INFRAESTRUTURAS REGULATÓRIAS COMPUTACIONAIS PARA DADOS DE SAÚDE[1]

COMPUTATIONAL REGULATORY INFRASTRUCTURES FOR HEALTH DATA

Wilson Engelmann[2]

[1] Este artigo é resultado parcial de pesquisa conduzida pelo autor no âmbito do seguinte projeto de pesquisa: Projeto de Pesquisa Principal: Combinação de processos on-chain e off-chain em tecnologia blockchain, bem como padrões GS1 EPCIS e HL7 FHIR aprimorados, para ampliar a rastreabilidade de dados e produtos de saúde. Projeto de Pesquisa de Pós-Doutorado (em desenvolvimento pelo autor): A interoperabilidade de códigos padrão em tecnologia blockchain: tornando a área da saúde compatível com a transferência internacional de dados pessoais sensíveis de saúde e rastreabilidade. Instituição Anfitriã: Korea Advanced Institute of Science & Technology - KAIST - Coreia do Sul; Supervisor: Prof. Dr. Daeyoung Kim; CNPq/MCTI (Conselho Nacional de Desenvolvimento Científico e Tecnológico/Ministério da Ciência, Tecnologia e Inovação, Brasil) nº 16/2024: "Apoio a Projetos Internacionais de Pesquisa Científica, Tecnológica e de Inovação"; Universidade do Vale do Rio dos Sinos - Unisinos (Brasil) e Auto-ID Labs no KAIST & AI[2] Laboratory (Coreia do Sul). Além desse projeto, o artigo se vincula aos seguintes projetos de pesquisa desenvolvidos pelo autor: a) Chamada CNPq n. 09/2023 - Bolsas de Produtividade em Pesquisa - PQ, projeto intitulado: "Experimentos no Direito: desafios e possibilidades para a regulação baseada em princípios da inteligência artificial e sua testagem em *Living Lab* Regulatório"; b) Chamada CNPq Universal 2023, projeto intitulado: "Direitos Humanos e Inteligência Artificial: da violação dos direitos da personalidade à necessidade de regulação das novas tecnologias".

[2] Doutor e Mestre em Direito Público, Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos - UNISINOS, Brasil; Estágio Pós-Doutoral em Direito Público - Direitos Humanos (Centro de Estudos de Segurança - CESEG) da

RESUMO

As arquiteturas distribuídas de inteligência artificial (IA) vêm provocando uma inflexão estrutural na governança global de dados em saúde. Em vez de modelos centrados na transferência massiva e na concentração de bases de informação, emergem as bases para um futuro paradigma de coordenação computacional distribuída, interoperabilidade regulatória e de Federated Learning (FL). Este artigo investiga como arquiteturas compostas por FL, blockchain permissionada e padrões globais de interoperabilidade - especialmente os padrões GS1 - podem constituir infraestruturas regulatórias computacionais aptas a operacionalizar a governança de dados em saúde, a soberania digital e a compliance by architecture em ecossistemas globais de saúde e de supply chain. A pesquisa adota uma metodologia jurídico-teórica, interdisciplinar e comparativa, articulando Direito Digital, teoria institucional, governança algorítmica e computação distribuída. O trabalho dialoga com o GDPR, a LGPD, o HIPAA, a AI Act europeia, o European Health Data Space (EHDS), o Data Act e as Guidelines 02/2025 sobre o processamento de dados pessoais por meio de tecnologias blockchain, publicadas pelo European Data Protection Board (EDPB). Sustenta-se que as arquiteturas distribuídas de IA podem deslocar a lógica tradicional de governança, baseada na transferência internacional de dados, para modelos de coordenação regulatória, baseados em interoperabilidade, rastreabilidade e verificabilidade computacional. Conclui-se que tais arquiteturas têm potencial para consolidar novas formas de soberania digital e de constitucionalismo computacional transnacional, por meio das possibilidades proporcionadas pela GS1 e seus standards.

Palavras-chave: Federated learning; Blockchain permissionada; Padrões GS1; Governança de dados em saúde; Soberania digital.

ABSTRACT

Distributed artificial intelligence (AI) architectures are causing a structural shift in global health data governance. Instead of models focused on massive data transfer and concentration, the foundations are emerging for a future paradigm of distributed computational coordination, regulatory interoperability, and Federated Learning (FL). This article investigates how architectures composed of FL, permissioned blockchain, and global interoperability standards - especially GS1 standards - can constitute computational regulatory

Universidade de Santiago de Compostela, Espanha; Docente e pesquisador do Programa de Pós-Graduação em Direito - Mestrado e Doutorado e do Mestrado Profissional em Direito Empresarial, ambos da UNISINOS; Bolsista de Produtividade em Pesquisa do CNPq; Fundador do Grupo de Pesquisa JUSNANO; E-mail: wengelmann@unisinos.br; ORCID: https://orcid.org/0000-0002-0012-3559.

infrastructures capable of operationalizing health data governance, digital sovereignty, and compliance by architecture in global health and supply chain ecosystems. The research adopts a legal-theoretical, interdisciplinary, and comparative methodology, articulating Digital Law, institutional theory, algorithmic governance, and distributed computing. This work engages with the GDPR, LGPD, HIPAA, the European AI Act, the European Health Data Space (EHDS), the Data Act, and Guidelines 02/2025 on the processing of personal data through blockchain technologies, published by the European Data Protection Board (EDPB). It argues that distributed AI architectures can shift the traditional governance logic, based on the international transfer of data, towards regulatory coordination models based on interoperability, traceability, and computational verifiability. It concludes that such architectures have the potential to consolidate new forms of digital sovereignty and transnational computational constitutionalism, through the possibilities offered by GS1 and its standards.
Keywords: Federated learning; Permissioned blockchain; GS1 standards; Health data governance; Digital sovereignty.

1 INTRODUÇÃO

A governança global de dados atravessa uma transformação estrutural impulsionada pela expansão dos usos da inteligência artificial (IA), pela digitalização dos ecossistemas econômicos e pela crescente centralidade da infraestrutura computacional na regulação contemporânea. Em setores críticos, especialmente na saúde e na supply chain farmacêutica, foco deste artigo, o problema jurídico deixou de ser apenas o compartilhamento de dados pessoais, sensíveis ou especiais, passando a envolver soberania informacional, interoperabilidade regulatória, rastreabilidade algorítmica e coordenação transnacional entre diferentes regimes jurídicos. Todos esses aspectos decorrem da crescente globalização das relações políticas, sociais e econômicas, conjugada à digitalização de tudo.

A governança internacional de dados foi construída sobre mecanismos de transferência transfronteiriça, consentimento contratual e centralização da informação. Esse modelo vem sendo pressionado por múltiplos fatores: a) crescimento exponencial do volume de dados sensíveis (a LGPD-Brasil classifica os dados de saúde como "dados pessoais sensíveis", art. 5º, II; o GDPR-EU trata os dados de saúde como "categoria

especial de dados pessoais", art. 9º; já o HIPAA-USA denomina os dados de saúde como "Protected Health Information" PHI), que se encontra no parágrafo 164. 312 letras: a, b, c, d, e, onde se podem ler sobre os cuidados com a integridade, a rastreabilidade e a proteção eletrônica do Electronic Protected Health Information (ePHI); b) expansão da IA generativa (IAG); c) o aumento dos riscos sistêmicos de concentração informacional; d) a fragmentação regulatória internacional e e) o fortalecimento de agendas de soberania digital. O cruzamento desses temas constitui o problema de pesquisa deste artigo, que parte da hipótese: a combinação entre FL, blockchain permissionada e standards globais de interoperabilidade (padrões técnicos ou standards GS1[3]) pode constituir uma nova geração de infraestruturas regulatórias computacionais capazes de operacionalizar uma governança transnacional de dados de saúde baseada em coordenação distribuída, soberania digital e compliance by architecture.

Nesse cenário, as arquiteturas distribuídas de IA surgem como importantes alternativas institucionais. O Federated Learning (FL), ao permitir o treinamento colaborativo sem a necessidade de centralização massiva de dados pessoais, notadamente os relacionados à saúde, oferece uma mudança paradigmática: a cooperação informacional deixa de depender da transferência integral de dados entre instituições e jurisdições. Ao mesmo tempo, tecnologias de blockchain permissionada vêm sendo utilizadas para fortalecer os mecanismos de auditabilidade, integridade transacional, governança de acesso e rastreabilidade regulatória. Entretanto, a utilização dessas tecnologias em ambientes regulados exige compatibilização rigorosa com princípios jurídicos relacionados à minimização de dados, ao direito ao esquecimento, à accountability e à proteção de dados pessoais.

Simultaneamente, padrões globais de interoperabilidade - com destaque para os standards GS1 - assumem importância estratégica na

[3] "A GS1 é uma plataforma de colaboração global e neutra que reúne líderes da indústria, governos, órgãos reguladores, instituições acadêmicas e associações para desenvolver soluções baseadas em padrões técnicos ou standards que abordem os desafios da troca de dados. Nossa escala e alcance - organizações membros locais em 120 países, mais de dois milhões de empresas usuárias e 10 bilhões de transações diárias - ajudam a garantir que haja uma linguagem comum para os negócios em todo o mundo" (GS1 - About, 2022).

coordenação de ecossistemas globais de saúde e de supply chain. Tais padrões fornecem uma linguagem operacional comum para a identificação, o rastreamento, a interoperabilidade e a sincronização de fluxos logísticos e informacionais.

O objetivo geral do artigo é estudar as condições de possibilidade da combinação entre FL, blockchain permissionada e standards globais, como o GS1, para funcionar como uma geração inovadora de infraestruturas regulatórias computacionais que apoiem uma governança transnacional de dados de saúde (considerando as diferentes denominações que recebem no Brasil, na UE e nos EUA), a partir de movimentos de coordenação distribuída, soberania digital e compliance by architecture. Como objetivos específicos, tem-se: a) analisar as transformações estruturais da governança global de dados; b) examinar os desafios e as possibilidades do Federated Learning; c) conhecer as características da blockchain permissionada e suas contribuições para as infraestruturas regulatórias computacionais; d) identificar as características dos padrões GS1 e suas conexões com a interoperabilidade global em cadeias globais de saúde; e) avaliar alguns aspectos vinculados aos dados de saúde no GDPR, na LGPD e na HIPAA; f) propor um modelo arquitetural para a conjugação dos atores e marcos normativos vinculados aos dados sobre saúde; g) apresentar algumas das limitações, dos riscos e tensões jurídicas ainda persistentes.

Metodologicamente, este artigo adota uma abordagem teórica interdisciplinar que combina análise jurídica, teoria da governança e estudos de infraestrutura computacional. A estrutura conceitual do artigo foi construída a partir de uma busca bibliográfica - utilizando as palavras-chave do resumo - nas bases de dados Web of Science, Academic Search Premier (EBSCO), Scopus e ScienceDirect.

O estudo dialoga diretamente com desenvolvimentos regulatórios recentes, especialmente: GDPR (UE); LGPD (Brasil); HIPAA (EUA); AI Act (UE); Data Act; European Health Data Space (EHDS) e Guidelines 02/2025, que destacam o processamento de dados pessoais na blockchain.

Declaração sobre o uso da Inteligência Artificial Generativa (IAG): em conformidade com o art. 9º, inciso I, alíneas "c", "d" e "f", da Política de Integridade da Atividade Científica do CNPq (Portaria CNPq n. 2.664/2026), informa-se que foi utilizada a ferramenta de Inteligência Artificial Generativa ChatGPT, desenvolvida pela OpenAI - baseada no

modelo GPT-5.5, plano Plus, em modo multimodal ativo, com ferramentas avançadas habilitadas - exclusivamente como apoio metodológico preliminar à pesquisa. A ferramenta foi empregada: a) para a realização de "brainstorming" inicial destinado à identificação e concepção de possíveis recortes temáticos e problemas de pesquisa a partir das palavras-chave constantes no resumo do trabalho; e b) para auxílio exploratório na identificação de fontes bibliográficas, periódicos científicos e referências acadêmicas de reconhecido impacto internacional. O pesquisador realizou a supervisão humana integral em todas as fases de desenvolvimento da pesquisa, incluindo a formulação do problema, da hipótese, dos objetivos e da metodologia; a organização do sumário e a seleção das referências; a análise crítica do material levantado, mediante leitura e organização de sínteses; a redação do texto; e a revisão final do trabalho. Todas as informações, sugestões e referências obtidas por meio da ferramenta foram posteriormente verificadas e validadas por meio de acesso direto aos materiais das respectivas revistas (nas bases de dados Web of Science, Academic Search Premier - EBSCO, Scopus e ScienceDirect); os materiais foram baixados, guardados e analisados criticamente pelo autor, que assume integral responsabilidade pelo conteúdo final da pesquisa, pela precisão das informações apresentadas e pela adequada atribuição das fontes utilizadas. Portanto, em nenhuma fase do desenvolvimento do estudo se utilizou qualquer conteúdo gerado diretamente pela ferramenta. O desenvolvimento foi realizado exclusivamente pelo autor da pesquisa, com a indicação correta das fontes e a observância das normas da ABNT. Com isso, também se respeitou integralmente o conteúdo do art. 9º, inciso II e todas as suas alíneas, cabíveis ao caso da presente pesquisa, da referida Portaria, especialmente as alíneas "a" até "d", "g" até "n", t, v.

O aspecto inovador do artigo reside na abordagem adotada em relação ao FL, à blockchain e aos padrões GS1, a saber: não são meras tecnologias, mas componentes institucionais de uma nova arquitetura regulatória transnacional. Vale dizer: se pretende fazer a articulação entre compliance by architecture, soberania digital, governança distribuída em saúde e padrões globais de interoperabilidade. Paralelamente, pretende-se destacar a oportunidade de substituir modelos de governança baseados na transferência internacional de dados de saúde por arquiteturas de coordenação distribuída de aprendizado. O desenvolvimento da pesquisa

tem bem clara a seguinte questão: o objetivo não é apresentar a FL como uma solução tecnológica dissociada dos contextos políticos e institucionais, mas sim analisar como as arquiteturas distribuídas podem remodelar as organizações normativas dos ecossistemas globais de dados de saúde.

O restante do artigo está organizado da seguinte forma: 2 Transformações estruturais da governança global de dados; 3 Aprendizagem Federada (LE) e a transição da governança por transferência para a governança por cooperativa; 4 Blockchain permissionada, auditabilidade e infraestruturas regulatórias computacionais; 5 Normas GS1, interoperabilidade global e ecossistemas da cadeia de abastecimento em saúde; 6 GDPR, LGPD, HIPAA e a emergência da soberania digital distribuída; 7 Proposta de um modelo arquitetônico integrado para ecossistemas globais de saúde; 8 As limitações, riscos e prejuízos jurídicos persistentes; 9 As considerações finais, reiterando as principais contribuições e as perspectivas para trabalhos futuros.

2 TRANSFORMAÇÕES ESTRUTURAIS DA GOVERNANÇA GLOBAL DE DADOS

Segundo documento publicado pela OECD (2026), a economia digital contemporânea é marcada pela centralidade estratégica dos dados como infraestrutura crítica para a inovação, a coordenação econômica e o exercício do poder regulatório. Nas últimas duas décadas, consolidou-se um modelo global caracterizado por plataformas centralizadas, pela acumulação massiva de dados e pela concentração da informação em poucos atores transnacionais (Digital Economy Trends 2026, 2026).

Esse movimento global é caracterizado por Shoshana Zuboff como o "capitalismo de vigilância", conceito lançado pela autora há algum tempo, que parte do pressuposto de que se trata de um "*new market form has quickly developed into the default business model for most online companies and startups, where valuations routinely depend upon 'eyeballs' rather than revenue as a predictor of remunerative surveillance assets*" (p. 81). Os "*eyeballs"* são os aspectos mais significativos para as empresas, o que sinaliza essa mudança: "*Surveillance capitalism establishes a new form of*

power in which contract and the rule of law are supplanted by the rewards and punishments of a new kind of invisible hand" (2015, p. 82). Esse conceito volta com força, em publicação posterior, onde se observa a emergência de "dados" com novas configurações, pois ingressam a subjetividade humana, os comportamentos cotidianos, as relações sociais e os afetos. Esse conjunto mostra que: "*human experience is claimed as raw material for datafication*" (Zuboff, 2019, p. 8). A transformação da vida e das relações que ela gera é digitalizada e posta nas redes, o que promove o fenômeno da "datificação". Portanto, observa-se uma transformação crescente nas estruturas fundamentais da sociedade, sobretudo pela força que a técnica adquire nesse contexto, substituindo a autoridade - especialmente a das instituições e do próprio Direito - pelo aprofundamento dos mecanismos de controle digital. Isso provoca o deslocamento dos direitos de decisão, que passam a ser geridos pela vigilância, o que promove a emergência de um mercado de controle comportamental (Zuboff, 2019).

No panorama da saúde digital, a questão torna-se ainda mais sensível. Dados médicos apresentam alto valor econômico, científico e estratégico, mas também envolvem direitos fundamentais relacionados à privacidade, à dignidade humana, à autodeterminação informativa e à proteção contra a discriminação algorítmica. Esses aspectos acabam se chocando com as características do "capitalismo de vigilância": a ampla liberdade de acesso aos dados das pessoas vem sendo limitada pelo Direito e pelas plataformas, especialmente quanto à garantia de transparência e de responsabilização (accountability) (De Gregorio, 2021). Exemplos desse movimento regulatório se encontram ao longo dos últimos anos, quando diferentes regimes regulatórios buscaram responder a esses desafios: o GDPR (General Data Protection Regulation) europeu consolidou uma abordagem baseada em direitos fundamentais e accountability (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016); a LGPD (Lei Geral de Proteção de Dados) brasileira incorporou os princípios de prevenção, necessidade e responsabilização (Brasil, 2018); a HIPAA (Health Insurance Portability and Accountability Act de 1996) norte-americana estruturou forte preocupação com integridade, rastreabilidade e proteção de ePHI (Protected Health Information (PHI) electronic); o AI Act europeu passou a regular os riscos sistêmicos de

sistemas de IA (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024) e o EHDS (European Health Data Space Regulation, 2025) propôs infraestrutura interoperável de compartilhamento seguro de dados de saúde.

Apesar desses avanços regulatórios, observa-se a persistência de uma tensão estrutural: os modelos tradicionais de IA dependem frequentemente de grandes volumes de dados para o treinamento de algoritmos. Essa lógica produz problemas jurídicos relevantes: ampliação dos riscos de vazamento, intensificação das assimetrias de poder, aumento da dependência tecnológica, dificuldades de auditoria, opacidade algorítmica e fragilidade da soberania digital. O "capitalismo de vigilância" exige uma grande quantidade de dados para o treinamento de tecnologias de IA. Por outro lado, o arcabouço regulatório-legislativo apresentado pretende limitar o acesso a esses dados. Por conta dessas forças em disputa, Rieke; Hancox; Li et al (2020) alertam que o avanço do Deep Learning (DL) na medicina, especialmente em áreas como radiologia e patologia, exige conjuntos vastos de dados curados para atingir precisão de nível clínico. No entanto, o acesso a esses dados é severamente limitado devido a preocupações com a privacidade e regulamentações rigorosas. Mesmo com técnicas de anonimização, os autores entendem que elas são insuficientes, pois técnicas modernas permitem a reconstrução do rosto de um paciente a partir de imagens de tomografia ou de ressonância magnética. Esse cenário cria "silos de dados" que impedem o treinamento de modelos robustos e generalizáveis.

É precisamente nesse ponto que as arquiteturas distribuídas passam a assumir relevância institucional.

3 FEDERATED LEARNING (FL) E A TRANSIÇÃO DA GOVERNANÇA POR TRANSFERÊNCIA PARA A GOVERNANÇA POR COORDENAÇÃO

A necessidade de dados gerados pelos diversos setores da sociedade, com ênfase nos relacionados à saúde (dados sensíveis ou especiais),

necessários ao funcionamento dos sistemas de IA, enfrenta limitações regulatórias específicas. Esses bloqueios são necessários para "tentar" controlar o avanço do "capitalismo de vigilância" (Zuboff, 2015; 2019) ou do "capitalismo informacional" (Cohen, 2019).

Cohen (2019) argumenta que as infraestruturas informacionais operam cada vez mais como mecanismos de ordenação social, e não apenas como sistemas técnicos. A concentração de dados em arquiteturas centralizadas cria dependências que afetam não apenas os mercados, mas também a autonomia institucional e a governança democrática. No domínio da saúde, essas assimetrias podem influenciar as agendas científicas, o acesso à inovação e até mesmo as prioridades de saúde pública. Isso sinaliza que o problema vai além das preocupações com a privacidade. As infraestruturas centralizadas concentram o próprio poder epistêmico. Instituições que controlam grandes conjuntos de dados frequentemente adquirem influência desproporcional sobre o desenvolvimento de modelos, os critérios de validação e os padrões algorítmicos. Essa concentração torna-se ainda mais problemática em contextos transnacionais, em que os dados gerados em uma jurisdição podem ser processados, armazenados ou monetizados em diferentes ambientes regulatórios. Como resultado, a centralização da informação cruza-se cada vez mais com debates mais amplos sobre soberania digital e assimetrias geopolíticas.

Diante dessas perspectivas críticas, analisa-se o papel do Federated Learning (FL) como uma das alternativas relevantes para as transformações arquiteturais recentes na engenharia de sistemas de IA (Sum; Pritee; Saha et al. 2026). Desde logo, destaca-se que esse caminho não se apresenta como a solução definitiva para as questões apontadas até o momento. Pelo contrário, é uma opção que deverá ser discutida, investigada cientificamente e testada, com a observação rigorosa de seus desdobramentos práticos.

De acordo com Kairouz; McMahan; Avent et al. (2021), "Federated Learning (FL) é um ambiente de aprendizado de máquina em que muitas partes interessadas (por exemplo, dispositivos móveis ou organizações inteiras) treinam colaborativamente um modelo sob a orquestração de um servidor central (por exemplo, um provedor de serviços), mantendo os dados de treinamento descentralizados. Ele incorpora os princípios de

coleta focada e de minimização de dados e pode mitigar muitos dos riscos e custos sistêmicos de privacidade decorrentes do aprendizado de máquina tradicional e centralizado". No FL, os dados permanecem armazenados localmente nas instituições participantes. O que circula entre os nós da rede são parâmetros de aprendizado, gradientes ou atualizações de modelo. Diferentemente dos modelos tradicionais de Machine Learning (ML), em que os dados são agregados em repositórios centralizados para treinamento algorítmico.

Essa diferença técnica possui consequências jurídicas relevantes: ao reduzir a necessidade de transferência internacional massiva de dados pessoais - no caso deste artigo, dados de saúde -, o FL torna-se compatível com princípios centrais de proteção de dados presentes nos documentos protetivos antes referidos.

O FL, de acordo com Rieke; Hancox; Li et al (2020), surge como uma alternativa para treinar algoritmos colaborativamente, sem a necessidade de compartilhar dados brutos. Em vez de centralizar as informações em um Data Lake, o processo de aprendizado ocorre localmente em cada instituição. Com isso, pode-se destacar que o FL não se trata meramente de uma técnica de aprendizado de máquina distribuído, mas sim de uma infraestrutura emergente de governança computacional capaz de operacionalizar a coordenação transnacional de dados, preservando a privacidade, respeitando as jurisdições e sendo semanticamente interoperável (Zekiye; Özkasap, 2023). Dessa forma, o FL evidencia algumas possibilidades promissoras, como a reorganização das relações de poder em torno dos dados, a redefinição da soberania informacional, a alteração dos mecanismos de compliance, a transformação da governança institucional e a produção de novas formas de coordenação regulatória. Vale destacar: o FL deixa de ser apenas Machine Learning Distribuído (MLD) e passa a ser uma arquitetura institucional de colaboração regulada, sem centralização informacional (Dayan; Roth; Zhong et al, 2021). O FL, em relação ao GDPR, atende especialmente a: minimização de dados, privacidade desde a concepção, privacidade por padrão, limitação da finalidade, responsabilização e segurança desde a concepção. No contexto da LGPD, o FL também dialoga fortemente com os princípios da necessidade, da prevenção, da segurança, da responsabilização e da adequação. No tocante ao HIPAA, o FL permite realizar o treinamento

colaborativo sem que os dados clínicos do PHI precisem sair dos hospitais ou serem centralizados, reduzindo riscos de violação de privacidade e facilitando a aderência às exigências regulatórias de proteção desses dados (Barbaria; Jemai; Ceylan et al, 2025; Pati; Kumar; Varma et al, 2024).

Em ambientes hospitalares globais, isso permite que hospitais europeus mantenham a conformidade com o GDPR, hospitais brasileiros observem a LGPD e as instituições norte-americanas preservem a compatibilidade com o HIPAA, sem a necessidade de uma unificação física integral das bases de dados (Habu; Dhabariya; Lal Pal et al 2025).

Do ponto de vista institucional, esse movimento gerado pelo FL representa uma transição paradigmática: a governança internacional deixa de ser baseada prioritariamente na transferência de dados e passa a operar por meio da coordenação interoperável de aprendizado distribuído. Essa mudança altera o próprio objeto da regulação. O foco deixa de ser apenas "quem transfere dados para quem" e passa a envolver: coordenação algorítmica, verificabilidade computacional, governança de parâmetros, auditabilidade distribuída e segurança criptográfica. Por isso, a pergunta passa a ser: "como coordenar a inteligência coletiva sem violar direitos fundamentais, a soberania regulatória e a autonomia institucional?" Esse questionamento é relevante, pois as arquiteturas avançadas de FL podem incorporar: "secure aggregation" (proteção criptográfica das atualizações locais), "*differential privacy*" (proteção estatística contra inferências), "*homomorphic encryption*", "*zero-knowledge proofs*" (Kairouz; McMahan; Avent et al, 2021). Tais mecanismos fortalecem a proteção contra inferência reversa, reconstrução de dados e ataques adversários. Mais do que uma simples solução tecnológica, o FL emerge como um mecanismo institucional para a reorganização da governança transnacional de dados.

A integração entre IA, blockchain e sistemas de saúde é apresentada como um dos campos mais promissores - e, simultaneamente, mais complexos - da medicina computacional contemporânea. Com a crescente adoção de abordagens orientadas por dados para a medicina de precisão, o suporte à decisão clínica e a gestão populacional em saúde, torna-se indispensável o desenvolvimento de mecanismos colaborativos capazes de garantir segurança, privacidade e conformidade regulatória no tratamento de informações médicas (Zafar, 2025). Nessa direção, o trabalho de Shahsavari; Baseri; Hafid et al (2026) propõe a combinação de FL e

blockchain para viabilizar análises médicas distribuídas sem compartilhamento direto de dados sensíveis. Embora o FL possibilite o treinamento colaborativo entre instituições, preservando a confidencialidade das bases de dados - em consonância com as normas HIPAA, GDPR e LGPD -, os autores destacam que essa abordagem ainda está sujeita a ameaças relevantes, como a manipulação de modelos e o vazamento de gradientes.

Para enfrentar essas limitações, o estudo examina o conceito de "Blockchain-based Federated Learning (BCFL)" (Issa; Moustafa; Turnbull et al, 2023), explorando características da blockchain, como a descentralização, a imutabilidade e os mecanismos de consenso, com o objetivo de ampliar a confiança, a rastreabilidade e a auditabilidade dos processos.

Qual o motivo dessa interrelação entre os dados de saúde, a blockchain e o FL? Segundo dados recentes (Blockchain in healthcare market size, share, and trends 2026 to 2035), o mercado global de blockchain aplicado à saúde movimentou aproximadamente US$ 12,92 bilhões em 2025, com expectativa de alcançar cerca de US$ 234,97 bilhões até 2035, apresentando uma taxa composta de crescimento anual (CAGR) de 33,65% no período de 2026 a 2035. Esse crescimento é impulsionado, sobretudo, pelo avanço da digitalização no setor e pela crescente demanda por tecnologias mais eficientes para o armazenamento, compartilhamento e gerenciamento de dados médicos (aqui compreendidos os dados de saúde e a comercialização de medicamentos).

4 BLOCKCHAIN PERMISSIONADA, AUDITABILIDADE E INFRAESTRUTURAS REGULATÓRIAS COMPUTACIONAIS

A tecnologia blockchain pode ser estruturada segundo distintos modelos de governança e controle de acesso, geralmente divididos em três modalidades: redes públicas, permissionadas e privadas (Belen-Saglama; Altuncua; Lu et al, 2023). Nas blockchains públicas, o ambiente é amplamente descentralizado e acessível, de modo que qualquer indivíduo

ou organização pode participar da rede e interagir com os registros armazenados. Por outro lado, as blockchains permissionadas adotam mecanismos de autorização restritivos, nos quais determinadas funções, especialmente a inserção e a validação de dados, permanecem reservadas a participantes previamente autorizados. Esse é o modelo que utilizaremos nesta seção para tratar dos dados de saúde (J., Andrew; Isravel; Sagayam et al, 2023). Quando tais competências são concentradas exclusivamente em uma única entidade, caracteriza-se a denominada blockchain privada. Associados a essa infraestrutura tecnológica encontram-se os "contratos inteligentes", instrumentos digitais programáveis capazes de executar automaticamente comandos previamente estabelecidos. Por meio deles, protocolos operacionais e regras negociais podem ser implementados de forma autônoma em ambiente distribuído, reduzindo a necessidade de intervenção humana ou de intermediários para assegurar o cumprimento das condições pactuadas (Kostick-Quenet; Compagnucci; Aboy et al, 2025).

Em ecossistemas regulados, especialmente na saúde e na cadeia de suprimentos farmacêuticos, as blockchains permissionadas apresentam vantagens significativas em relação às demais categorias. Enquanto blockchains públicas podem gerar problemas relacionados à imutabilidade absoluta, exposição excessiva de metadados e dificuldades de governança regulatória, as blockchains permissionadas permitem: controle de acesso, governança institucional, segmentação de permissões, rastreabilidade auditável e conformidade regulatória mais robusta (Amin; Akhtar; Hoque et al, 2025). Devido a esses aspectos, destaca-se, neste estudo, o uso da blockchain permissionada.

No contexto da saúde digital, a blockchain permissionada pode fortalecer: "logging" regulatório, "audit trails", integridade documental, rastreabilidade de acesso, governança de consentimento e verificação da integridade de modelos de IA. Apesar desses aspectos positivos, a compatibilidade entre a blockchain e a proteção de dados exigirá cautela. A pesquisa de Belen-Saglama; Altuncua; Lu et al (2023) destaca que a imutabilidade estrutural das cadeias distribuídas pode entrar em tensão com: direito ao esquecimento, direito à retificação, limitação temporal, minimização de dados, dificuldade de identificar controladores e operadores de dados, incertezas sobre a lei aplicável e as transferências internacionais.

Por essas razões, a literatura contemporânea (Zafar, 2025; Arabsorkhi; Khazaei, 2024; Haque; Islam; Hyrynsalmi et al, 2021; Mayer; Costa; Righi, 2020) e os próprios reguladores europeus (European Data Protection Board - EDPB, and Summary, 2025) vêm enfatizando que todos os dados pessoais devem ser armazenados off-chain e não diretamente on-chain. As Guidelines 02/2025 sobre o processamento de dados pessoais por meio de tecnologias blockchain, publicadas pelo EDPB, sinalizam na mesma direção e representam um dos marcos regulatórios mais importantes recentes sobre a compatibilidade entre blockchain e proteção de dados. Essas Guidelines partem de uma premissa fundamental: blockchain não está fora do escopo do GDPR. Ao contrário, qualquer utilização de blockchain envolvendo dados pessoais permanece integralmente submetida aos princípios europeus de proteção de dados. Ao mesmo tempo, as Guidelines reforçam a tendência crescente de transformar a infraestrutura computacional em objeto direto de regulação jurídica. A arquitetura deixa de ser mero suporte técnico e passa a constituir uma dimensão normativa da própria governança regulatória.

Modelos mais compatíveis com o GDPR tendem a utilizar a blockchain apenas para: "hashes" criptográficos, provas, registros de integridade, "logs" mínimos e referências verificáveis. Dados sensíveis permanecem off-chain, sob a governança institucional local. Essa arquitetura híbrida fortalece a compatibilidade regulatória sem renunciar à auditabilidade distribuída. Nesse panorama, a blockchain permissionada pode ser compreendida como uma infraestrutura regulatória computacional. A regulação deixa de depender exclusivamente de supervisão "ex post" e passa a ser parcialmente incorporada ao próprio design da infraestrutura.

Ao mesmo tempo, ao promover o acoplamento entre a Blockchain e a FL, observa-se que essa última assume o papel de implementar restrições regulatórias, impor limites arquiteturais e viabilizar a operacionalização do "compliance" (Zafar, 2025). Com esse movimento, o "compliance" não depende apenas de contratos, consentimentos ou documentos, mas também emerge da própria arquitetura técnica. Dessa forma, nasce o "compliance by architecture". Nesse cenário inovador, a relevância do LF vai além da otimização computacional. Arquiteturas federadas servem cada vez mais como mecanismos de minimização estrutural, reduzindo a

necessidade de transferência de informações sensíveis entre fronteiras institucionais e jurisdicionais (Zekiye; Özkasap, 2023). As estruturas tradicionais de privacidade frequentemente operam após a circulação de dados (Dayan; Roth; Zhong et al, 2021).

Os mecanismos de conformidade focam-se em autorizações, salvaguardas contratuais, estruturas de consentimento e obrigações de responsabilização posterior. O FL reformula parcialmente esta lógica ao incorporar a minimização diretamente à arquitetura de coordenação. Essa distinção é crucial. Em vez de regular a circulação irrestrita depois de esta ocorrer, o FL procura reduzir a necessidade estrutural da circulação desde o princípio (Shahsavari; Baseri; Hafid et al, 2026). A arquitetura, portanto, operacionaliza princípios fortemente associados à privacidade desde a concepção. Conjuntos de dados sensíveis permanecem armazenados localmente, enquanto as atualizações do modelo circulam por meio de protocolos computacionais controlados. Nesse sentido, o FL assemelha-se cada vez mais a uma infraestrutura de preservação da privacidade do que a uma mera técnica de otimização distribuída (Oladejo; Adebayo; Olufemi et al, 2025). Tecnologias adicionais reforçam ainda mais essa dinâmica (Rieke; Hancox; Li et al, 2020). Mecanismos de privacidade diferencial visam limitar os riscos de reidentificação. Protocolos de agregação seguros reduzem a exposição das contribuições locais. A criptografia homomórfica permite computação sobre informações criptografadas, enquanto ambientes de execução confiáveis reforçam as garantias de integridade durante o processamento distribuído (Akavaram, 2025; Kairouz; McMahan; Avent et al, 2021). Nenhum desses mecanismos elimina completamente os riscos. Ataques de inversão de modelo, vazamento de gradiente e inferência de pertencimento continuam sendo desafios importantes. No entanto, a arquitetura geral altera significativamente a distribuição da exposição informacional em ecossistemas colaborativos (Akavaram, 2025).

Para qualificar filosoficamente e juridicamente as relações entre a blockchain, FL e as infraestruturas regulatórias computacionais, busca-se emprestar uma categoria formulada por Hildebrandt (2018), a saber, "Legal protection by design", que visa integrar salvaguardas tecnológicas que garantam a capacidade humana de desafiar e contestar decisões automatizadas, isto é, uma arquitetura sociotécnica voltada à preservação

jurídica substantiva em ambientes computacionais. Portanto, propõe-se a substituição do "legal by design", caracterizado pela concentração na conformidade estrita com o texto legal ou a mera automação da conformidade jurídica (Hildebrandt, 2018, p. 34-35; Hildebrandt, 2020, p. 251-252). Diante dos desafios observados no cenário das tecnologias digitais, esse caminho não será isento de dificuldades. Apesar disso, a pesquisa pretende demonstrar a viabilidade de propor elementos de uma arquitetura de escolha que atenda a padrões mínimos, proporcionando proteção eficaz e prática. Vale dizer, se concorda com Hildebrandt (2018; 2020) que a formulação deve ser deslocada da automação da obediência normativa para a preservação da contestabilidade, da participação democrática e das garantias fundamentais. Essas se consideram para além dos direitos fundamentais previstos nas Constituições democráticas, a fim de incluir também a preocupação com o atendimento dos Direitos Humanos, isto é, as declarações internacionais - sejam internacionais, sejam regionais -, bem como as decisões de cortes internacionais que decidem casos sobre violações desses direitos.

Ao mesmo tempo, busca-se trazer à estrutura tecnológica uma reinterpretação de princípios jurídicos, aceitos em diversos regimes jurídicos e aplicáveis aos avanços tecnológicos, especialmente os promovidos pela IA, que se conectam às bases tecnológicas examinadas até o momento. Adotam-se alguns dos princípios divulgados em 2019 pela OECD, como a IA centrada no ser humano, crescimento inclusivo e sustentável, bem-estar, transparência e explicabilidade, robustez e segurança, e accountability. Além desses princípios, incorporam-se também alguns dos princípios publicados no "The AI Index 2026 Annual Report by Stanford University" (Sajadieh; Fattorini; Perrault et al, 2026): validade e confiabilidade, privacidade, gestão de dados, autonomia e agência humanas e contestabilidade.

Esses princípios são aceitos em diversos países e dialogam entre si. Os princípios funcionarão em um conjunto renovado de fontes do Direito, no qual se agregam, especialmente, os standards técnicos. Essas fontes do Direito viabilizam a concretização do "Legal protection by design". Tradicionalmente, as conexões entre a Teoria do Direito e a Teoria das Fontes do Direito se desenvolvem por meio da seguinte classificação: normas jurídicas como gênero, que abrange duas espécies: as regras (as leis

em geral, sobretudo a produção legislativa estatal) e os princípios jurídicos. Entretanto, os avanços tecnológicos e a globalização vêm evidenciando a emergência de uma nova categoria jurídica: os standards técnicos, como os da GS1.

5 STANDARDS GS1, INTEROPERABILIDADE GLOBAL E ECOSSISTEMAS DE SUPPLY CHAIN EM SAÚDE

A Teoria das Fontes do Direito tem acompanhado os avanços tecnológicos, por meio da valorização de outras formas de manifestação da regulação. Essa perspectiva é confirmada por uma publicação do World Bank (2025), na qual os standards são concebidos como catalisadores do desenvolvimento, da qualidade da infraestrutura e da confiança, na conjugação de esforços públicos e privados vinculados à economia, ao capital humano, ao meio ambiente e à governança. A partir desse conjunto de possibilidades de regulação por meio de standards, busca-se apresentar soluções para desafios globais, entre os quais se destacam as questões relacionadas ao setor da saúde.

A agência UNIDO (2025), que "é uma agência especializada das Nações Unidas (United Nations Industrial Development Organization, da sigla em inglês) com um mandato único para promover o desenvolvimento industrial inclusivo e sustentável", reforça a importância dos standards, pois impulsionam a "competitividade, a inovação e o crescimento econômico e industrial sustentável" (UNIDO, 2025). Portanto, há duas evidências sólidas que indicam a importância regulatória e organizacional dos padrões técnicos.

É nesse contexto que os padrões da GS1 assumem relevância estratégica. Vale destacar que a governança distribuída de dados em saúde depende não apenas de proteção jurídica e de segurança computacional, mas também de interoperabilidade semântica e operacional. A GS1 desenvolveu padrões globais voltados à identificação, à rastreabilidade e à interoperabilidade em cadeias globais de suprimento. Inicialmente associados ao varejo e à logística, esses padrões tornaram-se fundamentais

para os ecossistemas farmacêuticos, hospitalares e de dispositivos médicos (GS1 - About, 2022). Entre os principais mecanismos destacam-se: GTIN (Global Trade Item Number), GLN (Global Location Number), EPCIS (Electronic Product Code Information Services), DataMatrix, Serialização global de produtos, Digital Link, CBV (Core Business Vocabulary), entre outras categorias de padrões (GS1 Style Guide, 2025).

No setor de saúde, esses padrões permitem: rastreamento de medicamentos, combate à falsificação, interoperabilidade logística, sincronização de cadeias globais de suprimento, coordenação transnacional de eventos clínicos e logísticos. Todas essas características são fundamentais para viabilizar a estrutura de supply chain em saúde, especialmente no cuidado com os dados pessoais e sensíveis de saúde: "GS1 Healthcare vislumbra um futuro em que o setor de saúde alcance a implementação harmonizada de padrões globais em processos clínicos e de negócios, possibilitando interoperabilidade, qualidade ideal e eficiência na prestação de cuidados de saúde em benefício dos pacientes" (GS1 Healthcare Strategy 2023-2027).

A incorporação de padrões GS1 em arquiteturas distribuídas de IA tem implicações particularmente relevantes. Primeiro, os padrões oferecem uma linguagem interoperável global capaz de conectar múltiplos ecossistemas regulatórios (GS1 CBV - Core Business Vocabulary Standard, 2022). Segundo, permitem rastreabilidade verificável em sistemas distribuídos (GS1 Traceability, 2022). Terceiro, facilitam a integração entre hospitais, laboratórios, fornecedores, autoridades regulatórias, plataformas de IA, infraestruturas de blockchain e pacientes (GS1 Blockchain, 2022).

Em um cenário de FL aplicado à saúde global, padrões GS1 podem funcionar como uma camada semântica de interoperabilidade regulatória. Isso significa que a coordenação distribuída não depende apenas de infraestrutura computacional, mas também da padronização global dos fluxos informacionais (Nguyen; Bekrar; Le et al, 2025). Os padrões GS1 evidenciam um grande potencial para viabilizar o "diálogo" entre diversos sistemas jurídicos, especialmente quando operam em conjunto com o FL e com as possibilidades proporcionadas pelo amplo uso da blockchain. Além disso, dadas as características do FL, torna-se mais viável cumprir as determinações regulatórias da UE, do Brasil e dos Estados Unidos.

6 GDPR, LGPD, HIPAA E A EMERGÊNCIA DA SOBERANIA DIGITAL DISTRIBUÍDA

A expansão gradativa da economia digital gera crescente preocupação com a soberania digital. Os Estados (aqui entendidos como os Países) passaram a perceber que a dependência tecnológica excessiva compromete a autonomia regulatória, a capacidade institucional e a segurança estratégica dos dados, sejam privados ou públicos. Por isso, uma das implicações mais significativas do FL reside em seu potencial relação com formas distribuídas de soberania sobre dados. Em sistemas centralizados convencionais, as instituições frequentemente perdem o controle significativo sobre os ativos informacionais assim que os conjuntos de dados são transferidos para repositórios externos ou para plataformas computacionais. Mesmo quando há proteções contratuais, a governança operacional frequentemente se concentra em orquestradores centralizados (Li; Xu; Hu et al, 2025). O FL reorganiza parcialmente essas estruturas, preservando o controle local sobre os conjuntos de dados subjacentes. Hospitais, laboratórios e sistemas nacionais de saúde podem participar da produção colaborativa de inteligência, mantendo a governança sensível à jurisdição sobre as informações armazenadas localmente. Essa dinâmica torna-se particularmente relevante em ecossistemas de saúde transnacionais (Akhmetov; Latif; Tyler et al, 2025).

A União Europeia assumiu uma posição particularmente relevante nesse processo. O GDPR representou não apenas uma legislação de proteção de dados, mas também um instrumento geopolítico de afirmação regulatória. Posteriormente, o AI Act, o Data Governance Act (2022), o Data Act (2023) e o EHDS (European Health Data Space, 2025) ampliaram essa estratégia e o ecossistema regulatório aplicável aos dados de saúde. Além disso, devido ao "efeito Bruxelas", esse conjunto regulatório poderá ser aplicado fora do território europeu, principalmente por meio de cadeias negociais estrangeiras estruturadas com empresas localizadas na União Europeia.

No Brasil, a LGPD consolidou um alinhamento relevante aos princípios europeus, enquanto o debate sobre a soberania digital ganhou força em razão da crescente dependência de infraestruturas globais de

dados. Nesse aspecto, cabe destacar que, em janeiro de 2026, o Brasil e a União Europeia reconheceram a equivalência na proteção de dados. Com isso, amplia-se a segurança jurídica e cria-se um ambiente mais favorável à cooperação, à inovação e aos negócios digitais (Brasil, 2026).

Nos Estados Unidos, embora a abordagem permaneça mais fragmentada, regimes setoriais, como a HIPAA, continuam exercendo influência global na proteção de dados de saúde (Barbaria; Jemai; Ceylan et al, 2025; Anthoney, 2024).

Esses mecanismos não eliminam a complexidade regulatória, mas reduzem a dependência estrutural da propriedade centralizada de informações sensíveis. O modelo de governança passa da concentração de dados à coordenação distribuída. Com isso, observa-se um potencial relevante para conciliar a colaboração internacional, a inovação algorítmica, a preservação da autonomia regulatória e a minimização de transferências transfronteiriças (Luo, 2026; Haripriya; Khare; Pandey, 2025).

A utilização do FL, dos padrões GS1 e da blockchain será importante para estabelecer pontes entre os fragmentos regulatórios internacionais. Essa combinação reduz a necessidade de centralização física dos dados, pois a arquitetura permite o treinamento colaborativo, mantendo os dados sob governança local. Isso favorece os modelos de soberania digital distribuída. Nesse ponto, destaca-se algo inovador: a soberania deixa de depender exclusivamente do controle territorial dos fluxos de dados e passa a envolver o controle da arquitetura, a governança da interoperabilidade, a supervisão algorítmica, a gestão local de dados sensíveis e a auditabilidade verificável (Alexander, 2025). Essa transformação dará suporte ao que se pode descrever como "Soberania de Dados Distribuída": uma condição em que múltiplas instituições preservam a autoridade regulatória local, enquanto participam simultaneamente de ecossistemas computacionais compartilhados (Ram; Mahajon; Deogade, 2026).

Trata-se de uma mudança estrutural no modo como o Direito operacionaliza a governança transnacional, respeitando a soberania digital dos sistemas jurídicos relacionados e, ao mesmo tempo, oferecendo uma forma moderna e segura de promover o "compartilhamento" de dados de saúde sem infringir nenhum dos documentos legais aplicáveis ao caso. Com o cruzamento criativo dos sistemas jurídicos, permeado pela

valorização jurídica dos padrões GS1, do FL e da blockchain permissionada, observa-se, na prática, um modelo de governança entre alinhamentos públicos e privados, com o paciente e seus dados sensíveis ou especiais no centro. A partir disso, propõe-se, na sequência, um modelo estruturado que poderá dar conta da operacionalização da governança transnacional distribuída de dados de saúde.

7 PROPOSTA DE MODELO ARQUITETURAL INTEGRADO PARA ECOSSISTEMAS GLOBAIS DE SAÚDE

Considerando a perspectiva teórica apresentada até o momento, a seguir se expõe um modelo em cinco camadas principais, em formato de uma arquitetura que conjuga os elementos identificados na revisão da literatura que se desenvolveu para esse estudo:

1) Camada de dados locais: os dados clínicos permanecem armazenados localmente em hospitais, laboratórios ou outras instituições autorizadas. Não ocorre a centralização massiva de dados sensíveis. Cada instituição mantém a governança local, a conformidade regulatória própria, as políticas internas de segurança e o controle jurisdicional;
2) Camada de Federated Learning: os modelos de IA são treinados de forma colaborativa. Apenas parâmetros, gradientes ou atualizações de aprendizado circulam entre os participantes. A camada incorpora: "secure aggregation", "differential privacy", mecanismos anti-inferência e validação distribuída;
3) Camada de Blockchain Permissionada: a blockchain não armazena dados clínicos diretamente. Seu papel é: registrar logs auditáveis, verificar a integridade, controlar as permissões, registrar eventos críticos e assegurar a rastreabilidade regulatória. Os dados pessoais permanecem off-chain;
4) Camada de interoperabilidade, identificação e semântica distribuída: essa camada poderá incorporar infraestruturas globais de identificação distribuída baseadas nos padrões GS1 e em arquiteturas

como o ecossistema OLIOT (2026), originalmente desenvolvido para suportar o rastreamento global em ambientes de Internet das Coisas (IoT)[4]. Tais arquiteturas permitem a sincronização semântica de eventos, a identificação padronizada de ativos, a interoperabilidade entre organizações e a rastreabilidade verificável em cadeias transnacionais de saúde digital;

5) Camada de governança regulatória: essa é a camada jurídica propriamente dita e coordena accountability, auditoria, DPIAs ("Data Protection Impact Assessment", no caso do GDPR, em especial por conta do conteúdo do seu art. 9º, onde se encontram os dados especiais sobre saúde), governança institucional, supervisão algorítmica e conformidade transnacional. No caso da LGPD, tem-se o "Relatório de Impacto à Proteção de Dados" (artigos 5º, XVII, 10, § 3º e 38) e, na HIPAA, não se adota um nome semelhante - seja em relação ao modelo europeu, seja em relação ao modelo brasileiro -, mas há uma exigência de avaliação de riscos e de segurança (HIPAA Security Rule, 2024, artigos 45 CFR § 164.306; §164.308 e § 164.402).
6) Camada final de certificação: aqui se dá a expedição da chamada "Pedigree Certification", a ser emitida por intermédio do responsável pela blockchain permissionada, atestando que o "Legal Protection by Design" foi respeitado, incluindo os DPIAs ou seus equivalentes, e a regularidade do tratamento dos dados de saúde, a partir do sistema europeu, brasileiro ou americano, conforme for o caso.

Os "Pedigrees" foram inicialmente definidos no "Padrão de Pedigree", ratificado pela EPCglobal, da seguinte forma: "Um 'pedigree' é um registro

[4] Oliot ("Open Language for Internet of Things") é uma plataforma de infraestrutura de código aberto projetada para revolucionar a forma como dados e serviços são compartilhados. Ao aproveitar o sistema de código da GS1 e aderir aos seus padrões, a Oliot visa fornecer uma plataforma segura e distribuída para identificar, capturar e compartilhar dados. Além disso, a plataforma oferece um meio eficiente e flexível de registrar e descobrir serviços. A Oliot ganhou força global, tendo sido baixada em mais de 55 países, e continua a capacitar organizações em todo o mundo. A Oliot adotou tecnologias de ponta, como blockchain e big data, para facilitar uma abordagem eficiente e segura para o compartilhamento de dados e serviços. Ao incorporar esses avanços, a Oliot busca promover a colaboração, a inovação e a criação de valor, permitindo o compartilhamento e a utilização contínuos de dados e serviços entre diversas entidades. A Oliot já obteve implementações bem-sucedidas em vários projetos de cidades inteligentes, navios inteligentes e ônibus inteligentes (OLIOT, 2026).

certificado que contém informações sobre cada distribuição de um medicamento prescrito. Ele registra a venda de um item por um fabricante farmacêutico, quaisquer aquisições e vendas por atacadistas ou reembaladores e a venda final para uma farmácia ou outra entidade que administra ou dispensa o medicamento. O 'pedigree' contém informações sobre o produto, a transação, o distribuidor e o destinatário, além de assinaturas." Embora a descrição acima de um "pedigree" seja apresentada no contexto das cadeias de suprimentos farmacêuticas, a interpretação da definição destaca requisitos importantes para o desenvolvimento de um padrão genérico de ontologia de conteúdo para "pedigrees", que possa ser reutilizado em vários setores.

Recentemente, o conceito de "Pedigree baseado em eventos" foi proposto, utilizando a especificação EPCIS da EPCglobal para capturar eventos da cadeia de suprimentos e gerar conjuntos de dados de rastreabilidade a partir de um subconjunto relevante desses eventos (GS1 - Pedigree Standard, 2007; Solanki; Brewster, 2009; Solanki; Brewster, 2014).

O EPCIS - Electronic Product Code Information Services (GS1 - EPCIS and CBV Implementation Guideline, 2023) constitui o principal padrão de compartilhamento de dados desenvolvido pela GS1 para promover visibilidade informacional tanto no âmbito interno das organizações quanto ao longo das cadeias globais de suprimentos, envolvendo parceiros comerciais e demais stakeholders. Sua estrutura permite registrar e compartilhar informações interoperáveis relacionadas a produtos e ativos, contemplando elementos como identificação, temporalidade, localização, motivação dos eventos e condições operacionais associadas. Desse modo, o standard viabiliza a rastreabilidade do status, da movimentação e da cadeia de custódia dos bens em ecossistemas logísticos distribuídos. Com isso, pretende-se conectar o mundo físico ao digital.

De modo complementar ao EPCIS, o GS1 desenvolve o CBV (Core Business Vocabulary), que atua como um padrão associado, fornecendo definições padronizadas de valores semânticos utilizados no preenchimento das estruturas de dados previstas pelo próprio EPCIS. Sua função consiste em assegurar a consistência interpretativa e a interoperabilidade semântica entre diferentes sistemas, organizações e contextos operacionais (GS1 - Core Business Vocabulary - CBV, 2022). O

vocabulário comum favorece a comunicação e a compreensão das regras a cumprir. Isso não significa que haja uma aplicação automática, mas o ponto de partida das categorias é comum e, no CBV, há um "locus" acessível a todas as partes interessadas, inseridas na cadeia global de circulação dos dados de saúde.

A organização GS1 reconhece que os requisitos empresariais e as infraestruturas tecnológicas estão em constante transformação. Nesse cenário, o EPCIS vem sendo progressivamente aprimorado para ampliar os níveis de transparência relacionados à fabricação, à distribuição e à circulação de produtos ao longo de cadeias globais de suprimentos. Em consonância com os processos contemporâneos de transformação digital, sustentabilidade e economia circular, as versões mais recentes dos standards passaram a incorporar mecanismos padronizados para a inclusão de dados provenientes de sensores, bem como certificações relativas a produtos e processos, fortalecendo a utilização de uma linguagem comum entre sistemas interoperáveis (GS1 - EPCIS and CBV Implementation Guideline, 2023).

O modelo arquitetural proposto busca compatibilizar a inovação tecnológica, a proteção de dados e a governança regulatória em ecossistemas globais de saúde digital. Em vez de adotar estruturas centralizadas de armazenamento e processamento, a arquitetura fundamenta-se em uma lógica distribuída de coordenação institucional, na qual diferentes camadas exercem funções complementares de interoperabilidade ("o alinhamento e a colaboração com os parceiros da cadeia de suprimentos são essenciais. É aqui que os padrões entram em cena. Os padrões abertos da cadeia de suprimentos permitem a interoperabilidade entre todas as partes, estabelecendo um conjunto comum de regras para identificação, captura, compartilhamento e uso de dados"), rastreabilidade ("capacidade de rastrear a história, a aplicação ou a localização de um objeto"), auditabilidade (GS1 - Global Traceability Standard, 2017) e supervisão regulatória.

Na camada de dados locais, os dados clínicos permanecem sob a custódia das próprias instituições responsáveis pelo tratamento, preservando-se a soberania informacional, as exigências jurisdicionais e os princípios de minimização de dados previstos em marcos regulatórios como o GDPR, a LGPD e a HIPAA (Smietanka; Pithadia; Treleaven, 2020).

Esses três marcos regulatórios serviram para orientar a pesquisa. Sobre essa base, a camada do Federated Learning permite o treinamento colaborativo de modelos de inteligência artificial sem a necessidade de transferência massiva de dados pessoais, reduzindo os riscos associados à circulação transfronteiriça de informações sensíveis e incorporando mecanismos técnicos de proteção, como "differential privacy" e "secure aggregation"

A camada de blockchain permissionada atua como infraestrutura distribuída de verificabilidade institucional, assegurando a integridade, a rastreabilidade e a auditabilidade dos eventos relevantes do sistema, sem armazenar diretamente dados clínicos na cadeia. Paralelamente, a camada de interoperabilidade, identificação e semântica distribuída incorpora os standards GS1 EPCIS/CBV (GS1 - EPCIS and CBV Implementation Guideline, 2023) e a arquitetura de rastreamento distribuído associada ao ecossistema OLIOT (2026), permitindo a sincronização semântica de eventos, interoperabilidade organizacional e rastreabilidade verificável em cadeias transnacionais de saúde digital e logística hospitalar.

Por fim, a camada de governança regulatória opera como um eixo de coordenação jurídica e institucional da arquitetura, articulando mecanismos de "accountability", auditoria, avaliação de impacto sobre a proteção de dados (DPIAs e outras denominações que esse processo possa receber), supervisão algorítmica e conformidade regulatória transnacional. Nesse sentido, o modelo procura deslocar uma parte significativa da conformidade normativa para a própria infraestrutura tecnológica, aproximando-se de uma lógica de "compliance by architecture" aplicada à governança distribuída da saúde digital. Como forma de atestar a conformidade com todas as exigências regulatórias, o responsável pela blockchain permissionada emitirá o documento intitulado "Pedigree Certification" (Solanki; Brewster, 2014), que comprovará a regularidade e o devido cuidado com os dados de saúde.

8 LIMITAÇÕES, RISCOS E TENSÕES JURÍDICAS PERSISTENTES

Apesar do potencial da arquitetura distribuída aqui fundamentada, persistem desafios relevantes. Vale dizer que nem todos os riscos e tensões conseguem ser neutralizados.

Primeiro, o FL não elimina completamente os riscos que poderão ser lançados contra a privacidade. Ataques de "inferência reversa" (inferir informações sensíveis de forma genérica), de "model inversion" (buscam reconstruir atributos ou dados utilizados no treinamento do modelo) e de "membership inference" (buscam identificar se determinada pessoa integrou o conjunto de treinamento, gerando riscos relevantes à privacidade em contextos de saúde) são desafios importantes (Almutairi; Barnawi, 2023; Gosselin; Vieu; Loukil et al. 2022; Shokri; Stronati; Song et al, 2017).

Em segundo lugar, a blockchain permanece tecnologicamente e juridicamente complexa. Mesmo em redes permissionadas, como é o caso deste estudo, persistem problemas relacionados à governança institucional, à definição de responsabilidades, à gestão de chaves criptográficas, à interoperabilidade regulatória e à escalabilidade (Zhu; Bo; Peng, 2026; De Filippi; Mannan; Reijers, 2020). A questão que fica é: quem regula o funcionamento da blockchain?

Terceiro, a fragmentação regulatória internacional continua a gerar insegurança jurídica. Os standards da GS1, com sua arquitetura voltada a dados de saúde, visam superar esses desafios. Isso está explicitamente contido no "The GS1 Healthcare Strategy 2023-2027": "[...] C. [...] A implementação globalmente integrada dos padrões GS1 para compartilhamento de dados continua sendo a meta ambiciosa da GS1. Na prática, os sistemas de gerenciamento de dados para rastreabilidade são baseados em diferentes requisitos regulatórios, tanto regionais quanto nacionais. Como resultado, o foco da GS1 Healthcare é garantir que os padrões GS1 para compartilhamento de dados sejam utilizados para apoiar a implementação desses requisitos regionais/nacionais e permitir a interoperabilidade entre esses sistemas regionais/nacionais" (2022, p. 20).

A partir do positivismo jurídico, notadamente da perspectiva legalista, parte-se do pressuposto de que cada país cria seu próprio marco regulatório, adequado a uma época em que a globalização das relações socio-político-econômicas ainda era fraca. Observa-se, nos últimos anos, o aprofundamento de um novo processo em que o nacional e o global se interconectam, seja de modo físico, seja de modo digital, com ênfase nesse último: a digitalização de tudo. Nesse ambiente, diferente das possibilidades da vertente positivista-legalista, analisa-se o incremento da emergência de "regimes jurídicos globais", estruturados como conjuntos de princípios, regras, normas técnicas e processos decisórios, além de outros conceitos e estruturas alternativos, dos quais decorrem expectativas de ação em âmbitos funcionais predeterminados (Engelmann, 2023; 2022). Esse conjunto compreende muito mais do que apenas organizações formais, contratos e redes; representa "conjuntos de arranjos de governo", ou seja, redes de regras, normas e procedimentos que regulamentam o comportamento e controlam seus efeitos (Teubner, 2016, p. 116-118).

O conjunto normativo assim identificado não opera na lógica do "comando e controle", mas sim a partir de movimentos e mecanismos de governança, nos quais esses "arranjos de governo" se organizam com base em elementos estruturantes próprios da governança, tipicamente de coordenação e não de subordinação, como se observa nos modelos legislativos estatais. Ao lado dos modelos normativos mencionados, juntam-se também os códigos corporativos de conduta, os "corporate codes" (Teubner, 2016, p. 98). Esse é o movimento que fragmenta o arcabouço jurídico tradicional, evidenciando a incapacidade de um modelo regulatório, dada a sua centralidade nas questões de cada país (Engelmann, 2023).

Embora o modelo proposto reduza a necessidade de transferência massiva de dados, não elimina completamente os conflitos jurisdicionais. Além disso, "trusted infrastructures" podem gerar novas formas de concentração de poder tecnológico. Grandes provedores de infraestrutura computacional, de "cloud computing" e de IA continuam exercendo forte influência estrutural sobre os ecossistemas digitais globais (Alston; Law; Murtazashvili et al, 2022). De qualquer forma, os avanços na infraestrutura computacional não substituem completamente as instituições democráticas, a supervisão humana e os direitos fundamentais. Aqui

poderiam ainda ser agregados os direitos naturais, humanos e fundamentais (Engelmann, 2009), considerados um conjunto de direitos que qualificam qualquer desenvolvimento tecnológico. Por isso, são fundamentais e imprescindíveis, independentemente da denominação que possam receber; a centralidade da pessoa e sua proteção são o principal objetivo de cada categoria. Por isso, devem ser consideradas um grande conjunto, com denominações que variam de época para época e que promoveram o seu desenvolvimento estruturante.

9 CONSIDERAÇÕES FINAIS

As arquiteturas distribuídas devem ser compreendidas como instrumentos complementares de governança, e não como substitutos integrais da regulação jurídica. Os desenvolvimentos regulatórios estão passando por mudanças estruturais, especialmente quando aplicados a diversas tecnologias, como a IA e a blockchain. Nesses cenários, abrem-se várias possibilidades para pesquisas futuras. A transformação contemporânea da governança global de dados exige novas formas de coordenação regulatória capazes de conciliar a inovação tecnológica, a proteção de direitos naturais, humanos e fundamentais e a soberania digital (Engelmann, 2009).

Este artigo partiu da hipótese de que a combinação entre FL, blockchain permissionada e standards globais de interoperabilidade (standards GS1 - About, 2022) pode constituir uma nova geração de infraestruturas regulatórias computacionais capazes de operacionalizar uma governança transnacional de dados de saúde baseada em coordenação distribuída, soberania digital e "compliance by architecture", implementada por meio de mecanismos de "compliance/privacy/security by design". Dentro desse panorama, o argumento central desenvolvido foi que essas arquiteturas permitem um deslocamento paradigmático: de modelos baseados na transferência internacional massiva de dados sobre a saúde para modelos apoiados na coordenação distribuída de aprendizado e na interoperabilidade regulatória.

O FL reduz a necessidade de centralização de dados e fortalece a compatibilidade com os princípios de "minimização de dados", "privacy by

design" e "accountability". Com isso, atende-se às determinações contidas na GDPR, na LGPD e na HIPAA, que constituem as estruturas regulatórias abordadas no estudo. A blockchain permissionada oferece mecanismos de auditabilidade verificável, além de integridade distribuída e governança institucional compatíveis com esses ambientes regulados. As Guidelines 02/2025 do EDPB reforçam precisamente a necessidade de arquiteturas híbridas, de minimização dos dados "on-chain" e de uma governança institucional robusta.

Os standards da GS1 fornecem uma camada operacional de interoperabilidade global capaz de conectar ecossistemas de saúde e cadeias produtivas. O estudo incluiu uma "certificação de Pedigree", também desenvolvida pela GS1, que comprova a conformidade com os elementos estruturantes do "Legal Protection by Design". Quer-se dizer que a arquitetura digital evidencia a conformidade com o Direito democraticamente instituído, notadamente em suas bases de princípios naturais, humanos e fundamentais. Com isso, a referida certificação promove a harmonização entre a regulação local (nacional) e a global. Ao mesmo tempo, essa certificação preserva as possibilidades de resistência das pessoas afetadas e admite contestação perante instâncias jurídicas, distinguindo-se, assim, da mera tecnorregulação. Outro ponto importante: com a incorporação dessa certificação, abrem-se caminhos para projetar possibilidades de ação compatíveis com valores e princípios jurídicos, rejeitando-se tanto ambientes determinísticos quanto formas invisíveis de regulação e exigindo uma articulação interdisciplinar (e até transdisciplinar) entre a arquitetura tecnológica e a normatividade jurídica (adaptado a partir de: Hildebrandt, 2015, p. 218).

O estudo conclui que a próxima geração de governança internacional de dados tende a tornar-se cada vez mais arquitetural. A conformidade jurídica deixará de depender exclusivamente de contratos, consentimento ou mecanismos tradicionais de transferência internacional de dados e passará a ser parcialmente operacionalizada pela própria infraestrutura computacional. Nesse cenário, emergem as condições para os passos iniciais de um paradigma inovador de soberania digital distribuída, no qual a cooperação internacional e a proteção de direitos naturais, humanos e fundamentais não dependam necessariamente da centralização massiva de dados de saúde, como ocorreu neste estudo.

A pergunta central da governança digital contemporânea deixa de ser "quem possui os dados?" e passa a ser "como coordenar a inteligência coletiva sem dissolver a autonomia institucional, o pluralismo regulatório e os direitos de base (naturais, humanos e fundamentais)?". Aqui, o pluralismo regulatório relaciona-se ao diálogo entre as fontes do Direito, ultrapassando as fontes legislativas, a fim de integrar princípios e padrões técnicos. Essa transição redefine simultaneamente os avanços no uso da IA, a proteção dos dados, especialmente os relacionados à saúde, e a governança transnacional, abrindo possibilidades para a estruturação do constitucionalismo digital.

10 PERSPECTIVAS FUTURAS PARA A PESQUISA

Como segundo momento do modelo apresentado, se deverá colocá-lo em prática, observando os resultados e promovendo os ajustes necessários.

O campo aberto pela pesquisa apresentada neste estudo também evidencia a importância de avançar nas investigações sobre a teoria jurídica que poderá sustentar a constitucionalização digital computacional e a regulação algorítmica. Além disso, a conjugação do EHDS, do AI Act (em revisão), do "Trusted Data Space" e das Guidelines 02/2025, que disciplinam o processamento de dados pessoais por meio de tecnologias de blockchain, abre novos cenários de infraestrutura regulatória.

REFERÊNCIAS

ALEXANDER, X. Francis. Federated Learning for privacy-preserving smart healthcare: an architectural overview. *International Journal of Emerging Trends in Engineering and Technology*, v. 1 Issue 1, p. 1-10, July-September 2025 DOI: https://doi.org/10.64137/IJETET-V1I1P101.

ALMUTAIRI, Suzan; BARNAWI, Ahmed. Federated learning vulnerabilities, threats, and defenses: a systematic review and future directions. *Internet of Things*, v. 24, 2023, 100947. https://doi.org/10.1016/j.iot.2023.100947.

ALSTON, Eric; LAW, Wilson; MURTAZASHVILI, Ilia et al. Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics*, v. 18, p. 707-723, 2022. DOI:10.1017/S174413742100093X.

AMIN, Md Ruhul; AKHTAR, Nahin Akhtar; HOQUE, Md Ekramul et al. Blockchain-Enabled Traceability in Pharmaceutical Supply Chains: An Integrated Engineering and It Management Framework for Regulatory Compliance and Pandemic Resilience. *Journal of Computer Science and Technology Studies*, v. 7, n. 10, 2025, p. 343-356. DOI: 10.32996/jcsts

ANTHONEY, Caitlin. The intersection of GDPR and HIPAA. June 14, 2024. Disponível em: https://www.paubox.com/blog/the-intersection-of-gdpr-and-hipaa. Acesso em 19 maio 2026.

ARABSORKHI, Abouzar; KHAZAEI, Elham. Blockchain Technology and GDPR Compliance: A Comprehensive Applicability Model. *International Journal of Web Research*, v. 7, n. 2, p. 49-63, 2024, doi: http://dx.doi.org/10.22133/ijwr.2024.459490.1221.

AKAVARAM, Sravanthi. Privacy-preserving federated learning for multi-institutional healthcare systems. *World Journal of Advanced Research and Reviews*, v. 26, n. 02, 2025, p. 3263-3272. https://doi.org/10.30574/wjarr.2025.26.2.1921.

AKHMETOV, Adil; LATIF, Zohaib; TYLER, Benjamin et al. Enhancing healthcare data privacy and interoperability with federated learning. *PeerJ Computer Science*, v. 11, e2870, 2025. DOI 10.7717/peerj-cs.2870.

BARBARIA, Sabri; JEMAI, Abderrazak; CEYLAN, Halil İbrahim et al. Advancing Compliance with HIPAA and GDPR in Healthcare: A Blockchain-Based Strategy for Secure Data Exchange in Clinical Research Involving Private Health Information. *Healthcare* (Basel), v. 13, n. 20, 2594, 2025 Oct 15 DOI: 10.3390/healthcare13202594. PMID: 41154272; PMCID: PMC12563691.

BELEN-SAGLAMA, Rahime; ALTUNCUA, Enes; LU, Yang et al. A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, v. 4, 2023, 100129. https://doi.org/10.1016/j.bcra.2023.100129.

BLOCKCHAIN IN HEALTHCARE market size, share, and trends 2026 to 2035. Disponível em: https://www.precedenceresearch.com/blockchain-in-healthcare-market. Acesso em 15 maio 2026.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD).* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14 maio 2026.

BRASIL, 2026. Brasil e União Europeia reconhecem equivalência na proteção de dados. O reconhecimento recíproco fortalece a proteção de dados pessoais, amplia a segurança jurídica e cria um ambiente mais favorável à cooperação, à inovação e aos negócios digitais. Janeiro de 2026. Disponível em:

https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2026/01/brasil-e-uniao-europeia-reconhecem-equivalencia-em-protecao-de-dados-pessoais. Acesso em 16 maio 2026.

COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.

DAYAN, Ittai; ROTH, Holger R.; ZHONG, Aoxiao et al. Federated learning for predicting clinical outcomes in patients with COVID-19. *Nature Medicine*, v. 27, October 2021, p. 1735-1743. https://doi.org/10.1038/s41591-021-01506-3.

De FILIPPI, Primavera; MANNAN, Morshed; REIJERS Wessel. Blockchain as a confidence machine: The problem of trust & challenges of Governance. *Technology in Society*, v. 62, 2020, 101284. https://doi.org/10.1016/j.techsoc.2020.101284.

DE GREGORIO, Giovanni. The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, v. 19, n. 1, 2021, p. 41-70. Oxford University Press and New York University School of Law doi:10.1093/icon/moab001.

DIGITAL ECONOMY TRENDS 2026. Digital Cooperation Organization (DCO). Disponível em: https://det.dco.org/sites/default/files/2025-12/Digital-Economy-Trends-2026.pdf?token=eDT74_TLWzo3jHMyMf4r7t4KqICGV581eNOsqHKIQdM. Acesso em 14 maio 2026.

ENGELMANN, Wilson. Percursos para inovar a Teoria Geral das Fontes do Direito: modelos de autorregulação regulada para as nanotecnologias, *sandbox* regulatório e princípios. Constituição,

Sistemas Sociais e Hermenêutica [recurso eletrônico]: *Anuário do Programa de Pós-Graduação em Direito da Unisinos*, n. 18. Organizadores: Vichinkeski Teixeira, Lenio Luiz Streck, Leonel Severo Rocha. Blumenau, SC: Editora Dom Modesto, 2022. p. 327-341.

ENGELMANN, Wilson. O constitucionalismo organizacional no cenário do sistema jurídico global e digitalizado. Constituição, Sistemas Sociais e Hermenêutica [recurso eletrônico]: *Anuário do Programa de Pós-Graduação em Direito da Unisinos*, n. 19. Organizadores: Vichinkeski Teixeira, Lenio Luiz Streck, Leonel Severo Rocha. Blumenau, SC: Editora Dom Modesto, 2023. p. 337-348.

ENGELMANN, Wilson. A origem jusnaturalista dos direitos humanos: o horizonte histórico da Declaração Universal dos Direitos Humanos de 1948. Artigo apresentado no *CONPEDI - Conselho Nacional de Pesquisa e Pós-Graduação em Direito*, em julho de 2009, p. 6309-6327.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on processing of personal data through blockchain Technologies*, Version 1.1, Adopted on 08 April 2025. Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en. Acesso em 15 maio 2026.

EUROPEAN DATA PROTECTION BOARD (EDPB). Summary: Use of blockchains: how to protect individual's personal data, May 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-05/edpb-summary-022025-blockchains_en.pdf. Acesso em 15 maio 2026.

GOSSELIN, Rémi; VIEU, Loïc; LOUKIL, Faiza et al. Privacy and Security in Federated Learning: A Survey. *Applied Sciences*, v. 12, n. 19, 2022, 9901. https://doi.org/10.3390/app12199901.

GS1 - About. 2022. Disponível em: https://www.gs1.org/about. Acesso em 15 maio 2026.

GS1 Style Guide. Sets rules and conventions for gramatical style, naming conventions, figure and table use etc. to improve the quality and consistency of all GS1 documents. Release 5.6, Approved, Jul 2025. Disponível em: https://www.gs1.org/standards/gs1-style-guide/current-standard. Acesso em 15 maio 2026.

GS1 Healthcare Strategy 2023-2027. Disponível em: https://www.gs1.org/industries/healthcare/strategy. Acesso em 15 maio 2026.

GS1 CBV - Core Business Vocabulary Standard: specifies the structure of vocabularies and specific values for the vocabulary elements to be utilised in conjunction with the GS1 EPCIS standard. Release 2.0, Ratified, Jun 2022. Disponível em: https://ref.gs1.org/standards/cbv/. Acesso em 14 maio 2026.

GS1 Traceability. 2022. Disponível em: https://www.gs1.org/standards/traceability. Acesso em 15 maio 2026.

GS1 Blockchain. 2022. Disponível em: https://www.gs1.org/node/4261. Acesso em 15 maio 2026.

GS1 - EPCIS and CBV Implementation Guideline: Using EPCIS & CBV to increase supply chain visibility, Release 2.0, Ratified, Mar 2023. Disponível em: https://ref.gs1.org/guidelines/epcis-cbv/2.0.0/. Acesso em 18 maio 2026.

GS1 - Core Business Vocabulary (CBV): Standard specifies the structure of vocabularies and specific values for the vocabulary elements to be utilised in conjunction with the GS1 EPCIS standard, Release 2.0, Ratified, Jun 2022. Disponível em: https://ref.gs1.org/standards/cbv/. Acesso em 18 maio 2026.

GS1 - Pedigree Standard, 2007. Disponível em: https://www.gs1.org/standards/pedigree-standard/1; https://www.gs1.org/sites/default/files/docs/epc/pedigree_1_0-standard-20070105.pdf. Acesso em 18 maio 2026.

GS1 - Global Traceability standard: GS1's framework for the design of interoperable Traceability systems for supply chains. Release 2.0, Ratified, Aug. 2017. Disponível em: https://www.gs1.org/standards/gs1-global-traceability-standard/current-standard#1-Introduction+1-2-Scope. Acesso em 18 maio 2026.

HABU, Jamilu; DHABARIYA, Ajay Singh; LAL PAL, Bachcha et al. Decentralized Data Governance and Regulatory Compliance in Federated Learning and Edge Computing for Healthcare. *Research Square*, 09 May 2025. DOI: https://doi.org/10.21203/rs.3.rs-6295183/v1.

HAQUE, AKM Bahalul; ISLAM, AKM Najmul; HYRYNSALMI, Sami et al. GDPR Compliant Blockchains - A Systematic Literature Review. *IEEE Access,* v. 9, p. 50593-50606, 2021, doi: 10.1109/ACCESS.2021.3069877.

HARIPRIYA, Rahul; KHARE, Nilay; PANDEY, Manish. Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Nature Scientific Reports*, v. 15, 2025, 12482. https://doi.org/10.1038/s41598-025-97565-4.

HILDEBRANDT, Mireille. *Smart Technologies and the End(s) of Law*: Novel Entanglements of Law and Technology. Massachusetts, USA: Edward Elgar Publishing, Inc. 2015.

HILDEBRANDT, Mireille. Law as computation in the era of artificial legal intelligence: speaking law to the power of statistics. *University of Toronto Law Journal*, v. 68, Supplement 1, January 2018, p. 12-35. DOI 10.3138/utlj.2017-0044.

HILDEBRANDT, Mireille. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press, 2020.

HIPAA - Health Insurance Portability and Accountability Act of 1996, 2024. Disponível em: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html. Acesso em 14 maio 2026.

HIPAA Security Rule, 2024. Disponível em: https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html. Acesso em 20 maio 2026.

ISSA, Wael; MOUSTAFA, Nour; TURNBULL, Benjamin et al. Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey. *ACM Comput. Surv.*, v. 55, n. 9, Article 191, (January 2023). https://doi.org/10.1145/3560816.

J., Andrew; ISRAVEL, Deva Priya; SAGAYAM, K. Martin et al. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, v. 215, 2023, 103633. https://doi.org/10.1016/j.jnca.2023.103633.

KAIROUZ, Peter; McMAHAN, H. Brendan; AVENT, Brendan et al. Advances and Open Problems in Federated Learning.

Foundations and Trends in Machine Learning, v. 14, Issue 1-2, Jun. 2021, p. 1-210. DOI https://doi.org/10.1561/2200000083.

KOSTICK-QUENET, Kristin M.; COMPAGNUCCI, Marcelo Corrales; ABOY, Mateo et al. Patient-centric federated learning: automating meaningful consent to health data sharing with smart contracts. *Journal of Law and the Biosciences*, v. 12, n. 1, lsaf003. Published 2025 Apr 30. DOI:10.1093/jlb/lsaf003.

LI, Ming; XU, Pengcheng; HU, Junjie et al. From challenges and pitfalls to recommendations and opportunities: Implementing federated learning in healthcare. *Medical Image Analysis*, v. 101, 2025,103497, https://doi.org/10.1016/j.media.2025.103497.

LUO, Zhaoyang. AI-Enhanced Federated Learning Framework for Privacy-Preserving Healthcare Data Analytics: A Multi-Institutional Approach. *Journal of Advanced Computing Systems*, v. 6, n. 1, p. 61-79, January 2026. DOI: 10.69987/JACS.2026.60105.

MAYER, André Henrique; COSTA, Cristiano André; RIGHI, Rodrigo da Rosa. Electronic health records in a Blockchain: a systematic review. *Health Informatics Journal*, v. 26, n. 2, p. 1273-1288, 2020. DOI: 10.1177/1460458219866350.

NGUYEN, Thanh Tuan; BEKRAR, Abdelghani; LE, Thi Muoi et al. Federated Learning-Based Framework: A New Paradigm Proposed for Supply Chain Risk Management. *Engineering Proceedings*, v. 97, n. 1, 5, 2025. https://doi.org/10.3390/engproc2025097005.

OECD. *The OECD Going Digital Integrated Policy Framework 2026*: OECD Digital Economy Papers, March 2026, n. 381. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports

/2026/03/the-oecd-going-digital-integrated-policy-framework-2026_f24b6963/0254ae07-en.pdf. Acesso em 14 maio 2026.

OECD. *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019. https://doi.org/10.1787/eedfee77-en.

OLADEJO, Adedeji Ojo; ADEBAYO, Motunrayo; OLUFEMI, David et al. Privacy-Aware AI in cloud-telecom convergence: A federated learning framework for secure data sharing. *International Journal of Science and Research Archive*, v. 15, n. 1, 2025, p. 005-022. DOI: https://doi.org/10.30574/ijsra.2025.15.1.0940.

OLIOT - Open Source Project, 2026. Disponível em: https://gs1oliot.github.io/oliot/. Acesso em 18 maio 2026.

PATI, Sarthak; KUMAR, Sourav; VARMA, Amokh et al. Privacy preservation for federated learning in health care. *Patterns*, v. 5, Issue 7, 2024,100974, https://doi.org/10.1016/j.patter.2024.100974.

RAM, Niranjan; MAHAJON, Bidhan; DEOGADE, Meena Shamrao. From field to formulation: Designing a conceptual AI-integrated digital passport framework for medicinal plant traceability and quality assurance in Ayush supply chains. *International Journal of Ayurveda Research*, v. 7, n. 1, p. 82-92, Jan-Mar. 2026. DOI: 10.4103/ijar.ijar_300_25.

REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 14 maio 2026.

REGULATION (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) n. 300/2008, (EU) n. 167/2013, (EU) n. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689. Acesso em 14 maio 2026.

REGULATION (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, 2025. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500327. Acesso em 14 maio 2026.

REGULATION (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868. Acesso em 16 maio 2026.

REGULATION (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Disponível em: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng. Acesso em 16 maio 2026.

RIEKE, Nicola; HANCOX, Jonny; LI, Wengi et al. The future of digital health with federated learning. *NPJ Digital Medicine*, v. 3,

Article number 119, 2020. https://doi.org/10.1038/s41746-020-00323-1.

SAJADIEH, Sha; FATTORINI, Loredana; PERRAULT, Raymond et al. *The AI Index 2026 Annual Report*, AI Index Steering Committee, Institute for Human-Centered AI. Stanford, CA: Stanford University, April 2026. Disponível em: https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf. Acesso em 20 maio 2026.

SHAHSAVARI, Yahya; BASERI, Yaser; HAFID, Abdelhakim et al. Integration of Federated Learning and Blockchain in Healthcare: A Tutorial on Medical Data, Architectures, Privacy, Security, and Regulatory Compliance. *Journal of Medical Internet Research*. 20/01/2026:80178. DOI: 10.2196/80178.

SMIETANKA, Malgorzata; PITHADIA, Hirsh; TRELEAVEN, Philip. Federated Learning for Privacy-preserving data access. (September 15, 2020). Available at *SSRN*: https://ssrn.com/abstract=3696609 or http://dx.doi.org/10.2139/ssrn.3696609

SHOKRI, Reza; STRONATI, Marco; SONG, Congzheng et al. Membership Inference Attacks Against Machine Learning Models. *ArXiv*, 2017. https://doi.org/10.48550/arXiv.1610.05820.

SOLANKI, Monika; BREWSTER, Christopher. Detecting EPCIS exceptions in linked traceability streams across supply chain business processes. *SEM '14: Proceedings of the 10th International Conference on Semantic Systems*, p. 24-33, September 2014. https://doi.org/10.1145/2660517.2660524. Disponível em: https://www.cbrewster.com/papers/Solanki_ECWEB14.pdf. Acesso em 05 maio 2026.

SOLANKI, Monika; BREWSTER, Christopher. OntoPedigree: Modeling Pedigrees for traceability in supply chains. *Semantic Web 1* (2009), p. 1-10, 1, IOS Press. https://www.semantic-web-journal.net/system/files/swj980.pdf. Acesso em 05 maio 2026.

SUM, Anika Saba Ibte; PRITEE, Zinniya Taffannum; SAHA, Anik Kumar et al. A systematic review on privacy preservation in federated learning. *International Journal of Information Security*, v. 25, 2026, 65. https://doi.org/10.1007/s10207-026-01229-x.

TEUBNER, Gunther. *Fragmentos constitucionais*: constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

THE GS1 HEALTHCARE STRATEGY 2023-2027. November 2022. Disponível em: https://www.gs1.org/docs/healthcare/Strategy/GS1-Healthcare-Strategy-Final.pdf. Acesso em 18 maio 2026.

UNIDO - United Nations Industrial Development Organization. *UNIDO showcases the power of standards for sustainable industrial growth*, 14 October 2025. Disponível em: https://www.unido.org/news/unido-showcases-power-standards-sustainable-industrial-growth. Acesso em 15 maio 2026.

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

ZEKIYE, Abdulrezzak; ÖZKASAP, Öznur. Decentralized Healthcare Systems with Federated Learning and Blockchain. *Proceedings of 14th Turkish Congress of Medical Informatics*, p. 335-339, 2023. DOI: 10.48550/arXiv.2306.17188.

ZHU, Lingzi; BO, Zhao; PENG, Rao. Blockchain-Enabled Federated Learning: A Survey on System Design, Key Challenges, and Future Directions. *Electronics*, v. 15, n. 8, 1572, 2026. https://doi.org/10.3390/electronics15081572.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, v. 30, 2015, p. 75-89.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019.

WORLD BANK. *World Development Report 2025*: Standards for Development. World Bank, 2025. doi:10.1596/978-1-4648-2275-9.