XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

ZULMAR ANTONIO FACHIN

FABIANO HARTMANN PEIXOTO

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597
Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Fabiano Hartmann Peixoto; Zulmar Antonio Fachin – Florianópolis: CONPEDI, 2022.
Inclui bibliografia
ISBN: 978-65-5648-567-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Direitos Sociais, Constituição e Democracia na América Latina
1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governança. 3. Novas tecnologias. XI Encontro Internacional do CONPEDI Chile - Santiago (2: 2022: Florianópolis, Brasil).
CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O XI ENCONTRO INTERNACIONAL DO CONPEDI, com temática "Direitos sociais, Constituição e Democracia na América Latina", ocorrido entre os dias 13 e 30 de outubro de 2022, reuniu centenas de pesquisadores de diversos países. Com submissão extremamente substantiva, a linha de pesquisa Direito, Governança e Novas Tecnologias necessitou de subdivisão. A presente apresentação, então, refere-se aos trabalhos submetidos, selecionados e efetivamente apresentados e discutidos no GT Direito, Governança e Novas Tecnologias II.

Foi traço marcante a discussão sobre os impactos e as interfaces da tecnologia com temas tradicionais do Direito. Percebeu-se nela um papel extremamente relevante para o desenvolvimento do conhecimento e ensino jurídicos.

Fenômeno intensificado na última década, a tecnologia vem provocando análises e/ou avaliações no campo constitucional, processo e especialidades jurídicas. O cenário digital e cibernético teve abordagens multidisciplinares em trabalhos aprofundados. Assim, destacam-se as grande temáticas do GT:

• Inteligência Artificial

• Algoritmos

• Metaverso

• Lei Geral de Proteção de Dados

• Economia disruptiva

• Autodeterminação informacional

• Provas digitais

• Regulação internacional de dados

• Regulação de ciberespaço

• Compliance

• Inclusão digital

Centralmente, os trabalhos sobre Inteligência Artificial buscaram demonstrar a íntima relação entre compromissos éticos no uso ou desenvolvimento de sistemas com referenciais de direitos fundamentais. Discutiu-se, da mesma forma, os impactos dos novos sistemas de IA nos conceitos e alcances de institutos tradicionais do Direito, tais como a responsabilidade civil.

Igualmente presente, as análises de estratégias regulatórias também ocuparam relevante espaço no GT, especialmente no sentido dos desafios internacionais sobre a temática. Manifestações mais recentes da tecnologia no campo jurídico também foram apresentadas, destacando-se a interface dos direitos da personalidade no metaverso e a ampliação dos chamados "cookies" como ferramentas de potenciais fragilizações no sistema de proteção de dados.

Apresentado por pesquisadores do país anfitrião (Chile), aspectos da economia disruptiva em interface com a tecnologia promoveram debates sobre possíveis leituras chilenas das influências econômicas sobre o Direito e uma comparação com o panorama brasileiro.

Como não poderia ser diferente, os desafios da gestão e proteção de dados e os desdobramentos da Lei Geral brasileira também foram objeto de apresentação de pesquisas e demonstraram quantos novos desafios são postos à comunidade jurídica internacional.

Destacam-se, nesta breve apresentação, a análise e discussões sobre o incremento dos sistemas de certificação digital - tão intensificados em tempos de pandemia -, notadamente pelas inevitáveis dúvidas em razão do debate público-privado e das necessárias cautelas impostas pelos riscos de aumento na desigualdade entre cidadãos.

De uma maneira geral, as discussões do GT se encaminharam para a percepção de profundas alterações no modo tradicional de se observar o fenômeno jurídico, das inúmeras oportunidades apresentadas pela tecnologia e da proporcional necessidade de se observar riscos que as acompanham, especialmente sob a ótica de direitos fundamentais.

Dentro desta variedade interessante de relatos de pesquisa, os coordenadores desse grupo de trabalho convidam a todas e todos para a leitura na íntegra dos artigos.

Zulmar Antonio Fachin - Unicesumar e Faculdades Londrina - zulmarfachin@uol.com.br

Fabiano Hartmann Peixoto - Universidade de Brasília - fabiano_unb@unb.br

ANALISE DA CERTIFICAÇÃO DIGITAL NOS REGISTROS PÚBLICOS

ANALYSIS OF DIGITAL CERTIFICATION IN PUBLIC RECORDS ABSTRACT

Yasna Elizabeth Otarola Espinoza
Iuri Ferreira Bittencourt
Fabio Fernandes Neves Benfatti

Resumo

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: Certificado digital, Registros públicos, Segurança jurídica, Tecnologia, Vulnerabilidade

Abstract/Resumen/Résumé

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.

Keywords/Palabras-claves/Mots-clés: Digital certificate, Public records, Legal security, Technology, Vulnerability

Introdução

Este estudo em método dedutivo e bibliográfico, tem como objetivo trazer 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. Também será, oportunamente, traçado 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.

1. Certificado Digital no Contexto da Legislação Brasileira

Certificado digital é conectado em alguma máquina e esse, no que lhe concerne, detêm numeração como se fosse sua identidade. Ele 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 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, Portanto, isso permite com que ela circule pela rede camufladamente.

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, em tese, autenticidade de autoria dos agentes envolvidos — remetente/ destinatários.

Diante disso, destaca-se a presunção de autoria que será conferida da seguinte forma: a) com atuação de empresas privadas pelas certificadoras por intermédio da autoridade de registro - AR; b) com atuação dos registros públicos pelo certificado notarizado - certificadora notarial - quem irá conferir presunção será o Tabelião de Notas.

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

2 Vigencia e aplicação no Brasil.

No Brasil é 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, ele 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 a edição da lei 14.063/2020, permitindo no decorrer dos anos, o uso de assinaturas digitais e definindo diferenças entre as assinaturas avançadas e qualificadas.

No parágrafo acima mencionado define a norma embrionária que permitirá a certificadora privada garantir a presunção de autoria do usuário. Essa norma regulamenta a forma com que o usuário será submetido para se identificar e provar que ele é quem diz ser perante a certificadora privada.

3 Identificação do usuário e Autoridade de Registro.

O comando legal 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. Portanto, será repetida por ocasião de sua renovação, após expirar a validade (1 a 3 anos).

Verificam-se, que esta tecnologia foi tratada com tamanho ceticismo, incentivando, por consequência, a edição de uma lei que permitiu qualquer pessoa ser uma autoridade de registro e cadastrar o usuário sem passar pelo crivo de um notário.

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.

Para não deixar dúvidas, que tange o certificado digital, 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).

Assim, nota-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, ela 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 promete identificar o usuário da rede que 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 a identificação do usuário, bem como o arquivamento dos seus logs de registros, 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 - abalando a confiança nos certificados digitais. Ademais, continua o julgado:

> (…)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). 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) (…) 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 que o Marco Civil da Internet a Lei 12.965/2014 foi complacente com as empresas privadas de tecnologia, pois obrigam-s manterem arquivas dos *logs* de registros pelo prazo máximo de 6 (seis) meses, 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.

4 Defeitos do Negócio Jurídico na identificação de Fraudes.

Por outro lado, há também os eventos de fraudes que envolvem o certificado digital privado. Embora pouco divulgado pelo governo e pela mídia, mas, felizmente possível encontrar, em pesquisa, no 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 em torno de R$ 1.666,00(hum mil e seiscentos e sessenta e seis reais) mensais conforme fonte a seguir: **Fonte:** https://bit.ly/35PZsZw acesso dia 01/04/2022 às 10h41min

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:

> 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.

5 Da Arquitetura do ICP-Brasil na atividade certificadora.

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, segue alguns 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,

[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).

inclusive na ordem subjetiva, abaixo:

> 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

Além do exemplo Peruano acima mencionado, mister se faz trazer o exemplo Argentino 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):

> 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]

Conforme relatado pelo autor acima mencionado, verifica-se que a Argentina reconheceu a importância de escolher o notário para figurar como elo entre o usuário e a certificadora, determinando, portanto, que somente eles pudessem exercer a função de Autoridade de Registro (AR) de acordo com a política de certificação única da Autoridade Certificadora ONTI.

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.

---

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).

[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).

5. Conclusões

A legislação que disciplina as relações humanas e sua importância no certificado digital, 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, como por exemplo Certificado digital. Por se tratar de um software, ele deverá integrar com o mundo físico real por intermédio de uma interface. Esta, por sua vez, sugere que seja capaz de filtrar a vontade humana com mais acurácia. Assim, conforme o estudo verifica-se o Tabelião de Notas com capacidade peculiar a fim de exercer essa função.

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.

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

_____. **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.

_____. **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.

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

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.

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