Artigo

Identidade digital e a autonomia privada: reflexões constitucionais e civis sobre o reconhecimento notarial de pessoas no meio virtual

Digital identity and private autonomy: constitutional and civil reflections on the notarial recognition of people in the virtual environment

Ervin Hanke Neto[1], Luiz Gustavo Gibram Machado[2], Luiz do Carmo Cleto Rocha Filho[3] e Karina Viegas Brunialti[4]

[1]Especialista em Direito Tributário pela Pontifícia Universidade Católica do Paraná, Curitiba, Paraná. Tabelião de Notas e Protesto de Títulos da Comarca de Garuva, Santa Catarina. ORCID: 0009-0000-6631-4086. E-mail: ervin@tabelionatogaruva.com.br;
[2]Especialista em Direito Público pelo Centro Universitário Newton Paiva, Belo Horizonte, Minas Gerais. Oficial de Registro Civil das Pessoas Naturais da Comarca de Dois Vizinhos, Paraná. ORCID: 0009-0005-5653-4401. E-mail: luizggibram@gmail.com;
[3]Doutorando em Ciências Jurídicas pela Universidad del Museo Social Argentino, Buenos Aires, Argentina. Registrador Civil das Pessoas Naturais e RTDPJ da Comarca de Terra Rica, Paraná. ORCID: 0009-0005-0159-6752. E-mail: cartoriocletorocha@gmail.com;
[4]Doutoranda em Ciências Jurídicas pela Universidad del Museo Social Argentino, Buenos Aires, Argentina. Registradora de Imóveis, Civil das Pessoas Naturais e RTDPJ da Comarca de Porto Murtinho, Mato Grosso do Sul. ORCID: 0009-0005-9794-8766. E-mail: 1oficioportomurtinho@gmail.com.

Submetido em: 02/06/2025, revisado em: 15/06/2025 e aceito para publicação em: 24/06/2025.

RESUMO: O presente artigo discute, sob enfoque constitucional e civilista, os desafios e perspectivas do reconhecimento notarial remoto na era da identidade digital. Com o advento de atos normativos como os Provimentos nº 100/2020 e nº 149/2023 do CNJ, os serviços notariais passaram a operar também no ambiente virtual, baseados em tecnologias como biometria, certificados digitais e *blockchain*. Com isso, esse processo projeta o notário como agente de confiança em uma arquitetura algorítmica e gera tensões entre a preservação da autonomia privada, a proteção de dados pessoais e o direito fundamental à identidade. Nesse ínterim, a pesquisa parte da concepção dogmática da identidade como atributo da personalidade, reafirmando sua centralidade frente aos riscos de apropriação indevida, *profiling* abusivo e despersonalização algorítmica. Utiliza-se metodologia jurídico-dogmática com base em revisão bibliográfica crítica e análise documental. O estudo percorre quatro eixos principais: (1) a configuração jurídica da identidade digital, com destaque para sua dimensão relacional e informacional; (2) a estruturação normativa e técnica do reconhecimento notarial remoto; (3) as tensões constitucionais entre identidade, privacidade e autodeterminação informacional; e (4) os desafios regulatórios à fé pública digital. Conclui-se que a virtualização notarial deve ser acompanhada por uma governança híbrida e transparente, capaz de compatibilizar inovação tecnológica com segurança jurídica e proteção da dignidade humana. Propõe-se, dessa maneira, a consolidação de um ecossistema identitário descentralizado, centrado no usuário e sustentado por normas interoperáveis, sob a mediação do notariado como instância ética e institucional de verificação da verdade jurídica no século XXI.
Palavras-chave: Autodeterminação informacional; Reconhecimento remoto; Proteção de dados pessoais; Governança algorítmica.

RESUMO: This article discusses, from a constitutional and civil law perspective, the challenges and prospects of remote notarial recognition in the era of digital identity. With the advent of normative acts such as CNJ Provisions No. 100/2020 and No. 149/2023, notarial services have extended their operations to the virtual environment, relying on technologies such as biometrics, digital certificates, and blockchain. Consequently, this process projects the notary as a trusted agent within an algorithmic architecture, raising tensions between the preservation of private autonomy, the protection of personal data, and the fundamental right to identity. In this context, the research is grounded in the dogmatic conception of identity as an attribute of personality, reaffirming its centrality in the face of risks such as data misappropriation, abusive profiling, and algorithmic depersonalization. The methodology adopted is legal-dogmatic, based on critical literature review and documentary analysis. The study is structured around four main axes: (1) the legal configuration of digital identity, with emphasis on its relational and informational dimensions; (2) the normative and technical framework of remote notarial recognition; (3) constitutional tensions between identity, privacy, and informational self-determination; and (4) regulatory challenges to digital public faith. It concludes that notarial virtualization must be accompanied by hybrid and transparent governance capable of reconciling technological innovation with legal security and the protection of human dignity. Accordingly, the study proposes the consolidation of a decentralized identity ecosystem, user-centered and supported by interoperable standards, under the mediation of the notarial function as an ethical and institutional authority for verifying legal truth in the twenty-first century.
Keywords: Informational self-determination; Remote recognition; Personal data protection; Algorithmic governance.

1 CONSIDERAÇÕES INICIAIS

A virtualização acelerada das interações sociais, intensificada pela pandemia de Covid-19, trouxe para o centro do debate jurídico a delicada questão da identificação civil no espaço digital. Enquanto, de um lado, a tecnologia incrementa a eficiência dos serviços notariais, de outro desafia as bases dogmáticas da autonomia privada e da própria garantia constitucional da identidade, entendida desde Savigny como atributo indissociável da personalidade (Savigny, 2006) e, no Brasil, consolidada na obra clássica de Pontes de Miranda (Miranda, 1955). É nesse cenário que surge a identidade digital, que é uma construção informacional que, ao mesmo tempo em que projeta a pessoa na rede, a expõe a riscos inéditos de apropriação indevida de dados (Bioni, 2019).

O ponto de curvatura normativo deu-se com o Provimento nº 100/2020 da Corregedoria Nacional de Justiça, que instituiu o e-Notariado e regulamentou atos notariais eletrônicos (Brasil, 2020). A consolidação da matéria veio com o Provimento nº 149/2023, ao aprovar o Código Nacional de Normas — Foro Extrajudicial (Brasil, 2023). Ambos os atos projetam o notário como elo de confiança na era algorítmica e realçam a tensão entre segurança jurídica, proteção de dados pessoais (Lei nº 13.709/2018) e a liberdade contratual do indivíduo. Esses diplomas provocam o problema central investigado neste estudo: em que medida os mecanismos de reconhecimento notarial remoto preservam, ou eventualmente comprimem, a autonomia privada e o núcleo essencial do direito à identidade?

Nesse ínterim, o objetivo consiste em examinar, sob enfoque constitucional e civil, a adequação dos atuais modelos de reconhecimento notarial digital aos parâmetros de dignidade da pessoa humana, autodeterminação informacional e livre manifestação de vontade. Especificamente, busca-se reconstruir o conceito de identidade digital e seu tratamento dogmático; mapear a evolução regulamentar do reconhecimento notarial virtual e apontar desafios e perspectivas para aperfeiçoamento legislativo e técnico do sistema.

Metodologicamente, adota-se pesquisa qualitativa, de natureza jurídico-dogmática, alicerçada em revisão bibliográfica crítica de autores clássicos e contemporâneos, nacionais e estrangeiros, e em análise documental dos Provimentos do CNJ e de decisões judiciais correlatas. O método hermenêutico crítico permite confrontar fundamentos teóricos da autonomia privada com a realidade prática dos sistemas de certificação e biometria utilizados pelos cartórios, dialogando com as categorias analíticas da "confiança algorítmica" (Zuboff, 2023) e da "privacidade como poder" (Doneda, 2021).

A relevância do trabalho decorre de três fatores. Primeiro, a expansão exponencial dos atos notariais eletrônicos demanda discussão doutrinária que ultrapasse a mera leitura regulamentar, situando o fenômeno no âmbito dos direitos da personalidade. Segundo o regime jurídico brasileiro encontra-se em processo de harmonização com padrões internacionais de identidade digital, exigindo respostas dogmaticamente consistentes que preservem a tradição civilista sem obstar a inovação. Igualmente, a pesquisa atende ao imperativo constitucional de efetivar a dignidade da pessoa humana, demonstrando que a autenticação remota, se adequadamente desenhada, pode potencializar o exercício da autonomia, ao mesmo tempo em que mitiga riscos de exclusão e vigilância excessiva.

Com essa trajetória, o artigo se estrutura em quatro seções: (1) identidade digital e sua configuração jurídica; (2) reconhecimento notarial de identidade no contexto virtual; (3) tensões entre direito à identidade, proteção de dados e autonomia; e (4) desafios e perspectivas para o futuro do reconhecimento notarial digital. Cada parte dialoga com a doutrina e com o marco regulatório nacional, articulando-se para oferecer diagnóstico crítico e proposições concretas que contribuam para o aperfeiçoamento do sistema registral brasileiro no século XXI.

2 IDENTIDADE DIGITAL E SUA CONFIGURAÇÃO JURÍDICA

A identidade, desde as origens romanísticas, é concebida como atributo da personalidade, pois fixa a individualidade do sujeito perante a ordem jurídica. Savigny, ao tratar do *status hominis* como condição necessária ao exercício de direitos, já destacava que a identificação civil comporta dimensão ontológica ligada à dignidade da pessoa (Savigny, 2006). No civilismo brasileiro, Pontes de Miranda reforça que a identidade integra o conteúdo mínimo dos denominados "direitos da personalidade", assegurando ao indivíduo proteção contra a deturpação de seu ser (Miranda, 1955).

A abordagem contemporânea mantém o mesmo núcleo axiológico, preservando a pessoa contra usurpação ou manipulação de seus traços qualificativos, em sintonia com os arts. 11 a 21 do Código Civil e com o art. 1º, III, da Constituição, que erige a dignidade como fundamento da República (Diniz, 2023). Todavia, a doutrina atual tem ampliado a compreensão do direito à identidade, superando a leitura estritamente documental ou nominalista e incorporando dimensões subjetivas e relacionais da existência humana.

Nesse sentido, Almeida, Vedovato e Silva (2018) defendem que a identidade pessoal deve ser reconhecida como um direito da personalidade com estatura fundamental, estando diretamente relacionada à garantia do livre desenvolvimento da personalidade. Para os autores, o direito à identidade inclui os traços morais, ideológicos e sociais que estruturam a noção de "quem" o sujeito é no mundo jurídico e social. Ou seja, trata-se de uma construção que se manifesta em campos diversos, como o reconhecimento de pessoas trans, o direito ao esquecimento e o respeito à identidade genética.

Essa perspectiva é reforçada por Bolesina e Gervasoni (2018), ao indicarem que a identidade permite à pessoa "ser quem é" e "como é", protegendo seu projeto existencial presente e futuro. Esses autores destacam que, enquanto a personalidade indica o "como" do sujeito (seu temperamento, atitudes), a identidade refere-se ao "quem", uma dimensão ligada à autorreconhecimento e à autopercepção situada social e simbolicamente. De tal modo, a identidade é, ao lado da dignidade, um elemento

basilar para a efetivação dos direitos da personalidade no contexto do Estado Constitucional de Direito.

Em consonância, Siqueira e Moreira (2023) mostram como a construção identitária também é impactada pelas transformações tecnológicas no ciberespaço. A exclusão digital, por exemplo, pode representar uma forma de marginalização identitária, ao impedir que determinados grupos, como moradores de zonas rurais ou classes empobrecidas, participem da formação de suas representações pessoais e políticas no ambiente digital. A ciberdemocracia, nessa toada, deve ser compreendida como espaço de afirmação da identidade pessoal diante das novas formas de sociabilidade mediadas por tecnologias da informação.

Bem como, Affonso (2021) ressalta que o reconhecimento do direito à identidade implica também sua proteção contra representações falsas, distorcidas ou inverídicas, principalmente no contexto digital. A construção da identidade, sobretudo no ambiente virtual, desafia os instrumentos clássicos do direito civil, exigindo abordagens normativas mais sensíveis à pluralidade das identidades contemporâneas. O direito à identidade, nesse cenário, atua como escudo protetivo contra a instrumentalização do sujeito pela lógica do algoritmo, reafirmando sua centralidade como direito fundamental.

O advento da sociedade da informação amplia o espectro desse debate. Para Floridi (2014), a "infosfera" cria uma esfera ontológica na qual cada indivíduo passa a projetar um "gêmeo informacional", cuja existência é tão relevante quanto a presença física. Robles-Carrillo (2024) complementa que a identidade digital, resultado de credenciais, metadados e reputação algorítmica, deixa de ser mero espelho para adquirir autonomia funcional, habilitando atos jurídicos plenamente válidos no ciberespaço. Tais construções mostram a coexistência de um polo objetivo (dados oficiais) e de um polo subjetivo (auto-representação), exigindo releitura dogmática dos direitos da personalidade à luz da virtualização da vida civil.

A literatura recente insiste na pluralidade e na fragmentação do "eu" eletrônico. Pesquisa europeia conduzida por Vardanyan, Hamuľák e Kocharyan (2024) demonstra que a multipropriação dos dados identitários por plataformas e provedores abala o princípio da autodeterminação informativa ao sujeitar o titular a perfis que ele próprio não controla, fenômeno intensificado por modelos de negócio fundados na extração de dados (Zuboff, 2023). Acentua-se, igualmente, a tese de que o direito à identidade digital é corolário lógico do direito fundamental ao livre desenvolvimento da personalidade, devendo ser protegido contra usos não autorizados, *profiling* abusivo e *deepfakes*.

Do ponto de vista tecnológico, três vetores hoje estruturam a identificação de pessoas, como a biometria multivariada (impressões digitais, reconhecimento facial ou íris); certificados digitais emitidos no âmbito da ICP-Brasil, que viabilizam assinaturas eletrônicas qualificadas; e registradores distribuídos, principalmente *blockchains*, aptos a garantir imutabilidade e transparência dos atributos identitários. No plano normativo, o Decreto 10.977/2022 instituiu a Carteira de Identidade Nacional e padronizou atributos de interoperabilidade, ao passo que a Lei 14.534/2023 determinou que o CPF passe a ser número único e suficiente de registro civil, inclusive para versões digitais do documento. Ambas as normas reforçam a tendência de consolidação de um identificador universal que sirva de chave para serviços públicos e privados, inclusive via aplicativo gov.br e QR-code de verificação (Brasil, 2022; Brasil, 2023).

Esses marcos dialogam diretamente com a Lei 14.129/2021, o "Marco do Governo Digital", que estabelece princípios de interoperabilidade, privacidade desde a concepção e compartilhamento mínimo de dados, condicionando o Estado à adoção de padrões abertos e à prestação de contas sobre o ciclo de vida das informações do cidadão. A legislação complementa a LGPD (Lei 13.709/2018) ao exigir bases legais para o tratamento de dados biométricos, classificados como sensíveis, e para a geração de evidências criptográficas em cadastros públicos, exigências que vinculem entes federativos e prestadores delegados (Brasil, 2021).

No cenário internacional, o novo Regulation (EU) 2024/1183, denominado eIDAS 2.0, estabelece um quadro europeu de identidade digital interoperável, impondo aos Estados-membros o fornecimento de carteiras de identidade digital (*European Digital Identity Wallet*) controladas pelo titular, ancoradas em padrões abertos e com equivalência automática de confiança jurídica transfronteiriça. A norma reconhece explicitamente o princípio do "*self-sovereign identity*" (SSI) como parâmetro de segurança e privacidade, aproximando-o do conceito de autodeterminação informativa inaugurado pelo *Bundesverfassungsgericht* em 1983.

A tecnologia blockchain surge, nesse contexto, como promessa de descentralizar a fé pública e garantir identidades imutáveis e auditáveis sem dependência de repositórios centrais. Leitão, Machado e Cidrão (2022) demonstram, no âmbito notarial brasileiro, como registros em *blockchains* permissionadas poderiam conferir presunção de autenticidade comparável àquela derivada do art. 236 da Constituição, mitigando fraudes documentais. Em chave dogmática, Swan (2015) e Filippi e Wright (2018) defendem que a "confiança algorítmica" só se legitima se acompanhada de governança jurídico-institucional que assegure responsabilização por falhas de *software* ou oráculos contratuais, evitando lacunas de *accountability* em redes públicas.

No plano civil-constitucional brasileiro, a identidade digital também se projeta sobre a esfera negocial, onde contratos inteligentes, assinaturas biométricas e *log-records* possuem plena eficácia probatória, mas sujeitam-se ao regime dos arts. 422 e 421-A do Código Civil, exigindo boa-fé objetiva e proteção da parte mais vulnerável. O desvio de finalidade ou o sequestro de credenciais pode causar dano moral autônomo, dado o abalo à integridade psíquica do titular. Bem como, a jurisprudência já admite reparação quando o uso indevido de dados resulta em score negativo ou em usurpação de perfil virtual.

A par disso, a responsabilidade civil estatal é acionada quando vazamentos se originam de bases governamentais, pois incide o dever objetivo de segurança

previsto no art. 8º, § 1º, da LGPD. Em caso de certificadoras privadas, aplica-se o CDC, admitindo-se responsabilidade solidária entre a Autoridade Certificadora (AC) e o agente que subverteu o credential. O mesmo raciocínio vale para provedores de biometria que não realizam "*privacy impact assessment*", descumprindo art. 38 da LGPD. Bem como, a inserção da identidade digital no domínio dos direitos da personalidade impõe releituras axiológicas, pois a possibilidade de múltiplas representações de si mesmo convoca a teoria da intersubjetividade e a proteção da autenticidade relacional. Não se trata exclusivamente de garantir a imutabilidade dos dados, mas de assegurar ao indivíduo o poder de construir e reconstruir sua auto-imagem sem coerção algorítmica, condição imprescindível à autonomia privada na era da inteligência artificial.

3 O RECONHECIMENTO NOTARIAL DE IDENTIDADE NO CONTEXTO VIRTUAL

A fé pública notarial, concebida historicamente como garantia de autenticidade e de segurança jurídica, encontra no reconhecimento de identidade a sua manifestação nuclear, em que o tabelião testemunha quem é a parte que subscreve um ato, conferindo presunção de veracidade que se projeta sobre todo o instrumento (Miranda, 1955). No sistema latino de notariado, acolhido no Brasil desde o período colonial e positivado na Constituição de 1988 (art. 236) e na Lei 8.935/1994, essa verificação sempre exigiu a presença física do signatário e a conferência ocular de documentos de identificação. Contudo, a expansão das transações eletrônicas, a digitalização de documentos e, sobretudo, as demandas de distanciamento social durante a pandemia da Covid-19 aceleraram a migração dessa função para o meio virtual, impondo novos contornos dogmáticos ao tradicional reconhecimento de firma.

O ponto de mudança normativa deu-se com o Provimento CNJ n.º 100/2020, que instituiu o Sistema de Atos Notariais Eletrônicos (e-Notariado) e autorizou o reconhecimento de identidade por videoconferência, mediante emissão de certificado digital notarizado vinculado à biometria do usuário (Brasil, 2020). A norma ancorou-se na Medida Provisória 2.200-2/2001, que consagrou a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), e dialogou com a Lei 14.063/2020, responsável por classificar as assinaturas eletrônicas em simples, avançada e qualificada. Subsequentemente, o Provimento CNJ n.º 149/2023, incorporado ao Código Nacional de Normas do Foro Extrajudicial, consolidou o modelo e definiu, no art. 285, II, o "certificado digital notarizado" como "identidade digital de uma pessoa física ou jurídica, identificada presencialmente ou por videoconferência por notário investido de fé pública" (Brasil, 2023a). Trata-se de um conceito normativo próprio, distinto do certificado ICP-Brasil qualificado e das soluções privadas de assinatura avançada, porque agrega a chancela notarial e o respectivo dever de guarda da prova de vida audiovisual, reforçando a cadeia de custódia probatória (Loureiro, 2023).

Do ponto de vista dogmático-civil, o fenômeno representa a virtualização da "*capitis deminutio* mínima" da pessoa natural. A identidade, elemento da personalidade, passa a ser verificada e declarada em camada algorítmica, sem que se descaracterize a natureza pública preventivo-jurisdicional da atividade notarial (Tepedino; Schreiber, 2020). A doutrina ressalta que a legitimação constitucional da delegação privada (art. 236, caput) exige a preservação dos princípios da legalidade, da publicidade e da eficiência (Barroso, 2023). Logo, quaisquer soluções tecnológicas devem submeter-se ao controle normativo do CNJ, sob pena de se esvaziar a própria razão de ser da fé pública (Cassattari; Ferreira; Rodrigues, 2024).

Tecnicamente, o reconhecimento virtual é sustentado por três elementos: a realização de prova de vida por meio de recursos audiovisuais e biométricos em sessão criptografada, a verificação documental automatizada geralmente conduzida por tecnologia de reconhecimento óptico de caracteres (OCR) com cruzamento de dados em bases governamentais como CPF, CIN e Denatran, e por fim, a aposição de assinatura digital ou eletrônica vinculada a certificados emitidos no âmbito da ICP-Brasil ou ao certificado notarizado conforme previsto no Provimento nº 149/2023 (Leitão; Machado; Cidrão, 2022).

A plataforma e-Not Assina opera esses elementos em ciclo fechado, garantindo a inalterabilidade do vídeo, do *hash* do documento e dos metadados de geolocalização. Quando desejado, o ato pode ainda ser ancorado em *blockchain* permissionada, compondo camadas redundantes de auditabilidade sem afastar a centralidade do notário como oráculo de confiança (Leitão; Machado; Cidrão, 2022). O certificado digital notarizado, de emissão gratuita, tornou-se, assim, a credencial identitária que habilita o cidadão a praticar atos eletrônicos de forma remota, inclusive o reconhecimento de firma por semelhança no módulo e-Not Assina. Como observa Souza (2025), o modelo projeta sobre o ambiente virtual a presunção de veracidade típica do reconhecimento presencial, mas adiciona registro auditável em tempo real, mitigando fraudes e reduzindo custos transacionais nas operações civis e empresariais.

O componente axiológico da fé pública, que é a confiança institucional, suscita acesa controvérsia. Poderia a "confiança algorítmica" substituir a tutela humana do notário? A doutrina majoritária responde negativamente. Loureiro (2023) sustenta que a inteligência artificial, ainda que empregada em análise facial, não detém o poder de discernir fatores sociopsicológicos capazes de indicar coação ou incapacidade, tarefa que continua a exigir juízo profissional de legalidade. Nos Estados Unidos, onde *Remote Online Notarization* (RON) foi autorizado em 44 estados até 2024, estudos empíricos apontam acréscimo de segurança, mas também aumento de litígios sobre identidade fraudulenta, forçando legisladores estaduais a exigir *storage* mínimo de 10 anos dos arquivos de vídeo (Lewis, 2024).

A comparação internacional reforça a relevância da regulação pública. Naghmouchi *et al*. (2023), em análise de soluções eIDAS, BankID e Aadhaar, concluem que sistemas de identidade digital dependem de arcabouços legais claros de imputação de responsabilidade e da interoperabilidade entre identidades estatais e credenciais privadas, sob pena de fragmentação e insegurança. No

Brasil, a sinergia entre a Carteira de Identidade Nacional (Lei 14.534/2023) e o certificado notarizado tende a criar ecossistema híbrido em que a Administração Pública e os notários compartilham atributos verificáveis, ampliando o espectro de uso da identidade na esfera civil, contratual e registral.

Do ponto de vista da tutela de dados, o art. 6º, I, da LGPD (Lei 13.709/2018) impõe ao notário como controlador o dever de transparência sobre a coleta biométrica e o armazenamento de vídeos. A conjugação de base legal "cumprimento de obrigação legal" (art. 7º, II) e "exercício regular de direito" (art. 7º, VI) legitima o tratamento, mas não afasta a obrigação de elaborar Relatório de Impacto à Proteção de Dados (RIPD) quando o volume de certificados superar risco alto, conforme orienta a ANPD.

Em chave processual-civil, a ata notarial de videoconferência reforça a força probatória do ato (CPC, art. 384). O vídeo arquivado no repositório do Colégio Notarial do Brasil, dotado de *hash* e carimbo de tempo, é "meio idôneo de autoria e integridade" na acepção do art. 10, §1º, da MP 2.200-2/2001. Doutrinadores como Venosa (2024) defendem que, superada a materialidade, o ponto controvertido desloca-se à volição, requerendo análise de vícios de consentimento, tema que, por sua natureza, não se resolve por mera tecnologia, mas pela atuação interpretativa do notário durante a videoconferência.

No campo consumerista, o reconhecimento de identidade virtual é serviço pertinente (art. 22, CDC). A falha na verificação, por exemplo, *deepfake* não detectado, pode ensejar responsabilidade objetiva do delegatário, com regressividade possível contra provedores de biometria se demonstrado defeito na base de comparação (Frazão, 2018). Contudo, o Provimento 149/2023 reforça, no art. 308, que o notário deve manter logs de validação biométrica, distribuindo melhor a prova em eventual litígio.

A agenda regulatória projeta novos desafios. O Projeto de Lei 4/2025, ao exigir assinatura qualificada para documentos "com efeitos perante terceiros", reacende o debate sobre custo-efetividade e exclusão digital. Souza (2025) lembra que a assinatura avançada, chancelada pelo notário, já entrega elevado grau de certeza, em que obrigar a modalidade qualificada pode inviabilizar microempresas e contraria a diretriz de simplificação constante da Lei 14.195/2021.

4 TENSÕES ENTRE O DIREITO À IDENTIDADE, A PROTEÇÃO DE DADOS E A AUTONOMIA NO MEIO DIGITAL

Na sociedade em rede, a individualidade é mediada por dados que circulam em tempo real, convertidos em insumos econômicos e vetores de poder informacional (Solove, 2010; Zuboff, 2023). Essa mutação intensifica as tensões entre o direito à identidade, a proteção de dados e a autonomia privada, exigindo releitura constitucional e civilista dos institutos tradicionais.

A Constituição de 1988 consagra, no art. 5º, X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, fundamentos que, segundo Sarlet, conformam o "conteúdo mínimo existencial" da dignidade humana (Sarlet, 2021). A Emenda Constitucional 115/2022 elevou a proteção de dados a direito fundamental autônomo, alinhando-se ao precedente alemão do "Censo" que reconheceu a autodeterminação informativa como corolário da personalidade (BVerfG, 1983). Em julgamento paradigmático da ADI 6.387, o STF adotou a mesma premissa, declarando que o controle sobre fluxos informacionais integra a essência da liberdade individual (STF, 2020). Para Sarmento, tal entendimento impõe ao Estado o dever de criar condições para que o indivíduo molde sua identidade sem coerções manipulativas (Sarmento, 2010).

No plano infraconstitucional, a Lei 13.709/2018 (LGPD) insere cartórios e tabelionatos, tradicionais depositários da fé pública, no regime geral de proteção de dados, submetendo-os a princípios de finalidade, adequação, minimização e segurança. Loureiro observa que a publicidade registral, embora garanta eficácia *erga omnes*, deve ser compatibilizada com a privacidade, sob pena de violação ao art. 6º da LGPD (Loureiro, 2020). Estudos empíricos sobre a adoção de *blockchain* em atos notariais reforçam a necessidade de filtros finalísticos e registros de acesso para evitar exposição indevida de dados sensíveis (Leitão; Machado; Cidrão, 2022; Lemieux, 2016). Bioni acrescenta que a fé pública digital não pode legitimar tratamento excessivo nem dispensar a avaliação de impacto prevista nos arts. 38-40 da LGPD (Bioni, 2019).

O consentimento, previsto como base legal nos arts. 7º, I e 8º da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), representa, em seu núcleo normativo, a expressão da autonomia privada no contexto do tratamento de dados. Inspirado no modelo liberal-civilista, o consentimento é, em tese, a manifestação de vontade consciente e deliberada do titular de dados, que autoriza determinadas operações com suas informações pessoais. Contudo, a complexidade das relações digitais contemporâneas introduziu novos condicionamentos à sua validade jurídica, que é o consentimento deve ser livre, informado, inequívoco e revogável a qualquer tempo, conforme estipulado na legislação vigente. A mera formalização do ato consentido não basta para legitimá-lo, pois é indispensável que o titular possua efetivo controle sobre o ciclo de vida de seus dados.

Danilo Doneda foi um dos primeiros juristas brasileiros a alertar sobre os limites do consentimento como fundamento exclusivo da autodeterminação informacional. Para o autor, em ambientes marcados por assimetria informacional, o consentimento apenas poderá ser considerado legítimo quando estiver acompanhado de mecanismos concretos de transparência granular e controle *ex-post* (Doneda, 2006). Trata-se de um processo contínuo que exige condições materiais de compreensão, acompanhamento e intervenção sobre o tratamento dos dados.

Gustavo Binenbojm Mendes reforça essa crítica ao destacar que as políticas de privacidade frequentemente utilizadas por empresas de tecnologia, longas, genéricas e de difícil interpretação, tornam o consentimento uma ficção jurídica, esvaziando a autonomia do titular. Segundo o autor, práticas contratuais unilaterais do tipo "*take it or*

leave it", em que o usuário se vê obrigado a aceitar todos os termos para acessar um serviço essencial, transformam o consentimento em um "ato de adesão digital compulsório", o que compromete a integridade da autodeterminação informacional (Mendes, 2013).

Pesquisas recentes reforçam a insuficiência estrutural do modelo tradicional de consentimento. Nascimento e Silva (2023), ao analisarem experiências institucionais de implementação da LGPD, apontam a dificuldade prática de operacionalizar o consentimento ativo, bem como os desafios para manter registros confiáveis das operações de tratamento. Os autores sugerem que o consentimento só adquire efetividade dentro de um ecossistema regulatório que imponha obrigações de governança informacional, auditoria contínua e responsabilização por práticas abusivas.

Mesmo diante do avanço de tecnologias de autenticação e segurança, como a biometria, os certificados digitais e os sistemas baseados em *blockchain*, o ambiente digital segue permeado por riscos estruturais à identidade e à privacidade. A disseminação de técnicas como *deepfakes*, a clonagem de perfis em redes sociais e o comércio clandestino de dados expõem a fragilidade da chamada "confiança algorítmica". Como sublinha Zuboff (2023), a lógica do capitalismo de vigilância desloca o eixo da confiança da institucionalidade jurídica para sistemas automatizados de extração comportamental, enfraquecendo as garantias materiais de proteção à identidade.

Daniel Solove vai além ao demonstrar que dados aparentemente anônimos podem ser facilmente reidentificados mediante cruzamento de bases paralelas, o que permite a reconstrução de narrativas pessoais sem o conhecimento ou o consentimento do titular. Tal prática compromete o sigilo e pode gerar efeitos discriminatórios e excludentes, em franco contraste com os direitos fundamentais (Solove, 2010). Isso demonstra que o simples anonimato não é medida suficiente de proteção, e que a governança de dados exige controle normativo e técnico articulado.

Nesse cenário, a doutrina contemporânea tem defendido o fortalecimento das instituições jurídicas tradicionais como forma de restaurar a confiança na proteção da identidade informacional. Loureiro (2020) propõe que os serviços notariais, agora integrados ao ambiente digital, assumam o papel de *gatekeepers* da segurança informacional. Para isso, seriam necessárias trilhas de auditoria, validação biométrica de ponta a ponta (*end-to-end*) e sistemas de revogação de consentimento centralizados, todos operados com supervisão estatal. A fé pública, nesse contexto, não desaparece, pois se adapta à lógica digital para oferecer uma âncora jurídica contra a volatilidade algorítmica.

Das premissas expostas decorre que a salvaguarda da identidade no meio digital passa por uma hermenêutica que articule dignidade humana, proporcionalidade e responsabilidade algorítmica. A LGPD oferece o arcabouço, mas seu êxito depende da atuação ativa da Autoridade Nacional de Proteção de Dados e da internalização de boas práticas em todos os elos da cadeia notarial.

5 DESAFIOS E PERSPECTIVAS PARA O FUTURO DO RECONHECIMENTO NOTARIAL DIGITAL

Consoante discutido ao longo do artigo, a disseminação dos serviços notariais em meio virtual, impulsionada pelo Provimento n.º 100/2020 do Conselho Nacional de Justiça, deslocou o epicentro da confiança pública dos balcões cartorários tradicionais para ambientes digitais sustentados por infraestrutura criptográfica e plataformas de videoconferência autenticada. Tal migração provoca fissuras nas categorias jurídicas clássicas e exige reflexão dogmática sobre a identidade digital como projeção da personalidade civil (Loureiro, 2019; Lemieux, 2016). Afinal, se a fé pública nasce da presunção de veracidade dos atos notariais, a quem se atribui a função legitimadora quando a verificação identitária passa a depender de algoritmos de biometria facial, certificados ICP-Brasil e integrações em *blockchain*?

A reconstrução da confiança institucional na era da confiança algorítmica precisa partir do reconhecimento de que as tecnologias distribuem, mas não eliminam, relações de poder e de responsabilidade. No regime presencial, a credibilidade derivava da pessoa do notário, investida pela delegação estatal prevista no art. 236 da Constituição e submetida à fiscalização direta do Poder Judiciário (Loureiro, 2019). Na arquitetura digital, esse lugar de confiança é fragmentado entre o desenvolvedor do *software*, a autoridade certificadora, o provedor de nuvem e o próprio usuário, que precisa manipular as credenciais de autenticação (Tapscott, 2016). A doutrina de registros e arquivos adverte que algoritmos apenas transmutam o *locus* da fé pública para camadas técnicas, motivo pelo qual "não há 'sistemas sem confiança', mas sim deslocamentos da confiança" (Lemieux, 2016). Surge, portanto, a tarefa de desenhar uma governança híbrida, em que a responsabilidade subjetiva do notário permaneça ancorada nos princípios de legalidade, impessoalidade e eficiência, enquanto os protocolos computacionais forneçam evidências auditáveis da identidade verificada (Filippi; Wright, 2018).

Nesse sentido, a harmonização normativa entre segurança jurídica, inovação e direitos fundamentais opera em três frentes complementares. A primeira é a convergência constitucional entre os princípios da dignidade da pessoa humana, da proteção de dados pessoais e da livre iniciativa, que impõe ao legislador balancear autonomia privada e salvaguardas contra usos lesivos da informação (Sarmento, 2010; Brasil, 2018). A segunda refere-se à infraestrutura legal de assinaturas eletrônicas, delineada pela Medida Provisória n.º 2.200-2/2001 e aprimorada pela Lei 14.063/2020, instrumentos que classificam graus de confiabilidade das assinaturas e demandam interoperabilidade com sistemas notariais (Brasil, 2001; Brasil, 2020a). A terceira dimensão é comparativa, em que o Regulamento eIDAS europeu (Reg. UE 910/2014) instituiu níveis de identificação eletrônica reconhecíveis em toda a União, indicando que a portabilidade transfronteiriça dos atributos identitários se torna requisito para a economia digital global (União Europeia, 2014). A partir desse paradigma, a doutrina nacional propugna que a segurança jurídica seja diretriz

axiológica para sua legitimação (Mello, 2021; Leitão; Machado; CidrãO, 2022).

Em termos propositivos, impõem-se aprimoramentos legislativos e técnicos específicos. No plano infra-legal, o Provimento n.º 100/2020 deve ser alinhado ao Provimento n.º 74/2018, de modo a atualizar requisitos mínimos de cibersegurança, criptografia assimétrica e redundância de registros imutáveis em redes permissonadas mantidas pelos próprios cartórios, sob supervisão do CNJ (Brasil, 2018; Brasil, 2020b). No plano legal, a recém-sancionada Lei 14.382/2022, que criou o Sistema Eletrônico de Registros Públicos (SERP), carece de regulamentação que integre certificados ICP-Brasil aos registros notariais remotos e permita validação cruzada com bases governamentais, tais como CPF, Carteira Nacional de Identidade eletrônica e cadastros fiscais, evitando a proliferação de identidades múltiplas (Brasil, 2022). Do ponto de vista tecnológico, a literatura recomenda a adoção de padrões aberto, como *Decentralized Identifiers* (DIDs) e *Verifiable Credentials* (VCs), e a implementação de protocolos de prova de posse de chave (PoP) que substituam autenticações meramente baseadas em login-senha (Lacity, 2020). Outrossim, contratos inteligentes podem automatizar verificações de ônus fiscais, como ITBI e IPTU, antes da lavratura de escrituras, reforçando a função preventiva do notário (Filippi; Wright, 2018).

Nada disso, porém, prescinde da mediação entre tecnologia, subjetividade e juridicidade. A identidade, entendido como direito da personalidade, é atributo de processo contínuo de reconhecimento social, autopoiético, que requer espaço para manifestação de vontade e para a proteção contra reducionismos informacionais (Diniz, 2023). A teoria axiológica do Direito Civil contemporâneo, ao positivar a dignidade da pessoa humana como cláusula geral, impõe limites à despersonalização provocada por sistemas de pontuação automática ou por perfis presuntivos derivados de *big data* (Ferraz Jr., 2021). Desse ponto de vista, a "confiança algorítmica" só alcança legitimidade se acompanhada de mecanismos de transparência, auditoria e recorribilidade, possibilitando que o usuário compreenda e conteste eventuais recusas de reconhecimento identitário (Hawlitschek; Notheisen; Teubner, 2018). Com isso, a fé pública digital deve ser concebida como resultado de um diálogo normativo e técnico que salvaguarde a autodeterminação informacional sem inviabilizar a eficiência prometida pelas novas tecnologias.

Portanto, ressalta-se que o futuro do reconhecimento notarial digital depende de uma engenharia jurídico-tecnológica que reafirme, simultaneamente, a relevância institucional do notário como guardião da segurança jurídica e a potência disruptiva das arquiteturas algorítmicas de verificação de identidade. A reconstrução da confiança pública requer, pois, o aperfeiçoamento constante das normas de proteção de dados, a adoção de padrões abertos de interoperabilidade, a revisão das responsabilidades civis em rede distribuída e o respeito incondicional à dignidade da pessoa humana enquanto núcleo axiológico de todo o ordenamento.

6 CONSIDERAÇÕES FINAIS

As reflexões propostas neste artigo permitiram consolidar um campo teórico em torno da identidade digital como categoria jurídica autônoma e multifacetada, bem como da fé pública notarial em seu processo de virtualização. Entretanto, suplantar os marcos normativos e dogmáticos já assentados impõe a abertura de novos horizontes de investigação e regulação, capazes de responder aos dilemas emergentes da sociedade da informação em permanente mutação.

Primeiramente, impõe-se o reconhecimento de que a identidade digital pode ser tratada como um processo contínuo de construção subjetiva e relacional, cuja tutela deve acompanhar as mutações do sujeito jurídico na era da interconectividade algorítmica. O direito civil brasileiro, ainda calcado em uma lógica formalista e documental, necessita incorporar de modo sistemático a teoria da personalidade em sua vertente processual e fluida, o que exige uma atualização hermenêutica que dialogue com epistemologias transdisciplinares, como a sociologia das redes e a filosofia da informação.

Nesse contexto, o reconhecimento notarial digital deve ser compreendido como um *locus* privilegiado de interseção entre o Estado, a tecnologia e a subjetividade. A fé pública, ao migrar do papel para o código, não perde sua essência, tendo em vista que adquire camadas de complexidade que impõem nova postura do operador jurídico, pois é necessário garantir a integridade identitária da parte envolvida, protegendo-a de reducionismos algoritmizados. Surge, assim, a urgência de se pensar o notariado como instância de resistência à despersonalização digital, promovendo a autenticidade informacional como bem jurídico tutelável.

Igualmente, torna-se premente a criação de um modelo regulatório de identidade digital centrado no usuário, no qual se consolidem direitos procedimentais claros, tais como o direito à explicação das decisões algorítmicas, o direito à portabilidade identitária e o direito à exclusão de credenciais obsoletas, todos estes estruturados sob o princípio da autodeterminação informacional. A consolidação de um ecossistema de identidades descentralizadas (*self-sovereign identity*) controladas pelo titular, em sinergia com certificações estatais e notariais, poderá representar uma das mais promissoras vias para equilibrar eficiência técnica e dignidade da pessoa humana no século XXI.

Nesse panorama, a atuação das entidades notariais deverá ir além do mero cumprimento normativo, assumindo protagonismo na formação de uma nova cultura jurídica de confiança distribuída. Nessa toada, a integração com ferramentas como inteligência artificial auditável, biometria explicável e provas criptográficas reversíveis impõe um reforço dos princípios axiológicos do Direito Privado. Cabe ao notário, mais do que nunca, exercer função epistêmica e ética, preservando o vínculo entre identidade e verdade jurídica, ainda que sob novas roupagens.

Em conjunto, a evolução das práticas notariais digitais aponta para um campo inexplorado de pesquisas empíricas e experimentações normativas. Qual o impacto

real das assinaturas digitais notarizadas na redução de litígios? Quais os efeitos da fragmentação de identidades digitais nas comunidades periféricas? Como regulamentar a interoperabilidade entre sistemas notariais e plataformas privadas sem ferir a isonomia e o devido processo legal? Essas são apenas algumas das questões que se colocam à doutrina e à jurisprudência no horizonte próximo, exigindo do Direito uma abertura teórica que combine tradição institucional, inovação tecnológica e, sobretudo, compromisso humanista.

REFERÊNCIAS

AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, v. 27, n. 01, p. 251-251, 2021.

ALEMANHA. **Bundesverfassungsgericht.** BVerfG 65, 1. *Volkszählungsurteil* (Census Decision), 15 dez. 1983. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020783.html. Acesso em: 22 jun. 2025.

ALMEIDA, José Luiz Gavião de; VEDOVATO, Luis Renato; SILVA, Marcelo Rodrigues da. A identidade pessoal como direito fundamental da pessoa humana e algumas de suas manifestações na ordem jurídica brasileira. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 14, p. 33-70, jan./mar. 2018.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 10. ed. São Paulo: Saraiva, 2023.

BIONI, Bruno Ricardo. Proteção de dados pessoais. **A função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BOLESINA, Iuri; GERVASONI, Tamiris Alessandra. O direito à identidade pessoal no Brasil. **Saber Humano: Revista Científica da Faculdade Antonio Meneghetti**, v. 8, n. 13, p. 65-87, 2018.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 100, de 26 mai. 2020**. Dispõe sobre a prática de atos notariais eletrônicos no sistema e-Notariado. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3334. Acesso em: 22 jun. 2025.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 149, de 30 ago. 2023**. Institui o Código Nacional de Normas da Corregedoria Nacional de Justiça – Foro Extrajudicial. Brasília, DF: CNJ, 2023. Disponível em: https://atos.cnj.jus.br/atos/detalhar/5243. Acesso em: 22 jun. 2025.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 74, de 31 jul. 2018**. Estabelece padrões mínimos de tecnologia da informação para os cartórios. Brasília, DF: CNJ, 2018. Disponível em: https://atos.cnj.jus.br/files/provimento/provimento_74_31072018_01082018113730.pdf. Acesso em: 22 jun. 2025.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jun. 2025.

BRASIL. **Decreto n.º 10.977, de 23 fev. 2022**. Institui a Carteira de Identidade Nacional. Diário Oficial da União, Brasília, DF, 24 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d10977.htm. Acesso em: 22 jun. 2025.

BRASIL. **Emenda Constitucional n.º 115, de 10 fev. 2022**. Acrescenta a proteção de dados pessoais como direito fundamental. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/emc115.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 13.709, de 14 ago. 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 14.063, de 23 set. 2020**. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos. Diário Oficial da União, Brasília, DF, 24 set. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 14.129, de 29 mar. 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Diário Oficial da União, Brasília, DF, 30 mar. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 14.382, de 27 jun. 2022**. Institui o Sistema Eletrônico dos Registros Públicos – SERP. Diário Oficial da União, Brasília, DF, 28 jun. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14382.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 14.534, de 11 jan. 2023**. Determina o CPF como número único de identificação civil. Diário Oficial da União, Brasília, DF, 12 jan. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14534.htm. Acesso em: 22 jun. 2025.

BRASIL. **Lei n.º 8.935, de 18 nov. 1994**. Regulamenta o art. 236 da Constituição Federal. Diário Oficial da União, Brasília, DF, 21 nov. 1994. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8935.htm. Acesso em: 22 jun. 2025.

BRASIL. **Medida Provisória n.º 2.200-2, de 24 ago. 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. Diário Oficial da União, Brasília, DF, 27 ago. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 22 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n.º 6.387**. Diário da Justiça, Brasília, DF, 21 ago. 2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf. Acesso em: 22 jun. 2025.

CASSATTARI, Christiano; FERREIRA, Paulo Roberto Gaiger; RODRIGUES, Felipe Leonardo. **Tabelionato de Notas**. 7. ed. Indaiatuba: Editora Foco, 2024.

DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law**: The Rule of Code. Cambridge: Harvard University Press, 2018.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**: Direito Civil. Parte geral. 39. ed. São Paulo: Saraiva, 2023.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**: o novo paradigma de tutela da pessoa na sociedade da informação. Rio de Janeiro: Renovar, 2006.

EUROPEAN UNION. **Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 Apr**. 2024. Official Journal of the European Union, 30 Apr. 2024.

FERRAZ Jr., Tercio Sampaio. **Introdução ao estudo do direito: técnica, decisão, dominação**. 8. ed. São Paulo: Atlas, 2021.

FLORIDI, Luciano. **The Fourth Revolution: How the Infosphere is Reshaping Human Reality**. Oxford: Oxford University Press, 2014.

FRAZÃO, Ana. Algoritmos e inteligência artificial: repercussões da sua utilização sobre a responsabilidade civil e punitiva das empresas. **Jota**, Tecnologia, 15 maio 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-einteligencia-artificial. Acesso em: 22 jun. 2025.

HAWLITSCHEK, Florian; NOTHEISEN, Benedikt; TEUBNER, Timm. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. **Electronic Commerce Research and Applications**, v. 29, p. 50-63, 2018.

LACITY, Mary C. **Blockchain Foundations for the Internet of Value**. Fayetteville: Epic Books, 2020.

LEITÃO, André S.; MACHADO, Camila F.; CIDRÃO, Taís V. A tecnologia blockchain representaria o fim dos cartórios extrajudiciais? **Revista Prim@Facie**, v. 21, n. 47, p. 199-222, 2022.

LEMIEUX, Victoria Louise. Trusting records: is Blockchain technology the answer?. **Records management journal**, v. 26, n. 2, p. 110-139, 2016.

LOUREIRO, Luiz Guilherme. **Manual de Direito Notarial**: da atividade e dos documentos notariais. 5. ed. Salvador: Juspodivm, 2023.

LOUREIRO, Luiz Guilherme. **Registros Públicos: Teoria e Prática**. 10. ed. Salvador: Juspodivm, 2019.

MELLO, Celso Antônio Bandeira. **Curso de Direito Administrativo**. 34. ed. São Paulo: Malheiros, 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: os desafios da sociedade da informação. Rio de Janeiro: Elsevier, 2013.

MIRANDA, Francisco Cavalcanti Pontes. **Tratado de Direito Privado**. Tomo I. Rio de Janeiro: Borsoi, 1955.

NAGHMOUCHI, Montassar; LAURENT, Maryline; LEVALLOIS-BARTH, Claire; KAANICHE, Nesrine. Comparative analysis of technical and legal frameworks of various national digital identity solutions. **arXiv e-prints**, 2023.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. **Em Questão**, Porto Alegre, v. 29, e-127314, 2023.

ROBLES-CARRILLO, Manuel. Digital identity: an approach to its nature, concept, and functionalities. **International Journal of Law and Information Technology**, v. 32, n. 1, 2024.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 15. ed. Porto Alegre: Livraria do Advogado, 2021.

SARMENTO, Daniel. **Direitos Fundamentais e suas Restrições**. 2. ed. Rio de Janeiro: Lumen Juris, 2010.

SAVIGNY, Friedrich Karl von. **Sistema do Direito Romano Atual**. 3. ed. Trad. Amador Paes de Almeida. São Paulo: Saraiva, 2006.

SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires. Ciberdemocracia, construção da identidade e os direitos da personalidade. **Revista Direito & Paz**, v. 1, n. 48, p. 302-327, 2023.

SOLOVE, Daniel J. **Understanding privacy**. Harvard university press, 2010.

SOUZA, Evandio Sales de. PL 4/25 e a regulamentação das assinaturas eletrônicas: avanço ou retrocesso? **Migalhas de Peso**, 4 fev. 2025.

SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. Sebastopol: O'Reilly Media, 2015.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin, 2016.

TARTUCE, Flávio. **Manual de direito civil**: parte geral. 8. ed. São Paulo: Método, 2024.

TEPEDINO, Gustavo. Autonomia privada e o papel da vontade na atividade contratual. **Revista Brasileira de Direito Civil**, v. 2, n. 02, 2014.

TEPEDINO, Gustavo; SCHREIBER, Anderson. **Fundamentos do direito civil**: obrigações. Rio de Janeiro: Forense, 2020.

UNIÃO EUROPEIA. **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)**. Official Journal of the European Union, L 257, 28 ago. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910. Acesso em: 22 jun. 2025.

VARDANYAN, Lusine; HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep. Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination. **European Studies–the Review of European law, Economics and Politics**, v. 11, n. 1, p. 105-121, 2024.

VENOSA, Silvio de Salvo. **Direito Civil**: Parte Geral. 24. ed. São Paulo: Atlas, 2023.

ZUBOFF, Shoshana. The age of surveillance capitalism. In: **Social theory re-wired**. Routledge, 2023.