IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

D597

Direito, inovação, propriedade intelectual e concorrência [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Isabel Christine Silva De Gregori; Nivaldo Dos Santos; João Marcelo de Lima Assafim – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-586-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito e inovação. 3. Propriedade intelectual e concorrência. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

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

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

Apresentação

O IX Encontro Virtual do CONPEDI sob a temática “Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos”, ocorreu entre os dias 22 a 26 de junho de 2026. Dentro deste contexto, o Grupo de Trabalho “Direito, Inovação, Propriedade Intelectual e Concorrência” tem se constituído em um expressivo espaço de compartilhamento de pesquisas, oportunizando uma análise crítica de dilemas jurídicos decorrentes das transformações da sociedade contemporânea impulsionadas pela inteligência artificial e das plataformas digitais.

A coletânea de trabalhos propostos non grupo de trabalho, ressalta ainda mais a atualidade e urgência do enfrentamento de questões atinentes aos impactos das novas tecnologias no ordenamento jurídico.

O primeiro artigo é intitulado “A ata notarial como instrumento de higiene da decisão: vieses cognitivos, ruído e prova pré-constituída, partiu da premissa de que a a tomada de decisão humana, inclusive no âmbito jurídico, está sujeita a heurísticas, vieses cognitivos e ruído, fenômenos que podem comprometer a percepção, a interpretação e a documentação dos fatos.

A temática relativa à função social do Direito Autoral foi tratada pelo artigo intitulado “A crise do homo mensura e a função social do direito autoral: desafios regulatórios da autoria instrumental por ia no brasil e em perspectiva comparada.

A colisão entre a imutabilidade da tecnologia blockchain e o direito ao apagamento de dados

Outro tema de suma relevância apresentou o embate entre “A inovação farmacêutica e exclusão sanitária: uma análise crítica do sistema de patentes e das doenças negligenciadas, que abordou a lógica mercadológica predominante na indústria farmacêutica e contribui para perpetuação da exclusão sanitária.

A discussão dos novos paradigmas sucessórios na era da sociedade de informação tratou da autonomia privada como elemento central do sistema sucessório arguindo que a função social da herança de abarcar também os patrimônios informacionais.

Também foram objeto dos artigos apresentados no GT, temáticas versando sobre regulação e concorrência no setor da aviação, regulação de marketplaces, smart contracts em plataformas descentralizadas, proteção civil dos ativos digitais , sigilo aos dossiês de testes de eficácia e segurança para registro de medicamentos, proteção de ativos intangíveis digitais.

Desejamos uma boa leitura!

Os coordenadores

Isabel Christine Silva De Gregori (Universidade Federal de Santa Maria -UFSM)

Dr. João Marcelo de Lima Assafim (Universidade Federal do Rio de Janeiro – UFRJ)

Nivaldo Santos

ENTRE CRONOS E LETHE: A COLISÃO ENTRE A IMUTABILIDADE DA TECNOLOGIA BLOCKCHAIN E O DIREITO AO APAGAMENTO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS

BETWEEN CRONOS AND LETHE: THE COLLISION BETWEEN BLOCKCHAIN IMMUTABILITY AND THE RIGHT TO ERASURE OF PERSONAL DATA UNDER THE BRAZILIAN GENERAL DATA PROTECTION LAW

Thamires Ribas Lopes Smith [1]
Anna Christina Zenkner [2]
Taiany Radde Schmitt [3]

Resumo

O artigo enfrenta a compatibilização entre a arquitetura imutável da tecnologia blockchain e o direito ao apagamento de dados pessoais previsto no art. 18, VI, da Lei Geral de Proteção de Dados. O problema consiste em verificar em que medida a imutabilidade dos registros distribuídos é compatível com o regime de proteção de dados vigente no Brasil e quais arranjos jurídicos e técnicos viabilizam essa compatibilização. Adota-se abordagem qualitativa e método hipotético-dedutivo, com revisão bibliográfica nacional e estrangeira e análise documental dos marcos normativos brasileiro e europeu. Sustentam-se duas teses articuladas: a da equivalência funcional do apagamento, pela qual a inacessibilidade criptográfica robusta deve ser reconhecida como cumprimento do dever de eliminação, e a da complementaridade qualificada entre fé pública estatal e fé pública algorítmica. Conclui-se que a colisão é real, mas não irresolvível, e que sua superação depende de interpretação adaptativa, de governança desde a concepção e da construção de marco regulatório setorial que articule a Autoridade Nacional de Proteção de Dados, o Conselho Nacional de Justiça e as corregedorias estaduais.

Palavras-chave: Blockchain, Proteção de dados pessoais, Direito ao apagamento, Fé pública, Atividade notarial e registral

Abstract/Resumen/Résumé

General Data Protection Law. The problem consists in determining to what extent the immutability of distributed ledgers is compatible with the data protection regime in force in Brazil, and which legal and technical arrangements make such reconciliation feasible. The study adopts a qualitative approach and a hypothetical-deductive method, drawing on national and foreign literature and on documentary analysis of the Brazilian and European normative frameworks. Two articulated theses are advanced: the functional equivalence of erasure, whereby robust cryptographic inaccessibility should be legally recognized as fulfilment of the duty of elimination, and the qualified complementarity between state public faith and algorithmic public faith. It concludes that the collision is real but not unsolvable, and that overcoming it depends on adaptive interpretation, governance by design, and the construction of a sector-specific regulatory framework articulating the National Data Protection Authority, the National Council of Justice, and the state internal-affairs offices.

Keywords/Palabras-claves/Mots-clés: Blockchain, Personal data protection, Right to erasure, Public faith, Notarial and registry activity

1 INTRODUÇÃO

Há, na mitologia grega, duas categorias que organizam a experiência humana com a memória. Cronos, o tempo, é a permanência: tudo o que é registrado escapa ao desaparecimento e se torna eterno. Lethe, o rio do esquecimento que atravessava o Hades, é o seu reverso: a possibilidade de apagar, de recomeçar, de não ser eternamente refém do que se foi. Toda ordem jurídica que disciplina o registro de fatos sobre as pessoas precisa, em alguma medida, mediar essa tensão: assegurar a permanência do que importa lembrar e a possibilidade de esquecimento do que não deve persistir.

A tecnologia *blockchain* radicaliza Cronos. Ao instituir registros distribuídos, imutáveis e mantidos por redes destituídas de autoridade central, ela coloca em xeque pressupostos estruturais dos sistemas jurídicos modernos: a identificação de um responsável pelo tratamento de dados, a possibilidade de correção ou eliminação de informações já registradas e a submissão das atividades de processamento de dados pessoais à jurisdição estatal (Tapscott; Tapscott, 2017; Finck, 2018; De Filippi; Wright, 2018). A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018, doravante LGPD), ao consagrar o direito ao apagamento no art. 18, VI, e o Regulamento Geral de Proteção de Dados europeu (Regulamento UE 2016/679, doravante GDPR), no art. 17, fazem o gesto inverso: convocam Lethe.

Esse conflito atinge intensidade especial quando se examina a colisão entre a característica técnica mais distintiva do *blockchain*, a imutabilidade dos registros, e o direito ao apagamento de dados pessoais. em que medida a arquitetura imutável da tecnologia *blockchain* é compatível com o regime jurídico de proteção de dados pessoais vigente no Brasil, e quais arranjos jurídicos e técnicos são aptos a viabilizar essa compatibilização sem desnaturar nem a tecnologia nem o regime de proteção dos titulares?

A relevância da pesquisa decorre da elevação constitucional da proteção de dados pessoais a direito fundamental pela EC n.º 115/2022, da expansão regulatória das tecnologias de registro distribuído e da ausência de regulamentação específica da ANPD sobre *blockchain* e proteção de dados.

A hipótese de pesquisa sustenta que a colisão entre *blockchain* e direito ao apagamento, embora real, não é absolutamente irresolvível. Defendem-se, neste artigo, duas teses centrais e articuladas. A primeira é a tese da complementaridade qualificada entre fé pública estatal e fé pública algorítmica, pela qual o *blockchain* pode operar como camada técnica de integridade sem suprir a função substantiva de qualificação jurídica do tabelião e do registrador. A segunda é a tese da equivalência funcional do apagamento, segundo a qual a

inacessibilidade criptográfica robusta deve ser juridicamente reconhecida como cumprimento do dever de eliminação imposto pelo art. 18, VI, da LGPD, desde que observados parâmetros técnicos verificáveis pela autoridade reguladora. A segunda tese dialoga com a convergência recente da literatura internacional, examinada na quarta seção, da qual se distingue pelo referencial normativo brasileiro e pela articulação com a função notarial; a primeira não encontra equivalente na produção sobre o tema. Ambas pressupõem soluções de governança que combinem adaptações tecnológicas, como o armazenamento *off-chain* e a destruição de chaves criptográficas, com a construção de um marco regulatório setorial.

A pesquisa adota abordagem qualitativa e método hipotético-dedutivo, com revisão bibliográfica e análise documental dos marcos normativos brasileiros (LGPD, EC n.º 115/2022, Marco Legal dos Ativos Virtuais, Lei n.º 14.382/2022 que instituiu o Sistema Eletrônico dos Registros Públicos, e Provimentos do Conselho Nacional de Justiça relativos à atividade notarial e registral) e europeus (GDPR), bem como a análise jurisprudencial pontual da decisão proferida pelo Supremo Tribunal Federal nas ADIs sobre proteção de dados.

2 A TECNOLOGIA *BLOCKCHAIN*: ARQUITETURA, IMUTABILIDADE E TIPOLOGIAS

A compreensão dos conflitos jurídicos relacionados ao *blockchain* exige, inicialmente, a análise de sua estrutura técnica e das diferentes arquiteturas possíveis. Esta seção examina os fundamentos tecnológicos da cadeia de blocos e suas implicações jurídicas.

2.1 Fundamentos técnicos: registros distribuídos, criptografia e consenso

O *blockchain*, ou cadeia de blocos, consiste em uma estrutura de registro de dados distribuída entre múltiplos participantes de uma rede, sem a necessidade de uma autoridade central de controle. Cada bloco da cadeia contém um conjunto de transações ou informações, um identificador único (*hash*) calculado a partir de seu próprio conteúdo e o *hash* do bloco precedente, formando uma cadeia cronológica e matematicamente verificável de registros (Nakamoto, 2008).

A segurança e a integridade do sistema repousam sobre dois pilares técnicos. O primeiro é a criptografia assimétrica, que permite a cada participante operar com um par de chaves, uma pública e outra privada, para autenticar transações sem revelar sua identidade real. O segundo é o mecanismo de consenso distribuído, pelo qual todos os nós da rede devem validar

cada novo bloco antes de sua inserção na cadeia, tornando praticamente impossível a adulteração retroativa de registros sem o controle da maioria computacional dos nós participantes (Antonopoulos, 2020). A imutabilidade é, portanto, propriedade arquitetural do *blockchain,* e não escolha de design contingente: uma vez inserido um dado na cadeia, sua alteração ou eliminação exigiria o recálculo de todos os *hashes* subsequentes e a aprovação da maioria da rede, o que, em redes públicas com milhares de participantes, é tecnicamente inviável. Essa característica confere ao *blockchain* confiabilidade excepcional para aplicações como registros de propriedade, contratos autoexecutáveis (*smart contracts*), rastreabilidade de cadeias de suprimentos e emissão de ativos digitais (Savelyev, 2017).

2.2 Arquiteturas de *blockchain* e implicações jurídicas das tipologias

A categoria genérica *blockchain* abrange arquiteturas com graus variados de abertura e controle, cuja distinção é juridicamente relevante. Os *blockchains* públicos, dos quais Bitcoin e Ethereum são exemplos paradigmáticos, são acessíveis a qualquer participante sem autorização prévia e operam com protocolos de consenso baseados em prova de trabalho ou prova de participação. Os *blockchains* privados, em sentido estrito, são controlados por uma única entidade que define os participantes autorizados e as regras de funcionamento. Os *blockchains* de consórcio, por sua vez, são governados por um grupo determinado de instituições com interesses convergentes, modelo recorrente em iniciativas setoriais, como as do mercado financeiro e da indústria logística (Mougayar, 2016; Atzori, 2017).

Essa distinção tipológica importa porque as possibilidades de adequação à LGPD diferem significativamente entre as arquiteturas. Em *blockchains* públicos, a inexistência de uma entidade central com poder de gestão sobre a cadeia dificulta sobremaneira a identificação do controlador e do operador nos termos do art. 5.º, incisos VI e VII, da LGPD, bem como a implementação de mecanismos efetivos de exercício dos direitos do titular. Em *blockchains* de consórcio e privados, ao contrário, há atores identificáveis com competência decisória sobre os parâmetros de funcionamento da rede, o que permite a atribuição clara de responsabilidades e a adoção de protocolos de governança adequados às exigências regulatórias.

A regulação precisa diferenciar arquiteturas, conforme o grau de controle e a presença de agentes identificáveis, sob pena de aplicar indistintamente a redes que apresentam estruturas funcionalmente diversas exigências formuladas para o paradigma centralizado de tratamento de dados.

3 A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: LGPD, GDPR E O CONTEXTO CONSTITUCIONAL BRASILEIRO

A análise da compatibilidade entre *blockchain* e proteção de dados pressupõe a compreensão da evolução normativa da tutela dos dados pessoais no Brasil e na União Europeia. Esta seção examina os fundamentos da LGPD e do GDPR.

3.1 Dos antecedentes ao direito fundamental à proteção de dados

A proteção de dados pessoais, no Brasil, transitou de uma fase de tutela fragmentária e setorial para a consolidação como direito fundamental autônomo, em processo cuja sistematização se deve, em grande medida, à doutrina especializada. Doneda (2019) demonstra que a passagem da privacidade clássica, vinculada à esfera do isolamento individual, para a proteção de dados pessoais responde à transformação tecnológica que tornou os dados ativos econômicos e instrumentos de poder, leitura que dialoga com a de Rodotà (2008), para quem a proteção de dados é o eixo da autodeterminação informativa na sociedade da vigilância. A esse fundamento Mendes (2014) acrescenta um passo decisivo, ao sustentar que a proteção de dados constitui direito fundamental dotado de conteúdo próprio, distinto da privacidade em sentido estrito; Bioni (2021), por sua vez, problematiza os limites do consentimento como base legal de tratamento em ambientes de assimetria informacional, enquanto Sarlet (2018) oferece os fundamentos dogmáticos da eficácia dos direitos fundamentais que respaldam a aplicação direta das garantias constitucionais ao tratamento privado de dados.

A consolidação dogmática traduziu-se em transformação normativa expressiva. No julgamento das medidas cautelares nas Ações Diretas de Inconstitucionalidade 6.387, 6.388, 6.389, 6.390 e 6.393, ajuizadas contra a Medida Provisória n.º 954/2020, o Supremo Tribunal Federal reconheceu, sob relatoria da Ministra Rosa Weber, que a proteção de dados pessoais constitui direito fundamental autônomo, dotado de proteção constitucional anterior mesmo à sua positivação expressa no texto constitucional (Brasil, 2020). A Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, formalizou esse entendimento ao incluir o inciso LXXIX no art. 5.º da Constituição da República, que assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

O quadro constitucional, portanto, situa o direito ao apagamento de dados pessoais não como mera prerrogativa infralegal, mas como manifestação concreta de um direito fundamental que exige proteção efetiva e mecanismos de garantia adequados às transformações

tecnológicas. A interpretação dos dispositivos da LGPD deve, em consequência, observar o princípio da máxima efetividade dos direitos fundamentais, orientação metodológica consolidada no constitucionalismo brasileiro contemporâneo (Sarlet, 2018).

3.2 Princípios e estruturas da LGPD: titulares, controladores e operadores

A LGPD estrutura-se em torno de princípios fundamentais elencados no art. 6.º, dentre os quais se destacam, para os fins desta investigação, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Esses princípios funcionam como vetores interpretativos e como balizas para o exercício das atividades de tratamento de dados pessoais por agentes públicos e privados.

A arquitetura subjetiva da lei distribui responsabilidades entre três figuras centrais: o titular dos dados, definido como a pessoa natural a quem se referem os dados pessoais (art. 5.º, V); o controlador, a quem competem as decisões sobre o tratamento (art. 5.º, VI); e o operador, que realiza o tratamento em nome do controlador (art. 5.º, VII). A clara identificação desses agentes é pressuposto para a operacionalização do regime, especialmente para o exercício dos direitos do titular e para a apuração de eventuais infrações pela ANPD.

É precisamente nessa estrutura subjetiva que o *blockchain* público apresenta sua primeira fricção com o regime da LGPD. Como observa Finck (2018), em redes públicas sem controle central, a atribuição de responsabilidades de controlador é tarefa juridicamente complexa, pois inexiste, em sentido estrito, agente único com poder decisório sobre as finalidades e os meios de tratamento. A solução proposta na doutrina e nas primeiras orientações regulatórias europeias oscila entre considerar todos os mineradores e validadores como controladores conjuntos, atribuir essa qualidade aos desenvolvedores do protocolo, ou reconhecer um regime de responsabilidade distribuída orientado pelo princípio da prestação de contas, a accountability (Finck, 2018; CNIL, 2018). As Diretrizes 02/2025 do Comitê Europeu de Proteção de Dados, adotadas em abril de 2025 e sucessoras institucionais da análise inaugural da autoridade francesa, recomendam expressamente que, em *blockchains* públicas sem permissão, os nós constituam um consórcio ou outra entidade jurídica que assuma a posição de controlador, justamente para superar a indeterminação subjetiva apontada pela doutrina (EDPB, 2025). A solução regulatória europeia converge, portanto, para o reconhecimento de que a viabilidade do regime de proteção de dados em *blockchain* depende menos da aplicação

literal das categorias existentes do que da escolha arquitetural da rede, conclusão que orienta a análise desenvolvida nas seções seguintes.

3.3 O direito ao apagamento e a anonimização nos arts. 18 e 12 da LGPD

O art. 18 da LGPD assegura ao titular o exercício de direitos qualificados como direitos da personalidade no contexto digital. Entre eles destaca-se, no inciso VI, a eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas as hipóteses do art. 16, que admite a conservação para o cumprimento de obrigação legal ou regulatória, estudo por órgão de pesquisa, transferência a terceiro com observância dos requisitos legais e uso exclusivo do controlador, vedado o acesso por terceiro, com anonimização quando possível.

Impõe-se, neste ponto, distinção conceitual indispensável ao rigor da análise. O direito ao apagamento previsto no art. 18, VI, da LGPD não se confunde com o chamado direito ao esquecimento. Aquele consiste em prerrogativa de eliminação de dados pessoais submetidos a tratamento, dirigida ao controlador e ancorada no regime de proteção de dados; este, ao contrário, traduz a pretensão de obstar, em razão da passagem do tempo, a divulgação de fatos verídicos e licitamente obtidos, e foi declarado incompatível com a Constituição pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário n.º 1.010.606, Tema 786 da repercussão geral, sob relatoria do Ministro Dias Toffoli (Brasil, 2021). A invocação da imagem mitológica de Lethe, neste artigo, refere-se exclusivamente ao primeiro instituto, o apagamento de dados como técnica jurídica de tutela do titular, e não ao direito ao esquecimento rejeitado pela Corte.

O cumprimento desse direito pressupõe, tecnicamente, que o controlador detenha capacidade efetiva de identificar, localizar e eliminar os dados do titular nos sistemas em que são tratados. Essa premissa, trivial em bancos de dados convencionais, torna-se problemática ou mesmo impossível quando os dados são armazenados em uma cadeia de blocos imutável, especialmente em arquiteturas públicas descentralizadas (Politou; Alepis; Patsakis, 2018).

Dois dispositivos da LGPD oferecem caminhos interpretativos para a tutela desse direito em ambientes *blockchain*. O art. 5.º, III, define dado anonimizado como aquele relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O art. 12 estabelece que os dados anonimizados não serão considerados dados pessoais para os fins desta lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. O art. 13, § 4.º, por sua vez,

define a pseudonimização como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

A distinção entre anonimização e pseudonimização é crucial. Dados pseudonimizados continuam sujeitos à LGPD, ainda que com alguma flexibilidade no regime de tratamento. Dados verdadeiramente anonimizados escapam, como regra, ao âmbito de aplicação da lei. A pertinência dessa distinção para o contexto *blockchain* reside em que muitas das soluções técnicas propostas para conciliar imutabilidade e direito ao apagamento configuram, na realidade, formas de pseudonimização robusta, e não de anonimização irreversível, o que tem implicações regulatórias significativas (Bioni, 2021).

4 A COLISÃO TÉCNICA E JURÍDICA: IMUTABILIDADE X DIREITO AO APAGAMENTO

A partir dos fundamentos técnicos do *blockchain* e da estrutura normativa da proteção de dados, torna-se possível examinar a tensão entre a imutabilidade dos registros distribuídos e o direito ao apagamento.

4.1 A impossibilidade técnica e o problema da identificação do controlador

É nesta seção que a tensão inicialmente descrita se manifesta em sua forma mais aguda: a permanência arquitetural do registro confronta o dever jurídico de eliminação. O problema central reside em que o *blockchain* foi projetado precisamente para ser imutável. Qualquer dado inserido em uma cadeia pública, seja diretamente, seja como *hash* de um documento externo, torna-se parte permanente do registro histórico da rede. Isso inclui, em tese, dados pessoais que venham a ser inseridos em transações, como endereços de carteiras associados a identidades reais, informações de saúde em registros médicos baseados em *blockchain* ou dados contratuais com identificação das partes.

Do ponto de vista jurídico, essa imutabilidade gera cenário de impossibilidade objetiva de cumprimento do direito ao apagamento. O agente identificado como controlador, ou quem quer que assuma esse papel em uma rede *blockchain,* não dispõe, em regra, de poder técnico unilateral para eliminar dados da cadeia. Surge, portanto, conflito entre a norma jurídica, que impõe a eliminação, e a realidade técnica, que a torna impraticável (Finck, 2018; De Filippi; Wright, 2018).

A esse problema soma-se outro, de igual gravidade: a dificuldade de identificação do controlador em redes *blockchain* públicas. Em arquiteturas descentralizadas, sem entidade administradora única, a aplicação literal do conceito de controlador da LGPD conduz a alternativas todas insatisfatórias. Atribuir essa qualidade aos mineradores ou validadores produz responsabilidade solidária de milhares ou milhões de participantes anônimos espalhados por jurisdições diversas, com impossibilidade prática de fiscalização. Atribuí-la aos desenvolvedores do protocolo desconsidera que, uma vez lançada a rede, eles não detêm poder decisório sobre transações específicas. Atribuí-la a cada usuário que insere dados pessoais reduz a tutela do titular ao titular, esvaziando-a.

De Filippi e Wright (2018), em obra de referência sobre a regulação do blockchain, sustentam que a regulação de redes descentralizadas exige superação do paradigma jurídico fundado na identificação de um agente central de imputação, em direção a regimes de governança orientados pela accountability distribuída e pela responsabilidade do agente que efetivamente determina a inserção dos dados na cadeia. Essa proposição dialoga com a interpretação teleológica do art. 5.º, VI, da LGPD, que enfatiza o poder decisório sobre o tratamento, e não a execução técnica em si (Politou; Alepis; Patsakis, 2018).

4.2 Soluções técnicas: armazenamento *off-chain*, destruição de chaves e *blockchains* de consórcio

A solução mais promissora para o conflito entre imutabilidade e direito ao apagamento é a arquitetura *off-chain*. Consiste ela em armazenar os dados pessoais sensíveis fora da cadeia de blocos, registrando na *blockchain* apenas o *hash* criptográfico que confirma a integridade do documento externo. Os dados pessoais permanecem em sistemas convencionais, sujeitos integralmente às obrigações da LGPD, incluindo o direito ao apagamento, enquanto a imutabilidade do *blockchain* assegura a integridade do registro de referência sem expor as informações pessoais à cadeia (Politou; Alepis; Patsakis, 2018; Truong et al., 2019). Essa orientação encontra respaldo regulatório expresso: o Comitê Europeu de Proteção de Dados, em suas Diretrizes 02/2025, estabelece como regra geral que o armazenamento de dados pessoais diretamente na cadeia deve ser evitado sempre que conflitar com os princípios de proteção de dados, recomendando, quando o tratamento for necessário, a adoção da arquitetura *off-chain* (EDPB, 2025).

A destruição de chaves criptográficas configura abordagem complementar. Em sistemas nos quais os dados pessoais são armazenados em forma criptografada na *blockchain,*

a destruição da chave privada que permite a decriptação torna o dado praticamente inacessível, ainda que ele permaneça formalmente na cadeia. Truong *et al.* (2019) sustentam que esse mecanismo configura forma funcional de apagamento, pois o dado se torna ilegível e inservível para qualquer finalidade. A questão, contudo, não está pacificada na doutrina nem nas orientações das autoridades de proteção de dados, e exige análise técnica caso a caso quanto à robustez do esquema criptográfico empregado e à efetiva inviabilização do acesso (Politou; Alepis; Patsakis, 2018; Truong *et al.,* 2019).

Os *blockchains* de consórcio e privados oferecem flexibilidade adicional para implementação de mecanismos de conformidade. Por serem controlados por um conjunto determinado de participantes com identidades conhecidas, permitem a atribuição clara das responsabilidades de controlador e operador nos termos da LGPD, a implementação de protocolos de governança para o tratamento de solicitações de apagamento e a eventual adoção de mecanismos de criptografia reversível que possibilitem a inacessibilização controlada de dados específicos (Atzori, 2017).

4.3 Pseudonimização, anonimização e a tese da equivalência funcional do apagamento

A literatura recente deslocou o debate da incompatibilidade entre *blockchain* e apagamento para a construção de soluções técnicas e regulatórias. Zafar (2025) defende abordagem regulatória equilibrada, que concilie a inovação tecnológica com a integridade do regime de proteção de dados, e Esu (2025) propõe, a partir do direito europeu e britânico e do princípio da limitação de armazenamento, um paradigma do apagamento funcional, ancorado na definição ampla de eliminação que abrange a tornada inacessível dos dados quando a eliminação física for tecnicamente inviável. Há, portanto, convergência internacional incipiente em torno da ideia de que o apagamento pode ser cumprido por equivalência funcional.

É nesse ponto que se demarca a contribuição deste artigo. A tese da equivalência funcional do apagamento aqui sustentada parte da mesma intuição que anima a literatura internacional recente, mas dela se distingue em dois aspectos. O primeiro é o referencial normativo: enquanto Esu (2025) trabalha o princípio da limitação de armazenamento à luz do regime europeu e britânico, a formulação aqui proposta ancora-se especificamente no art. 18, VI, da LGPD, no conceito de dado anonimizado do art. 5.º, III, e na moldura constitucional brasileira da proteção de dados como direito fundamental autônomo, o que impõe parâmetros interpretativos próprios. O segundo é a articulação com a função notarial e registral, examinada na seção seguinte, dimensão ausente da literatura internacional e que confere à tese alcance que

extrapola a dogmática da proteção de dados. Sustenta-se, assim, que a inacessibilização técnica robusta de dados pessoais registrados em *blockchain,* mediante destruição irreversível das chaves criptográficas ou mecanismos equivalentes, deve ser juridicamente reconhecida como cumprimento do dever de eliminação imposto pelo art. 18, VI, da LGPD, desde que observados parâmetros técnicos verificáveis pela autoridade reguladora.

A evolução das orientações regulatórias europeias reforça a plausibilidade da tese. A Comissão Nacional de Informática e Liberdades francesa foi a primeira autoridade de proteção de dados a publicar orientação específica sobre o tema, reconhecendo que as soluções técnicas de pseudonimização e de criptografia robusta podem operar como medidas de conformidade no tratamento de dados pessoais em *blockchain,* sem que isso implique dispensa das obrigações de proteção de dados (CNIL, 2018). As Diretrizes 02/2025 do Comitê Europeu de Proteção de Dados aprofundaram essa análise, ao detalhar técnicas de limitação da identificabilidade dos dados, como o uso de funções de resumo criptográfico e de compromissos criptográficos que tornam a informação obscura quando os dados de origem são eliminados (EDPB, 2025). No contexto brasileiro, esse caminho interpretativo encontra apoio na Resolução CD/ANPD n.º 4, de 24 de fevereiro de 2023, que dispõe sobre o Regulamento de Dosimetria e Aplicação de Sanções Administrativas e estabelece como circunstância atenuante a adoção de medidas técnicas e organizacionais comprovadamente eficazes na mitigação de danos.

A consolidação da tese da equivalência funcional, contudo, depende de manifestação expressa da ANPD, seja por norma regulatória, seja por enunciado interpretativo. Sua ausência produz, atualmente, situação de insegurança jurídica que afeta tanto a proteção dos titulares quanto a viabilidade de iniciativas de inovação tecnológica fundadas em *blockchain.*

5 *BLOCKCHAIN,* FÉ PÚBLICA E REGISTROS PÚBLICOS: A INTERFACE COM A ATIVIDADE NOTARIAL E REGISTRAL

Esta seção examina a interface entre a atividade notarial e registral e a tecnologia *blockchain.* De um lado, a tradição secular do tabelião, fundada na qualificação humana e na imputação institucional de credibilidade pelo Estado; de outro, o desafio recente do token, fundado no consenso distribuído e na verificação matemática. Ambos disputam, ao menos aparentemente, o lugar da credibilidade jurídica na era digital. A análise que se segue sustenta que essa disputa, mais aparente que real, resolve-se em chave de complementaridade qualificada, primeira das duas teses originais sustentadas neste artigo.

5.1 Fé pública estatal e fé pública algorítmica: substituição ou complementaridade?

A função histórica da atividade notarial e registral é precisamente conferir autenticidade, segurança e eficácia aos atos jurídicos, atributos que o *blockchain* promete entregar de modo descentralizado e algorítmico. A coincidência funcional aparente entre as duas instituições, uma estatal e secular, outra tecnológica e recente, suscita o questionamento teórico sobre a relação entre elas, em chave de substituição ou de complementaridade.

No regime constitucional brasileiro, a atividade notarial e registral é exercida em caráter privado, por delegação do Poder Público, nos termos do art. 236 da Constituição da República, e regulamentada pela Lei n.º 8.935, de 18 de novembro de 1994. A fé pública atribuída aos atos notariais e registrais não decorre, como observa Brandelli (2011), da mera redução técnica de transações a forma documental, mas da imputação institucional de credibilidade pelo Estado, fundada em qualificação profissional, responsabilidade civil e disciplinar, controle pela Corregedoria de Justiça e adstrição a princípios deontológicos. A fé pública é, nesse sentido, instituição jurídica, e não apenas instrumento técnico de autenticação.

O *blockchain,* ao operar mediante consenso distribuído e criptografia, oferece o que parte da literatura denomina fé pública algorítmica ou trustless trust, na expressão consagrada por Werbach (2018), isto é, confiança construída por meio da arquitetura técnica do sistema, sem necessidade de intermediação institucional. A propriedade que confere essa segurança é a já mencionada imutabilidade, somada à transparência das operações registradas em redes públicas (Tapscott; Tapscott, 2017). o que o software permite, ele autoriza; o que ele impede, ele proíbe, não por força normativa, mas por inviabilidade técnica. A fé pública algorítmica é, nesse sentido, manifestação tecnológica do fenômeno mais amplo do code is law.

Sustenta-se, neste estudo, que a relação entre as duas formas de garantia não é de substituição, mas de complementaridade qualificada. A fé pública estatal cumpre funções que a tecnologia, isoladamente, não está apta a realizar, especialmente a qualificação jurídica do ato, a aferição da capacidade e do consentimento das partes, a interpretação da vontade declarada, a ponderação de interesses contrapostos e a função preventiva de litígios. O *blockchain*, por sua vez, pode operar como camada técnica de integridade do suporte informacional dos atos, garantindo que o conteúdo registrado não seja alterado, mas sem suprir a função substantiva de qualificação que pertence ao notário e ao registrador. Essa leitura é coerente com o diagnóstico de Cassettari (2020) sobre a evolução tecnológica da atividade notarial, em que a digitalização e a desmaterialização dos atos não dispensam, antes pressupõem, o exercício da função qualificadora.

5.2 O e-Notariado e os Provimentos do CNJ: *blockchain* como camada de integridade

O Conselho Nacional de Justiça tem promovido, na última década, transformação substancial da atividade notarial e registral por meio de atos normativos que estruturaram a prática eletrônica de atos extrajudiciais. O Provimento n.º 100, de 26 de maio de 2020, instituiu a prática de atos notariais eletrônicos por meio do sistema e-Notariado, regulamentando a videoconferência, a assinatura eletrônica notarizada e a Matrícula Notarial Eletrônica. O Provimento n.º 88, de 1.º de outubro de 2019, estabeleceu deveres de prevenção à lavagem de dinheiro e ao financiamento do terrorismo a serem observados pelos notários e registradores, com expressa atribuição de tratamento de dados pessoais dos clientes para fins de cumprimento da legislação de combate aos crimes financeiros. O Provimento n.º 149, de 30 de agosto de 2023, consolidou a normativa extrajudicial em Código Nacional de Normas, atualizando e sistematizando os atos anteriores.

Esse arcabouço normativo evidencia a opção institucional pela integração da tecnologia à atividade notarial e registral, sem prejuízo da preservação da fé pública estatal. A Central Notarial de Serviços Eletrônicos Compartilhados (CENSEC) e o e-Notariado constituem infraestruturas digitais nacionais que, em sua arquitetura, recorrem a mecanismos criptográficos de integridade comparáveis, ainda que não idênticos, aos empregados em redes *blockchain.* A lógica de carimbo do tempo e de cadeia de *hashes* vinculados a documentos eletrônicos é tecnologicamente análoga à do *blockchain,* ainda que centralizada em servidores das corregedorias e do Colégio Notarial.

5.3 A aplicação da LGPD às serventias extrajudiciais

As serventias extrajudiciais sujeitam-se integralmente à LGPD. O art. 4.º da lei excepciona expressamente apenas o tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, para fins jornalísticos, artísticos ou acadêmicos, e para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Cartórios não se enquadram em nenhuma dessas hipóteses. Tratam, ao contrário, de dados pessoais em larga escala, frequentemente sensíveis, no exercício de função delegada do Poder Público, o que reforça, e não atenua, a incidência do regime de proteção de dados.

Tensão particularmente delicada surge entre o dever de publicidade dos atos registrais, princípio estruturante da segurança jurídica imobiliária e empresarial, e o regime de proteção

de dados pessoais. A publicidade registral, prevista no art. 1.º da Lei n.º 6.015/1973 e em outros diplomas registrais, encontra fundamento na necessidade de oponibilidade dos atos a terceiros e na proteção da confiança jurídica, mas não é absoluta. Como observa Loureiro (2020), a publicidade registral comporta modulação conforme a finalidade do acesso, especialmente quando envolve dados pessoais sensíveis ou informações cuja divulgação ampla possa expor o titular a riscos desproporcionais.

A LGPD oferece bases legais específicas para esse tratamento, notadamente as do art. 7.º, II (cumprimento de obrigação legal ou regulatória pelo controlador) e III (execução de políticas públicas previstas em leis e regulamentos). A compatibilização entre publicidade registral e proteção de dados depende, portanto, de modulação interpretativa que distinga o acesso para finalidades juridicamente legítimas, como a verificação de propriedade ou de impedimentos matrimoniais, do acesso indistinto para finalidades comerciais ou de monetização. A introdução de *blockchain* como camada técnica de registros públicos exige que essa modulação seja considerada já na fase de concepção arquitetural dos sistemas, sob pena de criar exposições permanentes incompatíveis com o regime de proteção de dados.

5.4 Registro de imóveis, SERP e os limites do uso de *blockchain* em registros públicos

A Lei n.º 14.382, de 27 de junho de 2022, instituiu o Sistema Eletrônico dos Registros Públicos (SERP), criando infraestrutura nacional para a integração e o acesso unificado aos atos registrais. O SERP representa avanço expressivo na modernização dos registros públicos no Brasil, sem, contudo, adotar arquitetura *blockchain* em seu desenho original. A discussão sobre a viabilidade de incorporação dessa tecnologia a registros públicos, especialmente ao registro imobiliário, deve, portanto, ser conduzida com atenção tanto às possibilidades técnicas quanto aos limites jurídicos e institucionais aplicáveis.

Como observa Dip (2017), o registro de imóveis no Brasil articula princípios estruturantes, entre os quais a legalidade, a presunção de fé pública, a tipicidade, a especialidade objetiva e subjetiva, a instância e a prioridade, que não se reduzem à integridade do suporte informacional do registro, mas dependem do exame jurídico qualificado pelo registrador, agente delegado do Poder Público. A simples permanência de um dado em uma cadeia de blocos não realiza, por si, nenhum desses princípios. O que o *blockchain* pode oferecer, no contexto do registro imobiliário, é camada adicional de integridade do suporte informacional, complementar, e não substitutiva, da função qualificadora.

A análise jurídica permite extrair três limites para o uso de *blockchain* em registros públicos no Brasil. Primeiro, o *blockchain* deve operar como camada técnica complementar, e não como substituto da qualificação registral, função que permanece atribuída ao registrador como agente delegado do Poder Público. Segundo, a arquitetura adotada deve ser de consórcio ou permissionada, sob governança das corregedorias e dos colégios registrais, sob pena de submeter atos públicos a redes públicas globais sem controle jurisdicional adequado. Terceiro, os dados pessoais inseridos em transações registrais devem observar a lógica *off-chain*, com armazenamento dos dados sensíveis em sistemas convencionais sujeitos à LGPD e registro na cadeia apenas dos *hashes* de integridade, em arquitetura que assegure tanto a inviolabilidade do registro quanto a possibilidade de cumprimento dos direitos do titular.

6 RISCOS E IMPACTOS SOCIAIS: CAPITALISMO DE VIGILÂNCIA, DEEPFAKES E COMPLIANCE TECNOLÓGICO

A intersecção entre *blockchain* e dados pessoais apresenta riscos sociais que extrapolam a questão estritamente jurídica do direito ao apagamento. Em sua análise sobre o capitalismo de vigilância, Zuboff (2020) demonstra que a economia digital contemporânea opera mediante a extração massiva de dados comportamentais, transformados em ativos econômicos sem o consentimento substantivo dos titulares; a imutabilidade do *blockchain* agrava esse cenário, ao criar histórico permanente de comportamentos e relações pessoais passível de exploração por agentes comerciais ou estatais, ao que se soma o fenômeno dos *deepfakes,* cuja periculosidade se amplia quando documentos e vídeos sintéticos, uma vez inscritos em cadeias de blocos, geram evidências resistentes à remoção (Chesney; Citron, 2019). A resposta jurídica a esses riscos não pode operar exclusivamente no plano da tutela reparatória. O art. 46 da LGPD e o art. 25 do GDPR consagram o princípio da proteção de dados desde a concepção e por padrão (*privacy by design*), que impõe a implementação das medidas técnicas e organizacionais de proteção já na fase de desenvolvimento dos sistemas (Cavoukian, 2012); para o *blockchain*, isso significa arquitetar as soluções *off-chain*, a pseudonimização robusta e a governança descentralizada de dados antes da implantação da rede. O custo de conformidade, contudo, representa desafio adicional, pois a exigência de adequação simultânea às normas de proteção de dados, às regulações setoriais específicas e aos padrões técnicos de segurança pode criar barreiras à entrada que concentram o desenvolvimento de soluções *blockchain* em grandes corporações, o que reforça a necessidade de orientação regulatória clara e estável.

7 CONSIDERAÇÕES FINAIS

A pesquisa enfrentou o problema da compatibilização entre a arquitetura imutável da tecnologia *blockchain* e o regime jurídico de proteção de dados pessoais vigente no Brasil, com foco no direito ao apagamento previsto no art. 18, VI, da LGPD. As análises desenvolvidas confirmam a hipótese inicial, com dois ajustes relevantes. O primeiro é que a resolubilidade da colisão não é uniforme: depende da tipologia da rede, sendo significativamente mais viável em *blockchains* de consórcio e privados do que em arquiteturas públicas abertas. O segundo é que a superação do conflito não decorre apenas de interpretação jurídica, mas pressupõe atuação regulatória que ainda não se concretizou. Confirmada nesses termos, a colisão entre *blockchain* e direito ao apagamento revela-se conflito normativo real, mas não absolutamente irresolvível, cuja superação demanda articulação entre adaptações tecnológicas, interpretação adaptativa do regime de proteção de dados e construção de marco regulatório setorial.

Sustentaram-se, ao longo do artigo, duas teses articuladas. A tese da equivalência funcional do apagamento defende que a inacessibilidade criptográfica robusta, quando submetida a parâmetros técnicos verificáveis e à supervisão da autoridade reguladora, deve ser juridicamente reconhecida como cumprimento do dever de eliminação imposto pelo art. 18, VI, da LGPD. Ela acompanha a convergência da literatura internacional mais recente, de que são exemplos Zafar (2025) e Esu (2025), mas dela se demarca por ancorar-se no referencial normativo brasileiro e por articular-se à função notarial e registral. A tese da complementaridade qualificada entre fé pública estatal e fé pública algorítmica, por sua vez, não encontra equivalente na produção sobre o tema e constitui a contribuição mais própria desta pesquisa: defende que ambas as formas de garantia não se substituem nem se opõem, pois a primeira cumpre função substantiva de qualificação jurídica que a segunda não realiza, ao passo que a segunda oferece à primeira camada técnica de integridade que a fortalece sem desnaturá-la.

As propostas centrais da pesquisa concentram-se em três eixos: interpretação adaptativa das normas de proteção de dados, adoção de arquiteturas *blockchain* compatíveis com a LGPD e construção de regulação setorial específica para aplicações sensíveis.

O segundo eixo é o da governança *by design*. Defende-se que as organizações que desenvolvem e implantam soluções *blockchain* adotem, desde a concepção, arquiteturas *off-chain* e mecanismos de controle de acesso que permitam a conformidade com a LGPD sem comprometer a integridade da cadeia. A escolha entre arquiteturas públicas, privadas e de

consórcio deve ser orientada pela natureza dos dados tratados e pelas exigências regulatórias aplicáveis, com preferência, em contextos de tratamento de dados pessoais sensíveis ou em larga escala, pelas arquiteturas de consórcio com governança institucionalizada.

Defende-se, ainda, a construção de regulação específica para aplicações sensíveis de *blockchain*, com definição de responsabilidades, parâmetros técnicos mínimos e mecanismos de supervisão compatíveis com a LGPD.

Reconhece-se como limitação da pesquisa a ausência de verificação empírica da robustez técnica das soluções criptográficas examinadas. Tampouco se examinaram, em profundidade, as experiências regulatórias estrangeiras, que permaneceram como referência ilustrativa. Abrem-se, assim, agendas de pesquisa promissoras: a investigação empírica dos parâmetros técnicos de verificação da inacessibilidade criptográfica; o estudo comparado das primeiras manifestações regulatórias sobre *blockchain* e proteção de dados; e o aprofundamento da interface entre tecnologias de registro distribuído e a função qualificadora notarial e registral, eixo que esta pesquisa apenas inaugura e que reclama desenvolvimento autônomo.

O desafio jurídico contemporâneo não é escolher entre a permanência absoluta do registro e a eliminação absoluta do dado, mas construir modelos regulatórios capazes de compatibilizar inovação tecnológica e proteção dos direitos fundamentais.

REFERÊNCIAS

ANTONOPOULOS, Andreas M. **Mastering Bitcoin**: programming the open blockchain. 3. ed. Sebastopol: O'Reilly Media, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRANDELLI, Leonardo. **Teoria geral do direito notarial**. 4. ed. São Paulo: Saraiva, 2011.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 maio 2026.

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**: seção 1, Brasília, DF, 11 fev. 2022.

BRASIL. Lei n.º 8.935, de 18 de novembro de 1994. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. **Diário Oficial da União**: seção 1, Brasília, DF, 21 nov. 1994.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Lei n.º 14.382, de 27 de junho de 2022. Dispõe sobre o Sistema Eletrônico dos Registros Públicos (SERP). **Diário Oficial da União**: seção 1, Brasília, DF, 28 jun. 2022.

BRASIL. Lei n.º 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais. **Diário Oficial da União**: seção 1, Brasília, DF, 22 dez. 2022.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 88, de 1.º de outubro de 2019**. Dispõe sobre a política, os procedimentos e os controles a serem adotados pelos notários e registradores visando à prevenção dos crimes de lavagem ou ocultação de bens, direitos e valores e ao combate ao financiamento do terrorismo. Brasília, DF: CNJ, 2019.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 100, de 26 de maio de 2020**. Dispõe sobre a prática de atos notariais eletrônicos por meio do Sistema e-Notariado. Brasília, DF: CNJ, 2020.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 134, de 24 de agosto de 2022**. Estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais. Brasília, DF: CNJ, 2022.

BRASIL. Conselho Nacional de Justiça. **Provimento n.º 149, de 30 de agosto de 2023**. Código Nacional de Normas da Corregedoria Nacional de Justiça. Brasília, DF: CNJ, 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD n.º 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023.

BRASIL. Supremo Tribunal Federal. **Medida cautelar nas Ações Diretas de Inconstitucionalidade n.º 6.387, 6.388, 6.389, 6.390 e 6.393**. Relatora: Ministra Rosa Weber. Brasília, DF: STF, julgamento conjunto em 7 de maio de 2020.

BRASIL. Supremo Tribunal Federal. **RE n.º 1.010.606/RJ.** Tema 786 da repercussão geral. Rel. Min. Dias Toffoli. STF, 2021.

CASSETTARI, Christiano. **Tabelionato de notas**. 4. ed. São Paulo: Atlas, 2020.

CHESNEY, Robert; CITRON, Danielle Keats. Deep fakes: a looming challenge for privacy, democracy, and national security. **California Law Review**, v. 107, n. 6, p. 1753-1820, 2019.

CNIL. **Blockchain**: premiers éléments d'analyse de la CNIL. Paris: Commission Nationale de l'Informatique et des Libertés, 2018. Disponível em: https://www.cnil.fr. Acesso em: 10 maio 2026.

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

DIP, Ricardo. **Registro de imóveis**: princípios. São Paulo: Quinta Editorial, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ESU, Raphael. Blockchain and data protection: developing a functional erasure framework for storage limitation. **Information & Communications Technology Law**, 2025. DOI: 10.1080/13600834.2025.2600197.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 02/2025 on processing of personal data through blockchain technologies**. Bruxelas: EDPB, 2025. Versão adotada em 14 de abril de 2025, submetida a consulta pública. Disponível em: https://www.edpb.europa.eu. Acesso em: 12 maio 2026.

FINCK, Michèle. **Blockchain regulation and governance in Europe**. Cambridge: Cambridge University Press, 2018.

LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

LOUREIRO, Luiz Guilherme. **Registros públicos**: teoria e prática. 11. ed. Salvador: JusPodivm, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. [*S. l.: s. n.*], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 5 abr. 2026.

POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. **Journal of Cybersecurity**, v. 4, n. 1, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

TRUONG, Nguyen B. *et al.* GDPR-compliant personal data management: a blockchain-based solution. **IEEE Transactions on Information Forensics and Security**, v. 14, n. 12, p. 3150-3165, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016** (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4 maio 2016.

WERBACH, Kevin. **The blockchain and the new architecture of trust**. Cambridge: MIT Press, 2018.

ZAFAR, Ammar. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. **Journal of Cybersecurity**, v. 11, n. 1, 2025. DOI: 10.1093/cybsec/tyaf002.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.