

2º CICLO DE ESTUDOS EM DIREITO

ÁREA DE ESPECIALIZAÇÃO EM CIÊNCIAS JURÍDICO-POLÍTICAS

A relação dual entre as tecnologias de registo distribuído e o regime da proteção de dados na União Europeia

Marjorie Ninno de Carvalho Campos

M

2025



ABREVIATURAS E ACRÓNIMOS

AEPD - *Agencia Española de Protección de Datos*

ARF - *Architecture and Reference Framework*

BC4EU - *Blockchain for Europe*

Cfr. - conferir

CNIL - *Commission Nationale de l'Informatique et des Libertés*

DLT(s) - Tecnologia(s) de registo distribuído

EBP - *European Blockchain Partnership*

EDPB - Comité Europeu para a Proteção de Dados

EDPS - *European Data Protection Supervisor*

eIDAS / eIDAS 2 - Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 / Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de abril de 2024

EPRS - *European Parliamentary Research Service*

EUCI - *European Crypto Initiative*

EUDIW - Carteira Europeia de Identidade Digital

ICO - *Information Commissioner's Office*

INATBA - *International Association for Trusted Blockchain Applications*

p. / pp. - página / páginas

P2P - *Peer-to-peer*

PETs - *Privacy enhancing technology*

RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016

SSI(s) - Identidade(s) Auto-Soberana(s)

sec. / secs. - seção / seções

ss. - seguintes

UE - União Europeia

vol. - volume

W3C - *World Wide Web Consortium*

ZKP(s) - Prova(s) de conhecimento zero

ÍNDICE

RESUMO/ABSTRACT	03
INTRODUÇÃO	04
PARTE I - A INCIDÊNCIA DO RGPD SOBRE DLT	08
1. Conceitos relevantes: DLT e <i>blockchain</i>	08
2. A dificuldade de identificação do responsável pelo tratamento e subcontratantes	12
3. O direito ao apagamento	18
4. As <i>Guidelines</i> 02/2025 do EDPB	21
PARTE II - CONVERGÊNCIA ENTRE DLT E O RGPD	28
1. Respostas aos desafios de conformidade	28
2. <i>Blockchains</i> como um possível instrumento de harmonização com o RGPD	30
3. Identidades descentralizadas e SSI	32
4. Carteiras de identidade digital	33
4.1. A EUDIW	35
4.1.1. Arquitetura técnica da EUDIW	37
4.1.2. Intersecção com outras iniciativas europeias relevantes	40
4.1.3. A EUDIW e o RGPD: convergência normativa	43
CONCLUSÕES	50
BIBLIOGRAFIA	51

RESUMO

O presente estudo analisa algumas das principais tensões e os movimentos de convergência entre DLT (em especial, *blockchains*) e o regime proposto pelo RGPD, refletindo sobre a possibilidade de compatibilização entre arquiteturas descentralizadas e os princípios e normas do regulamento, como o da responsabilidade e o direito ao apagamento. Através da avaliação normativa, jurisprudencial, doutrinária e incluindo designações técnicas essenciais, são apresentados os desafios relacionados às características inerentes a tais infraestruturas na aplicação do diploma, propondo-se a harmonização entre ambos por via de soluções técnicas e jurídicas que reconheçam as especificidades e o potencial da DLT. Discorre-se acerca da utilização da tecnologia no contexto de identidades digitais, especialmente a EUDIW, como um exemplo de concepção de um ecossistema que promove o uso responsável e juridicamente viável de *blockchains* em conformidade com o direito à proteção de dados pessoais.

Palavras-chave: *blockchain*; DLT; Regulamento Geral sobre a Proteção de Dados; direito ao apagamento; princípio da responsabilidade; SSI; Carteira Europeia de Identidade Digital.

ABSTRACT

This study analyses some of the main tensions and convergence flows between DLT (particularly blockchains) and the framework proposed by the GDPR, reflecting on the possibility of reconciling decentralised architectures with the principles and rules of the regulation, such as the accountability principle and the right to erasure. Through normative, jurisprudential, and doctrinal analysis, including essential technical designations, it presents the challenges arising from the inherent characteristics of such infrastructures when applying the GDPR, and proposes harmonisation through technical and legal solutions that acknowledge the specificities and potential of DLT. The study also addresses the use of such technology in the context of digital identities, particularly the EUDIW, as an example of an ecosystem design that promotes the responsible and legally viable use of blockchains in accordance with the right to personal data protection.

Keywords: blockchain; DLT; General Data Protection Regulation; right to erasure; accountability principle; SSI; EU Digital Identity Wallet.

INTRODUÇÃO

Desempenhando um papel essencial na geração de conhecimento e aumento da produtividade, os dados tornaram-se centrais para a inovação e o crescimento económico¹. Diversas disciplinas viram-se profundamente impactadas pelo avanço tecnológico das últimas décadas e a disseminação da internet, acrescentada à informatização da sociedade, provocou transformações significativas na produção e acesso a dados, tornando-os omnipresentes no cotidiano, gerando novas oportunidades, mas também desafios atinentes à governança e ao uso responsável de informações². Apontada com frequência como transformadora, com potencial para remodelar significativamente processos económicos e sociais, a *blockchain*, tipologia máxima da DLT, desenvolveu-se incorporando funcionalidades cada vez mais complexas³. Com uma estrutura distribuída e resistente à manipulação, mostra-se como uma solução atrativa para o reforço da cibersegurança e integridade de dados, podendo incorporar certos mecanismos de privacidade⁴. Entretanto, a sua adoção exponencial suscita tensões regulatórias, nomeadamente o aparente conflito com determinados princípios e regras presentes no RGPD, motivando intenso diálogo entre investigadores, utilizadores e decisores políticos a fim de analisar a conformidade da infraestrutura com o quadro normativo vigente em matéria de proteção de dados pessoais⁵.

Esse sistema regulatório tem como principal diploma o RGPD pelo que é o presente diploma que este trabalho terá como parâmetro principal no que toca ao regime de proteção de dados pessoais desenhado no contexto europeu. O instrumento normativo mencionado visa

¹CONG, Lin William; XIE, Danxia; ZHANG, Longtian. *Knowledge Accumulation, Privacy, and Growth in a Data Economy*. *Management Science*, v. 67, n. 10, p. 6480–6492, 2021. Disponível em: <https://arxiv.org/pdf/2109.10028>. Acesso em: 16 jul. 2025. Sec. 1.

²Cfr. EMMERT-STREIB, Frank. *From the digital data revolution to digital health and digital economy toward a digital society: Pervasiveness of Artificial Intelligence* [em linha]. 26 ago. 2020. Disponível em: <https://arxiv.org/abs/2008.12672>. Acesso em: 16 jul. 2025. Sec. 1.

³Com Ethereum, por exemplo, vimos o surgimento de contratos inteligentes, abordados em momento posterior neste estudo.

⁴PUTHAL, D.; MALIK, N.; MOHANTY, S. P.; KOUGIANOS, E.; YANG, C. *The Blockchain as a Decentralized Security Framework [Future Directions]*. *IEEE Consumer Electronics Magazine*, vol. 7, n.º 2, p. 18–21, mar. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8287055>. Acesso em: 16 jul. 2025.

⁵A literatura especializada tem destacado a tensão entre as exigências do RGPD e *blockchains*, principalmente as de carácter público e não permissionadas. O *EU Blockchain Observatory & Forum* apontou em 2018 que “As *blockchains* públicas não permissionadas representam os maiores desafios em termos de conformidade com o RGPD” (Tradução livre). Apesar de o tema ser constantemente discutido à nível académico, os estudos ainda são limitados em escopo e abrangência, evidenciando sua complexidade e a ausência de consenso sobre soluções jurídicas ou técnicas totalmente satisfatórias. BELEN-SAGLAM, Rahime; ALTUNCU, Enes; LU, Yang; LI, Shujun. *A systematic literature review of the tension between the GDPR and public blockchain systems*. *Blockchain: Research and Applications*, v. 4, n.º 2, 2023. Disponível em: <https://doi.org/10.1016/j.bcr.2023.100129>. Acesso em: 16 jul. 2025. Sec. 1.

fortalecer a proteção dos indivíduos através, por exemplo, da instituição de princípios nucleares⁶, da exigência de bases legais pré-estabelecidas para o processamento⁷ e da promoção do controlo individual sobre os dados por meio de direitos garantidos⁸, definindo o conceito de dados pessoais como “informação relativa a uma pessoa singular identificada ou identificável”, sendo esta considerada o titular⁹. Convém assinalar que dados pseudónimos são ainda qualificados como dados pessoais, visto que apesar de reduzir os riscos de identificação, a técnica difere da anonimização (que ao ser aplicada acaba por excluir os dados anonimizados do escopo do regulamento por não referirem-se à uma pessoa identificável)¹⁰. De igual modo, é fundamental a distinção entre responsável e subcontratante (ou controlador e processador, respetivamente¹¹), definindo não apenas a repartição de responsabilidades mas igualmente determinando perante quem os titulares podem exercer seus direitos¹².

Considera-se como responsável aquele determina os meios e finalidades do tratamento¹³, enquanto os subcontratantes atuam por conta do primeiro, segundo suas instruções, apesar de terem alguma margem para decidir sobre os meios técnicos a

⁶Elencados no artigo 5º do RGPD.

⁷Postuladas no artigo 6º (1) do RGPD.

⁸Ver Capítulo III do RGPD.

⁹Abrange qualquer informação que permita a identificação direta ou indireta do indivíduo, independente da sua natureza. Existem categorias especiais de dados pessoais, elencadas no artigo 9º do RGPD, que englobam, por exemplo, dados biométricos. Para dados pessoais que enquadrem-se nesta categoria, medidas adicionais relativas ao seu processamento são exigidas pelo regulamento, como por exemplo, a necessidade de obtenção de consentimento explícito do titular para uma ou mais finalidades específicas. DIÁRIO DA REPÚBLICA. *Lexionário – dados pessoais*. Disponível em: <https://diariodarepublica.pt/dr/lexionario/termo/dados-pessoais>. Acesso em: 13 jul. 2025.; Cfr. Art. 4º (1) do RGPD.

¹⁰Considerando 26 do RGPD.

¹¹O RGPD utiliza-se da terminologia “responsável pelo tratamento” e “subcontratante”. Porém, neste estudo, utilizaremos também “controlador” e “processador” para referir a tais agentes.

¹²É fundamental uma identificação clara do controlador para a eficácia do sistema proposto no RGPD, pelo que sua própria lógica repousa na existência de um (ou mais) responsáveis que possam cumprir com as obrigações legais inerentes a este papel. De um lado, os titulares precisam saber a quem se dirigir para exercer seus direitos de forma plena e eficaz. De outro, potenciais controladores devem ser capazes de identificar sua condição *ab initio*, pois muitas das obrigações previstas no diploma, como as constantes no artigo 13.º, impõem deveres de informação aquando da coleta dos dados, e não em momento posterior. É ainda mais relevante o dever de transparência quando o tratamento tem como base legal o consentimento, cuja validade depende, segundo o artigo 4.º (11), de ser livre, específico e informado, pelo que a própria jurisprudência europeia reforça essa exigência, como observa-se no caso *Bara*, do qual conclui-se que a falta de informação acaba por comprometer o exercício de direitos fundamentais dos titulares. EPRS. *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (Relatório STOA, PE 634.445), Bruxelas, jul. 2019. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf). Acesso em: 14 jul. 2024. Sec. 4.; TRIBUNAL DE JUSTIÇA (Terceira Secção). *Smaranda Bara e o. v. Președintele Casei Naționale de Asigurări de Sănătate e outros*. Processo C-201/14. 1 out. 2015. ECLI:EU:C:2015:638.

¹³Pessoa singular ou coletiva, pública ou privada, vide artigo 4º (7) RGPD.

empregar¹⁴. Tais conceitos são definidos de forma funcional e autónoma, independentemente da forma contratual adotada, sempre com base nas atividades concretas desempenhadas pelas partes¹⁵. Como será aprofundado adiante, a responsabilidade resulta não apenas de disposições legais, mas também de uma análise factual das relações entre os envolvidos. Quando duas ou mais entidades determinam de forma conjunta as finalidades e os meios do tratamento surge a noção de controladores conjuntos¹⁶, exigindo que estes definam de forma transparente e documentada suas respectivas responsabilidades no cumprimento do regulamento. Uma correta qualificação dos papéis assumidos por cada interveniente no processamento é, portanto, essencial para a efetividade das obrigações previstas no RGPD¹⁷, evitando zonas de incerteza quanto à alocação de responsabilidades¹⁸.

No contexto de tecnologias descentralizadas essa qualificação encontra um desafio adicional: a dificuldade em determinar de forma clara quem são os controladores e processadores, especialmente quando múltiplos atores operam em diferentes camadas técnicas e organizacionais¹⁹, o que dificulta a implementação de políticas de proteção de dados adequadas.

Postulando princípios primordiais que orientam qualquer operação de tratamento de dados pessoais, como o da legalidade, limitação das finalidades, minimização e exatidão dos dados, limitação da conservação, bem como da integridade e confidencialidade²⁰, o

¹⁴Uma operação de tratamento, entretanto, pode não implicar a atuação de um processador, pelo que a existência deste advém de uma decisão do controlador.

¹⁵Um controlador seria, por exemplo, uma corretora de criptomoedas que coleta e gerencia dados de utilizadores com o objetivo de fornecer serviços financeiros, definindo como e por que os dados dos utilizadores são processados. Supondo que a referida corretora utiliza um provedor de identificação e verificação de identidade digital para evitar que a plataforma seja utilizada para fins ilícitos (ainda que tal provedor de serviços processe dados pessoais dos utilizadores da corretora, em nome e sob direção da corretora), o provedor de serviços seria então o processador de acordo com a definição elencada no RGPD. O controlador é portanto quem decide quais dados devem ser coletados e processados, enquanto o processador executa operações conforme as diretrizes fornecidas pelo primeiro.

¹⁶Cfr. Artigo 26º do RGPD. O diploma utiliza a terminologia “responsáveis conjuntos”. Porém, neste estudo utilizaremos também, de forma equivalente, “controladores conjuntos”.

¹⁷De acordo com o princípio da responsabilidade consagrado no artigo 5º (2) do RGPD: o responsável tem de cumprir os princípios previstos no artigo 5º (1) do diploma, e tem o dever de demonstrar concretamente esse cumprimento.

¹⁸A fim de que a cadeia de responsabilidade seja mantida, por exemplo, sempre que um processador pretenda subcontratar outro processador, este geralmente carece do consentimento prévio do controlador. EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Versão 2.1, adotada em 07 jul. 2021. Disponível em:

https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

Acesso em: 16 jul. 2025. *Executive Summary*.

¹⁹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec.4.5.1.

²⁰O da licitude, lealdade e transparência, minimização, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade. Cfr. Artigo 5º do RGPD.

regulamento, quando aplicado no contexto de DLT, devido à imutabilidade estrutural da tecnologia, traz à luz desafios técnicos e jurídicos relevantes, sobretudo quanto à transparência, limitação da finalidade e à possibilidade de correção ou apagamento. Uma análise atenta à arquitetura da rede e repartição de funções entre seus agentes faz-se necessária a fim de garantir a aplicação prática desses princípios em ambientes descentralizados²¹. Relativamente à licitude do tratamento, é indispensável que haja amparo numa das bases legais previstas de forma exaustiva no diploma²².

Desta forma, por exemplo, um banco pode tratar dados de clientes para cumprir exigências legais, com base jurídica numa obrigação legal, enquanto um serviço de *streaming* pode processar informações de utilizadores mediante a execução de um contrato com o titular, ao passo que o consentimento carece de manifestação livre, específica, informada e inequívoca por parte do indivíduo, o que pode levantar questões quanto à sua adequação numa DLT pública²³. Aos titulares são conferidos direitos fundamentais a serem cumpridos pelos controladores, como o direito de acesso, que é um pré-requisito para o exercício dos demais, o de retificação, o de apagamento, o da limitação ao tratamento, o da portabilidade, o de oposição e o de não submeter-se às decisões automatizadas²⁴. Alguns são mais facilmente conciliáveis com arquiteturas descentralizadas enquanto outros exigem adaptações técnicas para garantir a compatibilidade²⁵.

Depreende-se que, embora o RGPD vise a proteção do titular, ele também busca viabilizar a livre circulação de dados no espaço europeu, tornando essencial o equilíbrio entre

²¹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 6.

²²Como o consentimento do titular, a necessidade para execução de um contrato, o cumprimento de uma obrigação legal, o exercício de uma tarefa de interesse público, a proteção de interesses vitais e o interesse legítimo do responsável, desde que não sobreponham-se aos direitos e liberdades fundamentais do titular. A base legal prevista no artigo 6º (1) f) do RGPD é de aplicação flexível mas requer um exame cuidadoso de proporcionalidade e razoabilidade, conforme destacado no Considerando 47 do RGPD. A jurisprudência europeia aparenta reforçar que apenas o interesse económico do controlador não é suficiente para legitimar o tratamento, carecendo de um equilíbrio perante os direitos dos titulares, sendo que é especialmente relevante que este possa razoavelmente esperar esse tratamento aquando da coleta, o que quando aplicado no contexto da DLT pode mostrar-se desafiador. Por exemplo, apesar de um utilizador poder esperar que sua chave pública seja processada quando realiza uma transação de criptoativos, não é provável que tenha plena consciência de que aspetos pessoais rastreáveis possam ser revelados, podendo ser dificultada a aplicação de tal base legal neste contexto. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 6.1.6.

²³Onde o titular geralmente não tem controlo efetivo sobre o tratamento posterior dos dados. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 6.1.1.

²⁴Artigos 16º a 18º e 20º a 22º do RGPD.

²⁵Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 7.

salvaguardas jurídicas e o desenvolvimento de tecnologias emergentes como DLT²⁶. Desta forma, o objeto principal deste estudo é a análise dos movimentos de tensão e convergência entre as figuras. Através de uma análise jurídica com sensibilidade técnico-operacional, avalia-se tanto a arquitetura descentralizada (especialmente *blockchains*) e alguns dos desafios que esta enfrenta perante os marcos tradicionais do regulamento, bem como instrumentos técnicos, jurídicos, e iniciativas concretas com potencial de favorecer uma relação de conformidade, com o objetivo de identificar caminhos possíveis para a harmonização. Argumenta-se que a compatibilização entre DLT e RGPD pode ser atingida por meio de uma leitura funcional e proporcional do quadro normativo em questão, conjugada com soluções técnico-jurídicas emergentes. Na Parte I recorre-se primeiramente à uma contextualização sobre os conceitos técnicos pertinentes, seguida de uma discussão sobre os conflitos entre determinadas exigências do RGPD, especialmente a necessidade de identificação do controlador e do cumprimento efetivo do direito ao apagamento, e as características inerentes à *blockchains*, como a imutabilidade e descentralização. A Parte II culmina na investigação de modelos e iniciativas técnicas e regulatórias que propõem a compatibilidade entre entes dois domínios, destacando-se a EUDIW.

PARTE I - A INCIDÊNCIA DO RGPD SOBRE DLT

1. Conceitos relevantes: DLT e *blockchain*

No sentido de apresentar as principais definições e conceitos técnicos que farão parte deste estudo, clarifica-se que a DLT é uma arquitetura digital destinada ao registo descentralizado de dados que pode exibir diferentes configurações, com estruturas diversas no que toca à sua manutenção²⁷. Geralmente, é formada a partir de protocolos informáticos que operam em redes ausentes de um ponto central de controlo²⁸ e incorpora uma estrutura de base de dados descentralizada responsável pelo armazenamento, validação e acesso a informações²⁹, contendo uma rede de nós onde cada um detém uma cópia sincronizada do

²⁶AMMAR, Zafar. *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways*. Journal of Cybersecurity, 2025, vol. 11, n.º 1. Disponível em: <https://doi.org/10.1093/cybsec/tyaf002>. Acesso em: 13 jul. 2025.

²⁷E variando ao nível de desempenho, escalabilidade, transparência e descentralização.

²⁸SOLTANI, Reza; ZAMAN, Marzia; JOSHI, Rohit; SAMPALLI, Srinivas. *Distributed Ledger Technologies and Their Applications: A Review*. Applied Sciences, 2022. Disponível em: <https://www.mdpi.com/2076-3417/12/15/7898>. Acesso em: 13 jul. 2025. Sec. 2.

²⁹Na prática, há na verdade um surgimento crescente de novos tipos de intermediários, ao invés de observarmos sua diminuição: *exchanges* centralizadas, provedores de carteiras e oráculos ocupam cada vez mais funções

sistema, garantindo a integridade dos dados através de consenso entre seus participantes. Cada nó é livre para operar autonomamente, fortalecendo a resiliência e escalabilidade do sistema, comportando diversas aplicações práticas, como soluções de identidades digitais e criptomoedas³⁰.

O primeiro componente a referir da DLT é a forma como os dados organizam-se e são transmitidos, por meio de um desenho lógico de rede P2P³¹: geralmente não há um administrador central que é responsável por garantir a transferência de dados, já que os servidores (ou nós) estão conectados entre si³². A criptografia, elemento chave neste modelo, e serve tanto para proteção das informações quanto para assegurar a confiabilidade das transações registadas³³. Desta forma, DLT pode ser entendida como “um protocolo digital que possibilita, dentre outras funcionalidades, o registo, armazenamento e o acesso a determinada informação, por intermédio de criptografia, e de maneira descentralizada”³⁴ caracteriza-se por preservar todo o histórico transacional de maneira íntegra. São, portanto, criptograficamente seguras e imutáveis, tornando os dados facilmente verificáveis e reforçando a confiança na integridade do sistema. O registo é compartilhado entre vários nós, pelo que alguns deles mantém uma cópia completa do estado da DLT enquanto outros podem conter apenas uma parte das informações, o que assegura uma maior transparência entre os participantes da rede como um todo e simultaneamente otimiza a eficiência da infraestrutura³⁵.

A própria natureza distribuída da DLT permite o escalonamento da rede por meio da adição de novos servidores, que conforme crescem, movem o sistema cada vez mais no espectro de descentralização. Assim, à medida que o número de nós aumenta, a capacidade de

estratégicas no ecossistema. FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2019. Acesso em: 22 jul. 2025. pp. 18-19.

³⁰ALVES, Alexandre. *O uso de tecnologia de registo distribuído (DLT) na negociação de ações em ambiente de bolsa de valores: análise à luz da legislação do Brasil*. *Revista Eletrônica de Direito*, n.º 2, vol. 31, jun. 2023. Disponível em: https://cij.up.pt/client/files/0000000001/3-alexandre-alves_2164.pdf. Acesso em: 13 jul. 2025. pp. 62-64.

³¹ibidem.

³²Um exemplo familiar e que assenta nessa mesma arquitetura é o Torrent, plataforma de compartilhamento de arquivos digitais que ganhou destaque e notoriedade nos anos 2000.

³³A técnica deriva o seu conceito principal da antiguidade, onde já era possível observar métodos similares. Pode-se citar a Cifra de César como um exemplo, que data dos tempos do Império Romano, na qual as letras de uma determinada palavra eram trocadas por letras que encontravam-se três posições à frente no respetivo alfabeto da época.

³⁴Cfr. ALVES, Alexandre, *O uso de tecnologia de registo distribuído (DLT) na negociação de ações em ambiente de bolsa de valores: análise à luz da legislação do Brasil*, pp. 62 e 65.

³⁵ITU-T. *Distributed ledger technology overview, concepts, ecosystem*. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), *Technical Report FG DLT D1.2*, 1 ago. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf>. Acesso em: 28 jul. 2025. Sec 4.1.

um agente mal-intencionado interferir no mecanismo de consenso utilizado pelo sistema vê-se significativamente reduzida³⁶. As redes *blockchain*, uma das principais categorias de DLT e foco deste estudo, podem ser compostas por nós que armazenam localmente toda a cadeia de blocos, denominados *full nodes*, e por *lightweight nodes*, que dependem dos primeiros para acessar dados completos, sendo que ambos os tipos podem iniciar transações ao transmiti-las para a rede, mas apenas alguns *full nodes*, os mineradores, possuem a função de escrita na cadeia³⁷.

Os mecanismos de consenso³⁸, por sua vez, constituem o conjunto de regras e procedimentos de validação sob o qual continuamente operam as tais redes P2P³⁹. A definição de quem ficará responsável por validar o próximo bloco é um aspeto essencial neste contexto e é precisamente esse processo que ocorre por meio da implementação de um dos diversos mecanismos de consenso disponíveis⁴⁰. Estes podem tomar formas variadas em diferentes sistemas *blockchain*, como o *Proof of Work* (PoW), utilizado pela rede Bitcoin⁴¹. É considerado eficaz um algoritmo de consenso que desempenha um papel essencial na resiliência das redes *blockchain*, assegurando não apenas a coerência entre os dados a serem distribuídos, mas também um funcionamento contínuo e equilibrado de poder computacional entre os nós. Em contrapartida, um algoritmo que compromete gravemente a estabilidade do sistema e torna a rede vulnerável a paralisações em caso de ataque será mal concebido⁴².

A DLT pode apresentar variações relativas às classificações estruturais que impactam diretamente sua governança, privacidade e aplicabilidade jurídica⁴³. Especificamente no

³⁶Ibidem.

³⁷BELEN-SAGLAM, Rahime; ALTUNCU, Enes; LU, Yang; LI, Shujun. *A systematic literature review of the tension between the GDPR and public blockchain systems*, sec. 4.4.1.

³⁸Há diversos mecanismos de consenso que contêm diferenças entre si, apresentando cada um deles tanto vantagens como desvantagens. Um deles, por exemplo, é o proposto por Baird em 2016, denominado *Swirls Hashgraph* que pretendia resolver os problemas de justiça e escalabilidade associados à tecnologia *blockchain*. Cfr. SOLTANI, Reza; ZAMAN, Marzia; JOSHI, Rohit; SAMPALLI, Srinivas. *Distributed Ledger Technologies and Their Applications: A Review*, sec. 2.

³⁹O mecanismo de consenso de uma determinada *blockchain* é geralmente criado pelos programadores. Cfr. BUOCZ, Thomas; EHRKE-RABEL, Tina; HÖDL, Elisabeth; EISENBERGER, Iris, *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, *Computer Law & Security Review*, vol. 35, n.º 3, 2019, pp. 222–235. Disponível em: <https://doi.org/10.1016/j.clsr.2018.12.003>. Acesso em: 14 jul. 2025.

⁴⁰Aquando da implantação (aqui entendida como início da utilização) da rede.

⁴¹As tipologias mais conhecidas são PoW, *Proof of Stake* (PoS) e aqueles baseados em tolerância a falhas bizantinas (*Byzantine Fault Tolerance*). Cfr. ITU-T. *Distributed ledger technology overview, concepts, ecosystem*, sec. 4.3

⁴²HUSSEIN, Z.; SALAMA, M. A.; EL-RAHMAN, S. A., *Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms*, *Cybersecurity*, 2023, vol. 6, art. 30. Disponível em: <https://doi.org/10.1186/s42400-023-00163-y>. Acesso em: 13 jul. 2025.

⁴³A descentralização não é, portanto, atributo intrínseco das *blockchains*, podendo manifestar-se na infraestrutura física ou até mesmo na camada de governança. Redes publicamente reconhecidas como descentralizadas, como

contexto das *blockchains*, a primeira distinção a ser feita refere-se ao acesso à rede, pelo que uma *blockchain* pública é acessível a qualquer participante, enquanto uma privada limita o acesso a um determinado conjunto de utilizadores. As redes permissionadas, que requerem que os participantes obtenham aprovação para interagir ou validar transações, e diferem das não permissionadas, que são de participação aberta e não exigem autorização prévia. Releva mencionar também os modelos federados, onde múltiplas entidades participam do gerenciamento da rede, e *blockchains* de consórcio, operadas por um conjunto limitado e previamente selecionado de organizações consideradas confiáveis⁴⁴.

O ecossistema da DLT engloba diversos componentes interligados⁴⁵ e sua operação pressupõe a utilização de mecanismos criptográficos, pelo que a criptografia assimétrica é central neste contexto: baseia-se em um par de chaves onde a privada atua como assinatura digital do titular enquanto a pública é compartilhada e serve para verificação e identificação. O método permite que a autoria e integridade de uma transação (através da assinatura digital) sejam verificáveis, de modo que apenas o titular legítimo da chave privada poderia assinar a mensagem, sem revelar o conteúdo da transação. É também um exemplo de utilização de ZKP que reforça a privacidade nas interações em redes descentralizadas. As chaves digitais, assinaturas e endereço são, portanto, elementos centrais para a segurança e a confiabilidade das redes DLT.⁴⁶ Outra vertente relevante da tecnologia diz respeito aos contratos inteligentes, que são sistemas automatizados que executam transações digitais com base em regras pré-estabelecidas no próprio código⁴⁷. Servem na garantia de transparência, segurança e eficiência, podendo ajudar a reduzir custos e aumentar a confiabilidade no âmbito das transações digitais⁴⁸.

Bitcoin e Ethereum, não estão imunes a essas dinâmicas, envolvendo em seu desenvolvimento o domínio de poucos agentes. Cfr. FINCK, Michèle. *Blockchain Regulation and Governance in Europe*, p. 19.

⁴⁴Cfr. BELEN-SAGLAM, Rahime; ALTUNCU, Enes; LU, Yang; LI, Shujun. *A systematic literature review of the tension between the GDPR and public blockchain systems*, sec. 4.4.

⁴⁵Como o de hardware e dispositivos como carteiras físicas que asseguram o armazenamento seguro de chaves criptográficas. O de hardware é composto pelos diferentes tipos de nós que operam em rede, mantendo cópias do livro-razão distribuído e validando transações, garantindo descentralização e resiliência. Cfr. ITU-T. *Distributed ledger technology overview, concepts, ecosystem*, sec. 5.

⁴⁶Cfr. ALVES, Alexandre, *O uso de tecnologia de registo distribuído (DLT) na negociação de ações em ambiente de bolsa de valores: análise à luz da legislação do Brasil*, *Revista Eletrônica de Direito*, p. 65.

⁴⁷Estes permitem a configuração, por exemplo, de limites e permissões para transferências de ativos entre diferentes indivíduos, de acordo com critérios lógicos pré-definidos.

⁴⁸A ideia popularizou-se devido ao surgimento da Ethereum em 2015, que passou a fornecer uma plataforma flexível para a criação e execução de tais contratos programáveis, mas foi proposta por Nick Szabo já em 1994. Cfr. ZIBIN ZHENG; XIE, Shaoan; DAI, Hong-Ning; CHEN, Weili; CHEN, Xiangping; WENG, Jian; IMRAN, Muhammad. *An Overview on Smart Contracts: Challenges, Advances and Platforms*, arXiv, dez. 2019. Disponível em: <https://arxiv.org/abs/1912.10370>. Acesso em: 13 jul. 2025.; BUTERIN, Vitalik, *A*

As características e componentes de uma DLT⁴⁹ justificam o fato de a solução ter obtido relevância desde a sua concepção original e ganhado destaque em diversos domínios, como serviços financeiros, cibersegurança⁵⁰ e sistemas focados na saúde⁵¹. Conclui-se, face ao exposto, que um sistema baseado em DLT pode apresentar características de descentralização, desintermediação, ser distribuído, com dados replicados entre vários participantes. É geralmente consistente, à prova de violação e transparente, permitindo diversas implementações distintas a depender do uso concreto, e comportando modificações das características referidas acima, de forma a expandi-las ou restringi-las⁵².

2. A dificuldade de identificação do responsável pelo tratamento e subcontratantes

O regime normativo do RGPD institui um ecossistema jurídico próprio onde o responsável é agente decisor na realização da atividade de tratamento, afetando os titulares diretamente ou através de processadores, refletindo um modelo de governança relacional no qual funções e responsabilidades são claramente atribuídas aos respectivos sujeitos envolvidos⁵³. Parte-se da premissa de que há sempre um responsável pelo tratamento que é identificável, enquanto redes distribuídas geralmente descentralizam essa figura unitária, contendo variados arranjos de governança possíveis e tornando, portanto, complexa a definição de um controlador. Como apontado pelo EPRS, a jurisprudência também contribui

next-generation smart contract and decentralized application platform. White paper, [S. l.], dez. 2013 (atribuído; revisado jan. 2014), 36 p. Disponível em: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf. Acesso em: 22 jul. 2025. p. 1.

⁴⁹Com potencial de oferecer, por exemplo, a desburocratização de processos, uma crescente possibilidade de coordenação entre agências governamentais e fomento do envolvimento de cidadãos e co-produção de serviços públicos. Cfr. CAGIGAS, D.; CLIFTON, J.; DIAZ-FUENTES, D.; FERNÁNDEZ-GUTIÉRREZ, M.; HARPES, C., *Blockchain in government: toward an evaluation framework, Policy Design and Practice*, vol. 6, n.º 4, 2023, p. 397–414. Disponível em: <https://doi.org/10.1080/25741292.2023.2230702>. Acesso em: 13 jul. 2025. sec. 3.3 e 3.4.

⁵⁰ULLAH, H. S.; ASLAM, S., *Blockchain in Healthcare and Medicine: A Contemporary Research of Applications, Challenges, and Future Perspectives*. ArXiv, 2020. Disponível em: <https://arxiv.org/abs/2004.06795>. Acesso em: 13 jul. 2025.

⁵¹GHADI, Y. Y.; MAZHAR, T.; SHAHZAD, T. et al., *The role of blockchain to secure internet of medical things*. *Scientific Reports*, 2024, vol. 14, art. 18422. Disponível em: <https://doi.org/10.1038/s41598-024-68529-x>. Acesso em: 13 jul. 2025.

⁵²EDPB, *Guidelines 02/2025 on processing of personal data through blockchain technologies*. Disponível em: https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf. Acesso em: 12 jul. 2025. p. 5

⁵³PAPAKONSTANTINO, Vagelis; DE HERT, Paul. *The regulation of digital technologies in the EU: the law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality"*. *Technology and Regulation Journal*, maio 2022. Disponível em: SSRN: <https://ssrn.com/abstract=4123313>. Acesso em: 22 jul. 2025. sec. 3.1.

para a insegurança jurídica no que toca à determinação dos responsáveis pelo tratamento em ambientes descentralizados⁵⁴.

O departamento do Parlamento Europeu supramencionado sublinha que identificar antes do início do tratamento de forma clara a figura do controlador é um pressuposto essencial para a efetivação dos direitos dos titulares, visto que o cumprimento de obrigações legais (como os deveres informativos do artigo 13º do RGPD) requer que os possíveis controladores detenham clareza acerca da sua posição antes ou aquando da recolha dos dados, relacionando-se com os princípios de transparência, responsabilidade e legalidade do regime europeu de proteção de dados. A falta ou o fornecimento incorreto de informações por parte do controlador pode inviabilizar o acesso, a retificação e a oposição ao tratamento. Em virtude da centralidade dessas obrigações, a insegurança jurídica respeitante à qualificação dos agentes envolvidos num ecossistema *blockchain* tem o potencial de inviabilizar o cumprimento efetivo e a operacionalização do regulamento, dificultando também a distinção entre responsáveis e subcontratantes em ambientes descentralizados⁵⁵.

Para uma correta identificação da figura do controlador, deve-se proceder sempre a uma abordagem caso a caso, considerando a forma como estrutura-se tecnicamente e governamentalmente o sistema de registo distribuído utilizado. Ainda hoje não há um entendimento uniforme acerca dos papéis que determinados agentes detêm quando fala-se de operações de tratamento de dados pessoais numa *blockchain*, especialmente públicas⁵⁶ e a literatura especializada aponta que não há consenso absoluto sobre quem deve ser considerado controlador neste contexto. Existem, portanto, diferentes interpretações jurídicas acerca da diversidade dos papéis assumidos e uma dificuldade de aplicação de critérios tradicionais, como a determinação dos meios e das finalidades do tratamento, especialmente quando diversos participantes podem exercer influência sobre a operação ou a evolução do sistema⁵⁷.

⁵⁴A relação entre *blockchain* e o RGPD tem sido objeto de diversos debates académicos e institucionais, sobretudo, no que se refere à tensão estrutural entre os princípios e normas do regulamento com os elementos técnicos característicos das redes descentralizadas. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law? Executive summary*.

⁵⁵Mesmo que outra base legal que não o consentimento seja adotada, é mandatório que os titulares tenham acesso às informações exigidas pelos artigos 13º e 14º do RGPD para que possam exercer de forma eficaz os seus direitos. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 4.4.

⁵⁶Como se discutirá acerca do papel dos nós, por exemplo, nas páginas seguintes desta seção.

⁵⁷Discussão que será abordada em maior detalhe também na seção 4 desta Parte I. Ver também: EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 4.3

As orientações do Grupo de Trabalho do Artigo 29º destacam a importância dos “meios efetivos” na análise a ser feita para determinação do responsável pelo tratamento. Esses “meios efetivos” são entendidos como decisões de caráter substancial que integram, portanto, o núcleo essencial do tratamento de dados, ou seja, o “como” do processamento, incluindo, entre outros aspetos, a definição de quais dados serão objeto de tratamento e por quanto tempo. A tomada destas decisões centrais levaria à qualificação como controlador e resultaria na atribuição das respetivas responsabilidades sobre o tratamento. Em contrapartida, as questões técnicas e organizacionais relativas à execução do processamento poderiam ser exclusivamente atribuídas aos processadores⁵⁸. Em redes privadas, é comum a atribuição de decisões quanto aos meios de processamento a uma entidade legal ou consórcio empresarial, enquanto que em *blockchains* públicas é a estrutura de governança em vigor que exerce papel determinante na definição destes meios, onde tais escolhas são distribuídas entre os vários agentes do sistema, não observando-se, por conseguinte, uma entidade única e centralizada que é responsável pelas referidas decisões. Entretanto, a determinação do propósito é o critério principal que qualifica o responsável pelo tratamento de dados pessoais, onde também verifica-se um cenário de considerável fragmentação no contexto das tecnologias de registo distribuído e onde muitos atores distintos têm o potencial de serem considerados como tal⁵⁹.

A CNIL compartilha desta mesma visão e propõe que os participantes da rede que possuem permissão para registar informações nela e decidem fazê-lo com dados pessoais podem, potencialmente, assumir o papel de responsáveis pelo tratamento. A autoridade francesa postula que a qualificação como controlador dependerá da natureza da atuação do agente, pelo que pessoas singulares que processam dados numa *blockchain* com propósito exclusivamente pessoal ou doméstico não se enquadram na definição de responsável. Entretanto, quando a atividade de processamento possui caráter profissional ou comercial, mesmo se realizada por uma pessoa física, esta pode ser qualificada como controlador. Quanto às entidades jurídicas, estas assumem de forma mais óbvia a posição de responsável pelo tratamento. A CNIL postula ainda que quando vários participantes decidem conjuntamente realizar operações de tratamento com uma finalidade comum, estes podem ser considerados

⁵⁸ARTICLE 29 WORKING PARTY. *Opinion 1/2010 on the concepts of “controller” and “processor” (WP 169)*. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em: 14 jul. 2025. p. 14.

⁵⁹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 4.3

responsáveis conjuntos nos termos do artigo 26º do RGPD.⁶⁰ Deste modo, em *blockchains* privadas, não é raro encontrar uma entidade que define os meios e muitas vezes as finalidades do tratamento de dados⁶¹, qualificando-se como responsável, sem prejuízo de que quem mais utilize essa infraestrutura para fins próprios pode ser também considerado um controlador conjunto, entendimento consolidado no caso *Wirtschaftsakademie*⁶².

Quando o titular de dados interage diretamente com a rede, há argumentos para que a determinação dos papéis seja feita ao nível da infraestrutura, pelo que a análise jurídica adequada depende da perspectiva adotada⁶³. Principalmente em *blockchains* públicas, tratando-se de programadores de software, a sua função é geralmente limitada ao fornecimento e manutenção da infraestrutura, sendo estes desprovidos de poder decisivo sobre os fins ou meios concretos envolvidos no tratamento de dados pessoais, o que dificulta a sua qualificação como controladores, visão postulada pelo EPRS e outros autores⁶⁴. Entretanto, os programadores de contratos inteligentes podem, eventualmente, de acordo com a CNIL, serem enquadrados como responsáveis, dependendo do seu grau de envolvimento nas decisões sobre finalidades do tratamento (ou ainda processadores, como discutido abaixo, ou ainda meros provedores)⁶⁵.

Quanto aos nós, a sua tipologia e respetiva função na rede influenciará sua qualificação ou não como responsável⁶⁶. Desta forma, *Lightweight nodes*, por exemplo, na

⁶⁰CNIL. *Blockchain and the GDPR*. Paris: CNIL, 2018. Disponível em: https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf. Acesso em: 14 jul. 2025.

⁶¹Por exemplo, uma empresa que opera a uma rede privada e a utiliza para processamento de dados pessoais de seus clientes.

⁶²TRIBUNAL DE JUSTIÇA (Grande Secção). *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*. Processo C-210/16. 5 jun. 2018. ECLI:EU:C:2018:388.

⁶³A perspectiva adotada tanto pode envolver uma abordagem macro que interpreta o propósito do tratamento como a prestação de um serviço e os meios como relativos ao software utilizado pelos nós e mineradores, quanto uma abordagem micro, que mostra-se mais alinhada com a lógica do RGPD, focando na operação individual de tratamento onde a finalidade é o registo de uma transação específica e o meio é a escolha da plataforma utilizada. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 4.3.3.

⁶⁴Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 4.3.3; e autores como BUOCZ, Thomas; EHRKE-RABEL, Tina; HÖDL, Elisabeth; EISENBERGER, Iris, *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, sec. 5.3.5.

⁶⁵Cfr. CNIL. *Blockchain and the GDPR*.

⁶⁶Cf. TATAR, U.; GÖKÇE, Y.; NUSSBAUM, B., *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, *Computer Law & Security Review*, vol. 38, 2020, art. 105454. Disponível em: <https://doi.org/10.1016/j.clsr.2020.105454>. Acesso em: 25 jul. 2025. sec. 4.3. Os autores sustentam que, em certo sentido, “o que a UE considera um controlador de dados — uma pessoa ou organização confiável responsável pelos dados — é substituído pela arquitetura (código computacional) e pela matemática (criptografia) numa blockchain. Embora o código e a matemática possam ser mais confiáveis do que os controladores de dados terceirizados tradicionais em muitos aspetos, eles são menos humanos, menos responsáveis e menos flexíveis do que a variedade humana ou organizacional.” Tradução livre.

rede Bitcoin, geralmente carecem dos poderes de decisão relativamente aos meios e finalidades do tratamento, não enquadrando-se na definição de controladores. Os mineradores, no mesmo sentido, com frequência apenas procedem à validação técnica de transações, não determinando finalidades ou meios de processamento, posição defendida por diversos autores, visão suportada pela CNIL e pelo EPRS, entre outros autores⁶⁷. No que toca a *full nodes* há posições divergentes na doutrina que, por um lado, reconhece que estes não possuem capacidade unilateral de alteração do protocolo ou de escolha por um protocolo distintos, não possuindo as características de um responsável e, por outro lado, dependendo da percentagem de poder que detém sobre a rede, poderiam ser qualificados como controladores conjuntos. Há autores que defendem que, no contexto de redes públicas, todos os nós seriam qualificados como controladores, seja de forma individual ou coletiva, mas tal interpretação sofre críticas ao pressupor uma coordenação formal entre os nós quanto às finalidades e meios de tratamento, inexistente em *blockchains* públicas onde estes agentes não são, por exemplo, identificados previamente⁶⁸.

Múltiplos autores defendem que os utilizadores de *blockchains* tem o potencial de serem qualificados como responsáveis ao decidirem quais informações incluir numa determinada transação. A hipótese suscita questões relevantes, pois os utilizadores podem ser controladores e titulares de dados de forma simultânea, tornando certas obrigações do RGPD inócuas, ao mesmo tempo que levanta questões à volta da aplicabilidade da exceção doméstica elencada no artigo 2º do regulamento, cenário improvável quando trata-se de uma rede pública visto que neste caso os dados pessoais seriam compartilhados com um número indefinido de pessoas, visão postulada pelo EPRS⁶⁹.

Outro grupo de atores com potencial para serem considerado controladores são as aplicações. Com o desenvolvimento da tecnologia no contexto de *blockchains*, observou-se a formação de ecossistemas em camada, onde a rede é apenas a infraestrutura subjacente de tais aplicações que tem o poder de definir de forma autónoma os meios e as finalidades do

⁶⁷Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 4.3.3; CNIL, *Blockchain and the GDPR*; BUOCZ, Thomas; EHRKE-RABEL, Tina; HÖDL, Elisabeth; EISENBERGER, Iris. *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, sec. 5.3.4.

⁶⁸Esta é a visão, por exemplo, defendida em BUOCZ, Thomas; EHRKE-RABEL, Tina; HÖDL, Elisabeth; EISENBERGER, Iris. *Bitcoin and the GDPR: Allocating responsibility in distributed networks*. secs. 6., 4.4.1.2. e 4.4.1.3.

⁶⁹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 4.3.3;

tratamento. Desta forma, como refere o EPRS, a entidade responsável pela aplicação, por exemplo, uma carteira digital, tem o potencial de enquadrar-se na definição do artigo 4º (7) do RGPD. Pelo referido supra, infere-se que diversos agentes podem exercer influência no processamento⁷⁰, mesmo que de forma limitada, levando à situações onde um controlador é juridicamente responsável ao mesmo tempo que não possui controlo suficiente para cumprir suas obrigações, como a garantia de acesso e portabilidade dos dados. Ao mesmo tempo, a qualificação como responsável no contexto de tecnologias *blockchain* implica obrigações substanciais sob o RGPD, pelo que tal desalinhamento entre responsabilidade e controlo pode suscitar questionamentos relativos à aplicação do regulamento⁷¹, sendo de toda forma, essencial distribuir a responsabilidade em contextos descentralizados a fim de que os direitos dos titulares sejam garantidos, como sublinhado pelo Grupo de Trabalho do Artigo 29º⁷².

Uma análise caso a caso também é exigida para identificação do processador no contexto de operações de tratamento de dados no âmbito de uma *blockchain*. Em determinados casos, por exemplo, desde que a rede seja utilizada de acordo com as instruções do responsável, é possível que um prestador de serviço externo seja qualificado como processador se o respetivo controlador recorrer à sua infraestrutura para o processamento de dados pessoais, limitando-se a executar as operações, ausente de poder decisório autónomo sobre os elementos essenciais do tratamento, sem prejuízo de alguns atores poderem exercer ambas funções. Outros exemplos de processadores podem incluir prestadores de serviços de nuvem, empresas que oferecem *blockchain* como serviço (BaaS), e plataformas de *software as a service* (SaaS). Deve-se considerar que, de qualquer modo, para a identificação clara de quem atua como tal, é necessário estabelecer anteriormente e com precisão quem é o controlador em cada caso concreto, o que pode revelar-se, como abordado supra, complexo em arquiteturas descentralizadas, principalmente as públicas.

Dependendo do desenho, operadores de uma infraestrutura podem deixar de atuar como simples intermediários, assumindo a posição de controladores, especialmente quando plataformas ou aplicações externas operam sobre a *blockchain*, exercendo controlo de forma dominante sobre os meios e finalidades do tratamento. Desta forma, a fronteira entre controladores e processadores inseridos em tal estrutura exige uma sensibilidade à

⁷⁰Por exemplo, os programadores de contratos inteligentes ou as aplicações.

⁷¹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* secs. sec. 4.3.1. e 4.5.1.

⁷²Cfr. ARTICLE 29 WORKING PARTY. *Opinion 1/2010 on the concepts of “controller” and “processor”*, p. 1.

multiplicidade de modelos operacionais possíveis e um exame técnico-jurídico detalhado⁷³. Por exemplo, a CNIL defende que um programador de contratos inteligentes que processa dados pessoais em nome de um controlador pode ser considerado processador, assim como mineradores, em algumas circunstâncias⁷⁴, sobretudo em *blockchains* privadas e permissionadas. Entretanto, em redes públicas tal qualificação é mais controversa, devido à dificuldade de cumprir as inerentes obrigações, como por exemplo, a celebração de contratos conforme o artigo 28º do RGPD⁷⁵.

Do exposto pode-se compreender que uma adequada identificação de quem é considerado como responsável pelo tratamento, principalmente em contextos ausente de intermediários ou entidades centrais, como ocorre em principalmente em *blockchains* públicas, é um dos grandes desafios relevantes no contexto aqui apresentado. Ainda hoje a identificação de controladores e processadores neste entorno é um desafio significativo perante o cumprimento do RGPD e parece requerer um entendimento mais profundo da realidade técnica que envolve tais infraestruturas, bem como uma abordagem mais matizada a fim de garantir a aplicação dos princípios e normas do regulamento quando contrastados com as características inerentes à tais sistemas descentralizados. Outrossim, persistem discussões em torno da possível qualificação de agentes envolvidos num ecossistema de *blockchain*, especialmente nas de caráter público, como responsáveis ou subcontratantes, e que ganharam novo fôlego com a abertura para consulta sobre as *Guidelines 02/2025 on processing of personal data through blockchain technologies*, publicadas pelo EDPB⁷⁶. As diretrizes destacaram tensões já conhecidas entre características principais de uma infraestrutura descentralizada e o RGPD, pelo que serão analisadas em maior detalhe nas páginas seguintes.

3. O Direito ao apagamento

Um dos principais direitos dos titulares previstos no RGPD é o do apagamento, que, de acordo com o artigo 17º do texto, permite aos indivíduos solicitarem perante o responsável pelo tratamento, em tempo razoável, quando determinadas situações verifiquem-se, o

⁷³Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 5.

⁷⁴SURIPEDDI, Mani Karthik Suhas; PURANDARE, Pradnya, *Blockchain Technology and Data Privacy Regulations*, *Journal of Physics: Conference Series*, vol. 1964, 2021, art. 042005. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042005/pdf>. Acesso em: 25 jul. 2025. p. 8.

⁷⁵Cfr. CNIL. *Blockchain and the GDPR*.

⁷⁶Cfr. EDPB, *Guidelines 02/2025*.

apagamento de seus dados de forma permanente⁷⁷, garantindo que as informações pessoais não sejam mantidas por tempo indeterminado pelo controlador. Por resultado do princípio da responsabilidade⁷⁸, é o controlador quem está obrigado a garantir que o direito ao apagamento seja realizado de acordo com o disposto, considerando as circunstâncias específicas de cada caso concreto. É, portanto, um direito qualificado e condicionado, pois seu exercício depende de uma análise de proporcionalidade e verificação das hipóteses legais previstas no artigo do RGPD que o regula⁷⁹. De forma geral, o Considerando 4 do RGPD postula que “o direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação a sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade”. De modo complementar, o artigo 17º (3) do RGPD bem como o caso *Google vs. CNIL* (C-507/17) demonstram que o direito ao apagamento não é absoluto, territorialmente⁸⁰ e também no que toca ao seu âmbito de aplicação, sendo necessário ponderar, no caso concreto, no sentido apontado pelo EPRS, os limites técnicos e jurídicos à sua efetivação⁸¹ e também os interesses em jogo.

O desenho técnico das *blockchains*, por ser deliberadamente orientado à imutabilidade e resistência à modificação (a fim de garantir a integridade e confiabilidade da rede) conflitua estruturalmente com a lógica deste direito⁸². A dificuldade manifesta-se não apenas no

⁷⁷Como por exemplo, nas situações em que os dados já não são mais necessários para o propósito para o qual foram coletados, quando os dados foram ilicitamente tratados, ou indivíduo retirar seu consentimento para o processamento, ou ainda quando verifique-se alguma outra situação prevista no artigo 17º (1) do RGPD. Cfr. artigo 17º do RGPD.

⁷⁸Ao controlador é imposto um dever ativo de conformidade e prova, que exige a implementação de medidas organizacionais e técnicas que evidenciem a adesão contínua ao regulamento, no contexto do respeito pelo princípio da responsabilidade. Cfr. Artigo 5º (2) do RGPD.

⁷⁹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 7.3.

⁸⁰Também o âmbito territorial do direito ao esquecimento é de grande relevância no uso das *blockchains*, uma vez que em muitos casos estas têm natureza multijurisdicional. O assunto foi analisado no caso *Google vs CNIL*, onde o tribunal decidiu por estabelecer que o alcance territorial do direito ao esquecimento, no contexto de motores de busca, é limitado às fronteiras dos Estados membros da UE. Entretanto, pela leitura da decisão, decorre que o Tribunal tenta estabelecer uma aplicação e alcance global do direito ao esquecimento como um princípio geral. Isto é dito ao afirmar que, embora a legislação da União não imponha uma obrigação de remover links em todas as versões do motor de busca quando um pedido de remoção é concedido, também não o proíbe. Resulta que uma autoridade regulatória ou um tribunal de um Estado-Membro ainda tem a autoridade, levando em consideração as normas nacionais de proteção aos direitos fundamentais, de equilibrar os direitos do titular dos dados pessoais com a liberdade de informação do público e de instruir o operador do motor de busca, se necessário, a fim de remover os links em todas as suas versões. Cfr. TRIBUNAL DE JUSTIÇA (Grande Secção). *Google LLC v. Commission nationale de l’informatique et des libertés (CNIL)*. 24 set. 2019. Processo C-507/17. ECLI:EU:C:2019:772.

⁸¹Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 7.3.3

⁸²“O direito ao esquecimento, vinculado ao apagamento de dados pessoais, atinge, portanto, o cerne da imutabilidade do blockchain e de sua eficácia geral.” Tradução livre. Cfr. HERIAN, R. *Blockchain, GDPR, and*

apagamento de uma informação de forma isolada, mas na sua remoção de todos os blocos e réplicas armazenadas por todos os nós que são parte da rede, o que pode ser organizacionalmente impraticável e tecnicamente inviável. Existem técnicas recentes que poderiam servir para mitigar tais desafios, mas permanece uma barreira estrutural relevante neste contexto, principalmente em *blockchains* públicas não permissionadas: a dificuldade de desenvolver e implementar mecanismos de governança e coordenação eficazes entre os múltiplos participantes da rede que possam assegurar a conformidade coletiva perante um pedido de apagamento⁸³, pois a existência de cópias redundantes de dados impõe a necessidade de sua remoção em todas as instâncias⁸⁴.

À problemática soma-se o fato de que o termo “apagamento”, ainda que desenvolvido em determinados contextos específicos por entidades reguladoras ou de supervisão, como por exemplo com as Diretrizes 5/2019 relativas aos critérios do direito a ser esquecido pelos motores de busca ao abrigo do RGPD (Parte 1)⁸⁵, não é diretamente definido no RGPD, resultando em incertezas quanto à terminologia e a sua interpretação. Considerando as especificidades técnicas do caso concreto, a anonimização surge como uma possível medida para oferecer conformidade, em conjunto com inutilização prática dos dados. Por outro lado, ainda persiste a ausência de consenso entre autoridades de proteção de dados e tribunais europeus sobre a suficiência ou não destas soluções, como aponta o EPRS⁸⁶. No caso *Google Spain* (C-131/12)⁸⁷ é sugerido o entendimento de um apagamento prático, dentro da esfera de atuação do responsável pelo tratamento, enquanto que em outras decisões, como no caso *Nowak* (C-434/16)⁸⁸, o termo parece exigir a destruição plena e efetiva das informações.

fantasies of data sovereignty, *Law, Innovation and Technology*, vol. 12, n.º 1, 2020, p. 156–174. Disponível em: <https://doi.org/10.1080/17579961.2020.1727094>. Acesso em: 25 jul. 2025. sec. 3.

⁸³Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 7.

⁸⁴ARTICLE 29 WORKING PARTY. *Opinion 05/2012 on Cloud Computing*, WP 196, adotado em 1 de julho de 2012. Disponível em: <https://www.technethics.com/assets/Opinion-05-2012-on-Cloud-Computing.pdf>. Acesso em: 16 jul. 2025.

⁸⁵EDPB. *Diretrizes 5/2019 relativas aos critérios do direito a ser esquecido pelos motores de busca ao abrigo do RGPD (Parte 1)*, versão 2.0, adotada em 7 de julho de 2020. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_pt. Acesso em: 16 jul. 2025.

⁸⁶Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 7.3.1.

⁸⁷Cfr. TRIBUNAL DE JUSTIÇA (Grande Secção). *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Processo C-131/12. 13 mai. 2014. ECLI:EU:C:2014:317.

⁸⁸No caso é mencionado que um candidato em um exame escrito teria o direito de solicitar ao controlador a garantia de que suas respostas no respetivo exame (assim como os comentários do examinador a respeito destas) sejam apagadas após um determinado período de tempo (mas claramente não à sua retificação). Porém, pela

Subsiste, portanto, a ambiguidade e com ela, a falta de clareza para os responsáveis que utilizam arquiteturas descentralizadas no tratamento de dados pessoais sobre os padrões mínimos exigíveis para a conformidade com o direito ao apagamento à luz do regulamento.

Além da referida incerteza, sob o controlador recai uma obrigação de meios ao ter de adotar medidas para informar outros controladores ou processadores sobre um pedido de apagamento do titular, processo que vê-se dificultado em constelações descentralizadas onde identificar quem são os outros agentes responsáveis e como notificá-los pode tornar-se uma tarefa difusa e, muitas vezes, inexecutável. O raciocínio do supramencionado caso *Google Spain*, por analogia, poderia implicar a possibilidade de o exercício dos direitos do titular ser direcionado a outros atores controladores conjuntos. Assim sendo, os indivíduos teriam a possibilidade de acionar, num contexto de *blockchains*, interfaces específicas, como por exemplo, exploradores de blocos, para exigir a efetivação do seu direito⁸⁹. De qualquer modo, as tensões entre obrigações legais setoriais e direitos dos titulares observadas reforçam a necessidade de soluções regulatórias mais integradas e adaptadas às novas arquiteturas tecnológicas. Por conseguinte, um controlador pode ainda não ser capaz de apagar os dados sem eliminar a *blockchain* por inteiro em simultâneo⁹⁰, de modo que a utilização de outras técnicas que atinjam tal objetivo, ponderando os interesses em conflito, devem ser consideradas.

4. As *Guidelines 02/2025* do EDPB

Em abril de 2025 o EDPB publicou as *Guidelines 02/2025 on processing of personal data through blockchain technologies*⁹¹. As diretrizes analisam a relação entre certos princípios de proteção de dados presentes no RGPD com as características técnicas da *blockchain*, enfatizando os problemas para implementação, por exemplo, dos princípios postulados pelo artigo 5º do diploma e relativos à proteção de dados desde a conceção e por

análise do caso não fica esclarecido se essa declaração pode ser interpretada como uma afirmação geral de que o apagamento sempre equivale a destruição, o caso não lidou diretamente com o direito ao apagamento e deu-se fora do contexto de DLT. Cfr. CONCLUSÕES DA ADVOGADA-GERAL (Juliane Kokott). *Peter Nowak v. Data Protection Commissioner*. Processo C-434/16. 20 jul. de 2017. ECLI:EU:C:2017:582.

⁸⁹Esta obrigação que recai sobre o controlador é entretanto uma obrigação apenas de meios e não de fim, pelo que exige-se apenas que medidas razoáveis sejam tomadas para que o fim seja atingido. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* sec. 7.3.3.

⁹⁰GODYN, M.; KEDZIORA, M.; REN, Y.; *et al.* *Analysis of solutions for a blockchain compliance with GDPR*. *Scientific Reports*, Londres, v. 12, art. 15021, 2 set. 2022. DOI: 10.1038/s41598-022-19341-y. Disponível em: <https://www.nature.com/articles/s41598-022-19341-y>. Acesso em: 16 jul. 2025.

⁹¹Para consulta pública. Cfr. EDPB, *Guidelines 02/2025*.

defeito elencados no artigo 25º do mesmo texto, bem como a relevância do respeito pelos direitos dos titulares de dados pessoais, incluindo o direito ao apagamento e retificação, proporcionando ainda recomendações direcionadas à organizações que pretendem processar dados pessoais no âmbito de tecnologias *blockchain*⁹².

No que toca aos papéis e responsabilidades, o documento afirma que um modelo de governança descentralizado, típico das redes distribuídas e que resulta na multiplicidade de papéis e atores que possam vir participar no processamento de dados pessoais neste contexto, não releva no que toca à necessidade de cumprir-se com o RGPD, implicando a necessidade de um estudo claro acerca das correspondentes responsabilidades associadas aos respetivos papéis para cada atividade de processamento. Como não são atribuídas por lei, de acordo com o previsto no Artigo 5º (2) do regulamento, e como os participantes não são sempre iguais, defende-se uma análise factual que leve em conta diversos elementos, como a natureza do serviço a ser prestado, a relação entre os intervenientes e os modelos de governança, que assumem papel central na determinação das responsabilidades⁹³.

É clarificado que os nós, dependendo do tipo de *blockchain* em questão, podem desempenhar distintas funções no que toca ao tratamento de dados pessoais, vindo a assumir maior ou menor grau de responsabilidade jurídica, tendo em conta o contexto concreto. Há, por exemplo, situações onde tais participantes têm o poder de influenciar de forma relevante as finalidades e meios do tratamento, como observa-se na sua participação em decisões sobre *forks*⁹⁴ e alterações de protocolo, pelo que os nós podem ser enquadrados como responsáveis pelo tratamento, ainda que de forma conjunta⁹⁵. No âmbito de transferências internacionais de dados pessoais, quando os nós localizam-se fora da UE e especialmente quando não são previamente verificados ou contratualmente vinculados⁹⁶, destaca-se a necessidade de

⁹²Retomam, portanto, as dificuldades já exploradas nos capítulos anteriores. Segundo a EDPB, a utilização de blockchains pode ainda trazer riscos distintos no que toca os direitos e liberdades dos indivíduos causados pelas possíveis transferências internacionais, as várias partes interessadas, a alocação de responsabilidades e até mesmo novas operações de processamento necessárias para a manutenção do sistema. Cfr. EDPB, *Guidelines 02/2025*, pp. 2, 5 e 6.

⁹³Os modelos de governança definem a arquitetura técnica, como os formatos, protocolos e atualizações, e também os mecanismos organizacionais e jurídicos aplicáveis, incluindo obrigações contratuais e medidas de proteção de dados desde a conceção. Cfr. EDPB, *Guidelines 02/2025*, p. 9.

⁹⁴Um *fork* pode ser entendido como “uma mudança em um protocolo de *blockchain*, significando uma alteração fundamental nas regras de protocolo que regem a rede, o que, por sua vez, afeta o processo de validação de transações e blocos.” Tradução livre. Cfr. CONLON, Thomas; CORBET, Shaen; HOU, Yang (Greg); HU, Yang; OXLEY, Les. *Bitcoin forks: What drives the branches?*. *Research in International Business and Finance*, vol. 69, 2024. Disponível em: <https://doi.org/10.1016/j.ribaf.2024.102261>. Acesso em: 26 jul. 2025. sec. 1.

⁹⁵ Cfr. EDPB, *Guidelines 02/2025*, p. 10.

⁹⁶ Principalmente, portanto, no contexto de *blockchains* públicas.

assegurar, nestes casos, a conformidade com o RGPD, indicando a necessidade de respeito pelo Capítulo V do regulamento, através, por exemplo, da utilização de cláusulas-tipo de proteção de dados⁹⁷, o que, entretanto, torna-se impraticável no contexto de redes públicas descentralizadas⁹⁸.

Postula-se que o armazenamento de dados pessoais diretamente identificáveis numa *blockchain* pode trazer desafios no que toca ao respeito pelo RGPD, principalmente no que toca à sua imutabilidade. Apesar de modificações serem tecnicamente possíveis, podem ser inviáveis por geralmente exigir consenso por parte de todos os nós de uma rede, resultando no comprometimento da consistência e inviolabilidade do sistema, pelo que a combinação de soluções técnicas neste sentido, por exemplo, estruturas de governança, podem ser úteis a fim de alcançar a conformidade com o regulamento. Nesse cenário, uma persistência de dados pode dificultar o exercício de direitos dos titulares, pelo que a fim de mitigar os riscos atrelados a estes desafios, algumas abordagens são identificadas, como técnicas de criptografia, *hashing*, e *cryptographic commitments*, salientando que os dados criptografados e o *hash* permanecem qualificados como dados pessoais⁹⁹, não eximindo o responsável pelo tratamento do respeito pelo RGPD¹⁰⁰.

Especificamente no que refere-se ao cumprimento do direito ao apagamento, o texto recomenda que os dados pessoais, mesmo quando tratar-se de um *hash* ou dados criptografados¹⁰¹, não sejam armazenados numa *blockchain*, mas sim fora dela¹⁰². Caso contrário, aos responsáveis pelo tratamento cabe assegurar que tais dados possam ser tornados irreversivelmente anónimos perante um pedido para os apagar, e que dados complementares

⁹⁷ Cfr. EDPB, *Guidelines 02/2025*, p. 16.

⁹⁸ EUCI. *Response to EDPB Guidelines 02/2025 on Blockchain and Personal Data Processing*. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb-guidelines-02_2025-response-euci-with-signatories.pdf. Acesso em: 12 jul. 2025. pp. 12-13.

⁹⁹ O EDPB menciona, entretanto, que um *hash* que seja gerado por uma função criptográfica que seja robusta o suficiente e se associado a uma chave ou *salt* aleatório de tamanho apropriado, é geralmente verificável somente por quem possui os dados originais e os respetivos elementos de verificação. Assim, com a eliminação segura da tal chave ou do *salt*, torna-se então, em princípio, impossível estabelecer qualquer vínculo com os dados originais se o algoritmo permanecer seguro e nenhum dos elementos for comprometido ou configurado de forma insuficiente. Cfr. EDPB, *Guidelines 02/2025*, p. 12.

¹⁰⁰ O órgão defende ainda que quando o armazenamento de dados na cadeia for inevitável, é preferível que tal ocorra em forma de *proof of existence*, como através de um *hash*, com os dados que verificam a prova sendo mantidos fora da *blockchain*. Cfr. EDPB, *Guidelines 02/2025*, p. 13.

¹⁰¹ A posição tomada pelo EDPB quanto a qualificação de *hashes* e dados criptografados como dados pessoais, portanto, é similar à visão proposta em 2019 pelo EPRS. Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 3.

¹⁰² O texto, nas recomendações elencadas no Anexo A, recomenda explicitamente que os responsáveis não mantenham dados pessoais, além dos identificadores (*identifiers*) relativos à metadados, na *blockchain*. Cfr. EDPB, *Guidelines 02/2025*, p. 22.

armazenados fora da cadeia sejam eliminados. As diretrizes englobam outros direitos dos titulares de dados pessoais, como de informação, acesso e portabilidade, confirmando que tais direitos podem ser compatíveis com as características técnicas de uma *blockchain*. Tratando-se do direito de retificação, este deve ser considerado desde a constituição do sistema (assim como quando está em questão o direito ao apagamento) e poderia ser cumprido por meio de uma transação futura que anularia a anterior, mesmo que esta permaneça registada na rede¹⁰³.

As linhas orientadoras apresentaram temáticas amplamente debatidas no que toca a harmonização de requisitos impostos por leis de proteção de dados europeias com características inerentes à *blockchain*. Não obstante, promoveram controvérsia na comunidade¹⁰⁴. De fato, observa-se a preferência do EDPB por arquiteturas permissionadas, refletindo um viés em favor de configurações centralizadas e que, ao menos de forma aparente, aproximam-se mais de modelos tradicionais regulados pelo RGPD. Pode-se argumentar que acabaram por violar o princípio da neutralidade tecnológica e possivelmente ignorar os benefícios de arquiteturas descentralizadas, sendo preferível, em contrapartida, uma abordagem regulatória equilibrada, que fosse adequada aos riscos concretos envolvidos e ao grau de descentralização, que avaliasse a conformidade com base nos resultados efetivos em matéria de proteção de dados e não de forma tão assente na estrutura técnica do sistema, como no sentido sustentado pelo BC4EU¹⁰⁵.

Uma contradição com os princípios da proporcionalidade e subsidiariedade previstos no artigo 5.º do Tratado da União Europeia¹⁰⁶ e o requisito de coerência do direito da UE podem surgir ao aplicar-se o RGPD de forma a tornar *blockchains* públicas praticamente inoperantes, posição adotada pela EUCI em sua resposta às referidas diretrizes, que também reflete sobre os limites interpretativos do EDPB à luz do artigo 70º do RGPD, visto que adotar entendimentos que possam inviabilizar ou deslegitimar grupos de infraestruturas

¹⁰³Nos casos em que a retificação exige o apagamento dos dados pessoais, a EDPB defende que devem ser aplicadas as mesmas soluções adotadas para pedidos relativos ao exercício do direito ao apagamento. Cfr. EDPB, *Guidelines 02/2025*, pp. 20 e 21.

¹⁰⁴FORBES. *EU Privacy Laws To Delete See-Through Blockchains*. 1 mai. 2025. Disponível em: <https://www.forbes.com/sites/digital-assets/2025/05/01/eu-privacy-laws-to-delete-see-through-blockchains/>. Acesso em: 12 jul. 2025.

¹⁰⁵BLOCKCHAIN FOR EUROPE. *BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains*. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/bc4eu-response-to-edpb-consultation-on-gdpr-and-blockchain.pdf. Acesso em: 12 jul. 2025. sec. 1.

¹⁰⁶UE. Versão consolidada do Tratado da União Europeia. Jornal Oficial da União Europeia, C 202, p. 13, 7 jun. 2016.

descentralizadas parece ultrapassar o escopo do mandato deste órgão como construído no artigo supramencionado. A abordagem das diretrizes aparenta entrar em contradição com os objetivos estratégicos assumidos pela própria UE onde reconhece-se que a liderança europeia em tecnologias de próxima geração depende também da consolidação de infraestruturas descentralizadas. Além disso, a fim de haver coerência jurídica entre os instrumentos regulatórios que incidem sobre o ecossistema digital europeu e o RGPD, faz-se necessária uma interpretação que não inviabilize as tecnologias *blockchain*¹⁰⁷. A INATBA, em seu parecer acerca das diretrizes, vai em sentido similar e frisa que se a lógica da posição binária do EDPB perante tais tecnologias for implementada de forma consistente na UE, arrisca-se desacelerar a inovação e limitar a competição, além de criar fragmentação jurídica¹⁰⁸.

A qualificação de responsável pelo tratamento a validadores ou operadores de nós em redes públicas, por exemplo, perante um *fork*, parece apresentar-se problemática, visto que tais participantes geralmente não determinam as finalidades nem os meios essenciais do tratamento, mas executam de forma automatizada os protocolos que são definidos por programadores ou utilizadores. Os nós, nestes contextos, não escolhem que dados pessoais são incluídos numa cadeia, não interpretam o conteúdo das transações e, habitualmente, não têm acesso contextual suficiente que permita a identificação dos titulares. Assim, a sua atuação aproxima-se à de prestadores de infraestrutura técnica, como os operadores de telecomunicações, cuja função é meramente transmitir dados, pelo que exigir destes o cumprimento integral das obrigações do RGPD apresenta-se como materialmente inexequível em redes públicas e abertas, compostas por validadores descentralizados, anónimos e dispersos globalmente. Neste sentido, a BC4EU salienta que a abordagem proposta nas diretrizes aparenta desconsiderar a realidade técnica e operacional das *blockchains* públicas,

¹⁰⁷Múltiplos regulamentos europeus, como o Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho de 31 de maio de 2023 relativo aos mercados de criptoativos, o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro, o Regulamento (UE) 2024/1624 do Parlamento Europeu e do Conselho de 31 de maio de 2024 relativo à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, e o Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído, assumem a funcionalidade e também legalidade das *blockchains* públicas. Fragilizar a conformidade dessas infraestruturas com o RGPD equivaleria, em última instância, a esvaziar a eficácia de alguns destes regimes, que dependem da persistência, auditabilidade e verificabilidade dos dados em redes públicas. Cfr. EUCI, *Response to EDPB Guidelines 02/2025 on Blockchain and Personal Data Processing*, p. 3 e 4.

¹⁰⁸INATBA, *Response to EDPB Guidelines 02/2025 on the interplay of the AI Act and the GDPR*, 9 jun. 2025. Disponível em: https://inatba.org/wp-content/uploads/2025/06/INATBA-Response_EDPB-Guidelines-2025-06-09.pdf. Acesso em: 13 jul. 2025.

nas quais a participação é livre e muitas vezes realizada por indivíduos, pelo que impor a estes atores obrigações incompatíveis com a sua função estrutural pode trazer incerteza jurídica sistémica, dissuadir a sua participação e acabar por comprometer a segurança e resiliência da tecnologia. A responsabilidade poderia ser melhor colocada nos atores que efetivamente atuam com base na recolha, agregação ou exploração econômica de dados pessoais¹⁰⁹, como por exemplo, as aplicações que utilizam a *blockchain* como sua infraestrutura¹¹⁰.

Uma abordagem funcional e contextual, ancorada na intenção, capacidade e influência concreta dos tais agentes sobre as finalidades e meios de tratamento mostraria-se mais balanceada, visto que a atribuição nas diretrizes é feita de forma generalizada no contexto de *blockchains* públicas não permissionadas. Tal leitura encontra respaldo na jurisprudência consolidada à nível europeu, como nos supramencionados casos *Wirtschaftsakademie* (C-210/16) e *Google Spain*, onde ser qualificado como responsável pelo tratamento pressupõe uma influência efetiva sobre as finalidades e os meios do tratamento¹¹¹.

Especificamente quanto ao direito ao apagamento, da posição da EDPB resulta que em certos casos, a impossibilidade de exclusão de dados pessoais numa *blockchain* poderia levar à necessidade de eliminação da própria cadeia como um todo. Entretanto, em redes públicas não permissionadas os dados são replicados globalmente em milhares de nós e nenhum deles teria capacidade de apagar unilateralmente informações armazenadas, o que poderia configurar-se tecnicamente impraticável e possivelmente juridicamente desproporcional. Seria preferível reconhecer as limitações técnicas de infraestruturas descentralizadas e considerar, na interpretação do direito ao apagamento, o princípio da proporcionalidade e a coexistência e outros direitos fundamentais e interesses legítimos, como a integridade da *blockchain*, a proteção de terceiros e a promoção da inovação tecnológica. Este mesmo sentido pode ser observado na orientação do CNIL, que considera a utilização de determinadas medidas técnicas, como *crypto-shredding* e *zero-knowledge rollups*, como equiparáveis, ao menos funcionalmente, ao apagamento, desde que tornem os dados inacessíveis de forma

¹⁰⁹Cfr. BC4EU, *BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains*, sec 1.

¹¹⁰Ver seção 2 da Parte I onde discorre-se o defendido pelo EPRS “quando existe uma camada de aplicação, pode-se argumentar que a entidade legal que determina os propósitos do processamento de dados pessoais na camada de aplicação qualifica-se como controladora de dados.” Tradução livre.

¹¹¹Cfr. EUCL, *Response to EDPB Guidelines 02/2025*; TRIBUNAL DE JUSTIÇA (Grande Secção). *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*. Processo C-210/16. 5 jun. 2018. ECLI:EU:C:2018:388.; e Cfr. TRIBUNAL DE JUSTIÇA (Grande Secção). *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Processo C-131/12. 13 mai. 2014. ECLI:EU:C:2014:317.

permanente, mostrando-se compatível com o Considerando 26 e o artigo 17.º, n.º 1, alínea c) do RGPD¹¹².

A qualificação de metadados, dados criptografados e *hashes* como dados pessoais pelas diretrizes, quando possam ser razoavelmente associados a uma pessoa singular, também suscita questões jurídicas relevantes, especialmente quando contrapostas à jurisprudência europeia. Como afirmado no acórdão *Breyer* (C-582/14)¹¹³, os dados apenas constituem dados pessoais quando o responsável pelo tratamento dispõe efetivamente dos meios para identificar o titular, o que foi reiterado nos caso *Scania* (C-319/22)¹¹⁴, em que distinguiu-se a natureza dos dados em função da capacidade de reidentificação por diferentes operadores, reafirmando o critério da razoabilidade e da perspectiva da entidade concreta que efetua o tratamento. Através da análise dessa jurisprudência, percebe-se que dados criptografados cujas chaves de acesso se mantêm exclusivamente com os titulares não devem ser considerados dados pessoais para os efeitos do RGPD e este entendimento é especialmente relevante no contexto de *blockchains* que incorporam ZKPs, onde nem mesmo os agentes da infraestrutura detêm os meios para a reidentificação¹¹⁵.

Do exposto, pode-se concluir que a postura do EDPB no texto em questão sugere sensibilidade insuficiente às especificidades técnicas dos sistemas descentralizados, falta de granularidade ao aplicar conceitos jurídicos à tecnologia, especialmente *blockchains* públicas e não permissionadas que distribuírem responsabilidades e incorporam mecanismos de privacidade e transparência diretamente no protocolo. Em especial, a UE tem se posicionado positivamente na promoção da inovação digital, competitividade econômica e proteção de direitos fundamentais, como demonstrado em iniciativas como o EBSI e a Década Digital¹¹⁶.

¹¹²Cfr. BC4EU, *BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains*

¹¹³TRIBUNAL DE JUSTIÇA (Segunda Secção). *Patrick Breyer v. Bundesrepublik Deutschland*. Processo C-582/14. 19 out. 2016. ECLI:EU:C:2016:779.

¹¹⁴TRIBUNAL DE JUSTIÇA (Terceira Secção). *Gesamtverband Autoteile-Handel eV v. Scania CV AB*. Processo C-319/22. 9 nov. 2023. ECLI:EU:C:2023:837.

¹¹⁵GANGI, Paolo Maria. *Feedback in relation to the document “Guidelines 02/2025 on processing of personal data through blockchain technologies”*. Roma: Studio Gangi, 9 jun. 2025. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/feedback-edpb-gl-blockchain-v-1.0.pdf. Acesso em: 12 jul. 2025.

¹¹⁶ COMISSÃO EUROPEIA. *Europe’s Digital Decade: digital targets for 2030*. Estratégia “Uma Europa preparada para a era digital”, prioridades 2019–2024. Bruxelas, 2021. Disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt. Acesso em: 16 jul. 2025.

No entanto, ao interpretar rigidamente o RGPD, corre-se o risco de inviabilizar o uso de *blockchains* públicas e colidir com princípios estruturantes do direito da UE¹¹⁷.

PARTE II - CONVERGÊNCIA ENTRE DLT E O RGPD

1. Respostas aos desafios de conformidade

Não obstante os obstáculos relativos à aplicação do RGPD à *blockchain* anteriormente aludidos, algumas soluções têm o potencial de se aproximarem dos efeitos jurídicos exigidos. No contexto do direito ao apagamento, por exemplo, e como já introduzido em momento anterior, uma aproximação funcional ao apagamento é defensível e postulada como possível mecanismo de conformidade, por exemplo, pela CNIL¹¹⁸. Neste mesmo sentido, aponta-se como possíveis medidas a manipulação dos dados pessoais, obscurecendo-os por exemplo, a fim de torná-los anónimos¹¹⁹, ou ainda a utilização de *chameleon hashes*¹²⁰. Outras soluções propõem o armazenamento de dados *off-chain*, e nesse caso apenas um *pointer* ou *hash* é armazenado *on-chain*, permitindo que as informações pessoais sejam acessadas e excluídas sem comprometer a integridade da cadeia de blocos e, por consequência, da própria rede¹²¹. Cabe referir que *hashing* pode não ser suficiente para transformar dados pessoais em dados anónimos, levando à subsistência do risco de identificação¹²². A alternativa supramencionada, muitas vezes associada à utilização na rede de identificadores exclusivos (para cada indivíduo) que se correlacionam aos respetivos dados armazenados fora dela, evita a utilização da tecnologia de carácter descentralizado e imutável para o armazenamento dos

¹¹⁷Cfr. BC4EU, *BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains*. sec. 8

¹¹⁸Cfr. CNIL. *Blockchain and the GDPR*.

¹¹⁹Cfr. EDPB, *Guidelines 02/2025*, p. 20.

¹²⁰A abordagem proposta, que viabiliza o conceito de uma *redactable blockchain*, permite a modificação de blocos já registados mantendo a integridade estrutural da cadeia, possibilitando a geração de colisões controladas que comprometem a consistência do *hash*. Viabiliza a edição de dados sob determinadas condições, em *blockchains* públicas e privadas, mas suscita preocupações jurídicas e relativas à governança, requerendo robustos mecanismos de controlo, autenticação e transparência para garantir conformidade e confiança jurídica no sistema. Cfr. GODYN, M.; KEDZIORA, M.; REN, Y. *Analysis of solutions for a blockchain compliance with GDPR. Related Work*; ATENIESE, Giuseppe; MAGRI, Bernardo; VENTURI, Daniele; ANDRADE, Ewerton. *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends*. Cryptology ePrint Archive, report 2016/757, depositado em 11 maio 2017. Disponível em: <https://eprint.iacr.org/2016/757.pdf>. Acesso em: 16 jul. 2025.

¹²¹GONÇALVES, Ricardo Martins; DA SILVA, Miguel Mira; DA CUNHA, Paulo Rupino. *Olympus: a GDPR compliant blockchain system*. *International Journal of Information Security*, Londres, v. 23, n. 2, p. 1021–1036, 17 nov. 2023. DOI: 10.1007/s10207-023-00782-z. Disponível em: <https://link.springer.com/article/10.1007/s10207-023-00782-z>. Acesso em: 16 jul. 2025. sec. 3.

¹²²Como entende-se pelas *Guidelines 02/2025* do EDPB, sec. 29, que falham ao não aprofundar nas técnicas distintas que podem ser utilizadas no contexto do uso prático em questão.

dados, sem ocupar-se com a problemática do armazenamento dos dados pessoais na *blockchain* em si¹²³, e possui a vantagem de promover a integridade da rede dependendo de como a técnica é utilizada¹²⁴.

Além do exposto supra, há outras autoridades de proteção de dados nacionais com conceções equivalentes às da CNIL. A autoridade de proteção de dados da Áustria postulou que o controlador tem flexibilidade em relação aos meios técnicos de realização do apagamento e que a anonimização pode ser vista como um meio de atingi-la¹²⁵, indo no mesmo sentido que Grupo de Trabalho do Artigo 29^{o126}, bem como o ICO do Reino Unido, que argumenta que a colocação dos dados “fora de uso” pode satisfazer esse direito¹²⁷, assim como existem argumentos de que a destruição da chave privada tornaria os dados criptografados com uma chave pública inacessíveis¹²⁸. Outras possibilidades incluem *pruning*, permitindo a exclusão de transações e blocos antigos mantendo apenas os *headers* desses blocos (contendo os *hashes* dos dados removidos) mantendo a integridade da rede¹²⁹,

¹²³Como no caso da EBSI. Cfr. GONÇALVES, Ricardo Martins; DA SILVA, Miguel Mira; DA CUNHA, Paulo Rupino. *Olympus: a GDPR compliant blockchain system. International Journal of Information Security*, sec.3

¹²⁴Cfr. BELEN-SAGLAM, Rahime; ALTUNCU, Enes; LU, Yang; LI, Shujun. *A systematic literature review of the tension between the GDPR and public blockchain systems*, sec. 4.6.1.

¹²⁵DATENSCHUTZBEHÖRDE (Austria). *Decisão de 5 dez. 2018*, DSB-D123.270/0009-DSB/2018, que reconheceu a anonimização consistente como meio válido de exclusão ao abrigo do artigo 17.º do RGPD.

¹²⁶ARTICLE 29 WORKING PARTY. *Opinion 02/2014 on the application of the Article 29 Working Party's ruling on Data Protection in cloud computing: WP 196 revisited*. Adoptado em 1 de julho de 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 16 jul. 2025. Sec. 2.1.

¹²⁷Cfr. EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, sec. 7.3.1.

¹²⁸Ainda que essas soluções não impliquem estritamente a eliminação dos dados, que permanecem registados na rede, elas podem possibilitar o exercício efetivo do direito ao apagamento. A CNIL recomenda que a equivalência jurídica de tais medidas à luz do artigo 17º do RGPD seja cuidadosamente avaliada. Cfr. CNIL. *Blockchain and the GDPR*.

¹²⁹Consiste na exclusão de transações e blocos antigos, preservando os cabeçalhos desses blocos e mantendo a integridade da cadeia, implementada no Bitcoin em 2015. Pode oferecer maior privacidade ao limitar a recuperação de certas transações, mas pode comprometer a segurança do sistema e requer a adesão voluntária de todos os nós da rede, sendo mais eficaz em *blockchains* permissionadas do que em *blockchains* públicas, onde sua viabilidade é controversa. POLITOU, Eugenia; CASINO, Fran; ALEPIS, Efthymios; PATSAKIS, Constantinos. *Blockchain Mutability: Challenges and Proposed Solutions*. IEEE Transactions on Emerging Topics in Computing, 2019, pp. 1–1. Disponível em: https://www.researchgate.net/publication/336822518_Blockchain_Mutability_Challenges_and_Proposed_Solutions. Acesso em: 16 jul. 2025. Sec. 5.

*forgetting blockchains*¹³⁰, e outras iniciativas que propõem blockchains mutáveis¹³¹. Neste mesmo contexto, a AEPD demonstrou que é possível apagar dados de uma *blockchain* privada através de métodos práticos utilizando-se de um *hard fork*¹³² para integrar a conformidade com o RGPD, abrindo caminho para uma integração entre o regulamento e a referida tecnologia, numa combinação entre alterações técnicas e ajustes nos modelos de governança¹³³. Em redes públicas, como Bitcoin ou Ethereum, entretanto, uma modificação que resulta num *fork* pode implicar uma ruptura de consenso¹³⁴ e tornar a abordagem onerosa. Neste sentido, entende-se que as questões de conformidade extravasam a mera dimensão técnica, pelo que o próprio desenho da governança da rede influenciará a determinação da conformidade legal da sua utilização.

2. ***Blockchains* como um possível instrumento de harmonização com o RGPD**

O RGPD e *blockchains*, em essência, partilham um objetivo comum de reforçar a privacidade e a segurança dos dados pessoais, divergindo nos meios aplicados para atingir esse propósito. Como destacam Tatar, Gökce e Nussbaum, o primeiro coloca em destaque um ator identificável e responsável, enquanto a última recorre a mecanismos técnicos, como criptografia e transparência algorítmica. Porém, ambos os sistemas contêm princípios como a minimização de dados, integridade e rastreabilidade, ainda que realizados por vias distintas,

¹³⁰FARSHID, Simon; REITZ, Andreas; ROßBACH, Peter. *Design of a forgetting blockchain: A possible way to accomplish GDPR compatibility*. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Manoa: University of Hawai'i at Mānoa, 2020. Disponível em: <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ae96ec9e-978a-487d-a431-108909a0afd1/content>. Acesso em: 16 jul. 2025.

¹³¹Como por exemplo, sem a utilização de *hard forks*, proposta em PUDDU, I.; DMITRIENKO, A.; CAPKUN, S. *uchain: How to Forget without Hard Forks*. *IACR Cryptology ePrint Archive*, paper 2017/106. ETH Zurich, 2017. Disponível em: <https://eprint.iacr.org/2017/106.pdf>. Acesso em: 26 jul. 2025.

¹³²“Um *hard fork* ocorre quando uma parcela dos utilizadores de uma *blockchain* faz uma alteração significativa e permanente no protocolo técnico subjacente, produzindo uma *blockchain* divergente e paralela.” Tradução livre. Cfr. WEBB, Nick. *A Fork in the Blockchain: Income Tax and the Bitcoin/Bitcoin Cash Hard Fork*. *North Carolina Journal of Law & Technology*, vol. 19, n.º 4, 2018, p. 283. Disponível em: <https://scholarship.law.unc.edu/ncjolt/vol19/iss4/10>. Acesso em: 26 jul. 2025. sec. 1.

¹³³Cfr. PEHLIVAN, Ceyhan N. *Spanish AEPD: Harmonising blockchain with the GDPR's right to be forgotten*. *Linklaters Tech Insights*, 13 nov. 2024. Disponível em: <https://techinsights.linklaters.com/post/102jo4a/spanish-aepd-harmonising-blockchain-with-the-gdprs-right-to-be-forgotten>. Acesso em: 22 jul. 2025.

¹³⁴A depender do tipo de *fork*, da sua causa. A solução é, portanto, mais difícil de replicar numa *blockchain* de tal natureza devido à necessidade de amplo consenso. Cfr. YUUVAN, Douglas C. *Navigating the Evolution of Ethereum: Vitalik Buterin's Vision for DeFi Governance and Scalability*, ago. 2024. Disponível em: https://www.researchgate.net/publication/383425035_Navigating_the_Evolution_of_Ethereum_Vitalik_Buterin's_Vision_for_DeFi_Governance_and_Scalability. Acesso em: 22 jul. 2025. p. 9. e SHAHSAVARI, Y.; ZHANG, K.; TALHI, C. *A Theoretical Model for Fork Analysis in the Bitcoin Network*. In: 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, EUA, 2019, p. 237–244. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8946275>. Acesso em: 26 jul. 2025. sec. 1.

pelo que a superação das tensões entre os dois passa, segundo os referidos autores, pela mudança de foco que passa a incidir sobre os valores que o RGPD e as *blockchains* partilham¹³⁵.

Existem argumentos válidos no sentido de que *blockchains*, em diversos aspetos, podem não apenas ser compatíveis com o RGPD, mas também instrumentos de promoção dos objetivos propostos pelo regulamento. Com o avanço da regulação europeia, que parece tentar equilibrar inovação tecnológica com a proteção dos direitos fundamentais, é de notar que há pontos de convergência entre as duas figuras. Com o potencial de oferecer um novo paradigma no que toca a modelos de governança de dados, a referida tecnologia torna possível formas alternativas de compartilhamento, inclusive de forma automatizada através de contratos inteligentes (podendo reduzir custos operacionais e riscos associados), em muitos casos, sem a necessidade de um intermediário central, bem como sua inerente transparência facilita uma visão mais clara de quem teve acesso aos dados.

Os referidos atributos também podem reforçar um maior controlo dos titulares sobre os seus dados pessoais, viabilizando o cumprimento de direitos previstos no RGPD, como o direito de acesso e o direito à portabilidade¹³⁶. Há pesquisadores e autoridades que se aproximam dessa visão¹³⁷, na qual se reconhece as limitações, mas onde os direitos dos titulares podem ser compatíveis com implementações da tecnologia *blockchain*, por exemplo, pelo fato de informações armazenadas no livro-razão distribuído poderem se encontrar acessíveis a todos os participantes da rede. Nesse contexto, surgem iniciativas que utilizam soluções que refletem esse potencial, demonstrando que a tecnologia em questão pode servir no auxílio ao cumprimento de princípios do regulamento, como o da limitação da finalidade, e contribuir com mecanismos mais eficazes para detecção de violações e fraudes¹³⁸. A seguir são apresentados e analisados exemplos de projetos que incorporam de alguma forma a

¹³⁵Cfr. TATAR, U.; GÖKÇE, Y.; NUSSBAUM, B. *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, *Computer Law & Security Review*, sec. 5.1.

¹³⁶Elencados nos artigos 15º e 20º do RGPD, respetivamente.

¹³⁷Por exemplo, FERRARI, V., QUINTAIS, J. P., GIANNOPOULOU, A., BODÓ, B. *EU Blockchain Observatory and Forum Workshop on GDPR, data policy and compliance: (08.06.2018, Brussels) : Report . (Blockchain & Society Policy Research Lab Research Nodes; No. 2018/1)*. University of Amsterdam, Institute for Information Law. (2018). Disponível em: https://blockchain-society.science/wpcontent/uploads/2018/07/blockchain_society_research_nodes_1_GDPR_workshop_03072018.pdf. Acesso em: 26 jul. 2025; CNIL. *Blockchain and the GDPR: solutions for a responsible use of the blockchain in the context of personal data*. 2018. Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 12 jul. 2025.

¹³⁸Ibidem.

utilização de *blockchains*, com maior ou menor grau de descentralização, em simultâneo, propondo a harmonia com determinados princípios e normas contidos no RGPD.

3. Identidades descentralizadas e SSI

Observa-se, a partir de 2015, o surgimento do conceito de SSI, que visa colocar os seus portadores no controlo (termo aqui utilizado em sentido lato) a fim de que estes sejam não apenas o núcleo essencial, mas também os governantes da sua identidade¹³⁹. A SSI é um excelente exemplo de intersecção entre o RGPD e *blockchains*, precisamente porque é desenhada para colocar o titular como soberano de sua identidade¹⁴⁰ num contexto de descentralização e visto que DLT passou a ser aplicada também em sistemas de identidade digital¹⁴¹. Essa soberania fica palpável numa leitura dos doze princípios básicos da SSI publicados pela Fundação Sovrin, que estabelece um ecossistema que deve permitir aos detentores de direitos de identidade o controlo direto do uso dos seus dados de identidade digital¹⁴², a capacidade de os proteger¹⁴³, a possibilidade de fornecer prova verificável da autenticidade desses dados, bem como proteger sua privacidade e compartilhar o mínimo necessário perante uma determinada interação¹⁴⁴.

A fim de responder as limitações trazidas pela centralização, o modo de concretização técnica da SSI dá-se geralmente atrelado a sistemas que ao menos almejam a descentralização, pelo que os princípios da SSI servem como quadro referencial, mas a maioria dos projetos de identidade digital não cumprirá todos os seus critérios. Exemplos como o *Kiva Protocol*¹⁴⁵ e o *Building Blocks*¹⁴⁶ da ONU ilustram abordagens híbridas, onde há

¹³⁹PREUKSCHAT, Alex; REED, Drummond. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY: Manning Publications, 2021. Parte 1.

¹⁴⁰Como nota Herian, “Fundamentalmente, o RGPD visa facilitar modelos de soberania de dados na vida comercial e cívica que devolvam o controlo dos dados pessoais aos titulares dos dados (...)”. Tradução livre. Cfr. HERIAN, R. *Blockchain, GDPR, and fantasies of data sovereignty. Law, Innovation and Technology*, sec. 3.

¹⁴¹Cabe referir que a definição SSI está ainda em desenvolvimento no setor. AVELLANEDA, O. et al; *Decentralized Identity: Where Did It Come From and Where Is It Going?*, *IEEE Communications Standards Magazine*, vol. 3, n.º 4, dez. 2019, p. 10–13. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9031542>. Acesso em: 19 jul. 2025.

¹⁴²Ou delegando-o em agentes e tutores por si escolhidos, incluindo indivíduos, organizações, dispositivos e software.

¹⁴³Seja em repouso e/ou em movimento, para controlar os seus próprios identificadores e chaves de criptografia, e para empregar criptografia ponta-a-ponta para todas as interações.

¹⁴⁴SOVRIN FOUNDATION. *Os Princípios da Auto-Identidade Soberana (SSI)*, versão em português, 2020. Disponível em: <https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-Portuguese-v01.pdf>. Acesso em: 22 jul. 2025.

¹⁴⁵Kiva. *Kiva Protocol*. 2025. Disponível em: <https://kivaprotocol.com/>. (Acesso em: 22 de julho de 2025).

¹⁴⁶World Food Programme (WFP). *Building Blocks: Identity-based payments and blockchain*. 2025. Disponível em: <https://www.wfp.org/building-blocks>. (Acesso em: 22 de julho de 2025).

controle individual mas também centralização¹⁴⁷. Neste sentido, existe um número cada vez maior de organizações, como a *IDunion*¹⁴⁸ e o *Verifiable Organizations Network* (VON)¹⁴⁹, que visam implementar SSI num contexto prático, bem como a iniciativa *Ethereum Identity Kit* (EIK), uma plataforma de desenvolvimento que visa facilitar a integração de ferramentas de identidade descentralizada¹⁵⁰ e até a própria UE com a EUDIW¹⁵¹. Desta forma, no seguimento deste trabalho são analisadas iniciativas concretas neste sentido, com foco na EUDIW, ainda que se afastem ou não, em maior ou menor medida, da conceção ideal de uma SSI, pois incorporaram um ou mais dos elementos centrais do modelo proposto acima: descentralização, portabilidade, interoperabilidade e o reforço do controlo individual sobre os dados pessoais.

4. Carteiras de identidade digital

Identidades descentralizadas evoluíram em múltiplos formatos, como as baseadas em DLT e *blockchain*, e um dos seus elementos centrais são as soluções de carteiras de identidade digital, que permitem ao titular a gestão das suas credenciais¹⁵². Essas carteiras funcionam geralmente como repositórios onde é possível armazenar, gerenciar e compartilhar credenciais digitais de forma consentida¹⁵³, reforçando a privacidade e a segurança dos dados pessoais, em alinhamento com princípios fundamentais presentes no RGPD¹⁵⁴.

¹⁴⁷Wang, F., & De Filippi, P. *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*. *Frontiers in Blockchain*, 2, 496586. Disponível em: <https://doi.org/10.3389/fbloc.2019.00028> (Acesso em: 25 de julho de 2025).

¹⁴⁸IDunion Consortium. GitHub: IDunion. 2025. Disponível em: <https://github.com/IDunion>. (Acesso em: 22 de julho de 2025).

¹⁴⁹Verifiable Organizations Network (VON). VON – Identity-based ecosystems and governance. 2025. Disponível em: <https://gcblockchain-chainedeblocsgc.github.io/verifiable-organization-network.html>. (Acesso em: 22 de julho de 2025).

¹⁵⁰Principalmente em ambientes Ethereum, permitindo que programadores incorporem o *stack* de identidade dessa *blockchain*. Ethereum Identity Foundation. *Ethereum Identity Kit - Component library for ENS and EIP integration*. 2025. Disponível em: <https://ethidentitykit.com/>. Acesso em: 22 jul. 2025.

¹⁵¹Além disso, a SSI serve de base para carteiras de identidade digital, como a EUDIW. BABEL, M.; WILLBURGER, L.; LAUTENSCHLAGER, J. *Self-sovereign identity and digital wallets*. *Electron Markets*, v. 35, art. 28, 2025. Disponível em: <https://doi.org/10.1007/s12525-025-00772-0>. Acesso em: 25 jul. 2025.

¹⁵²KERSIC, V.; VIDOVIC, U.; VRECKO, A.; DOMAJNKO, M.; TURKANOVIC, M. *Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management*. *IEEE Access*, v. 11, p. 78135–78151, 2023. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10194951>. Acesso em: 25 jul. 2025. secs. 1. e 2.

¹⁵³ALLENDE LÓPEZ, Marcos. *Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets and Blockchain*. Washington, D.C.: Inter-American Development Bank, 2020. Disponível em: <https://publications.iadb.org/en/publications/english/viewer/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignty-Digital-Wallets-and-Blockchain.pdf>. Acesso em: 22 jul. 2025. sec. 7.4.

¹⁵⁴Veja, por exemplo, a figura do consentimento postulado no artigo 6º (1) alínea a) do RGPD.

O funcionamento típico de uma carteira de identidade digital no contexto de credenciais verificáveis costuma envolver distintos atores principais: o emissor da credencial, o titular, o sujeito e o verificador. Nesta configuração, o emissor da credencial é a entidade responsável por emitir credenciais verificáveis, que podem ser então armazenadas pelo titular em um repositório próprio, por exemplo, uma carteira digital. O titular, pode então gerar apresentações verificáveis dessas credenciais, e no contexto de SSI, detém o controle total e exclusivo sobre sua gestão, com autonomia para decidir quais informações compartilhar, quando e com quem. Geralmente, mas não obrigatoriamente, o titular é também o sujeito, a pessoa sobre quem as informações foram emitidas e o verificador é a entidade que processa e valida as credenciais apresentadas pelo titular¹⁵⁵. Todas as interações entre esses atores podem ser registradas numa rede *blockchain*, garantindo a transparência e integridade do sistema.

Como exemplo de carteira de identidade digital da atualidade, pode-se referir a QuarkID, desenvolvida como um protocolo SSI pelo governo de Buenos Aires. É descentralizada, pública, não permissionada, aberta, extensível, *multichain* e interoperável, permitindo que os indivíduos gerenciem e compartilhem documentos sem expor informações pessoais desnecessárias, através da utilização de *blockchain* e de técnicas como ZKPs¹⁵⁶. A FinID, iniciativa brasileira, configura-se por ser uma solução de identidade digital descentralizada que integra *blockchain*, concebida em especial para o setor financeiro, sendo projetada em consonância com as leis de proteção de dados aplicáveis¹⁵⁷. O projeto, de forma similar a EUDIW¹⁵⁸, demonstra o crescente interesse governamental em fomentar a adoção de iniciativas que coloquem os cidadãos sob o controle de seus dados pessoais, ao mesmo tempo em que ajudam a eliminar a necessidade de duplicação de informações e preenchimento

¹⁵⁵Como infere-se pelo modelo proposto no *Verifiable Credentials Data Model v2.0*. W3C. *Verifiable Credentials Data Model v2.0. W3C Working Draft*, 03 ago. 2023. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0>. Acesso em: 22 jul. 2025. sec. 1.2.

¹⁵⁶EXTRIMIAN. *QuarkID – Digital Identity Whitepaper*. 2023. Disponível em: https://github.com/ssi-quarkid/WhitePaper/blob/main/QUARK%20ID%20-%20Digital%20Identity%20-%20Whitepaper_en-US.pdf. Acesso em: 22 jul. 2025.; CRYPTO BRIEFING. *Buenos Aires Launches Blockchain-Based Digital Identity Protocol QuarkID*. 2023. Disponível em: <https://cryptobriefing.com/buenos-aires-quarkid-launch/>. Acesso em: 22 jul. 2025.

¹⁵⁷CPQD. *FinID: A identidade digital descentralizada para o setor financeiro*. CPQD, 2022. Disponível em: https://www.gov.br/agricultura/pt-br/assuntos/politica-agricola/inovacoes-financeiras-do-agronegocio/conheca-os-participantes-do-1o-workshop-de-inovacao-financeira-do-agronegocio/cpqd/cpqd_whitepaper-finid.pdf. Acesso em: 22 jul. 2025.

¹⁵⁸À nível europeu, a iniciativa da EUDIW é acompanhada de outros projetos baseados em SSI que empregam carteiras digitais, como o *European Self-Sovereign Identity Framework* (ESSIF) no contexto da EBSI e o *EU Digital Wallet Consortium* (EWC) que já estão testando carteiras digitais compatíveis com os requisitos técnicos e organizacionais do eIDAS 2 em casos práticos. Cfr. BABEL, M.; WILLBURGER, L.; LAUTENSCHLAGER, J. *Self-sovereign identity and digital wallets*.

repetitivo de formulários, reforçando também a segurança. Ao incorporar *blockchains*, muitas soluções de carteiras de identidade digital, especialmente as impulsionadas por iniciativas governamentais, tornam evidente o movimento crescente de intersecção entre arquiteturas descentralizadas e o regime jurídico em matéria de proteção de dados pessoais, apontando para uma maior convergência entre as potencialidades tecnológicas oferecidas pela infraestrutura e o quadro regulatório referido. Esse movimento ajuda a reforçar a hipótese de que a blockchain pode funcionar como uma aliada na materialização de sistemas de identidade digital seguros, auto-soberanos e juridicamente compatíveis.

4.1. A EUDIW

Nos últimos anos foi possível observar um aumento significativo de iniciativas regulatórias europeias no ramo de tecnologias digitais¹⁵⁹. É neste contexto que vemos surgir a EUDIW, um pilar central de um novo quadro jurídico de identificação eletrónica, regulamentada e estabelecida através do eIDAS 2¹⁶⁰. O diploma trouxe alterações ao eIDAS, e surgiu vinculado à Declaração Europeia sobre os direitos e princípios digitais para a década digital¹⁶¹, que visa a garantia de que todos os cidadãos e residentes da UE tenham acesso a uma identidade digital¹⁶². Tornou obrigatório o fornecimento da carteira, pelo que cada Estado-Membro terá de disponibilizar pelo menos uma solução interoperável da EUDIW até o final de 2026, a fim de garantir uma experiência que seja minimamente consistente por toda UE¹⁶³ e que possa superar as possíveis limitações advindas do regime do eIDAS¹⁶⁴.

Através de uma aplicação móvel, proporciona o armazenamento, gestão, e compartilhamento de credenciais eletrónicas, tanto em contextos públicos como privados,

¹⁵⁹Cfr. PPAKONSTANTINO, Vagelis; DE HERT, Paul. *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'* sec. 1.

¹⁶⁰AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*. [Madrid]: AEPD, 2024. Disponível em: <https://www.aepd.es/en/press-and-communication/blog/eidas2-the-eudi-wallet-and-the-gdpr-i>. Acesso em: 22 de julho de 2025.

¹⁶¹Como se retira dos Considerando 4 do eIDAS 2.

¹⁶²Que seja acessível, segura, e de confiança, facilitando o acesso à diversos serviços. A mesma declaração também reforça que todos têm direito à proteção de seus dados pessoais, incluindo o controlo sobre a forma como tais dados pessoais são compartilhados e utilizados.

¹⁶³Cfr. AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*.

¹⁶⁴Como por exemplo, o baixo número de esquemas nacionais notificados e consequentemente a aceitação supranacional deficiente que prejudica também a interoperabilidade, bem como preocupações legítimas referentes à privacidade e proteção de dados pessoais e uma fraca cobertura no que toca a atributos eletrónicos. Cfr. EY (Ernst & Young). *Regulation (EU) 2024/1183: The new framework for a European Digital Identity*. [S.l.]: EY, 2024. Disponível em: https://www.ey.com/en_gr/technical/tax/tax-alerts/ey-regulation-eu-2024-1183-the-new-framework-for-a-european-digital-identity. Acesso em: 22 jul. 2025.

permitindo ao utente o controlo sobre os seus dados pessoais, sendo de uso voluntário e gratuito para os cidadãos¹⁶⁵. O novo texto trouxe extensas reformas para fortalecer a confiança e a segurança no contexto das identidades digitais da UE, definiu as condições de emissão da EUDIW, e ampliou a gama de serviços de confiança qualificados abrangidos pelo tal regulamento, passando a incluir, entre outros exemplos, os livros-razão eletrónicos¹⁶⁶. Estes não podem agora, portanto, terem sua validade jurídica ou admissibilidade probatória negada unicamente devido a sua natureza eletrónica ou por não serem qualificados.

Ao mesmo tempo, o regulamento veio reforçar de forma explícita os princípios de proteção de dados pessoais, quando consagra que os titulares possam selecionar, combinar, armazenar, apagar, partilhar e apresentar os dados relativos à sua identidade sob seu controlo total e exclusivo, com a possibilidade de partilha de atributos de forma seletiva, a fim de divulgar apenas o que é estritamente necessário para a transação em questão¹⁶⁷. Um dos objetivos de tal enfoque parece ser o de garantir que a carteira digital possa operar em conformidade com o RGPD, fortalecendo direitos de minimização de dados e transparência, de forma que as disposições referentes ao quadro jurídico da identidade digital europeia não derroque obrigações presentes no regime normativo¹⁶⁸. Compreende-se, portanto, a exigência de que as entidades envolvidas procedam à implementação da carteira de acordo com os princípios do RGPD, por exemplo, os de privacidade desde o momento da conceção e por defeito¹⁶⁹.

A EUDIW, de um ponto de vista legal, deverá ser mutuamente aceita pelos Estados Membros da UE, numa implementação gradual, para que interações eletrónicas que exijam a identificação forte possam eliminar barreiras no que toca o fornecimento de serviços internacionais, fomentando a interoperabilidade¹⁷⁰. Desta forma, os prestadores de serviços que dependem hoje de identificadores emitidos por plataformas privadas, como por exemplo bancos e outras instituições financeiras, passam a poder contar com um sistema público

¹⁶⁵Cfr. AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*.

¹⁶⁶Cfr. Seções 10 e seguintes do eIDAS em sua versão atual.

¹⁶⁷Cfr. EY (Ernst & Young). *Regulation (EU) 2024/1183: The new framework for a European Digital Identity*. e artigo 5º-A (4) a) do eIDAS 2.

¹⁶⁸EDPS. *Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, COM(2021) 281 final. Bruxelas: EDPS, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf. Acesso em: 22 jul. 2025. p. 2.

¹⁶⁹Cfr. Artigo 25º do RGPD.

¹⁷⁰Cfr. AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*.

Europeu que é padronizado e que tem o potencial de mitigar possíveis falta de confiabilidade ou receios que possam existir no contexto de identificações digitais e uso indevido de dados pessoais por terceiros. Assim, o eIDAS 2 pretende garantir um direito à identidade digital aos cidadãos e residentes da UE que se alinha com o objetivo da Década Digital 2030 no qual pelo menos 80% da população tenha acesso a soluções de identificação digital¹⁷¹.

4.1.1. Arquitetura técnica da EUDIW

De um ponto de vista de implementação técnica, a EUDIW baseia-se num referencial comum europeu, com referencial expresso na ARF da carteira, contendo especificações, práticas recomendadas e padrões que visam assegurar a segurança e interoperabilidade no contexto das soluções nacionais de cada país¹⁷². A ARF prevê atores principais do ecossistema, como os utentes, os fornecedores de carteiras¹⁷³, os *Person Identification Data (PID) Providers*¹⁷⁴, e *Qualified Electronic Attestation of Attributes (QEAA) Providers*¹⁷⁵. Adicionalmente, estão presentes os conceitos de *Relying Parties* (ou utilizadores), entidades públicas ou privadas que requisitam acesso à atributos¹⁷⁶ com aprovação do utente, os de órgãos de supervisão e de acreditação nacionais, entre outros¹⁷⁷. Como forma de viabilizar a implementação, a carteira integra diferentes componentes e mecanismos de arquitetura para, por exemplo, proteger as chaves de assinatura e autenticação, podendo recorrer a elementos seguros armazenados no dispositivo do utente, ou integrar componentes externos¹⁷⁸.

¹⁷¹COMISSÃO EUROPEIA. 2030 *Digital Compass: the European way for the Digital Decade*. COM(2021) 118 final. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118>. Acesso em: 22 jul. 2025. sec. 3.3.

¹⁷²Sem abrir mão da necessária flexibilidade que permitirá futuros desenvolvimentos tecnológicos em conexão com este ecossistema. Cfr. AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*.

¹⁷³Que são Estados Membros ou organizações mandatadas ou reconhecidas por Estados Membros que disponibilizam a aplicação e que devem ser certificadas.

¹⁷⁴Que são geralmente entidades confiáveis que verificam a identidade e emitem um PID ao utente.

¹⁷⁵Os que mantêm uma interface para, quando requisitados, fornecer QEAA's e que em muitos casos têm também de verificar a identidade do utente.

¹⁷⁶Contidos, por exemplo, num PID ou QEAA.

¹⁷⁷O quadro técnico da EUDIW suporta a identificação eletrónica, prova de identidade, bem como a autenticação eletrónica com nível alto de garantia, diretamente através da carteira em nome do utente, no contexto da prestação de diversos serviços digitais, online e offline, públicos e privados.

¹⁷⁸Como *smartcards*, no caso de o dispositivo do utente não possuir suficiente segurança à nível de hardware, possibilitando também soluções híbridas. EUDIW CONSORTIUM. *Architecture and Reference Framework: Main Document*. [S.l.]: GitHub, 2024. Versão 2.4.0. Disponível em: <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#33-wallet-providers>. Acesso em: 22 jul. 2025. secs. 2., 3. e 4.3.2.

Desta forma, um utente possuirá carteiras vinculadas à sua identidade digital verificada, e que são por norma confirmadas por via de um documento oficial, de forma que a verificação inicial assegura um nível elevado de garantia, ou “LoA Alto”, de acordo com o proposto pelo eIDAS. As chaves criptográficas que estão associadas a tais credenciais são detidas pelo utente e preferencialmente armazenadas em elementos do dispositivo considerados seguros¹⁷⁹. Do ponto de vista tecnológico, a carteira em questão coloca, portanto, o utente no controlo de suas credenciais digitais, que se vê habilitado para decidir com quem as partilhar e quando. Abrindo espaço para outras iniciativas inspiradas no modelo de SSI¹⁸⁰, de um ponto de vista prático, funciona como uma aplicação móvel na qual o indivíduo tem a possibilidade de armazenar atestados eletrónicos de atributos pessoais que são emitidos por autoridades competentes. Estes correspondem a credenciais verificáveis segundo determinado padrão, como por exemplo, credenciais profissionais, diplomas e documentos de identificação¹⁸¹. Para ajudar a garantir a autenticidade e integridade dos dados contidos numa credencial, estas são também assinadas digitalmente pelos seus emissores.

Quando trata-se dos atestados eletrónicos de atributos pessoais, de um ponto de vista puramente legal, e de acordo com quem os emitiu, a carteira distingue diferentes categorias legais, como QEAs. Os tais atestados possuem elementos que os caracterizam, nomeadamente, um conjunto de atributos, metadados, provas, e é possível encontrar diferentes formatos padronizados em conexão com a emissão de atestados eletrónicos, como por exemplo, o ISO/IEC 18013-5¹⁸², e as *W3C Verifiable Credentials Data Model v 2.0*¹⁸³.

¹⁷⁹De forma a permitir que somente o tal utente tenha possibilidade de assinar digitalmente transações associadas à identidade ou ainda concretizar assinaturas eletrónicas qualificadas através da carteira.

¹⁸⁰SÜMER, Bilgesu. *The eIDAS 2.0 proposal and the uncertain future of electronic ledgers as trust services: Is blockchain here to stay?* CiTiP Blog, KU Leuven, 6 jun. 2023. Disponível em: <https://www.law.kuleuven.be/citip/blog/the-eidas-2-0-proposal-and-the-uncertain-future-of-electronic-ledgers-as-trust-services-is-blockchain-here-to-stay/>. Acesso em: 22 jul. 2025.

¹⁸¹Cfr. AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I)*.

¹⁸²Os atributos informam sobre o sujeito que é objeto do atestado, enquanto os metadados informam sobre o atestado em si, e as provas garantem a integridade e autenticidade desses atestados e possibilitam a divulgação seletiva de atributos. Há que considerar ainda o esquema de atributos, ou schema, que define a organização lógica, a estrutura, e formatação de cada atributo, bem como os mecanismos de prova que determinam o método a ser utilizado para criar as tais provas acima referidas. Cfr. EUDIW CONSORTIUM. *Architecture and Reference Framework*. secs. 3.8., 5.1., 5.2.5. e 5.3.2. ; ISO. (2021). *Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application*, ISO/IEC Standard No. 18013-5:2021. Disponível em: <https://www.iso.org/standard/69084.html>. Acesso: 27. jul. 25.

¹⁸³O modelo pode ser definido como um padrão desenvolvido pelo W3C que visa facilitar a emissão, partilha e verificação de credenciais digitais de forma privada e segura, suportando múltiplos usos e propondo um esquema genérico de atributos que é agnóstico quando trata-se de formatos de dados e mecanismos de prova. Cfr. W3C. *Verifiable Credentials Data Model v2.0*. sec. 1. e EUDIW CONSORTIUM. *Architecture and Reference Framework*. sec. 5.3.4.

Cabe destacar os livros-razão eletrónicos, principalmente no que toca ao seu processo de criação e atualização, que pode implicar a utilização de *blockchain*, com caráter facultativo. O conceito de livros-razão eletrónicos é introduzido no Considerando 68 do eIDAS 2, postulando que estes estabelecem uma ordem cronológica confiável de entradas de dados, numa sequência de registos de dados eletrónicos que garantem a integridade e exatidão cronológica destes, a fim de proporcionar serviços de forma mais eficiente quando combinados com outras tecnologias. Exemplos disso podem incluir a implementação de sistemas de colaboração supranacional entre instituições académicas, a cooperação aduaneira transfronteiriça e até mesmo a implementação de sistemas de votação eletrónica.

A natureza específica dos livros-razão eletrónicos, por exemplo no que toca à ordem cronológica sequencial de registos de dados, implica que estes diferem de outros serviços de confiança, como os selos temporais eletrónicos e os serviços de envio registado eletrónico, também previstos no regulamento. No sentido de assegurar a segurança jurídica e fomentar a inovação, faz-se necessária a criação, a nível europeu, de um quadro jurídico que preveja o reconhecimento de serviços de confiança no que toca ao registo de dados em livros-razão eletrónicos. Tal enquadramento confere a estes, quando qualificados, de uma presunção legal de unicidade e exatidão da sequência cronológica dos registos, bem como da própria integridade destes últimos. Procura-se, desta forma, evitar, por exemplo, que um mesmo ativo digital seja duplicado e alienado mais do que uma vez a partes distintas¹⁸⁴.

No que toca ao processo de criação e atualização de um livro-razão eletrónico, este pode variar consoante a respetiva arquitetura, se é distribuída ou centralizada, de modo que o eIDAS 2 preza pela neutralidade tecnológica. O legislador não privilegiou ou discriminou qualquer tecnologia a ser empregue na implementação deste novo serviço de confiança, abrindo caminho para implementação de *blockchains* no ecossistema. A carteira representa, portanto, uma solução híbrida que possibilita a integração de modelos federados e descentralizados, promovendo um ciclo de vida de dados mais eficiente e confiável através da utilização de credenciais verificáveis¹⁸⁵ e que permite a utilização de *blockchains* do seu ecossistema.

¹⁸⁴Cfr. Considerando 68 e secção 11 do eIDAS em sua versão atual.

¹⁸⁵COMISSÃO EUROPEIA. *Five DEP Grantees selected to support EBSI's node infrastructure, use case development and to pilot EBSI in the EU Digital Identity Wallet ecosystem*. Bruxelas: Comissão Europeia, 28 ago. 2023. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/DEP%2Bgrantees>. Acesso em: 15 jul. 2025.

4.1.2. Intersecção com outras iniciativas europeias relevantes

A fim de validar a carteira na prática, quatro projetos piloto foram lançados para testar a funcionalidade da EUDIW em contextos de uso comum, explorando no total 11 usos práticos principais que passam desde o acesso a serviços públicos e abertura de contas bancárias até assinatura de contratos e realização de pagamentos¹⁸⁶. Entre os projetos, o DC4EU¹⁸⁷ é o que apresenta maior relevância para a presente discussão, visto ser a primeira iniciativa europeia a fazer uso, em larga escala, da EBSI como fonte confiável de dados para implementação da EUDIW¹⁸⁸. Visa apoiar iniciativas relativas à educação e segurança social através do estabelecimento de serviços digitais interoperáveis, auxiliando na concretização da EUDIW, testando a aplicabilidade da carteira no âmbito da emissão de certificados educacionais e verificação de qualificações profissionais e também no campo da segurança social¹⁸⁹. De um ponto de vista político, o projeto alinha-se com outras iniciativas como a *EU Data Strategy*¹⁹⁰ e o próprio RGPD¹⁹¹.

A EBSI, iniciativa da UE da qual o DC4EU depende, foi concebida no contexto da criação da EBP¹⁹². Integrando a estratégia europeia de *blockchain* e Web3, que por via da EBP pretendia desenvolvê-la e viabilizá-la, foi desenhada a fim de proporcionar uma infraestrutura descentralizada que fosse segura e confiável, auxiliando diversos serviços públicos e

¹⁸⁶COMISSÃO EUROPEIA. *EUDI Wallet Implementation*. Bruxelas: Comissão Europeia, 2024. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>. Acesso em: 22 jul. 2025.; COMISSÃO EUROPEIA. *EUDI Wallet – Technical Specifications*. Bruxelas: Comissão Europeia, 2024. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications>. Acesso em: 22 jul. 2025.

¹⁸⁷DC4EU. *Home*. 2025. Disponível em: <https://www.dc4eu.eu/>. Acesso em: 22 jul. 2025.

¹⁸⁸OPI PIB. *Digital Credentials for Europe (DC4EU)*. Informação publicada no site do OPI – Estado Polonês, 2025. Disponível em: <https://opi.org.pl/en/project/digital-credentials-for-europe-dc4eu/>. Acesso em: 27 jul. 2025.

¹⁸⁹Através da participação na execução do *portable document A1* (PDA1) e do *European Health Insurance Card* (EHIC).

¹⁹⁰COMISSÃO EUROPEIA. *European Data Strategy*. Bruxelas: Comissão Europeia, 2020. Disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. Acesso em: 27 jul. 2025.

¹⁹¹DC4EU. *Digital Credentials for Europe*. 2025. Disponível em: <https://www.dc4eu.eu>. Acesso em: 27 jul. 2025.

¹⁹²A EBP pretende impulsionar, num contexto transfronteiriço, serviços para administrações públicas, cidadãos, empresas e ecossistemas relacionados para verificar informação e tornar tais serviços confiáveis, através da utilização de tecnologia *blockchain*. Cfr. COMISSÃO EUROPEIA. *Digital Building Blocks – EUDI Wallet Technical Architecture and Implementation*. Bruxelas: Comissão Europeia, 2024. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=668536422>. Acesso em: 27 jul. 2025; DC4EU CONSORTIUM. *D1.1 Project Management Handbook*, versão 1.0. set. 2023. Disponível em: https://dm158x9fyzgp.cloudfront.net/wp-content/uploads/2024/02/DC4EU_D1.1_Project_Management_Handbook_v.01.pdf. Acesso em: 27 jul. 2025. sec. 2.5.2.

interações digitais internacionais¹⁹³, e deverá ver sua capacidade e serviços expandidos no decorrer do tempo¹⁹⁴.

A EBSI desenvolveu diferentes estruturas a fim de suportar múltiplas utilizações práticas, agrupadas em áreas temáticas chave, como por exemplo credenciais verificáveis, assentes num padrão de compartilhamento que é auto-soberano e que coloca os titulares das credenciais no controlo total, decidindo quando, por quem e como tal informação é verificada¹⁹⁵. Neste sentido, alinha-se, portanto, com o princípio elaborado pelo Considerando 7 do RGPD, e utiliza-se também do padrão de credenciais verificáveis da W3C referido anteriormente. Cabe mencionar que nenhuma implementação da EBSI armazena dados pessoais on-chain, apenas registos de referência¹⁹⁶ e que, a fim de cumprir com leis de proteção de dados, garantir a privacidade dos titulares e impossibilitar a sua rastreabilidade, a EBSI desenvolve um *Credential Status Framework* que inclui mecanismos de revogação de credenciais, prevenindo que emissores ou terceiros possam fazer a ligação entre utentes e revogações¹⁹⁷, conciliando auditabilidade e transparência com o RGPD.

A arquitetura dessa iniciativa tem como componentes chave contratos inteligentes, APIs expostas publicamente online¹⁹⁸ e um livro-razão, que juntos propiciam o compartilhamento de dados de forma confiável, facilitando transações digitais¹⁹⁹. Conta com uma rede de nós distribuída que visa garantir que não haja um ponto único de falha na rede, promovendo a robustez e confiança do sistema e consubstanciando-se na primeira

¹⁹³DC4EU CONSORTIUM. *D8.1 Governance, Registries and Frameworks*, versão 1.0, fev. 2024. Disponível em:

https://dm158x9fyyzgp.cloudfront.net/wp-content/uploads/2024/02/DC4EU_D8.1_Governance-registries-and-frameworks_v1.0.pdf. Acesso em: 27 jul. 2025. p. 19.

¹⁹⁴COMISSÃO EUROPEIA. *Estratégia Blockchain e Web3*. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/blockchain-strategy>. Acesso em: 27 jul. 2025.

¹⁹⁵COMISSÃO EUROPEIA. *EBSI*. Bruxelas: Comissão Europeia, 2023. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI>. Acesso em: 27 jul. 2025.

¹⁹⁶Ao utilizar *blockchain*, no contexto da EBSI, a EUDIW pretende garantir a integridade e a autenticidade das credenciais emitidas ao utente, através de um registo transparente e imutável de todos os documentos emitidos (sem armazenar os documentos em si na rede). COMISSÃO EUROPEIA. *Verifiable Credentials Building Block*, 2023. Disponível em:

https://cartool-ec.github.io/eGovERA_BA_RA/id-3d54d4b1/elements/id-16ba8b9f19f84352bf0dd35068728937.html. Acesso em: 27 jul. 2025.

¹⁹⁷Cfr. COMISSÃO EUROPEIA. *EBSI*.

¹⁹⁸Neste contexto específico, permite que a conexão com a EBSI seja feita por quem a utiliza a fim de obter acesso à informação. Cabe salientar que a API é uma combinação de regras e protocolos, operando como um contrato entre as partes, que permitem que aplicações se comuniquem a fim de partilhar recursos, funcionalidades e informações. IQBAL, F. N.. *A brief introduction to application programming interface (API)*. 2023. Disponível em:

https://www.researchgate.net/publication/375828540_A_BRIEF_INTRODUCTION_TO_APPLICATION_PROGRAMMING_INTERFACE_API. Acesso em: 27 jul. 2025.

¹⁹⁹Cfr. COMISSÃO EUROPEIA. *EBSI*.

infraestrutura *blockchain* impulsionada pelo setor público na UE²⁰⁰. Uma das razões que mais fomentou investimentos na iniciativa foi o crescimento de fraudes, inteligência artificial generativa e *deep fakes*²⁰¹. Enquadrado neste cenário, há um ecossistema de nós que suporta aplicações diversas para casos específicos e que contava com 15 nós validadores ativos, operacionais e estáveis em fevereiro de 2025²⁰². Estes são os responsáveis por armazenar de forma descentralizada os componentes chave acima referidos e sincronizar suas cópias do livro-razão.

Do exposto, entende-se que a estratégia europeia, no que toca à *blockchain*, reconhece o potencial da tecnologia para melhorar a transparência, eficiência e segurança em diversos setores²⁰³. A postura adotada pela Comissão Europeia através de suas iniciativas demonstram apoio ao desenvolvimento e utilização, focando em determinadas áreas específicas, de tais arquiteturas, em consonância com valores e diplomas legais europeus, por conseguinte abarcando inclusivamente as leis de proteção de dados e de privacidade europeias. Por via de exemplo, é reconhecido que a *blockchain* pode contribuir para a implementação da EUDIW e ajudar a viabilizar outras formas de autenticação no contexto de identidades digitais, proporcionar altos níveis de cibersegurança, fornecer um alto nível de confiança, já sendo utilizada em projetos piloto (sempre de forma a garantir a conformidade com o quadro europeu no que toca a proteção de dados pessoais e privacidade)²⁰⁴. Elementos chave, como promover a segurança jurídica, a utilização de *blockchain* para sustentabilidade, apoiar a interoperabilidade e padrões comuns, ajudar a desenvolver habilidades relativas à *blockchain* e a criação de serviços públicos pan-europeus (que consubstanciou-se inclusivamente na criação da EBSI) fazem parte da estratégia²⁰⁵.

²⁰⁰COMISSÃO EUROPEIA. *European Blockchain Partnership*. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership>. Acesso em: 27 jul. 2025.

²⁰¹COMISSÃO EUROPEIA. *Blockchain: Creation of EUROPEUM-EDIC*. Bruxelas: Comissão Europeia, 22 maio 2024. Disponível em: <https://digital-strategy.ec.europa.eu/en/news/blockchain-creation-europeum-edic>. Acesso em: 27 jul. 2025.

²⁰²COMISSÃO EUROPEIA. *The EBSI Production-grade Network has reached the 15 validator nodes milestone*. Bruxelas: Comissão Europeia, 2025. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/The+EBSI+Production-grade+Network+has+reached+the+15+validator+nodes+milestone>. Acesso em: 27 jul. 2025.

²⁰³DC4EU Consortium. *D8.1 Governance, Registries and Frameworks*. p. 19.

²⁰⁴Cfr. COMISSÃO EUROPEIA. *European Data Strategy*.

²⁰⁵DAMVAKERAKI, Tonia. *Overview of the EU Blockchain Strategy*. EU Blockchain Observatory & Forum, maio 2023. Disponível em: <https://eufordigital.eu/wp-content/uploads/2023/04/Tonia-Damvakeraki-Overview-of-the-EU-blockchain-strategy.pdf>. Acesso em: 27 jul. 2025. p. 7.

Nesse contexto, a Comissão Europeia reconhece a importância de clareza do regime regulatório em relação às aplicações baseadas em *blockchain* e busca evitar a fragmentação do quadro jurídico europeu²⁰⁶, por exemplo, através da criação e recente entrada em vigor do Regulamento (UE) 2023/1114 (MiCA)²⁰⁷ e do Regulamento (UE) 2022/858 (*DLT Pilot Regime*)²⁰⁸. Também foi alterado o regime relativo à prevenção de lavagem de dinheiro e branqueamento de capitais no que tocam criptoativos²⁰⁹, houve introdução de livros-razão eletrônicos no contexto do eIDAS 2 supramencionado, e a inclusão de provisões a respeito de contratos inteligentes no Regulamento (UE) 2023/2854 (Lei de Dados)²¹⁰. Neste sentido, foi criada a *European Blockchain Sandbox* (EBS)²¹¹, a fim de prevenir a falta de uniformidade regulatória, fornecendo um ambiente propício para trocas e diálogos transfronteiriços entre autoridades de supervisão, reguladores e inovadores no campo da *blockchain*.

Em conexão com outros elementos chave da referida estratégia, a Comissão Europeia está envolvida com o desenvolvimento de modelos comuns para padronização de tecnologias descentralizadas, como o ISO TC 307²¹², e colabora com frequência com o setor privado, academia, e a comunidade à volta de tais tecnologias, como observa-se pela parceria representada pela INATBA, que visa levar a diante o ecossistema *blockchain* no território²¹³. A partir do estudo das iniciativas supramencionadas, é possível perceber o foco que a UE colocou nos últimos anos em desenvolver um quadro técnico e jurídico para o desenvolvimento de tecnologias *blockchain*, em conformidade com leis de proteção de dados pessoais e privacidade europeias. Diversos projetos e modelos demonstram a viabilização dessa compatibilidade, ainda que gradual e cautelosa, apontando que a descentralização e o respeito pelo RGPD podem coexistir.

4.1.3. A EUDIW e o RGPD: convergência normativa

²⁰⁶Cfr. COMISSÃO EUROPEIA. *European Data Strategy*.

²⁰⁷UE. Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 6 de junho de 2023.

²⁰⁸UE. Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2022.

²⁰⁹UE. Regulamento (UE) 2024/1624 do Parlamento Europeu e do Conselho, de 31 de maio de 2024.

²¹⁰UE. Regulamento (UE) (UE) 2023/2854 do Parlamento Europeu e do Conselho de 13 de dezembro de 2023.

²¹¹EUROPEAN BLOCKCHAIN OBSERVATORY & FORUM. *European Blockchain Sandbox*. Bruxelas: Comissão Europeia, 2024. Disponível em: https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en. Acesso em: 27 jul. 2025.

²¹²ISO/TC 307. *Blockchain and distributed ledger technologies – Technical Committee of ISO*. ISO, 2025. Disponível em: <https://www.iso.org/committee/6266604.html>. Acesso em: 27 jul. 2025.

²¹³Cfr. Comissão Europeia. *European Data Strategy*; DAMVAKERAKI, Tonia. *Overview of the EU Blockchain Strategy*. p. 8.

O desenvolvimento da EUDIW foi acompanhado de perto pelos órgãos europeus de proteção de dados, sendo que o EDPS publicou um parecer formal acerca da proposta relativa à carteira, confirmando que *blockchains*, quando utilizadas como registos eletrónicos qualificados, não seriam elemento obrigatório da carteira digital, mas funcionando como opcionais em certos casos específicos. A EUDIW, ainda que timidamente, é mais um passo na implementação de sistemas de identidades que caminham em direção à um modelo de SSI. Apesar de o EDPS sublinhar que, no caso de recorrer-se a tecnologias descentralizadas, as orientações relativas à proteção de dados pessoais deveriam ser respeitadas, salientando os já conhecidos possíveis problemas no que toca à irreversibilidade de registos em *blockchain*²¹⁴, a EUDIW nos moldes descritos é já uma realidade em andamento²¹⁵. De qualquer modo, é possível observar pela leitura do atual eIDAS²¹⁶, que o utente detém o poder de “solicitar, obter, seleccionar, combinar, armazenar, apagar, partilhar e apresentar de forma segura” sob seu controlo exclusivo dados de identificação pessoal. Assim, entende-se que é o próprio utente que solicita a emissão de uma credencial, reforçando a centralidade deste no modelo proposto.

A conformidade com o RGPD ocupa figura central no desenho da EUDIW, de modo que o artigo 2º do regulamento explicitamente não afasta a aplicação do quadro normativo vigente em matéria de proteção de dados pessoais. A partir de uma análise do Considerando 7 do RGPD, infere-se que o titular de dados pessoais deverá ter controlo sobre seus próprios dados, e a carteira vai no sentido de implementar e concretizar tal princípio na esfera da identidade digital europeia²¹⁷. Por exemplo, em alinhamento com o conceito de SSI e com o RGPD²¹⁸, um painel de controlo comum deve ser fornecido garantindo um alto grau de privacidade, transparência e controlo dos utentes sobre seus dados pessoais, de acordo com o proposto no Considerando 13 do eIDAS 2. O diploma, em seus considerandos e dispositivos, faz questão de explicitar que o tratamento de dados pessoais no ecossistema deve observar

²¹⁴Possivelmente conflitando com o direito ao apagamento ou retificação, e a possibilidade de transferências internacionais no contexto de participantes do ecossistema, por exemplo, nós, estarem fora dos territórios da UE. EDPS. *Formal Comments on the Proposal for a Regulation on a European Digital Identity*. p. 2.

²¹⁵COMISSÃO EUROPEIA. *EU Digital Identity Wallet – Home*. Bruxelas: Comissão Europeia, 2025. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home>. Acesso em: 27 jul. 2025.

²¹⁶Por exemplo no artigo 5º-A número 4 alínea a) do eIDAS em sua versão final.

²¹⁷Por exemplo, no artigo 5º-A número 14 da versão atual do eIDAS, entende-se que os utentes detém controlo sobre a sua carteira e os dados nela contidos.

²¹⁸Especialmente o Considerando 7 do RGPD.

integralmente o RGPD, incluindo nos casos em que livros-razão ou outros mecanismos tecnológicos forem utilizados²¹⁹. No referido painel de controlo comum, deverá ser possível a visualização, pelo utente, de suas transações, as *Relying Parties* com quem compartilhou informações, incluindo os atributos, e quais dados foram fornecidos²²⁰.

Os agentes envolvidos continuam sujeitos às obrigações e princípios do RGPD, pelo que é possível concluir que nada no regime da identidade digital em questão dispensa, por exemplo, a necessidade do consentimento por parte do titular para que uma *Relying Party* tenha acesso aos seus atributos²²¹, tal como de acordo com o ARF, o utente dá o seu consentimento ao verificador aquando da apresentação de atributos solicitados e é este quem tem o poder exclusivo de partilhar e apresentar os seus dados pessoais no contexto da carteira²²², como também continuam obrigados a informar os titulares do processamento de dados de acordo com o RGPD, garantir o exercício dos direitos dos titulares, como por exemplo o direito ao apagamento e o respeito pelos princípios base do respetivo regulamento, como o da limitação da finalidade²²³. Do diploma resulta que um fornecedor da carteira só pode recolher dados que sejam estritamente necessários para a prestação dos serviços em questão, sendo vetada a combinação de tais dados com informações processadas no contexto de outros serviços quando não há pedido expresso do utente, pelo que o armazenamento entre dados relativos a serviços distintos é feito de forma logicamente separada, prevendo a inobservabilidade que garante que os fornecedores da carteira não tenham possibilidade de acessar os detalhes referentes às transações feitas pelo utente²²⁴. O eIDAS 2 também especifica em maior detalhe conceitos e princípios já elaborados pelo RGPD, como os de proteção de dados desde a conceção e por defeito, minimização de dados²²⁵.

Ainda, às *Relying parties*, em conexão com o respetivo registo que lhes é exigido e que visa facilitar aos Estados-Membros a verificação acerca da legalidade de suas atividades, ficam impostas as obrigações de Avaliação de Impacto sobre a Proteção de Dados (DPIA), já

²¹⁹Bem como, quando relevante, a Diretiva 2002/58/EC do Parlamento Europeu e do Conselho. Cfr. Considerandos 9 e 12 do eIDAS 2.

²²⁰Cfr. Considerando 13 do eIDAS 2 e art. 5-A (4) d) do eIDAS atual.

²²¹Cfr. EUDIW CONSORTIUM. *Architecture and Reference Framework*. sec. 3.11.

²²²Cfr. EUDIW CONSORTIUM. *Architecture and Reference Framework*. sec. 3.11. e 6.6.4.1. bem como o artigo 5º-A (4) a) do eIDAS.

²²³No sentido dos Considerandos 13, 17 e 32 do eIDAS 2.

²²⁴Ainda que, em certos casos específicos, e sempre com o consentimento prévio e explícito do utente, os fornecedores da carteiras possam ter acesso a dados que sejam necessários para prestação de um serviço específico relacionados à EUDIW, de acordo com o Considerando 32 do eIDAS 2. Ver também artigo 5º-A (14) do eIDAS.

²²⁵Cfr. Considerando 12 do eIDAS 2.

que o eIDAS 2, no Considerando 17, traz a noção de que, sempre que o uso da carteira implicar um tratamento potencialmente de alto risco, conforme avaliação de impacto realizada, a autoridade de proteção de dados competente deve ser consultada²²⁶, especialmente no contexto de dados pessoais que enquadrem-se no artigo 9º do RGPD, como dados de saúde. Tal remissão ao proposto no artigo 35º deste diploma aparenta ter como objetivo garantir que utilizações inovadoras da carteira²²⁷ passem por um crivo preventivo de privacidade. Obrigações relativas a notificação de violações de dados pessoais nos termos do RGPD não são derogadas pelo eIDAS 2²²⁸ e o próprio registo a ser feito pelas *Relying parties*, também mencionado no supramencionado Considerando, serve ainda para promover a transparência e confiança no ecossistema.

Cabe ainda referir neste contexto que o RGPD, o Regulamento (UE) 2018/1725²²⁹, que foca na proteção de dados pessoais no âmbito do processamento por instituições europeias, e a Diretiva 2002/58/CE²³⁰, aplicam-se ao tratamento de dados pessoais aquando da implementação do eIDAS, como previsto pelo Considerando 12 do eIDAS 2, frisando a relevância do regime de proteção de dados pessoais no desenvolvimento da carteira. Consequentemente, é prevista a implementação de salvaguardas específicas estabelecidas pelo regulamento por parte dos fornecedores de meios de identificação eletrónica e de certificados eletrónicos de atributos, a fim de não possibilitar que estes combinem dados pessoais obtidos através das suas prestações de serviços com dados pessoais obtidos e processados em diferentes âmbitos, de forma que as informações processadas por estes últimos em conexão com a EUDIW devem estar logicamente separadas de outros dados²³¹.

Desta forma, quando um Estado-Membro²³² fornecer a carteira como meio de identificação eletrónica, deverá fazê-lo em conformidade com o RGPD.²³³ Adicionalmente, são previstos mecanismos para facilitar o exercício de determinados direitos do titular de dados pessoais, pelo que é importante considerar que um utente deverá ter a possibilidade de, no painel de controlo comum, exercer o direito ao apagamento de seus dados pessoais perante

²²⁶Cabe referir que pela leitura do artigo 35º (1) do RGPD, entende-se que “se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação”.

²²⁷Como, por exemplo, integrações com sistemas de saúde ou educação que envolvam o processamento de dados pessoais sensíveis.

²²⁸Cfr. Considerando 52 do eIDAS 2.

²²⁹UE. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018.

²³⁰UE. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002.

²³¹A semelhança do postulado para os fornecedores da carteira.

²³²Ou os seus organismos, ou terceiros atuando em seu nome.

²³³Como resulta do artigo 5º-A (17) do eIDAS.

uma *Relying Party*, bem como proceder à denúncia à autoridade nacional de proteção de dados competente, diretamente através da carteira, de possíveis pedidos para fornecimento de informações suspeitos ou ilegítimos²³⁴.

Inclusivamente, se um prestador qualificado de serviços de confiança deixa de cumprir os requisitos aplicáveis, também no que toca a conformidade com RGPD, este último pode vir a ser destituído de seu estatuto como tal²³⁵. A interligação entre os regulamentos discutidos neste capítulo pode ser observada também na cooperação entre as autoridades de controlo competentes criadas nos termos do artigo 51º do RGPD e as entidades supervisoras a serem designadas pelos Estados-Membros em território nacional como resultado da implementação do eIDAS 2²³⁶. A convergência com o regime normativo de proteção de dados da UE pode ser observada também na posição tomada pelo legislador do eIDAS 2 no Considerando 19, ao propor que a confiança no ecossistema da EUDIW seria ainda maior no caso de partes emitentes e gestoras serem obrigadas a, de acordo com o risco em questão, implementar medidas técnicas e organizacionais a fim de garantir um alto nível de segurança aos utentes e seus dados pessoais de acordo com o RGPD. Os próprios requisitos relativos à cibersegurança elencados no eIDAS 2 podem, de fato, contribuir para a proteção de dados pessoais e privacidade dos utentes²³⁷. A preocupação com a conformidade entre os regimes pode ser também observada no contexto do estabelecimento dos requisitos de consideração para regimes de confiança de países terceiros e sua equivalência perante o regime relativo aos serviços de confiança qualificados e prestadores proposto na UE²³⁸.

Importa referir que a divulgação seletiva de atributos, estabelecida no quadro jurídico da EUDIW²³⁹, é um dos elementos chave no contexto de atestados eletrónicos, empoderando o indivíduo, de forma granular, para decidir quais dados partilhar²⁴⁰, e possibilitando que este prove certa informação específica sem que outros dados pessoais não relevantes para o propósito em questão sejam revelados em conjunto. Por via de exemplo, a técnica permite no contexto da carteira que alguém que necessite provar que é maior de 18 anos não precise

²³⁴Cfr. Considerando 13 do eIDAS 2 e o artigo 5º-A (4) ii) do eIDAS.

²³⁵Um prestador qualificado de serviços de confiança é definido como um que “preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora” Cfr. artigos 3º (20) e 20º (3-B) do eIDAS.

²³⁶Reforçando a abordagem integrada. Cfr. Artigos 46º-A (4) g). e 46º-B (4) f) do eIDAS.

²³⁷Como se entende pelo Considerando 27 do eIDAS 2.

²³⁸Cfr. Considerando 47 do eIDAS 2.

²³⁹Cfr. artigo 5º-A (4) a) do eIDAS.

²⁴⁰Cfr. W3C. *Verifiable Credentials Data Model v2.0*. sec. 3.2.

compartilhar a totalidade de informações contidas em seu cartão de cidadão (como o nome completo ou até mesmo a data de nascimento), mas apenas sua data de nascimento ou um atestado relativo à sua idade, eventualmente gerado através de prova criptográfica, como por exemplo, “idade ≥ 18 ”²⁴¹.

Já que um titular de dados pessoais têm a possibilidade de apenas compartilhar dados que são estritamente necessários para cada finalidade específica, a solução técnica da EUDIW pretende resolver o processamento excessivo de dados pessoais, como foi salientado pelo EDPS²⁴². Tal recurso é viável graças a métodos considerados avançados de criptografia e inclui, por exemplo, as referidas ZKPs²⁴³, úteis para atender ao princípio de minimização de dados e proteção de dados desde a concepção e por defeito, bem como para conformidade automatizada com a preservação da privacidade. A utilização destes métodos na validação de atributos são inclusive explicitamente incentivados pelo eIDAS 2 como forma de preservar a privacidade dos indivíduos²⁴⁴.

Com o desenvolvimento tecnológico, existem atualmente diversos exemplos de PETs como as ZKPs, divulgação seletiva de atributos, já acima mencionados, mas também a *Multi-Party Computation* (MPC) que é um algoritmo criptográfico que possibilita que chaves privadas sejam divididas e distribuídas em múltiplas partes, permitindo que computação seja feita sobre cada uma mantendo os dados em segredo²⁴⁵, *hashes* que permitem a conversão de determinada informação em uma sequência de comprimento não variável de números e letras, criptografia homomórfica que permite cálculos em dados criptografados sem descriptografá-los e assim possibilitando o processamento seguro de informações confidenciais²⁴⁶, ambientes de execução confiáveis (TEEs) que são uma área segura de um

²⁴¹EDPS. *Formal Comments on the Proposal for a Regulation on a European Digital Identity*.

²⁴²Ibidem.

²⁴³Como outro exemplo do ZKPs, a Google Wallet utilizou-se da técnica para verificar a idade de usuários: CoinDesk. *Google Adds Blockchain Tech to Wallet to Let Users Prove Age Without Sharing Data*, 2 mai. 2025. Disponível em: <https://www.coindesk.com/markets/2025/05/02/google-adds-zero-knowledge-proofs-to-wallet-for-age-verification>. Acesso em: 27 de julho de 2025.

²⁴⁴Cfr. Considerando 14 do eIDAS 2.

²⁴⁵“Desenvolvido por Adi Shamir no final da década de 1970, o compartilhamento secreto de Shamir é um algoritmo de criptografia no qual uma chave privada é dividida em partes, distribuídas entre diferentes atores, de modo que cada um possui apenas parte do segredo, garantindo que ninguém o tenha inteiro. O segredo só pode ser obtido por meio da recombinação das partes.” Tradução livre. Cfr. IEEE. *What Is Multiparty Computation?* Digital Privacy Initiative, IEEE, 2025. Disponível em: <https://digitalprivacy.ieee.org/publications/topics/what-is-multiparty-computation/>. Acesso em: 27 jul. 2025.

²⁴⁶ROCHA, V.F.; LÓPEZ, J. *An Overview on Homomorphic Encryption Algorithms*. Relatório Técnico IC-PFG-18-28, Instituto de Computação, Universidade Estadual de Campinas, 2018. Disponível em: <https://www.ic.unicamp.br/~reltech/PFG/2018/PFG-18-28.pdf>. Acesso em: 27 jul. 2025. sec. 1.

processador computacional que garante que o código e os dados carregados nele sejam protegidos com relação à confidencialidade e integridade²⁴⁷, VPNs descentralizadas que são redes privadas virtuais descentralizadas que roteiam o tráfego por meio de vários nós independentes sem um servidor central²⁴⁸, e também mecanismos de rotação de chaves e desvinculação, que são medidas técnicas que reduzem a vinculação persistente de dados a identidades²⁴⁹.

Em conformidade com o proposto pelo CNIL para o uso responsável da *blockchain* no contexto de dados pessoais²⁵⁰, tais mecanismos inovadores de conformidade adaptados a ambientes descentralizados têm o potencial para, quando necessário, serem ferramentas essenciais de uma infraestrutura de conformidade, por exemplo, com o RGPD. Essas técnicas, quando aplicadas corretamente, oferecem a possibilidade de reduzir substancialmente os riscos e podem satisfatoriamente atender ao Artigo 25º do RGPD em ambientes distribuídos. Recentes desenvolvimentos regulatórios e institucionais reforçam ainda mais a viabilidade da verificação de identidade com preservação da privacidade, baseada, por exemplo, em ZKPs. Particularmente, um demonstrador público da CNIL de 2023 nesta matéria demonstra como provas de atributos criptográficos, geradas de forma local a partir de identidades eletrônicas emitidas pelo governo, podem permitir que os utentes comprovem que, por exemplo, atingiram a maioria legal, sem revelar quaisquer dados pessoais adicionais ou transmitir informações a terceiros²⁵¹.

A autoridade francesa confirmou que tal sistema funciona sem registros rastreáveis, bancos de dados centrais ou transferências de dados pessoais, alinhando com os princípios do RGPD da minimização de dados, limitação de finalidade e privacidade desde a concepção e por defeito. Assim, o suporte de tecnologias criptográficas avançadas pode prevenir indevidas correlações, em consonância com o proposto pelo eIDAS 2, que consagra como um requisitos

²⁴⁷TECHTARGET. *What is a Trusted Execution Environment (TEE)?* TechTarget, 2025. Disponível em: <https://www.techtarget.com/searchitoperations/definition/trusted-execution-environment-TEE> . (Acesso em: 27 de julho de 2025).

²⁴⁸INDUSTRYWIRE. *Decentralized VPNs: Are They the Future of Online Security?* IndustryWired, 2025. Disponível em: <https://industrywired.com/news/decentralized-vpns-are-they-the-future-of-online-security-8623872>. Acesso em: 27 jul. 2025.

²⁴⁹YLONEN, T.; TURNER, P.; SCARFONE, K.; SOUPPAYA, M. *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. NIST Interagency Report 7966. National Institute of Standards and Technology (NIST), out. 2015. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf>. Acesso em: 27 jul. 2025. p. 42.

²⁵⁰Cfr. CNIL, *Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*. p. 4

²⁵¹CNIL. *Demonstration of a Privacy-Preserving Age Verification Process*, 2023. Disponível em: <https://linc.cnil.fr/en/demonstration-privacy-preserving-age-verification-process>. Acesso em: 27 jul. 2025.

essencial a inexistência de uma associação entre informações e atividades à um indivíduo específico a fim de prevenir vigilância e perfilagem mesmo na presença de um possível vazamento de dados pessoais²⁵².

Do exposto, é possível concluir que a EUDIW tem o potencial de demonstrar uma convergência progressiva entre arquiteturas descentralizadas e a proteção de dados pessoais, ao incorporar princípios centrais do RGPD em seu desenho técnico e normativo, ao mesmo tempo em que permite a utilização de tecnologias como a *blockchain* no seu ecossistema. O quadro proposto preserva e operacionaliza direitos fundamentais dos titulares, reforçando a centralidade do indivíduo e, de forma simultânea, integra técnicas criptográficas como as ZKPs e a divulgação seletiva de atributos. Nesse contexto, a iniciativa indica que a coexistência entre *blockchain* e proteção de dados é tanto possível quanto desejável, consolidando a EUDIW como um exemplo de harmonização entre inovação digital em ambientes descentralizados e o RGPD.

CONCLUSÕES

A crescente utilização de DLT em diversos domínios traz consigo, de forma simultânea, desafios significativos para a plena conformidade com o RGPD e um conjunto de oportunidades e soluções a considerar. Devido à sua inerente imutabilidade, descentralização e transparência conflitarem, à primeira vista, com a aplicação de princípios e normas clássicas do regulamento, uma interpretação contextualizada que reconhece as particularidades técnicas e operacionais destas infraestruturas deve ser examinada. Este antagonismo não deve ser encarado como uma incompatibilidade absoluta, antes convém apreciá-lo como um convite à reflexão regulatória, técnica e institucional sobre novas formas de garantir o cumprimento do RGPD na era digital descentralizada. A análise apresentada revelou que há, de fato, obstáculos importantes a ponderar, especialmente no que toca à atribuição de responsabilidade entre os agentes e à implementação de mecanismos eficazes de apagamento de dados.

Concomitantemente, fica evidente o surgimento de abordagens técnicas e ferramentas que viabilizam uma maior afinidade entre arquiteturas descentralizadas e o regime postulado pelo quadro regulatório europeu em matéria de proteção de dados. Essas soluções fornecem um panorama de avanços tecnológicos auspicioso que, se implementadas satisfatoriamente,

²⁵² AEPD. *eIDAS2, the EUDI wallet and the GDPR (II)*. 11 de junho de 2025. Disponível em: <https://www.aepd.es/en/press-and-communication/blog/eidas2-the-eudi-wallet-and-the-gdpr-ii>. Acesso em: 27 jul. 2025.

possibilitam uma mitigação significativa dos seus impactos, quando não uma superação desses desafios. Através das suas políticas e estratégias recentes, a UE tem demonstrado uma intenção de integrar DLT ao seu plano mais amplo de transformação digital, manifestando uma compreensão de que sistemas que assentam num ambiente, ainda que em graus distintos, de descentralização (por exemplo nos contextos de identidade digital), podem não apenas coexistir com o direito à proteção de dados pessoais, mas também ser instrumento para sua promoção, reforçando seu valor social e económico.

O caminho mais adequado parece ser não o da exclusão ou desconfiança generalizada das tecnologias *blockchain*, mas sim o da construção conjunta e equilibrada de soluções jurídicas e técnicas que reconheçam as suas especificidades e potencial. Existe um espaço legítimo e necessário para a compatibilização entre o regulamento e a utilização de DLT: a integração do RGPD com a referida tecnologia não é apenas possível, mas também necessária, a fim de dar continuidade ao progresso tecnológico no espaço europeu sem renunciar à proteção dos direitos fundamentais à privacidade e proteção de dados.

BIBLIOGRAFIA

AEPD. *eIDAS2: The EUDI Wallet and the GDPR (I) e (II)*. [Madrid]: AEPD, 2024. Disponível em: <https://www.aepd.es/en/press-and-communication/blog/eidas2-the-eudi-wallet-and-the-gdpr-i;> <https://www.aepd.es/en/press-and-communication/blog/eidas2-the-eudi-wallet-and-the-gdpr-ii>. Acesso em: 22 jul. 2025.

ALLENDE LÓPEZ, Marcos. *Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets and Blockchain*. Washington, D.C.: Inter-American Development Bank, 2020. Disponível em: <https://publications.iadb.org/en/publications/english/viewer/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignty-Digital-Wallets-and-Blockchain.pdf>. Acesso em: 22 jul. 2025.

ALVES, Alexandre. *O uso de tecnologia de registo distribuído (DLT) na negociação de ações em ambiente de bolsa de valores: análise à luz da legislação do Brasil*. *Revista Eletrônica de Direito*, n.º 2, vol. 31, jun. 2023. Disponível em: https://cij.up.pt/client/files/0000000001/3-alexandre-alves_2164.pdf. Acesso em: 13 jul. 2025.

AMMAR, Zafar. *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways*. *Journal of Cybersecurity*, 2025, vol. 11, n.º 1. Disponível em: <https://doi.org/10.1093/cybsec/tyaf002>. Acesso em: 13 jul. 2025.

ARTICLE 29 WORKING PARTY. *Opinion 1/2010 on the concepts of “controller” and “processor”* (WP 169). Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em: 14 jul. 2025.

ARTICLE 29 WORKING PARTY. *Opinion 02/2014 on the application of the Article 29 Working Party’s ruling on Data Protection in cloud computing: WP 196 revisited*. Adoptado em 1 de

julho de 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 16 jul. 2025.

ARTICLE 29 WORKING PARTY. *Opinion 05/2012 on Cloud Computing*, WP 196, adotado em 1 de julho de 2012. Disponível em: <https://www.techethics.com/assets/Opinion-05-2012-on-Cloud-Computing.pdf>. Acesso em: 16 jul. 2025.

ATENIESE, Giuseppe; MAGRI, Bernardo; VENTURI, Daniele; ANDRADE, Ewerton. *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends*. *Cryptology ePrint Archive*, report 2016/757, depositado em 11 maio 2017. Disponível em: <https://eprint.iacr.org/2016/757.pdf>. Acesso em: 16 jul. 2025.

AVELLANEDA, O. et al; *Decentralized Identity: Where Did It Come From and Where Is It Going?*, *IEEE Communications Standards Magazine*, vol. 3, n.º 4, dez. 2019, p. 10–13. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9031542>. Acesso em: 19 jul. 2025.

BABEL, M.; WILLBURGER, L.; LAUTENSCHLAGER, J. *Self-sovereign identity and digital wallets*. *Electron Markets*, v. 35, art. 28, 2025. Disponível em: <https://doi.org/10.1007/s12525-025-00772-0>. Acesso em: 25 jul. 2025.

BELEN-SAGLAM, Rahime; ALTUNCU, Enes; LU, Yang; LI, Shujun. *A systematic literature review of the tension between the GDPR and public blockchain systems*. *Blockchain: Research and Applications*, v. 4, n.º 2, 2023. Disponível em: <https://doi.org/10.1016/j.bcra.2023.100129>. Acesso em: 16 jul. 2025.

BLOCKCHAIN FOR EUROPE. *BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains*. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/bc4eu-response-to-edpb-consultation-on-gdpr-and-blockchain.pdf. Acesso em: 12 jul. 2025.

BUOCZ, Thomas; EHRKE-RABEL, Tina; HÖDL, Elisabeth; EISENBERGER, Iris, *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, *Computer Law & Security Review*, vol. 35, n.º 3, 2019, pp. 222–235. Disponível em: <https://doi.org/10.1016/j.clsr.2018.12.003>. Acesso em: 14 jul. 2025.

BUTERIN, Vitalik, *A next-generation smart contract and decentralized application platform. White paper*, [S.l.], dez. 2013 (atribuído; revisado jan. 2014), 36 p. Disponível em: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf. Acesso em: 22 jul. 2025.

CAGIGAS, D.; CLIFTON, J.; DIAZ-FUENTES, D.; FERNÁNDEZ-GUTIÉRREZ, M.; HARPES, C., *Blockchain in government: toward an evaluation framework*, *Policy Design and Practice*, vol. 6, n.º 4, 2023, p. 397–414. Disponível em: <https://doi.org/10.1080/25741292.2023.2230702>. Acesso em: 13 jul. 2025.

CNIL. *Blockchain and the GDPR*. Paris: CNIL, 2018. Disponível em: https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf. Acesso em: 14 jul. 2025.

CNIL. *Blockchain and the GDPR: solutions for a responsible use of the blockchain in the context of personal data*. 2018. Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 12 jul. 2025.

CNIL. *Demonstration of a Privacy-Preserving Age Verification Process*, 2023. Disponível em: <https://linc.cnil.fr/en/demonstration-privacy-preserving-age-verification-process>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *2030 Digital Compass: the European way for the Digital Decade*. COM(2021) 118 final. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118>. Acesso em: 22 de julho de 2025.

COMISSÃO EUROPEIA. *Blockchain: Creation of EUROPEUM-EDIC*. Bruxelas: Comissão Europeia, 22 maio 2024. Disponível em: <https://digital-strategy.ec.europa.eu/en/news/blockchain-creation-europeum-edic>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *EBSI*. Bruxelas: Comissão Europeia, 2023. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *Estratégia Blockchain e Web3*. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/blockchain-strategy>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *EU Digital Identity Wallet – Home*. Bruxelas: Comissão Europeia, 2025. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *European Blockchain Partnership*. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *European Data Strategy*. Bruxelas: Comissão Europeia, 2020. Disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *Europe's Digital Decade: digital targets for 2030. Estratégia “Uma Europa preparada para a era digital”*, prioridades 2019–2024. Bruxelas, 2021. Disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt. Acesso em: 16 jul. 2025.

COMISSÃO EUROPEIA. *European Digital Identity Regulation*. Bruxelas: Comissão Europeia, 2024. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation>. Acesso em: 22 jul. 2025.

COMISSÃO EUROPEIA. *Digital Building Blocks – EUDI Wallet Technical Architecture and Implementation*. Bruxelas: Comissão Europeia, 2024. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=668536422>. Acesso em: 27 jul. 2025.

COMISSÃO EUROPEIA. *Five DEP Grantees selected to support EBSI's node infrastructure, use case development and to pilot EBSI in the EU Digital Identity Wallet ecosystem*. Bruxelas: Comissão Europeia, 28 ago. 2023. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/DEP%2Bgrantees>. Acesso em: 15 jul. 2025.

COMISSÃO EUROPEIA. *The EBSI Production-grade Network has reached the 15 validator nodes milestone*. Bruxelas: Comissão Europeia, 2025. Disponível em: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/The+EBSI+Production-grade+Network+has+reached+the+15+validator+nodes+milestone>. Acesso em: 27 jul. 2025.

CONG, Lin William; XIE, Danxia; ZHANG, Longtian. *Knowledge Accumulation, Privacy, and Growth in a Data Economy*. *Management Science*, v. 67, n. 10, p. 6480–6492, 2021. Disponível em: <https://arxiv.org/pdf/2109.10028>. Acesso em: 16 jul. 2025.

CONLON, Thomas; CORBET, Shaen; HOU, Yang (Greg); HU, Yang; OXLEY, Les. *Bitcoin forks: What drives the branches?*. *Research in International Business and Finance*, vol. 69, 2024. Disponível em: <https://doi.org/10.1016/j.ribaf.2024.102261>. Acesso em: 26 jul. 2025.

DAMVAKERAKI, Tonia. *Overview of the EU Blockchain Strategy*. *EU Blockchain Observatory & Forum*, maio 2023. Disponível em: <https://eufordigital.eu/wp-content/uploads/2023/04/Tonia-Damvakeraki-Overview-of-the-EU-blockchain-strategy.pdf>. Acesso em: 27 jul. 2025.

DATENSCHUTZBEHÖRDE (Áustria). *Decisão no processo DSB-D123.270/0009-DSB/2018*. 5 dez. 2018.

DC4EU. *Digital Credentials for Europe*. 2025. Disponível em: <https://www.dc4eu.eu>. Acesso em: 27 jul. 2025.

DC4EU CONSORTIUM. *D1.1 Project Management Handbook*, versão 1.0. set. 2023. Disponível em: https://dm158x9fyyzgp.cloudfront.net/wp-content/uploads/2024/02/DC4EU_D1.1_Project_Management_Handbook_v.01.pdf. Acesso em: 27 jul. 2025.

DC4EU CONSORTIUM. *D8.1 Governance, Registries and Frameworks*, versão 1.0, fev. 2024. Disponível em: https://dm158x9fyyzgp.cloudfront.net/wp-content/uploads/2024/02/DC4EU_D8.1_Governance-registries-and-frameworks_v1.0.pdf. Acesso em: 27 jul. 2025.

DIÁRIO DA REPÚBLICA. *Lexionário – dados pessoais*. Disponível em: <https://diariodarepublica.pt/dr/lexionario/termo/dados-pessoais>. Acesso em: 13 jul. 2025.

EDPB. *Diretrizes 5/2019 relativas aos critérios do direito a ser esquecido pelos motores de busca ao abrigo do RGPD (Parte 1)*, versão 2.0, adotada em 7 de julho de 2020. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_pt. Acesso em: 16 jul. 2025.

EDPB, *Guidelines 02/2025 on processing of personal data through blockchain technologies*. Disponível em: https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf. Acesso em: 12 jul. 2025.

EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Versão 2.1, adotada em 07 jul. 2021. Disponível em: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 16 jul. 2025.

EDPS. *Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, COM(2021) 281 final. Bruxelas: EDPS, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf. Acesso em: 22 de julho de 2025.

EMMERT-STREIB, Frank. *From the digital data revolution to digital health and digital economy toward a digital society: Pervasiveness of Artificial Intelligence*. 26 ago. 2020. Disponível em: <https://arxiv.org/abs/2008.12672>. Acesso em: 16 jul. 2025.

EPRS. *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (Relatório STOA, PE 634.445), Bruxelas, jul. 2019. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf). Acesso em: 14 jul. 2024.

EUCL. *Response to EDPB Guidelines 02/2025 on Blockchain and Personal Data Processing*. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb-guidelines-02_2025-response-euci-with-signatories.pdf. Acesso em: 12 jul. 2025.

EUDIW CONSORTIUM. *Architecture and Reference Framework: Main Document*. [S.l.]: GitHub, 2024. Versão 2.4.0. Disponível em: <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#33-wallet-providers>. Acesso em: 22 jul. 2025.

EY (Ernst & Young). *Regulation (EU) 2024/1183: The new framework for a European Digital Identity*. [S.l.]: EY, 2024. Disponível em: https://www.ey.com/en_gr/technical/tax/tax-alerts/ey-regulation-eu-2024-1183-the-new-framework-for-a-european-digital-identity. Acesso em: 22 jul. 2025.

FARSHID, Simon; REITZ, Andreas; ROBBACH, Peter. *Design of a forgetting blockchain: A possible way to accomplish GDPR compatibility*. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Manoa: University of Hawaii at Mānoa, 2020. Disponível em: <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ae96ec9e-978a-487d-a431-108909a0afd1/content>. Acesso em: 16 jul. 2025.

FERRARI, V., QUINTAIS, J. P., GIANNOPOULOU, A., BODÓ, B. *EU Blockchain Observatory and Forum Workshop on GDPR, data policy and compliance: (08.06.2018, Brussels) : Report . (Blockchain & Society Policy Research Lab Research Nodes; No. 2018/1)*. University of Amsterdam, Institute for Information Law. (2018). Disponível em: https://blockchain-society.science/wpcontent/uploads/2018/07/blockchain_society_research_nodes_1_GDPR_workshop_03072018.pdf. Acesso em: 26 jul. 2025

FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2019.

FORBES. *EU Privacy Laws To Delete See-Through Blockchains*. 1 mai. 2025. Disponível em: <https://www.forbes.com/sites/digital-assets/2025/05/01/eu-privacy-laws-to-delete-see-through-blockchains/>. Acesso em: 12 jul. 2025.

GANGI, Paolo Maria. *Feedback in relation to the document “Guidelines 02/2025 on processing of personal data through blockchain technologies”*. Roma: Studio Gangi, 9 jun. 2025. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/feedback-edpb-gl-blockchain-v-1.0.pdf. Acesso em: 12 jul. 2025.

GHADI, Y. Y.; MAZHAR, T.; SHAHZAD, T. et al., *The role of blockchain to secure internet of medical things*. *Scientific Reports*, 2024, vol. 14, art. 18422. Disponível em: <https://doi.org/10.1038/s41598-024-68529-x>. Acesso em: 13 jul. 2025.

GODYN, M.; KEDZIORA, M.; REN, Y.; et al. *Analysis of solutions for a blockchain compliance with GDPR*. *Scientific Reports*, Londres, v. 12, art. 15021, 2 set. 2022. DOI: 10.1038/s41598-022-19341-y. Disponível em: <https://www.nature.com/articles/s41598-022-19341-y>. Acesso em: 16 jul. 2025.

GONÇALVES, Ricardo Martins; DA SILVA, Miguel Mira; DA CUNHA, Paulo Rupino. *Olympus: a GDPR compliant blockchain system. International Journal of Information Security*, Londres, v. 23, n. 2, p. 1021–1036, 17 nov. 2023. DOI: 10.1007/s10207-023-00782-z. Disponível em: <https://link.springer.com/article/10.1007/s10207-023-00782-z>. Acesso em: 16 jul. 2025.

HERIAN, R. *Blockchain, GDPR, and fantasies of data sovereignty, Law, Innovation and Technology*, vol. 12, n.º 1, 2020, p. 156–174. Disponível em: <https://doi.org/10.1080/17579961.2020.1727094>. Acesso em: 25 jul. 2025.

HUSSEIN, Z.; SALAMA, M. A.; EL-RAHMAN, S. A., *Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms, Cybersecurity*, 2023, vol. 6, art. 30. Disponível em: <https://doi.org/10.1186/s42400-023-00163-y>. Acesso em: 13 jul. 2025.

IEEE. *What Is Multiparty Computation? Digital Privacy Initiative*, IEEE, 2025. Disponível em: <https://digitalprivacy.ieee.org/publications/topics/what-is-multiparty-computation/>. Acesso em: 27 jul. 2025.

INATBA, *Response to EDPB Guidelines 02/2025 on the interplay of the AI Act and the GDPR*, 9 jun. 2025. Disponível em: https://inatba.org/wp-content/uploads/2025/06/INATBA-Response_EDPB-Guidelines-2025-06-09.pdf. Acesso em: 13 jul. 2025.

INDUSTRYWIRE. *Decentralized VPNs: Are They the Future of Online Security?* IndustryWired, 2025. Disponível em: <https://industrywired.com/news/decentralized-vpns-are-they-the-future-of-online-security-8623872>. Acesso em: 27 jul. 2025.

ITU-T. *Distributed ledger technology overview, concepts, ecosystem. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), Technical Report FG DLT D1.2*, 1 ago. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf>. Acesso em: 28 jul. 2025.

KERSIC, V.; VIDOVIC, U.; VRECKO, A.; DOMAJNKO, M.; TURKANOVIC, M. *Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. IEEE Access*, v. 11, p. 78135–78151, 2023. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10194951>. Acesso em: 25 jul. 2025.

OPI PIB. *Digital Credentials for Europe (DC4EU)*. Informação publicada no site do OPI – Estado Polonês, 2025. Disponível em: <https://opi.org.pl/en/project/digital-credentials-for-europe-dc4eu/>. Acesso em: 27 jul. 2025.

PAPAKONSTANTINO, Vagelis; DE HERT, Paul. *The regulation of digital technologies in the EU: the law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality". Technology and Regulation Journal*, maio 2022. Disponível em: SSRN: <https://ssrn.com/abstract=4123313>. Acesso em: 22 jul. 2025.

PEHLIVAN, Ceyhun N. *Spanish AEPD: Harmonising blockchain with the GDPR's right to be forgotten. Linklaters Tech Insights*, 13 nov. 2024. Disponível em: <https://techinsights.linklaters.com/post/102jo4a/spanish-aepd-harmonising-blockchain-with-the-gdprs-right-to-be-forgotten>. Acesso em: 22 jul. 2025.

POLITOU, Eugenia; CASINO, Fran; ALEPIS, Efthymios; PATSAKIS, Constantinos. *Blockchain Mutability: Challenges and Proposed Solutions. IEEE Transactions on Emerging Topics in Computing*, 2019, pp. 1–1. Disponível em:

https://www.researchgate.net/publication/336822518_Blockchain_Mutability_Challenges_and_Proposed_Solutions. Acesso em: 16 jul. 2025.

PREUKSCHAT, Alex; REED, Drummond. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY: Manning Publications, 2021.

PUDDU, I.; DMITRIENKO, A.; CAPKUN, S. *μchain: How to Forget without Hard Forks*. *IACR Cryptology ePrint Archive*, paper 2017/106. ETH Zurich, 2017. Disponível em: <https://eprint.iacr.org/2017/106.pdf>. Acesso em: 26 jul. 2025.

PUTHAL, D.; MALIK, N.; MOHANTY, S. P.; KOUGIANOS, E.; YANG, C. *The Blockchain as a Decentralized Security Framework [Future Directions]*. *IEEE Consumer Electronics Magazine*, vol. 7, n.º 2, p. 18–21, mar. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8287055>. Acesso em: 16 jul. 2025.

ROCHA, V. F.; LÓPEZ, J. *An Overview on Homomorphic Encryption Algorithms*. Relatório Técnico IC-PFG-18-28, Instituto de Computação, Universidade Estadual de Campinas, 2018. Disponível em: <https://www.ic.unicamp.br/~reltech/PFG/2018/PFG-18-28.pdf>. Acesso em: 27 jul. 2025.

SHAHSAVARI, Y.; ZHANG, K.; TALHI, C. *A Theoretical Model for Fork Analysis in the Bitcoin Network*. In: *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, EUA, 2019, p. 237–244. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8946275>. Acesso em: 26 jul. 2025.

SOLTANI, Reza; ZAMAN, Marzia; JOSHI, Rohit; SAMPALLI, Srinivas. *Distributed Ledger Technologies and Their Applications: A Review*. *Applied Sciences*, 2022. Disponível em: <https://www.mdpi.com/2076-3417/12/15/7898>. Acesso em: 13 jul. 2025.

SOVRIN FOUNDATION. *Os Princípios da Auto-Identidade Soberana (SSI)*, versão em português, 2020. Disponível em: <https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-Portuguese-v01.pdf>. Acesso em: 22 jul. 2025.

SÜMER, Bilgesu. *The eIDAS 2.0 proposal and the uncertain future of electronic ledgers as trust services: Is blockchain here to stay?* *CiTiP Blog*, KU Leuven, 6 jun. 2023. Disponível em: <https://www.law.kuleuven.be/citip/blog/the-eidas-2-0-proposal-and-the-uncertain-future-of-electronic-ledgers-as-trust-services-is-blockchain-here-to-stay/>. Acesso em: 22 jul. 2025.

SURIPEDDI, Mani Karthik Suhas; PURANDARE, Pradnya. *Blockchain Technology and Data Privacy Regulations*, *Journal of Physics: Conference Series*, vol. 1964, 2021, art. 042005. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042005/pdf>. Acesso em: 25 jul. 2025.

TATAR, U.; GÖKÇE, Y.; NUSSBAUM, B., *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, *Computer Law & Security Review*, vol. 38, 2020, art. 105454. Disponível em: <https://doi.org/10.1016/j.clsr.2020.105454>. Acesso em: 25 jul. 2025.

TECHTARGET. *What is a Trusted Execution Environment (TEE)?* TechTarget, 2025. Disponível em: <https://www.techtarget.com/searchitoperations/definition/trusted-execution-environment-TEE>. Acesso em: 27 jul. 2025.

UE. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Jornal Oficial da União Europeia, L 119, 4 mai. 2016.

UE. REGULAMENTO (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024. Jornal Oficial da União Europeia, L 202, 6 maio 2024.

UE. REGULAMENTO (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014. Jornal Oficial da União Europeia, L 257, 28 ago. 2014.

UE. *Versão consolidada do Tratado da União Europeia*. Jornal Oficial da União Europeia, C 202, p. 13, 7 jun. 2016.

ULLAH, H. S.; ASLAM, S., *Blockchain in Healthcare and Medicine: A Contemporary Research of Applications, Challenges, and Future Perspectives*. ArXiv, 2020. Disponível em: <https://arxiv.org/abs/2004.06795>. Acesso em: 13 jul. 2025.

W3C. *Verifiable Credentials Data Model v2.0. W3C Working Draft*, 03 ago. 2023. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0> Acesso em: 22 jul. 2025

WEBB, Nick. *A Fork in the Blockchain: Income Tax and the Bitcoin/Bitcoin Cash Hard Fork*. *North Carolina Journal of Law & Technology*, vol. 19, n.º 4, 2018, p. 283. Disponível em: <https://scholarship.law.unc.edu/ncjolt/vol19/iss4/10>. Acesso em: 26 jul. 2025.

YLONEN, T.; TURNER, P.; SCARFONE, K.; SOUPPAYA, M. *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. *NIST Interagency Report 7966*. National Institute of Standards and Technology (NIST), out. 2015. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf>. Acesso em: 27 jul. 2025.

YOUVAN, Douglas C. *Navigating the Evolution of Ethereum: Vitalik Buterin's Vision for DeFi Governance and Scalability*, ago. 2024. Disponível em: https://www.researchgate.net/publication/383425035_Navigating_the_Evolution_of_Ethereum_Vitalik_Buterin's_Vision_for_DeFi_Governance_and_Scalability. Acesso em: 22 jul. 2025.

ZIBIN ZHENG; XIE, Shaoan; DAI, Hong-Ning; CHEN, Weili; CHEN, Xiangping; WENG, Jian; IMRAN, Muhammad. *An Overview on Smart Contracts: Challenges, Advances and Platforms*, arXiv, dez. 2019. Disponível em: <https://arxiv.org/abs/1912.10370>. Acesso em: 13 jul. 2025.

Jurisprudência

TRIBUNAL DE JUSTIÇA (Terceira Secção). *Smaranda Bara e o. v. Preşedintele Casei Naţionale de Asigurări de Sănătate e outros*. Processo C-201/14. 1 out. 2015. ECLI:EU:C:2015:638.

TRIBUNAL DE JUSTIÇA (Grande Secção). *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*. Processo C-210/16. 5 jun. 2018. ECLI:EU:C:2018:388.

TRIBUNAL DE JUSTIÇA (Terceira Secção). *Gesamtverband Autoteile-Handel eV v. Scania CV AB*. Processo C-319/22. 9 nov. 2023. ECLI:EU:C:2023:837.

TRIBUNAL DE JUSTIÇA (Grande Secção). *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Processo C-131/12. 13 mai. 2014. ECLI:EU:C:2014:317.

TRIBUNAL DE JUSTIÇA (Segunda Secção). *Patrick Breyer v. Bundesrepublik Deutschland*. Processo C-582/14. 19 out. 2016. ECLI:EU:C:2016:779.

TRIBUNAL DE JUSTIÇA (Grande Secção). *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. 24 set. 2019. Processo C-507/17. ECLI:EU:C:2019:772.

CONCLUSÕES DA ADVOGADA-GERAL (Juliane Kokott). *Peter Nowak v. Data Protection Commissioner*. Processo C-434/16. 20 jul. de 2017. ECLI:EU:C:2017:582.

FACULDADE DE DIREITO

