.

O país usuário ficará de mãos atadas para solucionar o problema, dependendo da boa vontade do país sede, abalando, por conseguinte, a sua soberania e a segurança jurídica.

Nesta esteira, importante mencionar o conteúdo de um artigo publicado na Folha de São Paulo, de autoria do Ministro Lewandowski, sobre o tema Soberania em um mundo digital, onde reflete essa problemática no mundo contemporâneo (LEWANDOWSKI, 2022):

> Desconhecida na antiguidade greco-romana e na Idade Média, a concepção jurídica de soberania somente se firmou nos albores da Era Moderna, quando determinados reis e príncipes passaram a concentrar o poder político em suas mãos, antes exercido de forma difusa pelos senhores feudais. Sem embargo, a dominação de um homem ou grupo de homens sobre outros pela força, crença ou tradição sempre existiu.
> Ocorre que, a partir das revoluções liberais-burguesas, deflagradas no século 18 contra o absolutismo monárquico, o poder do soberano — leia-se estatal —, apesar de ainda amplo, passou a ser limitado pelo direito. Melhor explicando: no âmbito interno, os Estados, embora possam impor suas leis e determinações coercitivamente dentro dos respectivos territórios, precisam respeitar os direitos e garantias fundamentais. Já no plano externo, não obstante atuem com total independência e desembaraço, devem observar as regras do direito internacional e os princípios universais que o informam.
> Nos tempos atuais, com o advento da internet, a ideia de territórios mapeados com minuciosa precisão, inteiramente submetidos às distintas jurisdições estatais, começou a competir com a nova realidade de um espaço virtual, sem fronteiras definidas, no qual as interações humanas, para o bem ou para o mal, ocorrem instantaneamente, com uma frequência cada vez maior, superando distâncias e barreiras geográficas.

Esta nova realidade digital é formada no ciberespaço, cuja soberania ainda é estranha como nos primórdios da civilização. Segue o artigo:

> Tal fenômeno suscita algumas indagações jurídicas ainda não inteiramente respondidas. Por exemplo: seria possível conferir a esse mundo digital um tratamento análogo aos espaços aéreo e marítimo, sobre os quais os Estados podem legitimamente impor as suas normas, ou estaria ele imune a qualquer disciplina legal, assim como ocorre com o alto-mar, a exosfera e os corpos celestes?
> A questão cresce ainda em complexidade quando se constata que esse espaço virtual é dominado por grandes empresas privadas transnacionais, conhecidas como "big techs", as quais sobrevivem, basicamente, da comercialização de nossos dados pessoais, contínua e massivamente capturados por meio de suas plataformas digitais, em geral disponibilizadas de forma gratuita.
> Esses dados, submetidos a uma análise estatística e com o auxílio de algoritmos, permitem prever — e o que é muito preocupante — induzir comportamentos individuais ou coletivos quanto a hábitos de consumo, inclinações afetivas e preferências políticas, colocando em risco, neste último caso, a livre formação e manifestação da vontade dos eleitores (LEWANDOWSKI, 2022, p. 1).

Conforme autor, um ambiente sem soberania estatal remete a hostilidade da minoria em favor de pequenos grupos privados que possam manipular o ambiente da maneira como acharem conveniente. Por fim, segue o artigo:

> Para piorar as coisas, sob a superfície aparentemente plácida desse mundo digital, existe uma camada profunda, inacessível aos usuários comuns, conhecida por dark web ou deep web, onde são gestadas as fake news mais insidiosas e toda a sorte de negócios ilícitos, operados mediante criptomoedas, com destaque para o tráfico de armas, drogas e pessoas. É o ambiente onde atuam com desenvoltura grandes organizações criminosas, grupos terroristas e até mesmo agências estatais com propósitos escusos.
> O intrincado dilema posto para os Estados democráticos por essa nova realidade, ainda não inteiramente compreendida, consiste em conciliar a sua obrigação constitucional de garantir a plena liberdade de expressão e comunicação com o seu dever institucional de reprimir mensagens —sobretudo aquelas impulsionadas em massa por robôs — que tenham o potencial de colocar em risco a vida, a segurança e, paradoxalmente, o próprio livre arbítrio dos cidadãos. (LEWANDOWSKI, 2022, p. 1).

O ciberespaço é um ambiente ainda muito novo e, deve ser explorado com atenção pelas nações. Muitas delas estão hiper conectadas pela rede, proporcionando um elo que nem sempre será controlado por elas.

Ademais, conforme já estudado neste artigo, a rede de internet é formada por cabos transatlânticos instalados em locais estratégicos no fundo do oceano, os quais são percorridos toda informação computacional — inclusive os conteúdos armazenados pela rede *blockchain*. Sabendo disso, países com interesses

nem sempre revelados conseguem acessar esses cabos por intermédio de navios espiões ancorados nos pontos em que eles se encontram. A propósito, importante mencionar (O ESTADO DE S. PAULO, 2020):

> A Marinha brasileira monitorou durante uma semana um navio russo de pesquisa e inteligência suspeito de espionagem na Europa e nos Estados Unidos. O sinal de alerta foi aceso no último dia 10, quando o Centro Integrado de Segurança Marítima do Rio de Janeiro detectou o Yantar, uma embarcação de tecnologia avançada de sensores, dentro da Zona Econômica Exclusiva (ZEE) do Brasil. O barco, nesse momento, já estava próximo do litoral carioca, **numa área de cabos submarinos de internet, atracando na noite do dia 18 no porto do Rio, onde deve ficar até o fim de semana.** Um militar consultado pelo Estado disse que o desligamento do sistema de identificação pode envolver tentativas de espionagem ou procedimentos fora da normalidade pelo navio. Para ele, a navegação do Yantar pela costa brasileira não era ilegal, mas seu "desaparecimento" por seis dias foi considerado estranho. Logo após um primeiro contato, o navio sumiu do monitoramento, levantando a hipótese de que o equipamento AIS, que permite a sua localização, tenha sido desligado. Uma operação de patrulha do navio foi imediatamente desencadeada. Sob suspeita, a embarcação foi embora da costa brasileira antes do programado. No fim da tarde do domingo, 16, um helicóptero da Marinha e um avião da Força Aérea Brasileira (FAB) localizaram a embarcação a 50 milhas (80 quilômetros) das praias do Rio. Numa primeira abordagem, a tripulação russa não atendeu às chamadas. Depois, deu resposta evasiva à pergunta sobre o trabalho que realizava. Autoridades americanas levantaram a suspeita de que os pequenos submarinos transportados pelo Yantar operam especialmente no rastreamento de áreas de cabos submarinos. Conexões **Os cabos submarinos ligam os servidores de internet de países de diferentes continentes. Estima-se que essas ligações respondam por 99% das comunicações transoceânicas e 97% das conexões de internet entre os servidores do mundo**. Nesta semana, o serviço de inteligência da Irlanda flagrou agentes russos investigando cabos submarinos de fibra ótica que conectam a Europa aos Estados Unidos. A segurança dos dados que passam pelos cabos é uma preocupação central de Washington e Europa. Na Zona Econômica, o Brasil tem direito exclusivo de exploração de todos os recursos marinhos, na água, solo e subsolo, como petróleo, gás natural e frutos do mar. (O ESTADO DE S. PAULO, 2020, p. 1).

Neste contexto, interessante o caso Edward Snowden, o qual quando questionado como funcionava o sistema Xkeyscore da NSA, declarou:

> Você podia ler o e-mail de qualquer pessoa do mundo, qualquer pessoa de quem você tivesse o endereço. Qualquer website: você pode ver o tráfego de entrada e saída. Qualquer computador onde estiver uma pessoa: você tem como observar. Qualquer laptop rastreado: você tem como acompanha-lo andando de ponto a ponto no mundo inteiro (BRIDLE, 2018, p. 199).

Qualquer movimentação pela internet, mesmo usando os grandes players como Microsoft, Yahoo, Google, Facebook, YouTube, Skype, Apple e outros, não estão isentos de dados serem espionados por quem interessa.

Além dessa possibilidade de interceptar os dados dos servidores desses gigantes da tecnologia, ainda há opção da captura dos dados brutos. Pois, a rede está interconectada pelo mundo por intermédios dos cabos de fibras ópticas transatlântico, os quais podem ser interceptados por mal-intencionados em busca de captura de dados, neste sentido transcreve a seguir: “revelou-se que o alcance das agências de inteligência ia ainda mais fundo, incluindo a coleta de dados brutos nos cabos que efetivamente transmitem a informação no mundo” (BRIDLE, 2018, p. 199).

Portanto, notam-se que ao depender de como é arquitetado os dados e informações a trafegar pela rede de uma nação soberana, poderão ser violados sem muito esforço, tendo como objetivo interesses nem sempre revelados. Assim, faz todo sentido avaliar a forma de projetar a circulação e o armazenamento de determinados dados.

Esse novo mundo construído na rede da internet, nem sempre oferece a segurança jurídica que uma sociedade soberana espera. Portanto, nota-se que a tecnologia blockchain é construída no ciberespaço, o qual carece de regulação. Além disso, interessante realizarmos o seguinte exercício de reflexão: imagine que, doravante, todo acervo dos Registros Públicos Brasilleiro fosse realizado e armazenados por intermédio dessa nova arquitetura tecnológica, por conseguinte, sabendo com que ela se utiliza de *nós* espalhados pelo mundo, conforme já estudado. Assim, toda operação computacional do seu acervo será processada pelos mineradores ao redor do mundo, notadamente, nos países que oferecem energia elétrica com preço baixo: Rússia, China e Paraguai. Nesses países serão possíveis o funcionamento perfeito da rede.

Hipoteticamente, algum desses países, ou uma aliança de mais de um país — que sozinho ou em decorrência dessa aliança, possam compor o consórcio de mineradores que perfazem mais de 51% dos blocos — entram em guerra e/ou por

algum motivo decidem cortar a internet e/ou a interrupção de energia elétrica. Logo, isso seria suficiente para desestabilizar todo sistema registral Brasileiro.

Esse exemplo é um dos vários existentes que demonstra a fragilidade da soberania de um país frente a essa realidade. Verifica-se, que nesta hipótese a soberania Brasileira não será respeitada. Por outro lado, não soa economicamente viável a construção de uma rede *blockchain* privada ou pública utilizando *nós* somente no território brasileiro, em razão do alto custo da energia elétrica e o clima no Brasil, bem como a necessidade de descentralizar a operação.

Portanto, percebe-se que a *blockchain* é uma tecnologia inovadora e interessante e pode ser vastamente utilizada em benefício da sociedade. Porém, por ser muito nova é salutar aprofundar seu estudo para saber utilizá-la melhor.

4.2.2 Registros Públicos

Em decorrência do covid-19, as pessoas experimentaram a necessidade do distanciamento social. Logo, para com que elas pudessem se relacionar e praticar determinadas atividades, foi necessário buscar a utilização da tecnologia de forma jamais vista, tais como: videoconferência, digitalização dos documentos, utilização das redes sociais, dentre outros.

Esta mudança de comportamento, contribuiu para a aceleração tecnológica bem como o aumento na virtualização das relações humanas e negociais. Neste cenário, se popularizou diversas modalidades como a arquitetura *blockchain*.

Por outro lado, tem se os registros públicos responsáveis pela captação, circulação e armazenamento de grande parte dos dados das relações humanas e negociais. Sendo que, este instituto é vastamente conhecido no Brasil e na maioria dos países ao redor do mundo por sua utilização milenar e alto grau de confiabilidade.

Neste sentido, não se busca aqui, aprofundar os dois institutos. Senão, realizar um panorama a fim de detectar alguns pontos relevantes para melhor análise sobre o tema.

Eles são compostos por várias atividades com base no artigo 236 da Constituição Federal (BRASIL, 1988), Lei de Registros Públicos 6.015/73 (BRASIL, 1973) e o estatuto dos notários e registradores a Lei 8.935/94 (BRASIL, 1994).

Para isso, será demonstrado como os registros públicos atuam como

receptador da vontade das pessoas e armazenam seus dados, refletindo na segurança e a garantia da imutabilidade das informações.

Dentre várias atividades dos Registros Públicos, trago para este estudo o Registro Civil das Pessoas Naturais, Tabelião de Notas e os Registros de Imóveis. Estas foram escolhidas para facilitar a compreensão, sem menosprezar as demais que continuam tendo valor à sociedade.

O Registro Civil das Pessoas Naturais é muito antigo, pois desde que surgiu o ser humano, de alguma forma, foi preciso registrar seu nascimento. Sendo que, nos primórdios, a sociedade era diminuta e, com passar do tempo, foi ganhando volume. Diante disso, tornou-se imprescindível o cadastro e o controle das pessoas.

Este controle é para o Estado realizar o censo político, social e militar, além de individualizar a pessoa, dentre outros. Todo o conteúdo de dados fora sendo captados e armazenados pelas autoridades à época, exemplo: os Hebreus, Império Romano, Igreja Católica (O Registro Eclesiástico) e atualmente pelo Estado.

Neste instrumento de construção e captação de informações eram respeitados protocolos de formalidades para inseri-las aos bancos de dados competentes. Dentre alguns dos protocolos citam-se: a solenidades, a presença de testemunhas, autoridades eclesiásticas, bem como intérpretes da Lei como os Notários.

No Brasil Colônia a Igreja era responsável por todo gerenciamento dos dados das pessoas. Ocorre que, nesta ocasião, somente os católicos transitavam neste banco de dados. Em decorrência da Proclamação da República, o Estado Brasileiro direcionou seus esforços para atingir o maior número de pessoas e não somente aos católicos. Neste sentido, foi sendo publicada leis para obrigar todas as pessoas que vivem no Brasil a terem que passar pelo Registro Civil/Cartório.

Assim, foi possível construir histórico de informações completo da vida de cada pessoa (nascimento, casamento, óbito, divorcio, nome, etc). Para isso, o Estado Brasileiro delegou essa função aos particulares para poderem estar à frente dos cartórios. Para tanto, serão escolhidos por um processo rigoroso de concurso público, profissionais do direito devidamente aprovado.

Ademais, foram sendo criado, pelo menos um registro civil em cada município Brasileiro, o cujo são denominados Cartórios de Registro Civil. Os quais são compostos por um plexo de bens, como livros, arquivos, computadores, espaço físico, etc. Seus objetivos são dar condições instrumentais para o registrador praticar seu

ofício.

Para com que o delegatário/registrador possa exercer sua atividade, além de certas formalidades, também deverá respeitar estritamente a Lei, aos comandos normativos e rigorosa fiscalização pelo Poder Judiciário. Isso irá traçar e direcionar todo seu modus operandi e rotina, a fim de o delegatário poder agir com prudência para atingir segurança jurídica.

Portanto, nota-se que, o registrador civil efetuará semelhantemente aos blocos que integram os *nós* da arquitetura tecnológica *Blockchain.*

Por outro lado, há o Tabelião de Notas, ou seja, Notário/Escriba, como queiram. O cujo é possível encontrar relatos de sua existência desde os tempos mais remotos, como exemplo nos textos bíblicos do antigo testamento no Livro de Deuteronômio:

> Assim, convoquei os chefes das tribos, homens sábios e experientes e os designeis para chefes de mil, de cem, de cinquenta e de dez, além dos oficiais, notários, para cada tribo. (DEUT. 1 : 15, BÍBLIA – ALMEIDA, 2009).
>
> Estabelecerás juízes, policiais e notários em cada uma das cidades que *Yahweh* teu Deus vai dar para as tuas tribos (DEUT. 16: 18, BÍBLIA – SAGRADA, 2009, Online).

De lá para cá, sua presença na sociedade é cada vez mais relevante. Pois, em muitos países sua função era, apenas, relatar com fidelidade os fatos e/ou atos das relações jurídicas, ou seja, Notário redator. No entanto, com a queda do liberalismo e surgimento do neoliberalismo, a presença do Estado na vida das pessoas foi crescente, repercutindo na atividade notarial.

Assim, o notário além de redator, também começou a acumular função de assessor jurídico e intérprete das leis para as pessoas, conforme Brandelli (2011):

> Notário é um assessor jurídico das partes, orientando-as juridicamente acerca do regramento pertinente aos atos que pretendem celebrar, bem como acerca das consequências jurídicas de tais atos, a fim de garantir a certeza e segurança jurídica a priori, zelando pela criação de atos jurídicos perfeitos, prevenindo litígios (BRANDELLI, 2011, p. 1).

Ademais, no que tange a atividade especificadamente no Brasil, importante mencionar Dalledone (2016):

> O Brasil colônia que adotava o ordenamento jurídico lusitano e um conjunto de regras próprias da Colônia, formadas a partir de costumes, contratos e privilégios, que por vezes acabavam prevalecendo sobre o sistema geral. Essa pluralidade de ordens jurídicas gerava constante incerteza do direito aplicável no Brasil, potencializada por fatores outros como a ausência de critérios uniformes de interpretação e a possibilidade de impugnação das Leis Régias, que perdurou até meados do século XVIII. É nesse contexto que importa situar a figura dos tabeliães de notas, oficiais da justiça que integravam a estrutura da Administração Municipal, encarregados de lavrar escrituras, contratos, testamentos, codicilos, atos de última vontade, enfim, formalizar a vontade das partes mediante a confecção de instrumentos revestidos de fé pública que lhes era outorgada pelo poder real. Serviam, portanto, como intérpretes de um arcabouço legislativo complexo e dinâmico, viabilizando o tráfego jurídico num ambiente em que poucas pessoas dominavam a leitura e a escrita (DALLEDONE, 2016, p.).

Na atualidade não difere, apesar do avanço tecnológico e a modificação da sociedade, o cerne da função notarial continua a mesma: interpretar a lei, receber a vontade das partes, construir e tutelar atos jurídicos, a fim de oferecer segurança jurídica.

Além de que, em pleno século XI, precisamente até o ano de 2022, data em que foi escrito este estudo, o Brasil contava com elevado índice do analfabetismo funcional em sua população. Por conseguinte, esta parcela da população é vulnerável para se envolver em determinados atos e negócios jurídicos. Assim, continuam sendo necessário a presença de um intérprete imparcial com as qualificações de um notário.

Por fim, há também o Registro de Imóveis que, com evolução da sociedade, o aumento significativo no volume e na complexidade dos negócios imobiliários, notadamente após a Revolução Industrial XVII, percebeu-se a importância de concentrar as informações imobiliárias.

As transações imobiliárias eram feitas entre as pessoas — espalhadas pela sociedade — por transmissões e trespasse obrigacional. Assim, o contratante entregava o documento ao sucessor e/ou adquirente — tradição ficta — entrega formal do documento ou escritura. Logo, os documentos construídos pelo notário ficavam esparsos pela sociedade, dificultando a publicidade dos negócios imobiliários.

Isso causava problemas como a dupla venda de um mesmo imóvel ou de alienações de imóveis livres que estavam gravados ou continham algum direito

real. Neste cenário, surgiu a ideia de os negócios imobiliários serem concentrados em um único local (banco de dados imobiliário). Essa inovação facilitaria o tráfego imobiliário, além de oferecer publicidade e segurança jurídica à sociedade.

Com a alternativa de centralizar as informações imobiliárias em um único local, também foi possível com que o proprietário de um imóvel oferecesse em hipoteca a fim de levantar crédito. Logo, em 1843, surgiu a Lei Orçamentária nº317, que criou o registro de hipotecas, proporcionando com que o imóvel servisse também de lastro para crédito.

Neste período, a Igreja Católica recebeu a função de cadastrar todo acervo imobiliário. Assim, os documentos de posse elaborados pelos notários eram transcritos no livro da Paróquia Católica (Registro do Vigário). Sendo registrado em duas vias, uma para a Paróquia e outro para o requerente.

Este novo modelo deu tão certo que foi criado por lei um órgão exclusivo para tratar do assunto, ou seja, os Cartórios de Registros de Imóveis que faz parte do rol de atividades dos Registros Públicos. Além disso, a fim de fomentar essa organização, o Brasil editou leis estabelecendo que, somente adquiri propriedade aquele quem efetivamente registrá-la no registro competente, artigo 1.227 do NCC (BRASIL, 2002).

Por conseguinte, os registros públicos estão ancorados pelo princípio da Publicidade Registral, “a publicidade é a alma dos Registros Públicos. É a oportunidade que o legislador quer dar ao povo de conhecer tudo que lhe interessa a respeito de determinados atos” (BALBINO FILHO, 1999, p. 9).

Portanto, grosso modo, nota-se que o Registrador Imobiliário é um ator, dentre outros, que recebe o título de propriedade confeccionado pelo notário (outro ator). O cujo, recebeu, tratou e qualificou a vontade das partes, para que, em seguida, pudesse ser encaminhada, qualificada novamente e, por final, armazenada ao acervo registral.

4.3 PONTOS DE CONFLUÊNCIAS

4.3.1 Pontos sobre Blockchain

Na ocasião em que a informação é inserida na rede, ela é armazenada nos blocos e criptografadas gerando um código *hash* único gerado pelos mineradores.

Para isso, os *nós* trabalham sem parar para resolverem problemas matemáticos a fim de, a todo tempo, criar códigos inéditos para manter a segurança das informações.

Quando elas já estiverem armazenadas nos blocos, somente poderão ser alteradas pelo consenso de 50% + 1% de toda a rede. Sendo que, a operação de inserção e/ou alteração dos dados são realizadas em *real time*. Assim, denota-se que esta velocidade nas operações é uma das características que atrai o interesse da sociedade moderna.

Essa tecnologia capta a vontade e os dados das pessoas por intermédio do comando da transação, o qual encaminha para os blocos armazená-las. Sendo que, promete, integridade e imutabilidade aos dados registrados, dentre outras vantagens.

Entretanto, a captação da vontade a serem inseridas nos blocos é efetuada de maneira bruta, ou seja, não há intermediação de um notário ou registrador efetue a organização e o arquivamento.

Realizando uma ligação prática dos institutos, é importante trazer um estudo de caso que está sendo implementado na República da Geórgia, o sistema de Registro de Imóveis na tecnologia *Blockchain* realizado por Shang e Price:

> Sistema de titulação de terras baseado em Blockchain na República da Geórgia, um projeto piloto desenvolvido em colaboração com o Bitfury Group, a Agência Nacional de Registro Público (NAPR) e o Blockchain Trust Accelerator. Ao usar a tecnologia Blockchain, o governo da Geórgia pretende ser um líder em governança e segurança e restaurar a confiança pública nas instituições e agências governamentais. Além disso, o NAPR criou o NAPReg, um banco de dados digitalizado que incluía informações cadastrais, como títulos de propriedade e fotos de satélite. Graças a este banco de dados, detalhes de propriedade de terras informações como nome, endereço e código cadastral podem ser facilmente encontradas. Na verdade, o Banco Mundial reconheceu a República da Geórgia pela qualidade de seu serviço de registro de imóveis. De acordo com o relatório do Banco Mundial, "Doing Business 2016", a República da Geórgia ficou em terceiro lugar entre 189 países em facilidade de registro de propriedade. O relatório mostrou que levou apenas um dia para registrar uma propriedade na Geórgia e o custo do registro representou apenas 0,1 por cento do valor total da propriedade. A eficiência do registro de terras da República da Geórgia excede em muito a dos países desenvolvidos, como os Estados Unidos e a Alemanha, onde demorou em média 15,2 e 39 dias, respectivamente, para registrar propriedades […] (SHANG; PRICE, 2018, p. 1-7).

O ex-presidente do NAPR, Ugrekhelidze, afirmou que, com a

tecnologia *Blockchain,* os cidadãos georgianos poderão acessar as informações sobre suas propriedades no site do NAPR e colocá-las à venda. Os *nós* da rede verificarão se o comprador tem fundos suficientes e se o vendedor possui a propriedade antes da conclusão da transação. Com a nova tecnologia, todas as informações sobre vendas e transferências de terras estarão acessíveis ao público e não serão facilmente alteradas pelos órgãos governamentais.

Ademais, na atualidade, há diversos estudos sendo desenvolvidos pelo mundo, a fim de implantar os contratos inteligentes (*smartcontract*) ancorados na tecnologia *Blockchain* para registrar as relações jurídicas entre as pessoas como exemplifica Mereles, Ortellado e Barreiro:

> [...] um contrato inteligente pode ser usado para modelar a venda de um bem físico. Vamos supor que dois participantes da rede *blockchain*, Alicia e Bob, onde Alicia tem uma casa registrada à venda e Bob decide comprá-la. Um contrato inteligente pode ser gerado, de forma que quando uma transação é gerada indicando que Bob transfere o dinheiro correspondente à casa para Alicia, o contrato inteligente pode gerar uma transação indicando que a posse da casa passa de Alicia para Bob e para sua realização, não serão utilizados agentes de controle externos ou mediadores. Após a venda de Alicia para Bob, se Alicia tentar vender sua casa novamente para outro participante, esta ação será rejeitada pelos participantes da rede *blockchain*, uma vez que ali está listada como propriedade de Bob. (MERELES; ORTELLADO; BARREIRO, 2019, p. 1).

Diante do que foi explanado, essa tecnologia armazena de forma descentralizadas os dados pelos *nós* espalhados pela sua rede. Por intermédio da transação ela recebe a informação, crua e sem tratamento, pelo comando da pessoa particular credenciada que possui um certificado digital.

Neste cenário, percebe-se que a tecnologia *Blockchain*, oferece, em tese, a função de armazenar e garantir a integridade do documento, sem a possibilidade de alterar, então, entram os contratos inteligentes, pois eles são imutáveis. Ocorre que, o que se tem visto é que não é recomendável sua utilização pura e simplesmente isolada, pois, há ausência de intérprete imparcial para curar a vontade humana a ser armazenada.

Ela poderá sim, fazer parte de todo o conjunto de procedimentos. Entretanto, não poderá ser utilizada como estão vendendo a ideia espalhada pelo marketing popular espalhado pela grande mídia. Sendo que, o adequado é avaliar a fusão do Instituto dos Registros Públicos, ao menos no Brasil, para ambos possam

unir forças e não um substituir o outro.

Embora a tecnologia blockchain ainda seja nova no ano de 2022, não se pode negar que seja um dos assuntos mais comentados neste ano, estando, portanto, no “hype” da sociedade conectada.

Por ser uma tecnologia sedutora, traduz a impressão de oferecer agilidade em vários aspectos, inclusive no cenário imobiliário. Assim, na esperança de poder ser usada nesse ambiente, ela está atraindo diversos investidores e cientistas tecnológicos que estão se debruçando em estudos e captações de investimentos, interessar-se poder proporcionar ao mercado imobiliário maior liquidez para seus ativos.

Neste trajeto, estão surgindo diversos “players” da área da tecnologia focados em projetos ancorados em Blockchain, smart contract e tokens não fungíveis — NFT.

Token não fungíveis podem ser denominados como código oriundo da criptografia que tem como finalidade a representação digital de alguma coisa. Neste sentido, DAYANA DE CARVALHO UHDRE, transcreve que:

> Michèle Finck aponta que, além das criptomoedas, outros criptoativos emergiram ao longo do tempo na forma de tokens ou moedas “coins”(...) Prossegue, salientando que os *tokens* podem ter diferentes propósitos e representar qualquer coisa – de bens e serviços a direitos, incluindo direitos de voto (UHDRE, 2021, 65 – 67).

Além desse conceito, importante trazer algumas classificações Uhdre(2021) também traz sobre o tema:

> John Hargrave, Navroop Sahdev e Olga Feldmeier definem token como sendo uma titularidade (representação) de uma parcela fracionária de valor de determinado ativo ou empreendimento:
> **1) Tokens monetário**(currency tokens), como o bitcoin, podendo ser usado para instrumento de troca(compra e venda)de bens do mundo real**;**
> **2) Tokens de plataforma** (platform tokens), como Ethereum, podendo ser usado como contraprestação para “rodar” transações numa plataforma blockchain;
> **3) Tokens lastreado em ativos** (asset-backed tokens) estão ligados a um ativo físico subjacente como propriedade imobiliária, arte ou colecionáveis. (UHDRE, 2021, 65 – 67).

Nessa esteira, muitos desses novos “players” se reuniram em um

evento realizado no dia 30 de junho de 2022 na cidade de São Paulo-Brasil — blockchain real estate – summit – debatendo e apresentando novidades tecnológicas que prometem facilitar a forma tradicional de concretizar negócios imobiliários.

Como exemplo, citam-se algumas das startups: HOUSI; NETSPACES; CITYZEEN; BLOCKBR; RIBUS; INSIGNA; MetaBlock; PROPTALKS, SOLIDBLOCK, REORA, FIBRE, ItauBBA; SYNC; PREXIS, dentre outras.

Não é objetivo deste estudo fazer publicidade para nenhuma delas, mas, apenas demonstrar que existe empresas de tecnologias antenadas em Blockchain, cada qual com suas peculiaridades e objetivos comerciais.

Dentre elas, destaca-se o *case* da empresa NETSPACES. Ela oferece uma plataforma para criar, transacionar e gerir propriedades digitais. Com isso, informa que possibilitará ao usuário eficiência e rapidez nos pagamentos para aquisição das propriedades, bastando um simples PIX.

Oferece também, democratizar a aquisição da propriedade imobiliária, disponibilizando, para isso, a oferta de TOKENS representativos de frações imobiliárias digitais lastreadas em propriedades imobiliárias físicas. Todo esse sistema é erigido na rede *Blockchain* por intermédio de contratos inteligentes proporcionando, portanto, imutabilidade e a confiabilidade nos seus registros.

> A diarista de 49 anos de Porto Alegre Docelina Conceição de Barros Severo, realizou o sonho da casa própria graças a uma nova modalidade de financiamento: o crédito utilizando propriedade digital como garantia. O negócio foi feito com o uso de NFT, que significa "tokens não fungíveis" em inglês. É um selo digital único associado a um item que garante sua autenticidade. Idosa usa NFT para comprar 20% de apartamento no RS: "Trabalhando como diarista, eu acabo não tendo os meios tradicionais para comprovação de renda, como, por exemplo, contracheque. Sempre encontrei barreiras para acessar financiamento em bancos, ainda mais por não ter nenhum valor guardado que pudesse ser dado como garantia. A solução da Netspaces foi o que permitiu o financiamento da minha casa. Isso tem um grande valor para mim e meus filhos", explica Docelina (G1 RIO GRANDE DO SUL, 2022, Online).

Ademais, é possível consultar seu endereço eletrônico https://netspaces.org/credito e encontrar publicidade veiculada nacionalmente onde informa a possibilidade de um NFT representar um imóvel, como segue (Figura 5):

Figura 5 - Nova modalidade de compra NFT como garantia.

Fonte: G1 Rio Grande do Sul (2022)

Como funciona:

> O diretor da Netspaces Jonathan Doering Darcie explica que a tecnologia visa facilitar o processo de compra e venda de imóveis.
> "Ao invés de você passar por um processo tradicional que envolve alguns atos públicos, um pouco mais de tempo, você migra pra um universo que você tem uma transação eletrônica, com um novo objeto, que é um NFT. **Você quer o que ele carrega consigo, que é um conjunto de direitos sobre um imóvel".**
> A NFT é um token que possui o conjunto de direitos do imóvel específico. No caso de Docelina, ele funciona como a garantia para que ela consiga adquirir o apartamento.
> "O que a gente fez foi trocar o objeto de garantia, que normalmente na operação é um imóvel e agora na NFT que vale a mesma coisa que o imóvel. Portanto para quem empresta na perspectiva de garantia há o mesmo conforto. Sabendo que, bom se é mudada a forma, é mais ou menos a mesma coisa em termos de conteúdo", diz Jonathan.
> O processo como um todo, segundo Jonathan, é mais leve e tem como objetivo proporcionar a experiência para mais pessoas.
> "O processo como um todo é muito mais leve. É uma experiência que as pessoas tem em geral em transações em alguns mercados. É um processo muito pesado na tradição. Quando traz a leveza as pessoas enxergam a compra de um imóvel como um processo ali que é muito sensível de que muitas vezes é o imóvel da vida da pessoa. Quando ao invés de ser uma dor que começa do dia que você gostou ao dia que é seu, você ter uma coisa mais leve", finaliza. (G1 RIO GRANDE DO SUL, 2022, Online).

Portanto, o que se depreende nos dizeres do diretor da Netspaces é que NTF – TOKEN irá representar o conjunto dos direitos sobre um imóvel, ou seja, um TOKEN, em tese, representar-se-ia desmaterialização de um imóvel específico.

Por outro lado, analisando o caso em concreto. A operação realizada

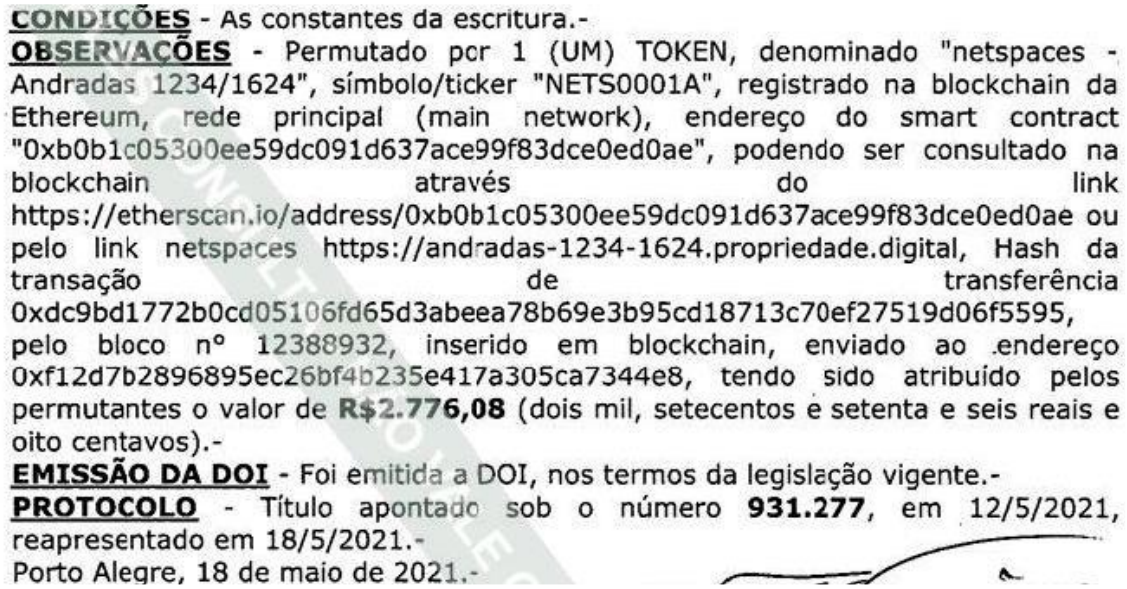
pela empresa de tecnologia supracitada, no âmbito do Estado do Rio Grande do Sul, sendo o único estado da federação brasileira que, até a presente data - julho de 2022 - regulamentou via ato administrativo do Tribunal de Justiça, a possibilidade de permuta de propriedade imobiliária com propriedade digital (NTF). Segue trechos do provimento 38/2021 Corregedoria-Geral da Justiça - Tribunal de Justiça - RS:

> PROVIMENTO Nº 038/2021 - CGJ
> Expediente nº 8.2021.0010/001575-8
> Matéria Notarial e Registral
> Agenda 2030 - ONS 16.6 - Desenvolver instituições eficazes, responsáveis e transparentes em todos os níveis
> Regulamenta a lavratura de escrituras públicas de permuta de bens imóveis com contrapartida de tokens/criptoativos e o respectivo registro imobiliário pelos Serviços Notariais e de Registro do Rio Grande do Sul.
> Art. 1º - Os Tabeliães de Notas apenas lavrarão escrituras públicas de permuta de bens imóveis com contrapartida de tokens/criptoativos mediante as seguintes condições cumulativas:
> I - declaração das partes de que reconhecem o conteúdo econômico dos tokens/criptoativos objeto da permuta, especificando no título o seu valor;
> II - declaração das partes de que o conteúdo dos tokens/criptoativos envolvidos na permuta não representa direitos sobre o próprio imóvel permutado, seja no momento da permuta ou logo após, como conclusão do negócio jurídico representado no ato;
> IV - que o valor declarado para os tokens/criptoativos guarde razoável equivalência econômica em relação à avaliação do imóvel permutado;
> IV - que os tokens/criptoativos envolvidos na permuta não tenham denominação ou endereço (link) de registro em blockchain que deem a entender que seu conteúdo se refira aos direitos de propriedade sobre o imóvel permutado (CORREGEDORIA-GERAL DA JUSTIÇA - Tribunal de Justiça – RS, 2021, Online).

Notam-se que na ocasião da formalização do negócio jurídico envolvendo permuta de imóvel físico com propriedade digital (NFT), deverá estar expresso na escritura pública que o TOKEN não detém nenhuma relação ou direitos da propriedade objeto da matrícula, nem no momento do negócio ou logo após.

Isso dá a entender que o negócio realizado teve natureza de permuta – coisa por coisa – mas não a transformação da propriedade real – bem imóvel - em propriedade digital. Ademais, segue abaixo cópia da primeira operação neste sentido representada pelo Registro n.º 6 na Matrícula 167.575 do Registro de Imóveis da 1º Zona de Porto Alegre/RS:

Figura 6 - Permuta de imóvel físico com propriedade digital (NFT).



CONDIÇÕES - As constantes da escritura.-
OBSERVAÇÕES - Permutado por 1 (UM) TOKEN, denominado "netspaces - Andradas 1234/1624", símbolo/ticker "NETS0001A", registrado na blockchain da Ethereum, rede principal (main network), endereço do smart contract "0xb0b1c05300ee59dc091d637ace99f83dce0ed0ae", podendo ser consultado na blockchain através do link https://etherscan.io/address/0xb0b1c05300ee59dc091d637ace99f83dce0ed0ae ou pelo link netspaces https://andradas-1234-1624.propriedade.digital, Hash da transação de transferência 0xdc9bd1772b0cd05106fd65d3abeea78b69e3b95cd18713c70ef27519d06f5595, pelo bloco nº 12388932, inserido em blockchain, enviado ao endereço 0xf12d7b2896895ec26bf4b235e417a305ca7344e8, tendo sido atribuído pelos permutantes o valor de **R$2.776,08** (dois mil, setecentos e setenta e seis reais e oito centavos).-
EMISSÃO DA DOI - Foi emitida a DOI, nos termos da legislação vigente.-
PROTOCOLO - Título apontado sob o número **931.277**, em 12/5/2021, reapresentado em 18/5/2021.-
Porto Alegre, 18 de maio de 2021.-

Fonte: Registro de Imóveis da 1º Zona de Porto Alegre - RS (2022)

Verifica-se que foi realizado um contrato simples de permuta conforme dispõe os artigos 533 e 481 do Código Civil brasileiro:

> Art. 481. Pelo contrato de compra e venda, um dos contratantes se obriga a transferir o domínio de certa coisa, e o outro, a pagar-lhe certo preço em dinheiro.
> Art. 533. Aplicam-se à troca as disposições referentes à compra e venda, com as seguintes modificações:
> I - salvo disposição em contrário, cada um dos contratantes pagará por metade as despesas com o instrumento da troca;
> II - é anulável a troca de valores desiguais entre ascendentes e descendentes, sem consentimento dos outros descendentes e do cônjuge do alienante.

Nesse contrato foi realizado a troca de fração ideal da propriedade imobiliária por um TOKEN com valor atribuído pelas próprias partes equivalente a R$ 2.776,08(Dois mil, setecentos e setenta e seis reais e oito centavos).

Token é um criptoativo com representação econômica. Este ativo digital é um exemplo, entre tantos outros de propriedade digital que, neste caso, não se vincula com a propriedade física objeto da matrícula acima mencionada.

Houve uma permuta como qualquer outra. Poderia ter sido realizada entre a fração ideal do mesmo imóvel por um veículo ou outra coisa com representação econômica.

Para não deixar dúvidas quando a possibilidade de se atribuir valor econômico a ativos digitais, segue a IN 1888 da Receita Federal que conceitua TOKEN como criptoativo, abaixo:

> O código 89 – Demais criptoativos não considerados criptomoedas (payment tokens): Diz respeito a criptoativos que prioritariamente não sejam utilizados como criptomoedas, tais como os diversos tokens de utilidade (utility tokens), usados para acesso a serviços específicos, como games e para fãs de clubes de futebol, assim como tokens vinculados a ativos reais ou direitos sobre recebíveis, tais como imóveis, ações, precatórios, consórcios contemplados, passes de jogadores de futebol, entre outros. (VALOR CONTÁBIL FISCAL, 2022, Online).

Imposto de Renda, trazendo ao IR pela primeira vez também menção à In1888 (2019 - Instrução Normativa, institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil.

> Criptoativo: a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal. (VALOR CONTÁBIL FISCAL, 2022, Online).

Em um primeiro momento, conquanto possa causar certa perplexidade visualizar a matrícula imobiliária recheada de números e códigos matemáticos, não se pode ignorar que, de forma inédita, houve o ingresso no fólio imobiliário de uma propriedade digital – TOKEN - construída com base na tecnologia blockchain.

Neste contexto, ressalta-se que não é o propósito deste estudo avaliar a questão jurídica dessa permuta. Se houve ou não a transformação de uma propriedade física em digital, ou se o TOKEN a partir do seu ingresso na matrícula imobiliária detém ou não vínculo de propriedade ou direitos relativos ao imóvel. Nem muito menos, avaliar como serão comercializados esses TOKENS digitais após realizar essa permuta, mas demonstrar que há uma nova era em que a tecnologia blockchain está se destacando em diversos setores da sociedade.

O fato é que essa nova tecnologia já invadiu uma das áreas mais

conservadoras, sinônimo da segurança jurídica – os registros públicos. Assim, a impressão que se tem é estarmos diante de um passo para desmaterialização da propriedade imobiliária. De repente, surgindo, em oportuno, alternativas rápidas, seguras e menos onerosas para suas transações.

4.3.2 Pontos sobre Registros Públicos

Os exemplos vistos, não são utilizados no Brasil. No entanto, trazendo para a realidade brasileira, o Conselho Federal Notarial/Colégio Notarial do Brasil, adotam o uso da tecnologia *Blockchain* para praticar alguns atos, tais como: validação, autenticação de documentos no formato digital e autorização eletrônica de viagem (AEV). Este Conselho construiu sua própria rede denominada *Notarchain*, a qual é a plataforma utilizada pelos cartórios conveniados.

Essa arquitetura é autorizada pelo Provimento 100 do CNJ (Conselho Nacional da Justiça). Ele estava sendo estudado há anos, porém, sem muito avanço. Assim, com advento da Covid-19, a entidade de classe dos notários não teve alternativa, senão finalizar o projeto com auxílio das autoridades competentes. O resultado foi a edição desse provimento, o qual destaca-se por sua inovação e confere uma porta de entrada para a evolução da atividade no Brasil.

A propósito, no que tange a inovação tecnológica, a instituição cartorária no Brasil sofre duras críticas por vender uma imagem de burocracia arcaica. Entretanto, oportuno mencionar, que ela é dividida em duas facetas. A que pertence aos servidores públicos que compõe toda estrutura da administração pública (Foro Judicial) e outra do foro extrajudicial que são os Registros Públicos.

Não é o objetivo deste estudo se debruçar nessas duas facetas, mas informar ao leitor que é importante diferenciá-las, a fim de separar o joio do trigo. Quanto ao instituto dos Registro Públicos, em decorrência da covid-19, foi possível enxergar certa preocupação da classe, legítima, pois, por um triz e graças ao provimento 100 do CNJ ela não foi engolida por startups privadas.

Neste sentido, relevante mencionar, o pensamento do filósofo austríaco Joseph Alois Schumpeter sobre a inovação e destruição criativa:

> [...] produzir outras coisas, ou as mesmas coisas com método diferente, significa combinar diferentes esses materiais e forças. Na medida em que as" novas combinações" podem com o tempo, originar-se das antigas por ajuste contínuo mediante pequenas etapas, há certamente mudanças, possivelmente há crescimento, mas não um fenômeno novo nem um desenvolvimento em nosso sentido. Na medida em que não for este o caso, e em que as novas combinações aparecem descontinuamente, então surge o fenômeno que caracteriza o desenvolvimento. (...) o desenvolvimento, no sentido que lhe damos, é definido então pela realização de novas combinações. (SCHUMPETER, 1988, p. 48).

Esse ensinamento resta claro a necessidade de investimento constante em inovação, pois, certamente alguém estará fazendo, o qual, pode ser, inclusive, seu concorrente.

No contexto de inovação, o estado de Vermont nos Estados Unidos, saiu na frente e enxergou que a tecnologia *Blockchain* é um banco de dados que deverá ser alimentado por informações tratadas, de maneira com que o governo local editou regramento para seu uso, no que tange as informações inseridas na rede *Blockchain*:

> [...] no que diz respeito aos procedimentos judiciais, reafirma a habilitação do blockchain em relação à autenticação, admissibilidade e presunções, expressando que um registro digital, registrado eletronicamente na cadeia de blocos, **é automaticamente autenticado se for acompanhado de declaração escrita de pessoa habilitada**, feita sob juramento, indicando a qualificação da pessoa para fazer a certificação, com alguns requisitos como data e hora de entrada, registro no blockchain, e que seja mantido na rede regularmente, dando-lhe autenticidade. (COVARRUBIAS, 2019, p. 1).[5]

Ademais, Covarrubias (2019) ao analisar o estado da Califórnia-EUA, bem como a França, no que tange a regulamentação da tecnologia Blockchain, chegou à seguinte conclusão:

[5] [...] con respecto a los procedimientos judiciales, reconhece la habilitación de blockchain en relación con la autenticación, la admisibilidad y las presunciones, expresando que un registro digital, inscripto electrónicamente en la cadena de bloques, se autentica de manera automática si va acompañado de una declaración escrita de una persona calificada, hecha bajo juramento, que indique la calificación de la persona para hacer la certificación, con alguns requisitos como la fecha y la hora del ingreso, el registro en la blockchain, y que se mantiene en la red de maneira regular, otorgándole autenticidade. (COVARRUBIAS, 2019, p. 1).

> Ou seja, se Bob tem uma casa e quer vendê-la para Alice, ele precisa passar por vários procedimentos para transferir a propriedade, lidando com cartórios, e possivelmente advogados. Pelo exposto, conclui-se que, para ter um sistema baseado em comprovação de existência ou titularidade, a solução não é meramente um registro com blockchain [...] (COVARRUBIAS, 2019, p. 1).[6]

Assim, esta tecnologia não se sustenta isoladamente para determinadas funções, como, por exemplo, as oferecidas pelos Registros Públicos. Logo, ambos os institutos poderão um complementar o outro.

Observe a importância de uma pessoa qualificada participar desse procedimento. No Brasil, destaca-se o e-Notariado que está agindo desta forma, captando a vontade da pessoa, tratando-a para poder integrá-la a rede privada *blockchain*.

Portanto, os Registros Públicos, dentre várias funções, têm o condão de qualificar a vontade da pessoa e armazená-la, inclusive realizando uso dessa tecnologia. Desta forma, todo esse procedimento proporcionará segurança, autenticidade e integridade para as relações e atos jurídicos.

Sob outra perspectiva, os Registros Públicos captam informações por intermédio de pessoas qualificadas. Ou seja, agentes delegados profissionais do direito, os quais traduzem, tratam e moldam a vontade das pessoas ao ordenamento jurídico. Para que, ao final, após rígida análise da situação fática são transformados em atos jurídicos autênticos para, em seguida, possam ser armazenados em seu acervo.

Evidentemente toda tecnologia deve ser aferida e apurada sua viabilidade ao caso concreto. Pois, caso ela se mostre eficiente deve sim, ser utilizada pela sociedade. No entanto, o que não se aconselha é trilhar um caminho aberto pelo “efeito manada”. Ainda mais, no que tange a temas sensíveis que serviram para construir a história da humanidade.

Portanto, destaca-se o método adotado pelo estado de Vermont nos EUA. Que, determinou a condição de utilizar a tecnologia *blockchain* se os dados ali inseridos passarem, previamente, por uma pessoa qualificada para emitir uma certidão outorgando autenticidade.

---

[6] Es decir, si Bob tiene una casa y quiere venderérsela a Alice, tiene que pasar por diversos procedimientos para transferir la propriedad, tratar con oficinas de registros, notarios y, posiblemente, abogados. De lo anterior se concluye que, para tener un sistema basado en prueba de existência o de propriedad, la solución no es meramente un registro con blockchain [...] (COVARRUBIAS, 2019, p. 1).

Por fim, remetemos esta metodologia à função notarial, que oferece todas as condições intelectuais necessárias para preparar e tratar as informações objeto de armazenamento na rede *Blockchain*. Assim, ambos os institutos poderão se unir para oferecer serviço de qualidade que a sociedade almeja.

Diante do que foi dito nos capítulos anteriores, verifica-se que os Registros Públicos, dentre várias funções, são considerados veículos de captação da vontade das pessoas, transformando-as em atos jurídicos autênticos e registrando-os em seus bancos de dados.

CONSIDERAÇÕES FINAIS

Isto posto, neste estudo foi possível elencar síntese da história do notariado. A qual, advém de uma profissão milenar, que desde antes de Cristo o povo hebreu delegava aos escribas a função de relatar acontecimentos e fatos relevantes para serem guardados e/ou utilizados como meio de prova.

Essa profissão também foi fundamental para o império romano, sendo que, na ocasião, o imperador delegava aos notários a função certificante para consagrar determinadas relações jurídicas, as quais eram revestidas de vigorosas solenidades.

Atualmente, no âmbito do sistema jurídico mundial e, notadamente, o brasileiro, verificou-se que os Registros Públicos mantêm sua função certificante nas relações jurídicas.

Ocorre que, a sociedade avança em conhecimento, ciência e tecnológica, a qual, traz consigo novos produtos com fito de facilitar a vida das pessoas. Um desses produtos decorre da sociedade contemporânea da informação. Ela é composta pelo acesso a inúmeros componentes eletrônicos que, dentre suas funções, uma delas é o compartilhamento de informações em massa pelo ambiente digital.

Este ambiente é formado por parcela de componentes e periféricos físicos — metais — sendo naturalmente expostos aos efeitos da oxidação. Além deste, o ambiente também é composto por programas construídos pela linguagem binária, cuja desconhecida pela maioria da população.

Ademais, foi destacado que este ambiente digital é construído no ciberespaço composto pela internet. Esta é uma arquitetura que compões imensidão de cabos transatlântico e intercontinentais responsáveis em ligar os computadores em todos os cantos do mundo.

Sendo que, com o alto fluxo de informações a trafegar pela rede, empresas de tecnologias iniciaram a corrida pela possibilidade de oferecer segurança e inviolabilidade para os arquivos pela internet. Com resultado, apresentaram certificado digital que vem prometendo privacidade e autenticidade na autoria para as informações transitada pelo ambiente. Aliando-lhe, está a assinatura eletrônica que, em tese, proporcionou maior agilidade nas transações negociais à sociedade contemporânea, possibilitando, portanto, que um cidadão, não precise mais se

deslocar ao balcão de um cartório para reconhecer sua firma.

Diante dessa novidade, não seria outra a reação de uma sociedade eufórica e superficial, senão abraçar a ideia e expandi-la massivamente pelo mundo. Ocorre que, como bem detalhado neste estudo, nem tudo são flores.

Logo, foi possível desmistificar o certificado digital apresentando peculiarmente seu real funcionamento e o que ele, de fato, pode entregar para a sociedade. Além disso, esclareceu-se a figura da autoridade de registro e sua função. Abordando a possibilidade de ser considerada um início da “uberização” do notariado.

Ademais, também foi possível apresentar o que a república da Argentina e a Peruana fizeram para conter esse fenômeno, escolhendo, por conseguinte o Tabelião de Notas como figura adequada para ser a interface entre o usuário e a certificadora.

Por outro lado, detalhamos como que realmente a arquitetura *blockchain* funciona. Suas vantagens, bem como suas desvantagens que, por sinal, pode interferir na soberania de um país.

Além disso, demonstramos que ela é um produto tecnológico estático, o qual, em tese, apresenta condições de guardar arquivos no ambiente digital sem que os mesmos possam ser alterados. Entretanto, essa tecnologia não apresenta maneiras de como ela deveria ser alimentada pelas informações. Assim, estar-se-ia aberta para qualquer pessoa, sem discriminação, alimentá-la.

Neste sentido, restou evidente a necessidade de regulamentar a entrada das informações junto a rede *blockchain*. Assim, sugere-se um modelo adotado no estado de Vermont nos Estados Unidos EUA, o qual dispõe que as informações para terem ingresso a *blockchain* e ser automaticamente autenticada desde que seja acompanhado de declaração escrita de pessoa habilitada, elaborado sob juramento, indicando a qualificação da pessoa para efetuar a certificação, com alguns requisitos como data e hora de entrada, registro no *blockchain*, e que seja mantido na rede regularmente, dando-lhe autenticidade.

Trazendo para o modelo brasileiro, este agente seria justamente o Tabelião de Notas, o qual detém todas as características necessárias para saber tratar e qualificar a vontade do cidadão aos moldes do nosso ordenamento jurídico.

REFERÊNCIAS

ALBO, Santiago; DI CASTELNUOVO, Franco. **Nuevas tecnologías aplicadas a la función Notarial**. Caba - Argentina: Di Lalla Ediciones, 2019.

ARANHA, Diego. 2018. As urnas eletrônicas de votação são seguras? **Entrevista,** O Globo, Épica, 2018. Disponível em: https://epoca.globo.com/diego-aranha-giuseppe-janino-23143406 Acesso em: Abr. 2022.

ARRUDA, Felipe. A história dos processadores. **TecMundo, Seção História**, 2011. Disponível em: https://www.tecmundo.com.br/historia/2157-a-historia-dos-processadores.htm Acesso em: Jun. 2022.

BALBINO FILHO, Nicolau. **Registro de Imóveis**. São Paulo. Saraiva, 1999.

BALDISSERA, Julia; SILVEIRA, Raphael Schwinden da. **Proposta de um modelo para detecção de fraudes na emissão de certificados digitais na ICP-brasil**.UNIVERSIDADE FEDERAL DE SANTA CATARINA DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA, FLORIANÓPOLIS 2017

BENFATTI, Fábio Fernandes Neves. **Direito à Inovação**. Curitiba: CRV, 2017.

BÍBLIA. **A Bíblia Sagrada**: Antigo e Novo Testamento. 4.ed. Rev. e Ampl. Barueri / São Paulo: SBB, 2009. Tradução João Ferreira de. Almeida

BRANDELLI, Leonardo. **Teoria Geral do Direito Notarial**. São Paulo: Saraiva, 2011.

BRANDELLI, Leonardo. **Teoria geral do direito notarial**. São Paulo: Saraiva, 2007.

BRASIL – e-Notariado. **Tenha todos os serviços de um cartório na palma da sua mão**. 2022. Disponível em: notariado.org.br Acesso em: Abr. 2022.

BRASIL – INTI. **ITI alerta sobre tentativas de fraudes de clonagem de certificados digitais**, 2018, p. 1) Disponível em: https://bit.ly/3KnfHfR Acesso em: Abr. 2022.

BRASIL - **Lei 9.609/98.** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília: Senado Federal, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm Acesso em: Abr. 2022.

BRASIL. **Decreto nº10.497, 2020**. Brasília: Senado Federal, 1994. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.497-de-28-de-setembro-de-2020-279960744 Acesso em: Abr. 2022.

_____. **Lei 8.935/1994**. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços. Brasília: Senado Federal, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8935.htm Acesso em: Abr. 2022.

_____. **Lei nº 14.063**, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes. Senado Federal, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm Acesso em: Abr. 2022.

BRASIL. **Medida Provisória N 2.200-2**, de 24 de Agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília: Senado Federal, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm Acesso em: Abr. 2022.

BRIDLE, James. **A nova idade das trevas**: a tecnologia e o fim do futuro. São Paulo: Todavia, 2018.

CNN BRASIL. **Novo golpe do saque do FGTS fez mais de 10 mil vítimas; veja que cuidados tomar**. 2022. Disponível em: Acesso em: https://bit.ly/3xbYWjO Abr. 2022.

CORREGEDORIA-GERAL DA JUSTIÇA - TRIBUNAL DE JUSTIÇA – RS. **IN 1888** 2019. Disponível em: Acesso em: https://blconsultoriadigital.com.br/in-1888-2019/ Abr. 2022.

COVARRUBIAS, llamas Zadamig Jersain. Justícia y registros públicos: la tecnologia al servicio de la justicia y la seguridad jurídica. Ciudad de Mexico, MX: Thomson Reuters, 2019.

CRETELLA JÚNIOR, José. **Curso de direito romano**. São Paulo: Forense, 1978.

DALLEDONE, Rodrigo Fernandes de Lima. **Função Pública Notarial**: Regime jurídico e Fiscalização Judicial. Curitiba, Prismas, 2016.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**: teoria das obrigações contratuais e extracontratuais. São Paulo: Saraiva, 2002.

FUJITA, Jorge Shiguemitsu; MATHEUS, Rosemeire Solidade da Silva. Atividade notarial frente às transformações de uma sociedade digitalizada: fé pública na sociedade da informação. **Argumenta Journal Law**, Jacarezinho – PR, Brasil, n. 35, 2021, p. 478-501. Acesso em: **Erro! A referência de hiperlink não é válida.**

http://seer.uenp.edu.br/index.php/argumenta/article/view/2086/pdf Abr. 2022.

GONÇALVES, Luis Flávio Fidelis. **Reconhecimento de Firma: Limites da Qualificação Notarial**. 2014. Disponível em: https://bit.ly/35VCu3k Acesso em: Abr. 2022.

G1 RIO GRANDE DO SUL. Nova modalidade de compra NFT como garantia. G1 RIO GRANDE DO SUL, 2022. Disponível em: http://glo.bo/3ajneiZ Acesso em: Abr. 2022.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI. **ITI alerta sobre tentativas de fraudes de clonagem de certificados digitais**, 2018, p. 1) Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/o-iti acesso 03/04/2022 às 03/04/2022 https://bit.ly/3rd0INJ Acesso em: Abr. 2022.

JACOMINO, Sérgio. Cartório digital e os simulacros da fé pública. 2016. Disponível em: https://cartorios.org/2016/09/18/6978/ Acesso em: Abr. 2022.

JACOMINO; Sérgio; UNGER, Adriana J. **NFT´s – a tokenização imobiliária e o metaverso registral.** 2022. Disponível em: https://www.migalhas.com.br/arquivos/2022/4/7CEF9CFF30BB7E_Tokenizacao.pdf Acesso em: Abr. 2022.

LEWANDOWSKI, Ricardo. **Soberania em um mundo digital**. Folha de S.Paulo; Revista Consultor Jurídico, Mar. 2022.

LOUREIRO, Luiz Guilherme. **Registros públicos**: teoria e prática. Salvador: jusPODIVM, 2017.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. São Paulo: Malheiros Editores, 2016.

MERELES, Eduardo; ORTELLADO, Juan; BARREIRO, Javier. **Uso de blockchain na administração pública**. Universidad de La República Uruguay, 2019.

NALINI, José Renato. **Novas perspectivas no acesso à justiça**. 2021

NORTON, Peter. **Introdução à Informática**. São Paulo: Makron Books, 1996.

NULL, Christopher. O Futuro do PC. **Revista PCWORLD**. São Paulo, 2006.

O ESTADO DE S. PAULO. **Navio russo suspeito de espionagem coloca Marinha Brasileira em alerta.** 2020. Disponível em: Acesso em: http://glo.bo/3JI2jBS Abr. 2022.

PECK, Patrícia Pinheiro et al. **Fundamentos dos negócios e contratos digitais**. São Paulo: Revistas dos Tribunais, 2019.

RODRIGUES, Silvio. **Direito Civil**. São Paulo: Saraiva, 2020.

SANTOS, Márcia Elisa Comasseto dos. **Fundamentos teóricos e práticos das funções notarial e registral imobiliária**. Porto Alegre: Norton, 2004.

SANTOS, Kássio Cabral Pereira dos. **Utilização de ontologias de referência como abordagem para interoperabilidade entre sistemas de informação utilizados ao longo do ciclo de vida de produtos**. 2011. Dissertação. UTFPR, Curitiba 2011.

SCHUMPETER, J. A. **Teoria do desenvolvimento econômico**: uma investigação sobre o lucros, capital, crédito, juros e o ciclo econômico. São Paulo: Nova Cultural, 1988.

SHANG, Qiuyun; PRICE, Allison. **A blockchainbased land titling project in the republic of Georgia**. 2018. Disponível em: https://bit.ly/3DRkaVo Acesso em: Jul 2021.

SIMPLÍCIO JUNIOR, Marcos. A. Segurança da Informação. Engenharia de Computação. Univesp - Universidade Virtual do Estado de São Paulo, 2019. Disponível em: https://bit.ly/3DQA6Hw Acesso em: Abr. 2022.

STALLINGS, William. **Criptografia e Segurança de Redes**: Princípios e práticas. São Paulo: Pearson Prentice-Hall, 2008.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. **Provedor de internet tem obrigação de fornecer IP de usuário que invadiu e-mail**. Disponível em: https://bit.ly/3LM3K3q Acesso em: Abr. 2022.

TEBALDI, Lucas; GUARDIA, Hélio Crestana. Serviço de autenticação, identificação e registro de usuários para redes sem fio públicas usando infraestrutura em nuvem **Tecnologias, Infraestrutura e Software**, São Carlos, v. 4, n. 2, p. 155-164, mai-ago 2015. Disponível em: http://revistatis.dc.ufscar.br/index.php/revista/article/download/312/111 Acesso em: Abr. 2022.

TANENBAUM, Andrew Stuart. **Redes de computadores**. Rio de janeiro: Campus, 1994.

TECMUNDO- ONLINE. **Bitcoin consome tanta energia quanto toda a Suíça, afirma estudo**. 2019. Disponível em: Acesso em: https://bit.ly/3jACOrz Abr. 2022.

TECNOBLOG.NET. **Quer mudar o IP no PC?** 2017. https://tecnoblog.net/responde/alterar-mudar-ip-no-pc/ Acesso em: Abr. 2022.

UHDRE, Dayana de Carvalho. **Blockchain, tokens e criptomoedas**. São Paulo: Almedina, 2021.

ULBRICH, Henrique César. **Universidade H4CK3R**. São Paulo: Digerati Books, 2009.

VALOR CONTÁBIL FISCAL. Como declarar Bitcoins e criptomoedas. 2022. Disponível em: https://www.valorcontabilfiscal.com.br/como-declarar-bitcoins/ Acesso em: Abr. 2022.

VEJA-ABRIL. Sem internet, mineração de Bitcoin no Cazaquistão fica fora do ar [...]. **Revista Veja-Abril Online**, 2022. Disponível em: https://bit.ly/3LM7odG Acesso em: Abr. 2022.

VELOSO, Fernando Castro**. Informática, conceitos Básicos**. São Paulo: Elsevier, 2017.

WAZLAWICK, Raul Sidnei. **Engenharia de software**: conceitos e práticas. São Paulo: Elsevier, 2015.

ZANIOLO, Pedro Augusto. **Crimes Modernos o impacto da tecnologia no direito**. Salvador: jusPodivm, 2021.

REVOREDO, **Tatiana. Blockchain – tudo o que você precisa saber**. The Global Strategy: Publicada pela Amazon, 2019.

FREIRE, **João Pedro. Blockchain e Smart Contracts implicações jurídicas**. Coimbra: Almedina, 2021.