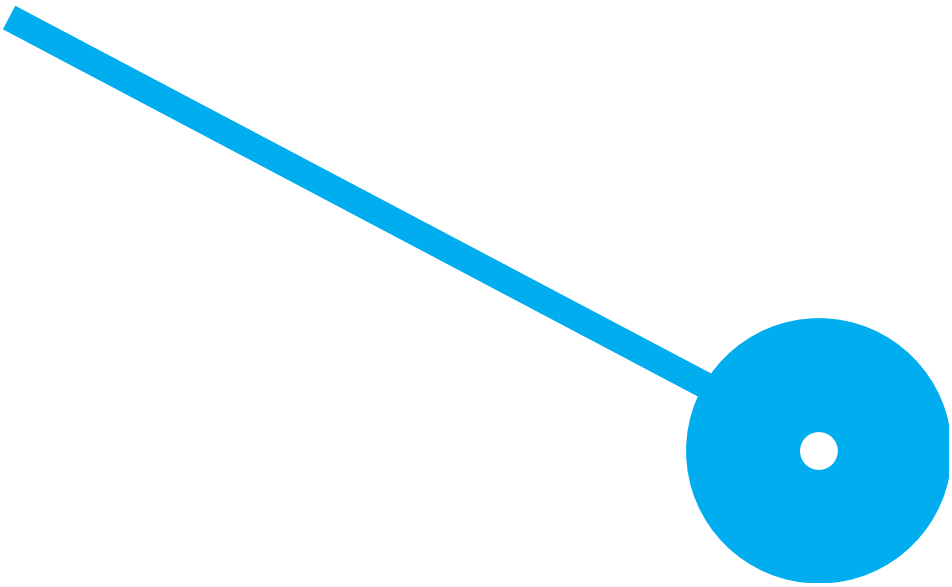
ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M MESTRADO
Práticas Jurídico Digitais

Uma abordagem computacional e jurídica na gestão de consentimentos para o processamento de dados pessoais

Sílvia Catarina Monteiro Freitas Ferreira

OUTUBRO/2025



Este trabalho não inclui as críticas e sugestões feitas pelo Júri

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M MESTRADO
Práticas Jurídico Digitais

Uma abordagem computacional e jurídica na gestão de consentimentos para o processamento de dados pessoais

Sílvia Catarina Monteiro Freitas Ferreira
8050147

Orientador(es)

Professora Doutora Patrícia dos Anjos Oliveira Nogueira de Azevedo

Professor Doutor Marco Filipe Vieira Gomes

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Práticas Jurídico Digitais pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto.

OUTUBRO/2025

Este trabalho não inclui as críticas e sugestões feitas pelo Júri

Declaração de Integridade

Eu, Sílvia Catarina Monteiro Freitas Ferreira, estudante nº 8050147, do Mestrado de Práticas Jurídico Digitais da Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto, declaro que não fiz plágio nem auto-plágio, pelo que o trabalho intitulado "Uma abordagem computacional e jurídica na gestão e consentimentos para o processamento de dados pessoais" é original e da minha autoria, não tendo sido usado previamente para qualquer outro fim. Mais declaro que todas as fontes usadas estão citadas, no texto e na bibliografia final, segundo as regras de referenciação adotadas na instituição.

DEDICATÓRIA

Ao meu pai,

Que acreditou mesmo antes de eu saber que era capaz e que me ensinou, que é preciso lutar e perseverar para vencer.

Partiu cedo demais e não está para aqui para acompanhar esta conquista, mas cada página desta dissertação carrega a memória do seu exemplo de força e a sua fé incondicional em mim. Este trabalho é também teu.

Ao Vítor Ruivo,

Pessoa que conheci neste mestrado e que, em tão pouco tempo, se tornou um amigo para sempre. Mesmo atravessando uma fase de provação, ensinou-me o verdadeiro valor do ser humanos: a forma como se está presente e de como esse simples gesto pode transformar o mundo num lugar melhor.

O vítor foi luz e chão nos momentos em que duvidei ser capaz. Abdicou do seu tempo para me ajudar, ensinar e incentivar, enquanto ele trava ao mesmo tempo as suas batalhas, num verdadeiro espírito altruísmo.

A tua coragem e determinação vivem nestas páginas e a minha gratidão também.

AGRADECIMENTOS

O trabalho que aqui apresento é o culminar de umas jornadas mais exigentes e transformadoras da minha vide pessoal e académica. Foi um caminho de aprendizagem e que me desafiou a sair da minha zona de conforto e a olhar para o direito a partir da realidade digital e tecnologia, uma perspetiva para a qual, inicialmente, não estava sensibilizada. Termino hoje este percurso com a certeza de que crescer, é enfrentar estes desafios e reaprender a cada dia a ver o mundo com novos olhos.

Agradeço à Professora Doutora Patrícia dos Anjos Oliveira Nogueira de Azevedo e ao Professor Doutor Marco Filipe Vieira Gomes, meus orientadores, aos quais expresso a mais profunda gratidão pela orientação e acompanhamento e pela disponibilidade constante. O vosso apoio, confiança e conhecimento científico, foram determinantes para concretizar esta dissertação.

Ao meu marido, pelo amor incondicional, pela paciência e por nunca me deixar desistir, mesmo quando eu própria duvidava. Aos meus filhos, pela compreensão e carinho durante estes dois anos em que estive mais ausente, esta conquista é também vossa.

À minha turma do Mestrado em Práticas Jurídico-Digitais, agradeço pelo espírito de entreajuda, camaradagem, alegria e disponibilidade, que tornou esta caminhada mais leve e motivadora.

Um agradecimento muito especial à Carla Pinto, cuja presença se revelou uma fonte de inspiração, pela sua bondade genuína e empatia natural. Foi apoio e incentivo e é a prova que quando partilhada, a generosidade transforma os caminhos de qualquer pessoa.

Por fim, a todos os que de uma forma mais ou menos visível ou até silenciosa, contribuíram para que este trabalho fosse possível, deixo a minha sincera gratidão.

ABSTRACT

This dissertation proposes an approach that combines Law and Computing as a way of rethinking and optimizing the current process of collecting, managing, and validating consent for the processing of personal data in a digital environment, within the legal framework of the GDPR.

In this vein, we present a reflection on the concept and evolution of consent as the basis for the lawfulness of processing in light of the GDPR and its expression in the law on the individual's informational self-determination. We highlight weaknesses, such as consent fatigue, opacity, and informational fragmentation, with a critical analysis of the legal framework, case law, and relevant guidelines, which have shown that consent, as it currently stands, is distorted from the free expression of will and thus compromises the sovereignty of the individual in the protection of informational rights.

n response to this problem, this paper proposes the design of a conceptual model of computational architecture for a centralized consent management platform, based on the principles of privacy by design, interoperability, and security, integrating mechanisms of pseudonymization, hashing, traceability, and immutable registration, as a guarantee of legal validity, transparency, and auditability.

The proposed solution has been found to be technically robust and focused on the data subject, reinforcing their self-determination, complying with the GDPR, and enabling the future inclusion of organizations and entities responsible for supervising and enforcing the GDPR.

Keywords: Consent, data protection, GDPR, computer security, computational architecture.

Resumo

A presente dissertação propõe uma abordagem que combina o Direito e a Computação, como forma de repensar e otimizar o atual processo de recolha, gestão e validação de consentimento para o tratamento de dados pessoais em ambiente digital, no enquadramento jurídico do Regulamento Geral sobre a Proteção de Dados (RGPD).

Nessa senda, apresentamos uma reflexão sobre o conceito e evolução do consentimento, enquanto fundamento de licitude do tratamento à luz do RGPD e a expressão deste no direito na autodeterminação informacional do indivíduo. Balizamos as fragilidades, como a fadiga do consentimento, opacidade, fragmentação informacional, com uma análise critica pelo enquadramento jurídico, jurisprudência e orientações relevantes, que demonstraram que consentimento, tal como se apresenta atualmente, se apresenta desvirtuado da livre manifestação de vontade e com isso se mostra comprometida a soberania do individuo na tutela do direito informacional.

Em resposta a esta problemática é proposto neste trabalho a conceção um modelo conceptual de arquitetura computacional para uma plataforma de gestão centralizada de consentimento, assente em princípios de *privacy by design*, interoperabilidade e segurança, integrando mecanismos de pseudonimização, *hashing,* rastreabilidade e registo imutável, como garantia de validade jurídica, transparência e auditabilidade.

Verificou-se que a solução proposta se apresenta como tecnicamente robusta e centrada no titular dos dados em reforço da sua autodeterminação, servindo o cumprimento do RGPD e possibilitando a inclusão futura de organizações e entidades responsáveis pela fiscalização e cumprimento do RGPD.

Palavras-chave: Consentimento, proteção de dados, RGPD, segurança informática, arquitetura computacional.

Índice

Índice de Figuras

Índice de Tabelas

ACRÓNIMOS

ABAC	Attribute-Based Access Control – Controlo de Acesso Baseado em Atributos
AES	Advanced Encryption Standard – Norma de Criptografia Avançada
AI Act	Artificial Intelligence Act – Regulamento Europeu sobre Inteligência Artificial
API	Application Programming Interface – Interface de Programação de Aplicações
APD/GBA	Autorité de Protection des Données / Gegevensbeschermingsautoriteit – Autoridade Belga de Proteção de Dados
Art.	Artigo
CCts	Cláusulas Contratuais-tipo
CMP	Consent Management Platform – Plataforma de Gestão de Consentimentos
CNIL	Commission Nationale de l'Informatique et des Libertés – Comissão Nacional de Informática e Liberdades (França)
CNPD	Comissão Nacional de Proteção de Dados (Portugal)
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator – Gerador Pseudo-Aleatório Criptograficamente Seguro
DGA	Data Governance Act – Regulamento da Governação de Dados
DPC	Data Protection Commission – Comissão de Proteção de Dados (Irlanda)
DSA	Digital Services Act – Regulamento dos Serviços Digitais
EDPB	European Data Protection Board – Comité Europeu para a Proteção de Dados
EEE	Espaço Económico Europeu
EUDIW	European Digital Identity Wallet – Carteira Europeia de Identidade Digital
GDPR / RGPD	General Data Protection Regulation – Regulamento Geral sobre a Proteção de Dados
HSM	Hardware Security Module – Módulo de Segurança de Hardware

ISO	International Organization for Standardization – Organização Internacional de Normalização
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission – Organizações Internacionais de Normalização e Eletrotécnica
JWT	JSON Web Token – Token Web JSON
KMS	Key Management System – Sistema de Gestão de Chaves
MFA	Multi-Factor Authentication – Autenticação Multifator
NIST	National Institute of Standards and Technology – Instituto Nacional de Padrões e Tecnologia (EUA)
OIDC	OpenID Connect – Protocolo de Identidade Aberta
PDP	Policy Decision Point – Ponto de Decisão de Políticas
PEP	Policy Enforcement Point – Ponto de Aplicação de Políticas
RBAC	Role-Based Access Control – Controlo de Acesso Baseado em Funções
REST	Representational State Transfer – Transferência de Estado Representacional
SCCs	Standard Contractual Clauses – Cláusulas Contratuais Padrão
SHA-3	Secure Hash Algorithm 3 – Algoritmo de Hash Seguro versão 3
TJUE	Tribunal de Justiça da União Europeia
TLS	Transport Layer Security – Segurança da Camada de Transporte
TSA	Time-Stamping Authority – Autoridade de Carimbagem Temporal
X.509	Padrão de certificação digital X.509 – Certificados Digitais
ZTA	Zero Trust Architecture – Arquitetura de Confiança Zero

1. Introdução

A proteção de dados pessoais é nos dias de hoje um desafio constante, que pela ótica jurídica quer pela tecnológica, conforme afirma (Mantelero, 2018). Numa era em que a utilização das tecnologias para interações sociais e comerciais se intensifica, é premente a necessidade de garantir que a recolha e tratamento dos dados pessoais dos utilizadores, seja efetuada de forma licita, respeitando os princípios e assegurando os direitos fundamentais dos titulares dos dados.

Para colmatar parte desta problemática, a União Europeia apresentou o Regulamento (EU) 2016/679, conhecido como Regulamento Geral da Proteção de Dados (RGPD), que apresenta um quadro normativo que promove a uniformização da proteção dos dados no espaço europeu. Este regulamento permite assim, harmonizar a forma como os dados são tratados por cada um dos Estados membros e a responsabilização dos responsáveis pelo tratamento de dados.

Além deste valioso contributo, outras evoluções tecnológicas contribuíram e positivaram soluções para o tratamento dos dados pessoais, como acontece com a tecnologia *Blockchain* ou a Inteligência Artificial, que contribuíram para reforçar e promover a proteção de dados, permitindo assegurar a segurança dos dados e também a transparência e a rastreabilidade, imutabilidade no caso da *blockchain*, automatização de formalismos de conformidade, riscos medidas de implementação de princípios de *privacy by design* no caso da Inteligência Artificial (Giannopoulou, 2021; Godyn et al.,2022; Lukács & Váradi, 2023; Zhao et al., 2024). A Comissão Europeia reconhece os benefícios do uso destas tecnologias na recolha e tratamento de dados, principalmente quando a recolha dos dados se destina a fins diversos (Comissão Europeia, 2020).

1.1. Enquadramento e relevância do tema

O aumento das interações sociais, comerciais e administrativas, contribuiu para colocar o consentimento no centro da proteção de dados pessoais. Contudo, a forma como se obtêm os consentimentos nos *websites*, tem gerado inúmeras críticas e grandes desafios práticos. Métodos como caixas pré-selecionadas, *banners* confusos de *cookies* e solicitações repetitivas de consentimento, contribuem para o fenómeno conhecido como a "fadiga do consentimento. Em consequência, os utilizadores tendem a aceitar automaticamente os termos, sem compreender verdadeiramente as suas implicações, fragilizando o princípio do consentimento informado, previsto no RGPD, que garante que o utilizador tem o controlo sobre os seus dados, permitindo-lhes revogar o consentimento a qualquer momento sem prejuízo. Ressalta-se, a título de exemplo um caso mediático ocorrido em França, onde a Comissão Nacional de Informática e Liberdades (CNIL), multou a Google em 100 milhões de euros, por práticas inadequadas relacionadas como uso de cookies, ou ainda a

empresa Amazon, que por ter violado o RGPD, viu aplicada uma multa recorde de 746 milhões de euros (Pinto Ramos, 2022; Pavlou, 2011; União Europeia, 2016; Jornal de Negócios, 2022; Cátia Rocha, 2021). O RGPD estabelece orientações claras e precisas sobre a e gestão de consentimentos, que devem ser livremente dados, informados, específicos e revogáveis (Artigo 4.º, n.º 11). O considerando (17) do mesmo regulamento, identifica as empresas como prestadores de serviços da sociedade da informação, atribuindo-lhes responsabilidades específicas na obtenção e gestão de consentimentos. Assim e usando a terminologia do RGPD, doravante as empresas serão identificadas como prestadores de serviços da sociedade da Informação. Apesar de existirem soluções para a gestão de consentimentos, grande parte delas estão direcionadas para soluções empresariais, conhecidas como *Consent Management Platform*, identificadas pela sigla (CMP) ou em português, plataformas de gestão de consentimento. Estas têm como finalidade a obtenção, gestão e tratamento dos consentimentos prestados pelos utilizadores, para acesso aos seus dados pessoais, para determinada finalidade, previamente identificada pela empresa que necessita do acesso aos dados pessoais, e que assegurar neste processo o cumprimento do RGPD. Apesar das plataformas de gestão de consentimento remontarem a 2009, com a aplicação da Diretiva da *ePrivacy*, é com a entrada do RGPD em 2018, que estas plataformas passam a ter outra relevância para assegurar e cumprir com as alterações propostas. Apesar de todas as evoluções, existem ainda limitações nomeadamente quanto à centralização, interoperabilidade e facilidade de uso e acesso pelos titulares dos dados pessoais.

Este Artigo propõe uma análise de uma solução teórica, que inova ao sugerir a criação de uma plataforma descentralizada baseada na tecnologia *blockchain*, que permita aos titulares dos dados, gerirem os seus consentimentos de forma simplificada, sem com isso comprometer os princípios basilares da segurança e privacidade, abordaremos ainda os desafios técnicos e éticos associados à implementação num contexto global.

1.2. Problema de investigação

O regulamento geral da proteção de dados estabelece o consentimento, como um dos fundamentos para o tratamento de dados pessoais concretamente no Artigo 6, n.º 1, a), cujos requisitos se encontram plasmados no Artigo 7.º do mesmo diploma. Apesar do desenho jurídico da proteção idealizada pelo RGPD parecer suficiente, a realidade digital parece não corresponder a essa eficácia na proteção. Falamos aqui da fadiga do consentimento em consequência de no dia-a-dia dos utilizadores da *web*, serem confrontados com um elevado número de solicitações para prestarem o consentimento para o tratamento de dados pessoais, que é fornecido pelos utilizadores, sem leitura ou qualquer análise prévia do conteúdo e alcance do ato de consentir que ali prestam, tornando este requisito de validade

do consentimento, num ato reflexo do dia-a-dia (Nouwens et al., 2020). Acoplado a este fenómeno, temos ainda o formalismo em detrimento da substância, que mais não é do que a identificação do consentimento apenas como meio de obtenção do consentimento através de caixa pré-selecionada ou "cliques" em *banners* de *cookies* ou ainda a aceitação global de termos de utilização e não como a substância jurídica que forma a autodeterminação do titular dos dados, tal como resulta de vários estudos[1] sobre este tema e que concluem que o consentimento é retratado como um formalismo burocrático por força da sua obtenção, conforme descrito.

Acrescem ainda a estas problemáticas o uso estratégias de *design* manipulativo, conhecidas por *dark patterns*, que pela sua configuração induzem o utilizador a fazer escolhas e com isso comprometem a liberdade de escolha, como é o caso das caixas pré-selecionadas com cores que destacam a opção a selecionar e dificultam a opção de recusar ou rejeitar, ferindo do requisito da liberdade que é necessário à validade do consentimento (Mathur et al., 2019a), conforme decorre do Artigo 7.º do RGPD.

Por último existe ainda um paradoxo da privacidade, segundo o qual os titulares expressam a sua preocupação com o tratamento dos seus dados pessoais, porém continuam a partilhar os seus dados e a prestar o consentimento sem conhecimentos do conteúdo e alcance ou manipulados pelo meio em que se apresenta a recolha do consentimento. Trata-se de uma contradição entre o que os titulares reconhecem e o seu comportamento ao prestar consentimento, que coloca em causa o consentimento, tal como estatui o RGPD. Tendo em conta as questões de investigação acima identificadas, levantamos a seguinte questão: O consentimento prestado em plataformas digitais, assegura realmente a autonomia informacional do titular dos dados e a proteção prevista no RGPD? No capítulo 2, iremos desenvolver estes problemas de investigação e durante este trabalho proceder análise critica dos modelos vigentes e propor soluções que possam mitigar estes problemas.

1.3. Objetivos do estudo

A presente dissertação tem como finalidade a análise crítica e levantamento das limitações do consentimento prestado para o tratamento de dados em contexto digital, de forma a compreender se

[1] A problemática da redução do consentimento a um mero formalismo digital, que nos estudos empíricos sobre o tema apontam o fenómeno da fadiga do consentimento bem como o uso de *dark patterns*, comprometem a autodeterminação informacional dos titulares dos dados (Schermer et al., 2014); (Nouwens et al., 2020); (Machuletz & Böhme, 2020) (European Data Protection Board (EDPB), 2023)). Este tema será desenvolvido com maior detalhe no capítulo 2.

o consentimento tal como é prestado nos dias de hoje, assegura a autodeterminação informacional dos titulares dos dados tal como resulta do RGPD.

Inicialmente iremos proceder à análise da figura do consentimento jurídico, conforme se encontra previsto e regulado no RGPD, verificando entre outros os pressupostos, requisitos de validade e principais interpretações da doutrina e jurisprudência (Voigt et al. 2017). Após esse enquadramento passaremos a analisar os desafios relativos à recolha do consentimento em ambiente digital, com especial atenção a questão da fadiga dos utilizadores e a utilização das técnicas manipulativas de obtenção do consentimento e também uma breve análise ao desafio comportamental relativa ao paradoxo da privacidade (Norberg et al., 2007).

Após o enquadramento e a análise evolutiva do conceito de consentimento, faremos a análise crítica requisitos dos sistemas de gestão consentimentos CMP, tendo como finalidade o levantamento das potencialidades e limitações destes modelos à luz do RGPD e das normas internacionais aplicáveis em matéria de gestão da segurança da informação e da privacidade (*ISO_IEC 27701_2019*, 2019; ISO_IEC 29100_2011, 2011).

Pretendemos propor e demonstrar a viabilidade técnica e jurídica de uma abordagem computacional, que permita que os titulares dos dados, possam de forma segura e transparente exercer os direitos que lhes são inerentes e que se encontram previstos no RGPD. Pretendemos também demonstrar que as entidades responsáveis, poderão ter acesso, a todas as ferramentas necessárias para evidenciar o cumprimento do RGPD, e comprovar a regularidade dos consentimentos e do tratamento dos dados recolhidos. Com este trabalho pretendemos demonstrar não só as limitações atualmente existentes relativas à recolha de consentimentos em meio digital, mas também contribuir com uma proposta académica de cariz mais prático, que responda aos desafios jurídicos e digitais da proteção de dados em contexto digital.

1.4. Metodologia

Este estudo fundamenta-se numa abordagem qualitativa, exploratória e descritiva, que associa a análise jurídica e a revisão técnico-científica relativas às tecnologias da informação. Esta abordagem tem como escopo principal a análise critica das limitações do consentimento no contexto digital, e em face dessa análise, a apresentação e fundamentação da proposta de arquitetura computacional capaz de oferecer a solução adequada aos problemas levantados.

Este estudo subdivide-se em três fases que se complementam entre si. Nesta fase, iremos analisar os modelos de CMP e outros sistemas alternativos de gestão de consentimentos, como o *MyData*, o *Consentu*a, o *Solid Pods* ou o *IBM Data Consent Manager*. Estes modelos foram selecionados tendo em conta que, têm na sua conceção o titular dos dados como utilizador e a preocupação de cumprir com o RGPD na ótica do titular dos dados, no todo ou em parte. Nesta análise serão verificadas as

funcionalidades de cada modelo, a lógica de funcionamento e a forma de obtenção do consentimento de acordo com o RGPD, com esta informação poderemos estabelecer uma base de comparação (Yin, 2018).

Aqui se inclui a análise documental de diretivas da União Europeia, revisão de literatura técnica sobre plataformas de gestão de consentimentos, jurisprudência e ainda a análise qualitativa-comparativa de modelos de gestão de consentimentos e dados existentes no mercado, com vista realçar a necessidade de um modelo adaptado ao cumprimento dos princípios do RGPD. Esta metodologia terá uma estrutura de três fases. A primeira, que se resume a identificação e descrição das suas funcionalidades, a segunda, que analisa critérios técnicos e jurídicos do RGPD e comparação com as normas internacionais ISO e por último uma síntese, que as lacunas e não conformidades encontradas e que permitirão apar com a análise documental e revisão de literatura, desenhar a arquitetura que nos propomos desenvolver para solucionar os problemas desta investigação.

Nesta última fase, compilamos as lacunas encontradas e as não conformidades na recolha do consentimento nos modelos analisados. Com esta avaliação critica, baseada na revisão de literatura e ainda na análise documental, servirá de molde para o desenvolvimento da arquitetura proposta, á qual acrescerá as boas práticas jurídicas e técnicas, combinando o rigor da interpretação jurídica dos comandos normativos, com a integração técnica de soluções computacionais.

Esta metodologia encontra acolhimento em outras investigações (Nouwens et al., 2020; Schermer et al., 2014), que tiveram o consentimento no contexto digital, como tema principal e com bons resultados, pelo que seguimos a mesma metodologia.

1.5. Estrutura da dissertação

A presente dissertação é composta por seis capítulos, que combina a perspetiva jurídica do tema e a dinâmica técnico-computacional. O primeiro capítulo, resume o enquadramento geral, o objeto de estudo, os objetivos a ele inerentes, metodologia e a formulação do problema, nomeadamente o consentimento no contexto do económico digital e os desafios que enfrentam os titulares para o exercício dos seus direitos e por fim a apresentação da estrutura da dissertação. O segundo capítulo analisa o problema de investigação, identificando as questões centrais guiam o desenvolvimento deste trabalho.

O capítulo três apresenta a revisão da literatura estruturada de acordo em dois pontos principiais: a evolução histórica do consentimento, aborda os requisitos de validade do consentimento à luz do RGPD, os direitos dos titulares, assim como os princípios e obrigações do RGPD, a analise de jurisprudência relevante do Tribunal de Justiça da União Europeia (TJUE), e outra legislação de relevo, como a europeia, nacional e *soft law*, e ainda as normas técnicas ISO/IEC.

O capítulo quarto, apresenta a proposta de arquitetura conceptual, tendo por base uma arquitetura modular direcionada para o titular dos dados, com a apresentação individualizada das camadas, com descrição de alguns componentes técnicos fundamentais e outros aspetos como a pseudonimização[2], *hashing*, encriptação, anonimização, rastreabilidade e a integração de inteligência Artificial, concluindo-o uma análise jurídica da arquitetura proposta.

O quinto capítulo introduz a implementação técnica e a interoperabilidade da arquitetura desenhada, identificando as tecnologias, linguagens, *frameworks*, bases de dados e APIS a utilizar. Também aqui exploramos outra tecnologia, a *Blockchain* permissionada[3] e o seu registo imutável e ainda os *smart contracts*, com a verificação automática de consentimentos, a interoperabilidade institucional e transfronteiriça.

No sexto capítulo, procede-se a uma análise crítica da arquitetura proposta, avaliando a sua conformidade como RGPD e sua aplicação extraterritorial, assim como os principais desafios jurídicos e tecnológicos e implicações éticas e práticas da sua implementação.

Por último, o sétimo capítulo, sintetiza os resultados alcançados, com uma análise da aplicabilidade e eficácia da solução apresentada e sugestões para investigações futuras.

[2] Técnica de proteção de dados definida no Artigo 4.º, n.º 5 do RGPD como "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares". Desenvolvida em pormenor no ponto 4.4.1.

[3] Blockchain permissionada (do inglês *permissioned blockchain*) designa uma rede de registo distribuído em que o acesso, validação de transações e participação são restritos a entidades previamente autorizadas, ao contrário das *blockchains* públicas onde qualquer participante pode ler e validar transações (Androulaki et al., 2018). Desenvolvida em pormenor no ponto 5.1.

2. Problema de Investigação

O consentimento é um dos fundamentos de licitude para o tratamento de dados pessoais e a sua importância, decorre da dupla função que desempenha.

A primeira função é o requisito deste ato para a licitude do tratamento dos dados, como estabelece o Artigo 6.º, n.º 1, alínea a) do RGPD, por outro lado como um mecanismo de confiança nas relações digitais, pois desta forma o titular tem a liberdade de controlar a utilização dos seus dados pessoais.

O consentimento encontra-se previsto e regulado no Artigo 6.º e 7.º do RGPD e a esta função legitimadora esta também associada a um conjunto de requisitos de validade deste ato, que garantem a manifestação de vontade do titular de forma informada e ponderada e não um ato reflexo e manipulado.

Como define Menezes Cordeiro (2022), "por consentimento entende-se, nos termos do Artigo 4.º, 11), i) uma manifestação de vontade, livre, especifica, informada e explicita; (ii) através da qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco;(iii) que os dados que lhe digam respeito sejam objeto de tratamento." Contudo, na prática verificamos que existe diferença entre o corpo normativo, tal como a definição acima apresentada e os mecanismos de recolha do consentimento e a complexidade das plataformas digitais, que comprometem a validade e aplicação das normas jurídicas (Bygrave, 2014; Nouwens et al., 2020).

Tendo por base o levantamento das problemáticas já identificadas de forma sucinta no ponto 1.2, passaremos agora a desenvolver cada uma deles.

O presente capítulo apresenta cinco secções. A secção 1.1, onde efetuamos o enquadramento e a relevância do tema, a secção 1.2, onde identificamos o problema da investigação, definindo as principais lacunas técnicas e práticas, que pela sua relevância merecem o estudo desenvolvido. Na secção 1.3, são apresentados os objetivos gerais e específicos da dissertação, conjugando-os com a problemática central. Na secção 1.4, apresentamos a metodologia adotada, demonstrando-se a investigação efetuada e as opções epistemológicas e técnicas adotadas. E por fim a secção 1.5, onde apresentamos a estrutura global da dissertação, demonstrando a organização e a sequência na articulação de cada capítulo.

2.1. Consentimento superficial ou não informado: fadiga e formalismo

O conceito de consentimento superficial ou não informado, pode ser compreendido como a manifestação de vontade do titular dos dados, prestada de forma desinformada e rápida[4]. A título de

[4] Sobre este fenómeno do consentimento superficial ou não informado (*uninformed consent*), veja-se o Artigo *Uninformed Consent." Special Issue on The Big Idea: Tracked. Harvard Business Review*), (Leslie K. John, 2018), no qual a autora evidência a prática dos titulares dos dados,

exemplo, o consentimento prestado através do clique numa caixa pré-formatada, sem leitura prévia dos termos e condições de privacidade aplicáveis. Este conceito é semelhante ao apresentado por Leslie K. John, (2018), quanto ao *uninformed consent*, que o autor define como o consentimento prestado sem informação suficiente e também o que Pinto Ramos, (2022), define como a fragilidade do consentimento *online*, que frequentemente é reduzido a uma mera formalidade burocrática.

Relativamente aos requisitos do consentimento, Menezes Cordeiro, (2022), sublinha que o consentimento deve respeitar os requisitos dos negócios jurídico nomeadamente, manifestação de vontade inequívoca, livre específica, informada e represente um ato positivo inequívoco. Outras investigações como o estudo de Utz et al., (2019) e Nouwens et al., (2020)[5] apresentam nas suas conclusões que a maior parte dos utilizadores não lê as políticas de privacidade das plataformas digitais a que acedem diariamente, antes de prestarem o consentimento e desta forma criam padrões de aceitação rápida *(click fatigue*), para aceder de forma mais rápida aos serviços digitais que pretendem. A esse fenómeno dá-se o nome de fadiga do consentimento (*consent fatigue*), que ocorre quando os utilizadores são sujeitos a múltiplas notificações, avisos e pedido de consentimento, que reduzem a capacidade de análise do utilizador, gerando a sobrecarga cognitiva e com isto o um reflexo da fadiga através do consentimento sem conteúdo ou informação.

Devemos ainda referir neste contexto que a publicidade comportamental (*behavioral advertising*), segundo o que nos ensina Turow,(2011), na sua obra "*How the New Advertising Industry Is Defining Your Identity and Your Worth"*, representa uma técnica de *marketing* digital que personaliza a publicidade com recurso a monitorização das atividades dos utilizadores *online*, com a utilização de *cookies* ou outras tecnologias de monitorização, com vista à criação de perfis individuais de consumo e preferências, que permite às empresas criar campanhas de forma eficiente. Para que seja possível a recolha e tratamento dos dados é necessário o consentimento dos titulares para a instalação dos *cookies* ou outras tecnologias de recolha. Na prática esses pedidos de consentimento com recurso a *banners* e caixas de aceitação pré-definidas e com outros *dark pattern*s, dos quais nos acercaremos no próximo ponto, geram o consentimento automático e desprovido de informação necessária à tomada de decisão, distinto do previsto no RGPD. A esta problemática poderíamos ainda acrescentar o consentimento prestado a favor de terceiros, com interesses legítimos, com pré-seleção na aceitação do consentimento. Do ponto de vista jurídico, este tipo de consentimento não satisfaz os requisitos de validade de RGPD, pis o Artigo 4.º, n.º 11 do RGPD, exige que o consentimento seja específico e

prestarem consentimentos não informados e modelos de recolha - https://www.hbs.edu/faculty/Pages/item.aspx?num=55059 - consultado a 5 de agosto de 2025.

[5] (Nouwens et al., 2020), realizaram no seu trabalho, "*Dark Patterns after the GDPR: Scarping Consent Pop-ups and demnostrating their influence"* uma análise a 680 sites europeus, tendo verificado que apenas uma minoria dos mecanismos de recolha de consentimento cumpria os requisitos do RGPD. Os autores demonstraram neste trabalho que a ausência de um botão de recusar ou o recurso a designs enviesados afeta a validade jurídica do consentimento obtido.

informado e que seja distinta do consentimento principal. Nesse mesmo sentido, o (European Data Protection Board, 2020a)), nas *Guidelines* 05/2020 *on consente*, reitera que a menção a "fornecedores" ou "parceiros" sem individualização, viola o princípio da transparência e não cumpre com o disposto no Artigo 7.º, n. º1 do RGPD, porque não permite fazer prova da recolha do consentimento para o tratamento pelo responsável pelo tratamento. Este tipo de consentimento considerado como consentimento em "bloco", alicerçado no interesse legítimo presumido de fornecedores/parceiros com invocação do Artigo 6.º, n.º 1, alínea f) do RGPD, abre as portas para uma discussão mais profunda que não é a que queremos aqui desenvolver, consideramos a importância da falta de justificação e identificação individualizada dos "terceiros" e os *dark patterns*, matéria de relevo para a problemática que aqui exploramos.

Em suma, percecionamos que o ato de consentir cada vez mais se encontra esvaziado de substância e subsumido à rotina do utilizador das plataformas digitais. É caminho fértil para novas formas de manipulação, como os *dark patterns* que colocam o utilizador em vulnerabilidade e agudizam a distância entre a efetiva eficácia jurídica do consentimento e a formalidade do consentimento, que iremos desenvolver no ponto seguinte.

2.2. Dark Patterns e manipulação do utilizador

Dark patterns consistem em "interfaces de *design* que induzem, enganam ou coagem os utilizadores a tomar decisões contrárias ao seu interesse" (Mathur et al., 2019a), que limitam a liberdade dos titulares dos dados e comprometem a sua autodeterminação informacional.

No dia-a-dia os utilizadores das plataformas digitais são confrontados com *banners de cookies*, *pop-ups* ou *checkboxes* ou outros mecanismos de recolha de consentimentos, grande parte deles pré-formatados para resposta padrão, com opções que não são claras e que não evidenciam, nem cumprem com o disposto no Artigo 4.º, n.º 11 (European Data Protection Board, 2020b) relativo aos requisitos do consentimento nomeadamente, livre, específico, informado e inequívoco, tendo contribuído para um fenómeno denominado de "fadiga do consentimento".

A Comissão Europeia no seu relatório[6] sobre práticas digitais relativas a *banners de cookies*, concluiu que a grande maioria dos *websites* comerciais na União Europeia, recorrem a mecanismos de aceitação rápida dos *cookies*, colocando botões de "aceitar tudo" em destaque e a opção de recusa oculta ou em menus secundários, sem a opção "rejeitar tudo", com o mesmo destaque o que viola também o Artigo 5.º da Diretiva da *ePrivacy*. Estas práticas ferem a validade dos consentimentos prestados, por

[6] *Report of the work undertaken by the Cookie Banner Taskforce Adopted (2023) - European data Protetion Board - https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en?utm_source=chatgpt.com* - Consultado a 5 de Agosto de 2025

não cumprirem com o Artigo 4.º, n.º 11 e Artigo 7 do RGPD e ao mesmo tempo contribuem também para a fadiga do consentimento, pois levam à aceitação imediata das condições apresentadas pela indução na escolha da opção a selecionar, comprometendo a liberdade de escolha.

Apesar de os responsáveis pelo tratamento de dados, recorrerem a soluções de CMP ou plataformas de gestão de consentimento, todas elas se direcionam às empresas responsáveis e quando acessíveis ao titular dos dados são limitadas no uso e alcance.

Verificamos então que o mercado nos oferece soluções que permitem ao titular, efetuar a gestão das predefinições de controlo e acesso aos dados, ainda assim com limitações quando se trata da informação relativa a terceiros e o seu acesso. A legitimação do acesso a dados pessoais pelos "terceiros" é efetuada através do fundamento do interesse legítimo, previsto ano Artigo 6.º, n.º 1, alínea f) do RGPD. É importante salientar, que Kyi et al., (2023) vêm contribuir para o reforço da ideia da utilização abusiva deste fundamento em vez do consentimento como licitude na recolha e tratamento de dados pessoais, frisando ainda que a apresentação do fundamento de interesse legitimo ludibria o titular dos dados e impede de compreender qual a fonte de licitude aplicável. Esta prática viola também o princípio da transparência previsto no Artigo 5.º, n.º 1, a) do RGPD e permite uma contradição entre o Artigo 13.º do RGPD, que impõe a necessidade da identificação do responsável pelo tratamento e a especificidade fins do tratamento, permitindo que à margem do que estabelece o RGPD, se possa tratar dados pessoais sem consentimento, ao abrigo de um vazio legal, que compele o utilizador a aceitar os termos e condições.

Coloca-se ainda como problema no âmbito da investigação o risco de transferência dos dados prevista no capítulo V do RGPD. Muitas plataformas internacionais acabam por processar os dados recolhidos de cidadãos do Espaço Económico Europeu (EEE), fora da EU, quando a recolha ocorre na EU, em desrespeito para com o regulamento (caso *schrems II,* desenvolvido no ponto 3.3).

A esta evidência, acresceremos ainda o paradoxo da privacidade, que como veremos no seu conjunto contribui para a conclusão da problemática, que aqui nos traz.

2.3. Paradoxo da privacidade

Este fenómeno representa uma das maiores discrepâncias mais discutidas na literatura em matéria de proteção de dados, que representa a preocupação com as questões da privacidade e da proteção de dados dos titulares, em contraposição com adoção de comportamentos reais que demonstram a aceitação automática dos consentimentos, redundando numa contradição entre a perceção e ação. No estudo clássico de Norberg et al., (2007) e Z. T. Zarsky, (2017), demostrou que existe por um lado, o reconhecimento da necessidade de proteger os dados e a sua esfera privada, usando a sua autodeterminação informacional, por outro revelam dados pessoais de forma voluntaria e rápida, em

algumas circunstâncias para a obtenção de benéficos tangíveis imediatos (falamos no acesso a serviços gratuitos, descontos ou conteúdos exclusivos, entre outros). Alguns dos factos motivadores desse comportamento, segundo os mesmos autores, trata-se da desvalorização dos riscos a médio ou longo prazo, como desconhecimento ou relativização das consequências jurídicas da utilização dos dados de forma ilegítima, pelo responsável pelo tratamento ou por terceiro, ou por demonstrarem confiança nas entidades que recolhem os dados e na utilização legitima para os fins que precederam à recolha.

Cabe também dizer que, segundo os mesmos autores, que influencia este comportamento o facto de as políticas de privacidades serem apresentadas de forma extensa e com linguagem excessivamente técnica, que acabam por desencorajar a leitura e levar o utilizador a aceitar de forma automática.

Analisando o consentimento prestado, segundo esta problemática, diremos que é formalmente válido, contudo substancialmente deficiente. Na sua substância padece de fragilidades materiais como a falta de uma verdadeira escolha, consciente e informada, que não cumpre com os requisitos materiais do consentimento previstos no Artigo 4.º n. º11 do RGPD, «manifestação de vontade, livre, específica, informada e inequívoca». Tambe o Comité Europeu para a proteção de dados (European Data Protection Board (EDPB), 2023)nas diretrizes sobre a *dark patterns* em plataformas digitais, reforça esta mesma ideia de que a manipulação e uso de interfaces manipulados, compromete a substância do consentimento e reduz este ato a um requisito de forma.

Desta forma o paradoxo da privacidade, cumulado com a fadiga do consentimento e as práticas manipulativas de interfaces, pese embora seja acautelada pelo legislador europeu, continua a enfrentar dificuldades de aplicação e concretização pratica.

3. Revisão da literatura

A revisão de literatura configura uma fase de suma importância na nossa investigação, pois é com recurso ao conhecimento existente, quer teórico quer prático e pela sua identificação, análise e síntese, que efetuar um levantamento critico dos estudos anteriores, promover a identificação das lacunas que dele advêm, os pontos de convergência e divergência que reforçam a relevância da nossa investigação (Hart, 2018).

A espinha dorsal e central desta investigação refere-se ao consentimento para o tratamento de dados no contexto dos ecossistemas digitais[7], e aqui será analisado sob várias perspetivas, como a sua evolução histórica, a sua crescente importância enquanto fundamento de licitude à luz do RGPD, à qual acrescemos outra legislação e normas aplicáveis, bem como a interpretação dada pela jurisprudência europeia e outros contributos académicos recentes.

Esta análise tripartida, permite-nos afirmar que o consentimento é uma figura que transcende o conceito jurídico, trata-se de um instrumento híbrido que incluído tanto o normativo jurídico, como a tecnologia e o comportamento humano (Acquisti et al., 2015; European Data Protection Board, 2020b)

Desta forma a organização deste capítulo começa com a evolução historia do consentimento (3.1), enquadramento no RGPG (3.2), prosseguindo com a análise da jurisprudência europeia (3.3), e de seguida com os contributos académicos recentes nesta matéria (3.5) e finaliza com o estudo sobre as principais plataformas de gestão de consentimento, explorando as mais relevantes funcionalidades, tecnologias e limitações (3.6). Esta estrutura permite uma projeção do conhecimento adquirido de forma critica e que servirá para que possamos fundamentar a proposta de arquitetura que será desenvolvida nos capítulos seguintes.

3.1. Enquadramento histórico do consentimento

O conceito do consentimento tem na sua génese uma evolução histórica, que foi moldada até à atual conceção conhecida pela associação à proteção de dados, muito por conta do RGPD. Esta figura tem as suas fundações no direito privado e contratual, no qual era visto como formalidade para a validade de um acordo, veio mais tarde a demonstrar outro valor, o ético. Este último, devido à evolução biomédica e haveria de configurar princípio da autodeterminação informacional, tal como hoje reclamamos para o contexto digital. Também Faden & Beauchamp, (1986), já na década de 80 constataram que o conceito de consentimento tinha evoluído e era mais do que "um mero requisito

[7] Por ecossistemas digitais entende-se o conjunto interconectado de plataformas, serviços digitais, infraestruturas tecnológicas, utilizadores e entidades que interagem e partilham dados de forma interoperável. Segundo a Comissão Europeia (2020), estes ecossistemas assentam em princípios de confiança, segurança, portabilidade e governança de dados, caracterizando-se pela multiplicidade de agentes (responsáveis pelo tratamento, subcontratantes, intermediários) e pela complexidade dos fluxos de dados transfronteiriços e transetoriais.

formal", tendo evoluído e tornado num princípio ético-jurídico, que visava a dignidade a proteção da pessoa. Nesta senda iniciaremos a análise histórico, por forma a compreendermos a evolução deste conceito de formalismo contratual a princípio.

3.1.1. Origem no direito privado e o direito biomédico

Tal como referimos acima, o consentimento tem raízes no direito privado, e principalmente no direito romano, onde era entendido como um consenso (*consensus*) das partes num negócio jurídico, que está latente no aforismo latino, *consensus mutuus facit legem,* que significa que o consentimento mútuo faz a lei e que reforça a necessidade de acordo mútuo entre as partes, prestado de boa-fé para a concretização de negócios jurídico com validade. Está máxima eleva o direito privado à autonomia da vontade dos contratantes e a expressão dessa vontade realizada através do consentimento mútuo, (Buckland & MacNair, 1965), que mais tarde substituído pelo *ius commune*[8] e mais tarde pelo Código de Napoleão de 1804[9] e ainda o *Bürgerliches Gesetzbuch* de 1900[10].

O consentimento no âmbito de um contrato foi tido na evolução jurídica ocidental, como uma manifestação livre e consciente de vontade, dotada de eficácia constitutiva. Esta figura foi impulsionada pelo jusnaturalismo moderno, com autores como *Grotius*, *Locke* e *Kant*, que nas suas visões ideológicas, associaram o consentimento ao ideal da liberdade individual e da autodeterminação racional (Habermas, 1996). Como ensina Menezes Cordeiro, (2021) ,o consentimento constitui a sua expressão mais imediata do princípio da autodeterminação privada nos contratos. Era assim entendido que o consentimento era fonte de licitude e legitimação para os atos jurídicos, reforçando as crenças relativas à liberdade e vontade individual (Canaris, 2007). Contudo este modelo não era absoluto e mais tarde demonstrou-se que a declaração de vontade por si só, poderia não bastar estar coberta de vícios, (teoria dos vícios de vontade - erro, dolo e a coação), que comprometeriam a validade formal e invalidassem o consentimento prestado e em resultado limitaram-se os efeitos das declarações viciadas (Almeida Costa, 2010) . Já no século XX, em consequência das críticas ao princípio da autonomia absoluta da vontade, originaram-se outras correntes, baseadas na boa-fé objetiva e proteção da parte mais fraca (Canaris, n.d.). Estas novas correntes têm especial interesse para aplicação do consentimento na proteção de dados, pois à semelhança do que hoje se perceciona, o consentimento enquanto formalismo por si só, não é

[8] *Ius commune* – (do latim, "direito comum") – Sistema jurídico que vigou entre a Idade Média e o Seculo XIX, na Europa Continental e agregava o Direito Romano e o Direito Canónico e serviu de base ao desenvolvimento do Direito Moderno.

[9] O Código Napoleónico (1804), constituiu um marco histórico por instituir o consentimento como princípio fundamental do direito civil, unificando aquilo que até então eram costumes, Direito Romano e Canónico, reconhecendo a importância da vontade individual, em especial nos contratos e no casamento.

[10] *Bürgerliches Gesetzbuch* – (Código Civil Alemão) – Em vigor desde 1 de janeiro de 1900 e cimentou a definição de contrato enquanto negócio jurídico, com base na declaração de vontade (*Willenserklärung*), figurando o consentimento como elemento da autonomia privada.

suficiente. É necessário garantir que o consentimento seja prestado de forma livre e informada e que não resulte de problemas estruturais (Kosta, 2013).

Relativamente ao direito biomédico, o consentimento revelou-se a sua importância ética após os julgamentos de Nuremberga[11] (1947), que revelaram as práticas médicas nazis, sem consentimento informado dos pacientes e é com a publicação do Código de Nuremberga[12] de 1947 que se estabeleceu pela primeira vez, o consentimento informado como absolutamente essencial, que mais tarde viria a ser reafirmado na declaração de Helsínquia[13] (1964), da Associação Médica Mundial, que determinou a obrigatoriedade do consentimento informado e esclarecido em todas as investigações clínicas(Faden & Beauchamp, 1986).

Cremos assim, que tanto a evolução do direito privado, na qual o consentimento assegurou a liberdade negocial, como no direito biomédico, no qual se solidificou o consentimento como mecanismo contra abusos e garantia da autodeterminação individual, contribuíram para o conceito atual controlo informacional e de autodeterminação

3.1.2. A Autodeterminação informacional e proteção de dados

Se no direito privado o consentimento se afirmou como garantia da autonomia negocial e no direito biomédico, permitiu a acautelar a integridade física e moral dos indivíduos, a chegada à sociedade da informação demonstrou uma profunda alteração do conceito jurídico do consentimento.

O acórdão do Tribunal Constitucional Federal Alemão, referente ao caso Censo[14] (*Volkszählungsurteil*) e que remonta a 15 de dezembro de 1983 é tido como um ponto de viragem desta transformação, por ser reconhecida na sua sentença pela primeira vez, o direito fundamental à autodeterminação informacional (*Informationelle Selbstbestimmung*).

> "*(…) quem não pode prever de forma razoável quais as informações sobre si que são conhecidas em determinados contextos, e quem não pode avaliar suficientemente as possíveis consequências desse conhecimento, vê seriamente comprometida a sua liberdade de agir*". (BVerfGE 65,1, 43)

[11] Os Julgamentos de Nuremberga (1946-1947), em especial *o Doctors´Trial*, no qual julgaram médicos nazis responsáveis por experiências médicas em prisioneiros sem consentimento verdadeiro e informado destes, que revelaram experiências que resultaram em violações graves da integridade humana e mais tarde, em consequência destes resultou a publicação do Código de Nuremberga.

[12] O código de Nuremberga (1947) foi o primeiro documento a exigir expressamente o consentimento informado em investigações médicas, tornando-o condição de validade ética e jurídica.

[13] A declaração de Helsínquia (1964), da associação Médica Mundial, consolidou esse princípio, tornando-o vinculativo para a prática clínica e científica internacional.

[14] O acórdão "*Volkszählungsurteil*)" (1983) é considerado na doutrina como um marco no direito à autodeterminação informacional, e autores como(Habermas, 1999) , (Donela, 2019) e (Schwartz, 1989), destacam o impacto desta decisão no debate global sobre privacidade, por outro lado, (Bygrave, 2014) e (Kranenborg, 2016) frisam a sua influência na Diretiva 95/46/CE e no RGPD.

Neste acórdão o Tribunal Constitucional Alemão, clarifica que não basta a liberdade individual de consentir sem limitações, é também necessário que os indivíduos possam com certo grau de previsibilidade e controlo perceber por onde circulam as suas informações pessoais, caso isso não se verifique não há autonomia prática, e a autodeterminação é apenas um direito formal, quando deveria ser uma condição material de liberdade de agir.

Esta análise vinculou o tratamento de dados e elevou-o a expressão da dignidade humana e liberdade individual, deixando o consentimento de ser apenas um requisito formal de validade, passando a constituir um requisito de legitimidade para a recolha e tratamento de dados pessoais. A influência deste acórdão marcou a Diretiva 95/46/CE, que, no seu Artigo 2.º, h), estabeleceu o consentimento como "qualquer manifestação de vontade, livre, específica e informada", exigindo assim um consentimento informado e positivo, conforme o texto do acórdão.

Na doutrina europeia Bygrave, (2014) e Lynskey, (2015)referem que a proteção de dados deixou de ser apenas a defesa contra violações, para se tornar num direito positivo, como acesso e controlo sobre os fluxos de circulação dos dados pessoais e refere que agora o consentimento é um mecanismo de gestão da informação, eficaz, quando apoiado por garantias de transparência e responsabilização.

Este caminho findou no RGPD, que fixou o consentimento como base legal para o tratamento (Artigo 6.º), clarificando a sua definição (Artigo 4.º, n.º 11) e exigindo que este seja prestado de forma inequívoca, especifica, informada e livre. Resulta assim, desta evolução que o direito da autodeterminação informacional, combina o consentimento contratual, biomédico e digital, tratando-se assim de um mecanismo de autonomia e dignidade humana.

3.1.3. O consentimento no RGPD: princípios e obrigações

Como já se referiu, o Regulamento Geral da Proteção de dados (RGPD) representa o apogeu da evolução histórica do consentimento, com um papel de relevo nas bases de licitude no tratamento de dados pessoais. Longe dos conceitos iniciais, pouco claros e densos, o RGPD obriga a que o consentimento seja prestado de forma livre, especifica, informada e inequívoca e desta forma afastando o inicial conceito de formalismo contratual. Com este novo conceito, o legislador apresentou também obrigações para os responsáveis pelo tratamento dos dados, que passam agora para além da recolha, a ter de demostrar e documentar, o consentimento prestado através da manifestação de vontade dos titulares (Artigo 7.º). Para (Kosta, 2013) para além de um requisito formal, o consentimento representa também um meio de execução da autonomia individual, que encontra a sua função na informação, da revogabilidade e da efetiva possibilidade de escolha. Já Menezes Cordeiro (2018) acrescenta, que o consentimento deve ser verificável e rastreável, sob pena de se reduzir a uma "ficção de autonomia".

Propomos então, uma análise de dois pontos essenciais, a definição atual e os requisitos de validade previstos nos Artigos 4.º, 6.º e 7.º do RGPD e ainda a revogabilidade e a granularidade, como garantias de autodeterminação.

3.1.4. A definição legal atual e os requisitos de validade (Artigo 4.º, 6.º e 7.º do RGPD)

É o RGPD que impõe agora um novo conjunto normativo, que além de redefinir o consentimento, exige rigorosos critérios para a sua validade (Artigo 4.º, n.º 11). Os quatro elementos da manifestação da vontade: "livre, específica, informada e inequívoca, formam a pedra basilar da validade do consentimento, e encontram o complemento no Artigo 6.º e 7.º, que configuram como base da licitude no tratamento dos dados pessoais.

a) Consentimento livre

A liberdade importa que não exista coação ou condicionantes e uma dessas circunstâncias está plasmada no Artigo 7.º, n.º 4, que estatui que o consentimento, quando condicionado à execução de um contrato ou prestação de serviço, quando dele não seja necessária essa manifestação de vontade, não é considerado livre.

Mariana Eduarda Gonçalves (2017), tal como a doutrina sobre este requisito entende, que pode existir um risco de um "controlo ilusório", sempre que os utilizadores são confrontados com escolhas impostas em bloco.

b) Consentimento específico

O consentimento deve ser prestado para finalidades determinadas, não estando contempladas finalidades genéricas ou indistintas. O considerando 43 do RGPD, sublinha a necessidade da granularidade do consentimento ou dito de outra forma, que ao titular é devida a possibilidade de consentir para cada finalidade de forma separada. A jurisprudência do Tribunal de Justiça da União Europeia (TJUE), implementado este entendimento nas decisões e por conseguinte, rejeitando a validade de consentimentos amplos, incluídos em termos e condições gerais da utilização.

c) Consentimento informado

Verdadeiramente associado ao princípio da transparência (Artigo 5.º, n.º 1, al. a), estabelece que a informação colocada à disposição do titular, deve ser clara, acessível e compreensível, d forma a que o titular dos dados, consiga compreender a finalidade da recolha dos seus dados. Relativo a este requisito importa referir o acórdão do TJUE, conhecido como Planet49 (Processo C-673/17, 2017), sobre o qual mais à frente nos debruçaremos), que enfatiza que as informações devem estar acessíveis e não camufladas em clausulas complexas ou com remissões para documentos extensos e complexos, por forma a garantir que o titular tem pleno conhecimento do que está a consentir.

d) Consentimento inequívoco

Este requisito remete-nos para a necessidade da obtenção de um ato positivo e claro, dos quais se explui as práticas *opt-out* ou presunções tácitas. Lynskey (2015), diz-nos que a exigência imposta, permite sustentar a legitimação do consentimento e reflete também a fragilidade deste perante a manipulação de interfaces digitais (*dark patterns).*

e) Ónus da prova e rastreabilidade

Por forma a afastar a mera formalidade do consentimento, o RGPD estabelece no Artigo 7.º, n.º 1 que cabe ao responsável pelo tratamento de dados provar que o consentimento foi prestado de forma válida. Esta obrigação implica ainda que o responsável adote forma de registo, documentação e rastreabilidade, que permitam sempre que necessário, demostrar o cumprimento deste normativo e a validade do consentimento prestado. Como ensina (Menezes Cordeiro, 2021), não devemos ter o consentimento como um ritual, mas como um ato jurídico, que pode ser verificado e reconstruído e o que obriga não apenas a uma análise formal, mas uma análise material. Este normativo é complementado por normas técnicas, como é o caso da ISO/IEC 27560:2023, que estabelece as estruturas interoperáveis de registo do consentimento e asseguram granularidade, rastreabilidade e revogabilidade. A conjugação de soluções como as normas do RGPD e a normalização técnica, permite que as organizações efetivem as obrigações e consigam demonstrar e comprovar a sua execução.

Aqui chegados, podemos afirmar que o RGPD, transformou o consentimento num mecanismo forte, impondo liberdade, especificidade, informação clara, ato positivo e inequívoco e prova documental do desse consentimento. Não obstante, continuamos a padecer de problemas estruturais, e para essa realidade nos alertam Solove, (2010)e Hijmans, (2016)relembrando que os requisitos de validade do consentimento continuam frágeis e afetados pela fadiga do consentimento, interfaces manipulativas, a sobre utilização do consentimento como base legal e é aqui que fundamentamos a pertinência deste trabalho, entre o desnível resultante da robustez normativa e a fragilidade pratica, e da necessidade de novas soluções técnicas e jurídicas que permitam de forma concreta a efetividade do consentimento enquanto mecanismo de contro informacional.

3.1.5. Revogabilidade e granularidade

Outro dos grandes contributos do RGPD resultou da consagração da revogabilidade do consentimento e da granularidade na estrutura do consentimento.

Esta, como a alteração do conceito histórico, encontra a fundamentação na necessidade de asseguramos que a manifestação de vontade dos titulares não se esgote apenas no ato de consentir e que este não se torne num ato irreversível, mas sim, num procedimento ajustado às necessidades e escolhas individuais.

Prevê o Artigo 7.º, n.º 3 que o "titular dos dados tem o direito de retirar o seu consentimento a qualquer momento", deste Artigo resulta ainda, que o a retirada do consentimento deve ser tão fácil, quanto a concessão e torna esta norma o consentimento dinâmico, em face às redações anteriores. Nas palavras de Joana Covelo de Abreu (2017), a revogabilidade permite que a vontade do titular "não se cristaliza numa decisão passada, mas acompanha a sua liberdade atual".

3.2. Jurisprudência relevante no TJUE sobre o consentimento

De forma a obter os elementos necessários para criar uma arquitetura computacional ajustada à realidade, analisamos a jurisprudência do Tribunal de Justiça Europeu, nesta matéria. Acercamo-nos das questões colocadas em matéria de consentimentos nomeadamente, a interoperabilidade e registo, a liberdade real de aceitação do consentimento e vieses, transferência e a proteção de dados desde a conceção e por defeito.

Existem outras decisões de relevo nestas matérias, porém selecionamos as que mais conhecidas e as que mais impacto tiveram no dia-a-dia dos cidadãos e que por serem reconhecidas quantos às consequências decorrentes da apreciação judicial, resolvemos apresentar e basear na elaboração desta arquitetura.

3.2.1. Meta vs Bundeskartellamt (C-252/21, de 4 de julho de 2023)

O acórdão *Meta* vs *Bundeskartellamt* (Processo C-252/21., 2021),representa uma das decisões mais relevantes em matéria de jurisprudência do TJUE, quanto à recolha, tratamento e proteção de dados e também sobre o direito da concorrência, em contexto digital

O acórdão tem origem numa decisão da entidade alemã da concorrência (*Bundeskartellamt*), que proibiu a *Meta* de efetuar a recolha e partilha de dados pessoais de utilizadores, entre diferentes entidades do seu grupo (designadamente *Facebook, Instagram*, *Whatsapp* e outros), sem a existência prévia dos consentimentos válidos, livres e individualizados para cada uma dessas entidades, pelos titulares dos dados. Tendo a entidade da concorrência fundamentado a decisão, no entendimento que o comportamento a empresa *Meta* corresponde a um abuso da posição dominante no mercado das redes sociais, conceito que decorre do direito da concorrência da União Europeia.

Remetida para apreciação do TJUE, é proferido a quatro de julho de 2023 o acórdão e nas suas conclusões resulta a existência de uma infração das regras da concorrência, bem como a desigualdade do poder entre o responsável pelo tratamento de dados e o titular dos dados e essa desigualdade afeta a liberdade da manifestação da vontade e por conseguinte a validade do consentimento.

Este acórdão analisou ainda a recolha e partilha de dados entre empresas de grupo *Meta*, com base na aceitação da prestação do serviço pela empresa, contra aceitação do consentimento, com base no fundamento de execução do contrato (Artigo 6.º, n.º 1, al. b) do RGPD), tratando-se assim de um

"**consentimento condicionado**" (*take-it-or-leave-it*), que violam princípio da licitude, liberdade e da especificidade do consentimento, conforme resulta do RGPD.

Deste acórdão resulta a necessidade de uma maior intervenção das entidades de controlo, uma vez que em circunstâncias como as de uma empresa cujo poder económico e posição de poder, limita os direitos e liberdade dos titulares de dados, apresentando o consentimento como uma mera formalidade não como o direito fundamental de autodeterminação informacional. Revela assim a necessidade de mecanismos eficazes de controlo e demonstração de cumprimento dos princípios do RGPD, para o tratamento de dados e diretamente alinhados com o tema aqui desenvolvido.

3.2.2. IAB Europe (C-604/22, de 7 de março de 2024)

Por força de uma decisão Autoridade Belga de Proteção de Dados (APD/GBA) contra a *IAB Europe* (entidade responsável pelo desenvolvimento o *Transparency and consent Framework* (TCF)) a *Conseil d´État da Bélgica* procedeu ao reenvio prejudicial ao TJUE.

A questão em análise é relativa à qualificação jurídica do *TC String*. Em particular o *TC String* é definido neste acórdão, como um código gerado pelo sistema TCF e que armazena as opções previamente selecionadas pelos utilizadores e posteriormente partilha com entidades terceiras.

O TJUE(Processo C-604/22, 2022) foi chamado a pronunciar-se sobre três questões essenciais: a primeira, se o *TC string* é considerado ou não um dado pessoal, segunda, se a *IAB Europe*, deve ser considerada entidade responsável pelo tratamento dos dados e, terceira, se o sistema TCF cumpre com os requisitos de validade do consentimento à luz do RGPD.

O TJUE pronunciou-se e a sete de março de 2024 e decidiu que deve entender-se como dado pessoal o sistema TCF, uma vez que está associado a um identificador único, como é o caso do IP ou ID do dispositivo, assim cumprindo como o disposto no Artigo 4.º, n.º 1 do RGPD, permitindo a identificação ainda que indireta do utilizador. E ainda que *a IAB Europe* é responsável pelo tratamento dos dados pessoais, embora não tenha acesso direto ao conteúdo do *TC String*, é associada à figura responsável pelo tratamento de dados[15], apresentada no Artigo 4.º, n.º 7 do RGPD, porque define os meios e as finalidades do tratamento no âmbito do TCF. Por último, o TCF não cumpre os requisitos de validade do consentimento, previstos no Artigo 7.º do RGPD, em especial a complexa *interface*, bem como a existência de predefinições como as opções de aceitação e a inexistência de controlo por parte do utilizador de forma efetiva e acessível sobre os seus dados.

[15] «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;RGPD

Acresce ainda que o consentimento não pode decorrer de uma presunção, nem ser obtido através de "*dark patterns* [16]"ou no português "padrões obscuros", definidos como estratégias utilizadas no meio digital para induzirem os utilizadores ao erro ou a tomar decisões contrárias aos seus interesses, maioritariamente em situações de recolha de consentimento ou subscrições. Com isto o TJUE aponta que a obtenção de consentimentos, através de designs manipulados não é considerada valida pois não cumpre com os requisitos de validade do RGPD.

De especial interesse, este acórdão integra no leque de dados pessoais, alguns sistemas aparentemente neutros, e desta forma enquadrando-os no RGPD e conferindo aos utilizadores o reforço da segurança e evidência a necessidade da existência de plataformas de gestão de consentimentos (*Consent Management Plataforms)*[17] que efetivamente analisem o cumprimento da validade dos consentimentos prestados e não apenas os formalismos necessários aos fins publicitários, reforçando a necessidade da arquitetura que aqui se propõe, direcionada ao titular e que permita o cumprimento do RGPD e o exercício dos direito dos titulares.

3.2.3. Schrems II (C-311/18 – 16 de julho de 2020) – Transferências internacionais

O caso *Schrems II* (Processo C-311/18, 2020)tem origem numa queixa apresentada por um cidadão austríaco, *Maximilian Schrems*, junto da entidade de controlo irlandesa, a Comissão de Proteção de dados da Irlanda (DPC). Em suma *Schrems* insurgiu-se contra a transferência de dados da empresa *Facebook Ireland* para a *Facebook Inc*. nos Estados Unidos, representado uma alteração na forma como os dados são tratados em países terceiros.

Schrems contestou a licitude da transferência de dados para os servidores da Facebook nos Estados Unidos. Chamado a decidir a questão, o TJUE apresenta a decisão a 16 de julho de 2020, da qual resulta a declaração de invalidade da Decisão 2016/1250 da Comissão Europeia, que aplicou o *Privacy Shield*, um acordo sobe a transferência de dados pessoais entre a Europa e os Estados Unidos da América, por não existir um nível de proteção equivalente ao Europeu, nem a tutela jurisdicional efetiva dos titulares dos dados e ainda pelo acesso indiscriminado aos dados pessoais pelas autoridade públicas e de segurança nacional Americana, em violação dos princípios da necessidade e proporcionalidade do RGPD.

Ainda nesta decisão, o TJUE valida a utilização das cláusulas contratuais-tipo (CCts) ou *Standard Contratual Clauses* (SCCs)*,* desde que complementadas por outras medidas adicionais como a pseudonomização, encriptação ou restrições contratuais por forma a equilibrar a proteção com o

---

[16] "*A dark pattern is a user interface that has been carefully crafted to trick users into doing things, such as buying insurance whith their purchase or signing ip for recurring bills"* – Brignull, H (2010). *Dark Patterns – Deception Vs Honesty in UI Design - darkpatterns.org*

[17] *Consent Management Plataforms (CMPs)* são ferramentas digitais concebidas para recolher, gerir e documentar o consentimento do utilizador para o tratamento de dados pessoais, assegurando a conformidade com a regulamentação da privacidade como o Regulamento Geral sobre a Proteção de Dados (RGPD). Este entendimento é amplamente usado na literatura académica, no que concerne à implementação e desafios da privacidade de dados (Günther, Scheid, & Zwitter, 2021)

RGPD. Deste acórdão e para o tema releva o facto de o consentimento por si só não representar fundamento suficiente para as transferências de dados fora da EEE, impondo também a adoção de mecanismos adicionais, que devem ser avaliados pelo responsável do tratamento, caso a caso, direcionando-nos para a necessidade do uso de mecanismos técnicos e juridicamente rigorosos. Por outro lado, a necessidade de uma plataforma de gestão centralizada, que permita adequar de forma automatizada os requisitos a cumprir para o país de destino, bem como a revogação em tempo real e a rastreabilidade da exportação de dados e ainda, reforça a necessidade da proteção segundo o modelo *privacy by design*, prevista no Artigo 25.º do RGPD, a interoperabilidade as auditorias continuas.

3.2.4. Planet49 (C-673/17)

Este acórdão representa um marco jurisprudencial, relativo ao consentimento válido em contexto digital, principalmente no que aos *cookies* e tecnologias de monitorização dos utilizadores diz respeitos.

> *"O consentimento não é validamente prestado se a armazenagem de informações ou o acesso a informações já armazenadas no equipamento terminal do utilizador de um site da Internet for autorizado mediante uma caixa assinalada por defeito que o utilizador deve desmarcar para recusar o seu consentimento" (TJUE, C-676/17,* §63).

A apreciação do TJUE (Processo C-673/17, 2017)decorre de uma questão prejudicial remetida pelo *Bundesgerichtshof* (Tribunal de Justiça Federal da Alemanha), no âmbito de um processo que opõe a empresa *Planet49 GmbH*, cuja atividade consistia na organização de sorteios *online*, mas cuja participação dos utilizadores estava condicionada à aceitação dos cookies de terceiros para fins publicitários, com recurso a caixas de verificação pré-selecionadas (*pre-ticked checkboxes*).

Ao tribunal de Justiça da União Europeia competiu analisar a licitude do tratamento de dados pessoais pela *Planet49*, à luz dos Artigos 5.º, n.º 3 da Diretiva *ePrivacy* (2002/58/CE), conjugado com 4.º, n.º 11 e 7.º do RGPD. Da sentença resulta que o consentimento não pode ser fornecido através de caixas de verificação pré-selecionadas, pois esta circunstância coloca em crise a validade do consentimento, por não se consubstanciar na manifestação de vontade livre, informada e inequívoca. O tribunal estabelece ainda que, não é admissível o consentimento por omissão ou inércia e que ao consentimento do titular

deve corresponder uma ação positiva (*opt-in*). No que aos *cookies*[18] diz respeito, é ainda clarificado que os responsáveis pelos tratamentos dos dados devem prestar informações claras e de forma acessível e ainda sobre as categorias de *cookies* de terceiros.

Como reforço da necessidade da arquitetura proposta, este acórdão demostra a necessidade de uma plataforma que permita a obtenção do consentimento, quando necessário ao tratamento de dados, de forma licita e sem "*dark patterns*", nem uso de outros subterfúgios como as caixas pré-selecionadas. Reforça a designação da "fadiga do consentimento" sentida pelos titulares e ainda a complexidade dos mecanismos de recolha dos consentimentos, que se afastam do conceito do direito da autodeterminação informacional dos titulares.

3.3. Outra legislação e normativos aplicáveis

O regime jurídico do consentimento e os seus requisitos de validade e efetividade, não se esgotam apenas no Regulamento Geral da Proteção de dados e encontram noutros instrumentos, a força e condições de aplicação prática. A análise de toda a panóplia de diplomas aplicáveis, carece de uma divisão para que seja possível a sua análise e interligação. Dividimos o primeiro grupo em legislação europeia e nacional, como a Diretiva 2002/58/CE (*ePrivacy*), Diretiva (EU) 2019/770, a relativa a conteúdos e serviços digitais, ou ainda o mais recente Regulamento (EU) 2024/1689 (IA act).

O segundo grupo resume os diplomas complementares europeus e nacionais (*Soft law*), como as diretrizes e pareceres , como as Guidelines 05/20220 do EDPB sobre o consentimento e deliberações emitidas pela Comissão Nacional de Proteção de Dados e o terceiro grupo com as normas técnicas internacionais, nomeadamente aos ISO/IEC, como a ISO/IEC 27701:2019 (gestão da privacidade) e a ISO/IEC 27560:2023 (*consent record information structure*), que permitem compreender como operacionalizar os procedimentos do consentimento (recolha, gestão, revogabilidade).

A interpretação destes três grupos de diplomas, tem suma importância para complementar abordagem interdisciplinar que pretendemos desenvolver, nomeadamente o cruzamento eficiente o direito e a tecnologia apoiada na regulamentação complementar.

3.3.1. Outra legislação e normativos aplicáveis

Para além do RGPD, existem ainda outros diplomas e instrumentos que permitem reforçar e complementar os princípios que emanam RGPD, permitindo com isso a sua concretização prática. Estes normativos, permitem a uniformização da gestão e tratamento de dados no espaço europeu,

[18] Um pequeno ficheiro em formato de texto colocado no seu computador ou dispositivo móvel, através do navegador de internet (browser) durante uma visita a uma plataforma digital, tendo como finalidades as de armazenar, recuperar ou atualizar dados.

abrangendo áreas como as comunicações eletrónicas, serviços digitais, reutilização de dados e identidade eletrónica.

A Diretiva 2002/58/CE (União Europeia, 2002), conhecida como Diretiva *ePrivacy* tornou-se fundamental no setor das comunicações eletrónicas, numa altura em que se verificava um crescimento das comunicações digitais e que a sua antecessora não conseguia solucionar os desafios que emergiam desta nova realidade. Foi transposta para ordenamento jurídico português, através da Lei n.º 41/2004[19] e com ela foram apresentadas novas inovações com vista assegurar de forma harmonizada a privacidade e a proteção de dados nas comunicações digitais.

Uma dessas inovações é o consentimento prévio, previsto no Artigo 5.º, n.º 3, que prevê a necessidade do consentimento prévio (*opt-in*) para o armazenamento e acesso à informação nos equipamentos dos utilizadores, como por exemplo num computador ou telemóvel, tendo desta forma alterado o procedimento existente, que estabelecia que o utilizador de se manifestar caso não quisesse o acesso à sua informação ou o a utilização dos *cookies* (*opt-out*), assim reforçando a necessidade de um consentimento livre e informado para as comunicações eletrónicas, em especial para os e-mails de *marketing* e *cookies*. Ainda sobre os *cookies*, a diretiva tornou claro em que circunstâncias o consentimento poderia não ser necessário, para a sua utilização. Por força da interpretação dada pelo grupo de trabalho do Artigo 29 (que atualmente é o EDBP), no seu Parecer 04/2012, ao Artigo 5.º, n.º 3, foi possível dispensar o consentimento para acesso a informação estritamente necessária e no seguimento de uma solicitação de prestação de serviço pelo utilizador. Dentro desta hipótese temos estes exemplos: *Cookies* de sessão: que são necessários para que o utilizador possa efetuar compras num *site* ou efetuar registo e manter a navegação de forma autenticada; *cookies* de autenticação: que permitem que o utilizador faça login e não necessite de o refazer nos acessos posteriores a cada página que visita; *cookies* de equilíbrio de carga (*load balancing*), ajudam a distribuir o tráfego de forma a garantir que o *site* se mantém a funcionar.

Outra das inovações destacadas e com profunda relevância para o princípio da transparência e responsabilização (*accountability*) que mais tarde faria parte dos princípios do RGPD, falamos da notificação em caso de violação de dados, por parte dos prestadores de serviços de comunicações, prevendo o Artigo 4.º, que estes devem informar a autoridade nacional de controlo, sempre que tal se verifique, antecipando-se ao RGPD, embora limitada à área da comunicação digital.

Resumidamente, a Diretiva *ePrivacy*, permitiu antecipar dois dos mais fundamentais princípios do RGPD, inovando no setor das comunicações e deixando a clarificação sobre a exclusão do consentimento relativos a *cookies.*

[19] Sucessivamente alterada pela Lei n.º 46/2012 e pela Lei n.º 16/202522 (Lei das Comunicações eletrónicas)

Regulamento 2022/2065, (2022)Em complemento, o , conhecido como *Digital Service act* (DSA), foi aprovado a 19 de outubro de 2022 e à sua criação presidiram os ideais de maior segurança, transparência e responsabilidade no comércio eletrónico, por se tratar de um regulamento que visava todos os estados-membros. Contribuiu para a adoção de novas regras sobre a segurança e a transparência, mas também sobre a responsabilidade das plataformas em linha. Relativamente ao consentimento, proibiu de forma expressa a utilização de *dark patterns*, conforme resulta do seu Artigo 25.º, conforma já vimos os interfaces manipulativos que condicionam a decisão dos titulares dos dados. O *Digital Service act* (DAS) aparece como um complemento do RGPD, que contribui para o consentimento livre e informado, sem condicionantes enganosas e ainda, para na transparência publicitária. Assim, o regulamento deve ser visto à semelhança do anterior diploma, como um complemento que se mostra relevante para a cabal aplicação do RGPD.

O Regulamento 2022/868 (Parlamento Europeu e do Conselho, 2022), designado por *Data Governance act* é uma inovação, porque configura um mecanismo que promove a partilha e reutilização de dados. A reutilização ocorre através dos intermediários de dados, figura criada por este regulamento e que serve de ligação entre os titulares e os responsáveis pelo tratamento, que tratam os dados para fins de interesse geral e não interesse próprio. Na qualificação de interesse público inclui-se os fins de investigação científica ou saúde pública, sendo atribuído a este conceito de reutilização de dados, o nome de altruísmo de dados. Para que tal seja possível e à semelhança do que temos vindo a identificar é necessário o consentimento do titular dos dados e esse consentimento deve ser prestado de forma livre, informada, especifica e revogável, como condição de legitimidade ao tratamento dos dados. Este regulamento representa o reconhecimento europeu da necessidade de modelos híbridos, e não apenas individuais, em que o consentimento é baseado em técnicas e instituições de confiança e do reforço do controlo pelas instituições responsáveis pelo controlo reforçando a nossa visão de um modelo central de gestão de consentimento.

(Parlamento Europeu e do Conselho, 2023),Por sua vez, o regulamento Regulamento 2023/2854 ou *Data Act (Data Governance Act* (DGA)*),* visa a uniformização das regras referentes ao acesso e recolha dos dados gerados por dispositivos, produtos ou serviços digitais, quer sejam públicos ou privados. Trata-se assim de um regulamento complementar ao *Data Governance act.* Nas suas disposições destacamos o direito de acesso a dados que são gerados por dispositivos e serviços, pelos titulares quando usem um dispositivo conectado como por exemplo um *smart device* ou *wearables,* estando o fabricante obrigado a disponibilizar ao titular os dados gerados de forma gratuita e de forma fácil e rápida. Outra das disposições que qui destacamos é o reforço do papel do consentimento enquanto fonte de licitude, para a partilha de dados entre entidades públicas e privadas em situações de interesse público, como sucedeu na pandemia do *covid19*, sem colocar de lado aplicação das bases

legais prevista no Artigo 6.º do RGPD, impondo ainda regras relativas à portabilidade e interoperabilidade entre serviços *cloud* e *edge computing.*

Relevante para a fundamentação deste trabalho o *Data Act* apresenta um conjunto de novas obrigações de acesso e partilha de dados que poderão afetar o comércio digital e cuja eficiência dependerá da forma como as empresas a implementarem na prática, mas para o tema importa a latente necessidade de meios técnicos adequados à gestão centralizada e interoperabilidade, que resulta da dispersão de dados e com ela o rico de fragmentação, opacidade e insegurança jurídica.

(Parlamento Europeu e do Conselho, 2024a)No concerne ao Regulamento Regulamento 2024/1183 eIDAS2, veio atualizar a anterior *electronic IDentification, Authentication and trust Services* (eIDAS), que introduziu a carteira de Identidade Digital Europeia (*EUDIW Wallet*). A carteira é um mecanismo de identificação, válido em todos estados-membros, seguro e uniforme, onde é possível gerir vários documentos como Carta de condução, dados bancários, entre outros, numa aplicação certificada por cada um dos estados-membros.

O eIDAS2 assenta na criação de um Regime Europeu para a Identidade Digital, com vista a uma solução uniforme para todos cidadão e empresas, de todos os estados-membros, através da implementação da Carteira Europeia da Identidade Digital (EUDIW), que impõe que os estados-membros forneçam aos seus cidadãos uma Carteira digital onde seja possível armazenar os seus dados de identificação e outros atributos e para conseguir a universalidade do seu uso prevê-se a interoperabilidade em toda a União Europeia. Reforça também o controlo dos dados pelo utilizador e ainda a minimização de dados, com a partilha dos dados estritamente necessários. Este regulamento representa um novo modelo de identificação e gestão de dados pessoais, permitindo que ao mesmo tempo o utilizador se identifique e preste consentimento para partilha de dados pessoais de forma explícita e identificável, conforme Artigo 6.º A. Esta inovação implica em si um novo desafio para a plataformas de gestão de consentimento, que deixarão apenas de lidar com *cookies* ou termos de aceitação e passam a integrar um modelo europeu de identidade digital soberana.

Tal como o modelo que aqui queremos propor, também o modelo EUDIW está voltado para o *user centric*, ferramentas de gestão em temo real, que permitem ao utilizador gerir, revogar ou alterar consentimentos, e interoperabilidade e acesso entre várias entidades. Trata-se de um avanço cujas funcionalidade poderão facilitar o acesso quer a serviços públicos quer a privados, mas que comporta riscos decorrente da interoperabilidade entre carteiras de vários estados-membros e as questões de segurança, como a *privacy by desing* e ainda desigualdades da aplicação prática por Parte dos estados-membros. Consideramos que é uma inovação que sustenta a necessidade de uma arquitetura cujo desenho unifique funcionalidades e permita o utilizador o exercício dos seus direitos, dentro de uma construção segura, que obriga a repensar as arquiteturas existentes.

Por último, no plano nacional, a lei de execução que corresponde à Lei n.º 58/2019, (2019), como o próprio nome identifica é um diploma que assegura a execução do RGPD no ordenamento português. Longe de ser apenas uma lei acessória, a sua publicação permitiu aproximar o conteúdo da diretiva europeia à realidade nacional, e ainda estabelece as bases de atuação da Comissão Nacional de Proteção de dados, entidade responsável pelo controlo em território nacional. Na garantia da aplicação das normas do RGPD é ainda previsto nesta lei o regime sancionatório aplicável a contraordenações em matéria de proteção de dados pessoais, mostrando assim a garantia da execução efetiva do RGPD.

3.3.2. Soft Law europeu e nacional

Para além da legislação obrigatória em matéria de consentimento no tratamento de dados pessoais, parece-nos ajustado referir a *Soft law* europeia e nacional, que permite a implementação e interpretação prática do RGPD e demais leis obrigatórias neste plano, servindo ainda de orientação em situações menos claras para responsáveis pelo tratamento de dados.

Destacamos aqui as diretrizes do Comité Europeu para a proteção de dados (EDBP), com especial interesse para o tema a Diretriz 05/220 sobre o consentimento e proteção de dados, que estabelece que a retirada do consentimento, deve ser tão fácil quanto a sua concessão, destacando-se aqui os meios de retirada devem ser iguais aos que precederam a concessão e estarem acessíveis da mesma forma que esta o mecanismo de aceitação e ter o efeito imediato. Outra medida que daqui decorre é a não rejeição de consentimentos obtidos, dentro dos termos de e condições de utilização, pela falta de especificidade, informação e liberdade, defendendo esta diretriz o consentimento enquanto decisão ativa e granular.

Em 2023, o mesmo Comité (EDBP) publicou o Relatório da *Taskforce* sobre *cookies Banners*, um documento que resulta da colaboração entre estados-membros e avalia as práticas sobre a recolha de dados em *websites*, tendo como principal foco o levantamento de falhas comuns a todos. Este relatório permite corroborar que a grande maioria dos *banners de cookies* não se encontra em conformidade com o RGPD, e a falhas mais comuns são a falta de opção para recusar, ou por inexistência ou por não se encontrar visível, a falta de informação ou a sua insuficiência, quando se trata de identificar as finalidades do tratamento dos dados, o tipo de cookies em uso e a identificação dos terceiros. Destaca ainda a utilização de *dark patterns*, que destacam a opção aceitar e ocultam a opção rejeitar, contribuindo para uma aceitação condicionada pela manipulação de cores e botões destacados. Esta prática, também ela discutida na jurisprudência que aqui se analisou relativa ao *Planet49* e que destaca alguns dos problemas que aqui estudamos relativos ao consentimento e seus requisitos.

Mais atual, o Parecer 08/2024 do Comité (EDBP), de 17 de abril de 2024, avalia a validade do consentimento quando prestado no âmbito do modelo de "consentir ou pagar" (*consent or pay*),

referentes a prestadores de serviços em linha. O modelo consiste na escolha entre consentir no tratamento de dados, para o seu uso em publicidade comportamental ou pagar uma taxa, para usar esse serviço sem o tratamento de dados, usado como por exemplo pelo grupo *Meta* (*Facebook* e *instagram*). Analisando este modelo, o EDBP considerou que não cumpre os requisitos do consentimento previsto no RGPD e sugere que os prestadores ofereçam um serviço gratuito equivalente, sem publicidade, para que o consentimento seja considerado efetivamente verdadeiro. Deste parecer retiramos a falta de liberdade e o desequilíbrio de poder entre prestadores de serviços em linha e os utilizadores, titulares dos dados e levantamos novamente a questão: estaremos realmente a prestar um consentimento livre, se não temos alternativa equivalente? Este parecer indica-nos que não e releva novamente a necessidade de um novo modelo que permita a escolha efetiva pelos titulares e proteja a sua autodeterminação informacional.

Em Portugal, a Comissão Nacional de proteção de Dados (CNPD), tem implementado de forma prática as toda a panóplia de *soft law*, como as diretrizes, orientações e pareceres do Comité (EDBP), adaptando à realidade nacional.

Compreendemos desta forma, que a *soft law*, acompanha o consentimento que apenas se torna efetivo quando existem mecanismos capazes de assegurar a sua aplicação prática, a transparência e a segurança na sua execução. Assim, os diplomas não vinculativos do Comité **EDPB**, bem como a execução nacional pela CNPD, indicam-nos que existe a necessidade de adotar novas estratégias técnicas, que reforcem a execução do direito da autodeterminação informacional e esbatam as falhas que exploramos, uma ideia que também compartilhamos neste trabalho (European Data Protection Board, 2020b, 2023; European Data Protection Board (EDPB), 2023).

3.3.3. Normas técnicas e ISO/IEC relevantes

Para além dos diplomas obrigatórios e a *soft law*, existem também normas técnicas, que servem de ponte entre os princípios do RGPD e a implementação técnica e assumem cabal importância, por fornecerem os formalismos e boas práticas, que permitem às empresas comprovar o cumprimento do RGPD.

De entre as ISO/IEC, destacamos as que abaixo se indicam e importam a definição dos requisitos de demonstram a conformidade, transparência e a rastreabilidade e audibilidade do consentimento, pelas empresas e organização responsáveis pelo tratamento de dados.

A norma Interational Organization for Standardization (ISO), (2011) (*Privacy framework*), da qual resultam os onze princípios fundamentais da proteção de dados, destacando-se a necessidade do consentimento e escolha, transparência e responsabilização (*accountability*) e representa uma base conceptual para todas as outras normas, permite uniformizar práticas organizacionais com o RGPD e é uma linguagem universal para todos os estados-membros. A International Organization for

Standardization (ISO), (2020) (*Online privacy notices and consent*), que define as diretrizes concretas para os avisos de privacidade e recolha do consentimento *online*, estabelecendo que a informação prestada aos utilizadores deve ser clara, concisa e facilmente compreendida, proibindo práticas manipulativas que induzam os utilizadores em erro. Esta norma à semelhança da jurisprudência do TJUE (*Planet49)* e cas orientações do Comité (EDPB), estabelecem a necessidade de designs de interfaces mais transparentes.

Mais atual, a ISO/IEC 27560:2023 (*consente record information structure),* esta norma técnica fundamental, é responsável pelo modelo técnico de estrutura de registo e informação do consentimento, para cumprimento do Artigo 7.º, n.º 1 do RGPD, garantindo a granularidade, rastreabilidade e revogabilidade e permitindo também a sua auditabilidade e interoperabilidade e com isto que a gestão do consentimento não é uma mera formalidade, mas um processo continuo e comprovável. No que toca à norma ISO_IEC 27701_2019 (2019) (*Privacy Informmation management System -PIMS),* representa uma extensão da International Organization for Standardization (ISO), (2019)e International Organization for Standardization (ISO), (2022) e tem por base o apoio às organizações para a construção de um Sistema de gestão de Informação e privacidade (PIMS), que auxilie as organizações em todo o ciclo de vida do tratamento dos dados pessoais.

Por último, a norma International Organization for Standardization (ISO), (2021) *(Deletion of PII*), orientada para o direito ao esquecimento previsto no Artigo 17.º do RGPD, ou direito a ser esquecido, tem como objetivos criar diretrizes para a eliminação ou anonimização de dados pessoais.

Todas as normas indicadas, representam diretrizes, que visam a adoção de mecanismos que permitam transformar o consentimento esta fonte de licitude, mais do que um requisito formal, um verdadeiro processo funcional e auditável.

3.3.4. Contributos académicos

A literatura académica debate também o consentimento enquanto fonte de licitude no RGPD e as suas limitações, preconizando soluções para estas fragilidades. Tendo em consideração a multidisciplinaridade deste trabalho, dividimos os contributos em três grupos: a análise jurídica, análise comportamental do utilizador e da inovação tecnológica.

Na critica internacional, iniciamos esta síntese por Solove, (2010), que defende que o consentimento no contexto digital, corre o risco de se tornar apenas um ritual jurídico vazio, sem que o titular tenha o poder de escolha consciente e livre. Nesta senda, Nissenbaum, (2010), defende a teoria da *integridade contextual*, que defende que o problema não esta na forma de recolha, mas sim, na falta de adequação nas práticas das plataformas em contraposição com as expectativas dos utilizadores. Esta visão é também acompanhada por *(Acquisti et al., 2015)*, que demostram através do estudo empírico que a capacidade de decisão humana é limitada por fatores psicológicos, e no campo da privacidade

são afetados por vieses do presente, como o ganho imediato, ou pelo paradoxo da privacidade, reconhecendo a importância da proteção da privacidade, mas atuando de forma contrária e ainda a sobrecarga cognitiva, com a repetida e excessiva quantidade de pedidos diários, que comporta o fenómeno da fadiga do consentimento, sem que consigam reconhecer os riscos e comprometem com isso a autodeterminação informacional. Estas limitações cognitivas, contribuem para o sucesso dos mecanismos de *dark patterns*, como enfatizam Mathur et al., (2019b), que após a analise a milhares de *websites*, confirmaram que a sua grande maioria utiliza designs manipulativos para obter o consentimento. Defende Lynskey, (2015), que o consentimento não deve ser encarado como uma "panaceia", porque a sua validade é muitas vezes comprometida por assimetrias de poder e de informação neste sentido, Bygrave, Lee A (2002), indica-nos que o consentimento por si não se basta e é necessário uma abordagem mais ampla, composta por mecanismos jurídicos, institucionais e técnicos[20].

No que diz respeito à análise tecnológica, os autores como Finck & Pallas, (2020), exploraram a utilização da tecnologia *blockchain* e o seu potencial na gestão de consentimento. Deste estudo resultou a melhoria da gestão do consentimento com recurso com recurso a essa tecnologia, por conta da imutabilidade dos e auditabilidade dos registos, mas também problemas de opacidade e rigidez técnica, também Zarsky, T (2016)[21], propõe o uso de uma tecnologia emergente, como é o caso da inteligência artificial, cujos resultados na sua perspetiva, dependem da forma como é concebida, implementada e supervisionada.

Os contributos doutrinários portugueses vão além da mera interpretação do RGPD e Menezes Cordeiro, (2018, 2021) define o consentimento como um verdadeiro ato jurídico, que faz depender a sua validade da sua demostração e rastreabilidade, distanciando-o da mera formalidade. Considerando ainda a extensão do conceito, Pinto Ramos, (2022), defende uma visão mais ampla do consentimento, propondo a centralização na pessoa e não apenas na abordagem contratual, que na visão de Gonçalves, (2024), padece do problema das assimetrias do poder, cujas consequências do crescimento desta realidade, se não existirem mecanismos eficazes que supervisionem a efetividade e a transparência, podem dar a falsa sensação de controlo e Pinheiro, (2015b), enfatiza na sua obra *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade Informacional*, como expressão da autodeterminação informacional e fundamento do direito fundamental à proteção de dados.

[20]Segundo L. A. Bygrave, (n.d.) o consentimento não é suficiente para a proteção dose dados, pelo que deve ser complementado por mecanismos jurídicos, que imponham imites e obrigações aos responsáveis pelo tratamento de dados, outros institucionais, como é o caso das autoridades nacionais de controlo (aqui CNPD) e técnicos, com recurso a mecanismos como *software* de anonimização, sistemas de gestão de consentimentos e outros que garantem a privacidade por padrão (*privacy by design*).

[21]Zarsky, (2016), salienta que os sistemas algorítmicos sofrem de opacidade, que é a originada pela falta de compreensão da informação, que leva à tomada de decisão e de rigidez, em consequência da falta de maleabilidade das regras, que são apresentadas e forma automática e inflexível sem possibilidade de adaptação e que coloca em causa os requisitos do consentimento à luz do RGPD.

Dos contributos académicos depreendemos que o consentimento, enquanto fundamento de licitude para o tratamento de dados, encontra nesta era digital várias limitações quanto à sua validade e eficácia. Verificamos que é necessária uma mudança de paradigma, promovida pela combinação de legislações cada vez mais robusta, por *designs* criados, seguindo o padrão orientado para a privacidade (*privacy by design)* e o reconhecimento das assimetrias de poder e manipulação, assim como a supervisão mais ativa da autoridade de controlo. Cremos poder contribuir com este trabalho para esbater estas limitações, com base no conhecimento adquirido.

3.4. Casos de estudo sobre Consent Management Plataform

As *Consent Management Plataform*[22] são fruto da necessidade de gerir de forma estruturada o consentimento em ecossistemas digitais[23]. Outra circunstância que contribuiu para o aparecimento destas plataformas, deveu-se à entrada em vigor do RGPD (União Europeia, 2016) em 2018 e da Diretiva *ePrivacy* (União Europeia, 2016) e têm como objetivo fornecer um conjunto de meios que permitam recolher, armazenar, atualizar e demonstrar a validade dos consentimentos obtidos de acordo com o RGPD. Apesar da evolução destas ferramentas, vários estudos indicam que apresentam ainda limitações estruturais, aqui incluídos os *dark patterns*, que que limitam a escolha do utilizador (Nouwens et al., 2020), a falta de interoperabilidade da qual resulta o excesso de pedidos de consentimento, aos quais acrescem os *dashboards* complexos (Berens et al., 2024).

Desta forma é importante proceder à análise de alguns casos de estudo de CMP, que permitirão compreender as que mais se aproximam dos modelos *user centric*, as suas funcionalidades e tecnologias e as falhas recorrentes, de forma a fundamentar a necessidade de um novo modelo mais robusto e juridicamente sólido.

MyData

O *MyData*[24], embora não seja verdadeiramente uma CMP é um modelo alternativo de gestão de dados, com origem na Finlândia (Poikola et al., n.d.-a) e na sua base tem o movimento que se dedica à defesa do direito da autodeterminação informacional, na qual o individuo deve decidir o uso e acesso dos seus dados pessoais, assente no conceito *humam-centric*, com *Personal Stores Data* (PSD).

---

[22] A evolução das CMP pode ser dividida em três fases, na primeira, na qual surgem os *banners* de *cookies* mais rudimentares, cujas limitações são a falta de transparência e escolhas manipuladas (Schermer et al., 2014), a segunda fase surge em consequência da entrada em vigor do RGPD e o surgimento de jurisprudência como o acórdão *Planet49* e o aparecimento de tecnologias que permitiam a granularidade do consentimento e ainda mecanismo de prova de conformidade(Tribunal de Justiça da União Europeia, 2019), a terceira fase, corresponde ao atual cenário em que os modelos integram já ferramentas consolidadas, alinhadas com o principio do *privacy by design* (Art.. 25.ºº do RGPD) e as boas práticas (European Data Protection Board, 2020b)

[23] Ecossistemas digitais são ambientes interligados de plataformas e serviços, infraestruturas e utilizadores que partilham e reutilizam dados de forma interoperável. Segundo (European Commission, 2020) estes ecossistemas assentam em princípios de confiança, segurança, interoperabilidade e gestão de dados

[24] O *MyData Global* é uma organização sem fins lucrativos, fundada em 2018 e sediada em Helsínquia na Finlândia, que promove um ecossistema internacional de gestão de dados centrada no utilizador e os operadores, definidos como intermediário de confiança e organizações (Langford et al., 2022).

Em termos de funcionamento o *MyData*, apresenta um sistema de gestão em que os dados são controlados por operadores de confianças, como empresas e plataformas digitais que permitem ao titular dos dados ver os dados que são partilhados, decidir quem pode aceder e para que finalidade e tempo, transferir dados, bem como revogar ou eliminar o consentimento prestado.

Cumprindo com as *Guidelines* do EDPB (European Data Protection Board, (2020) ;(2023)) e o RGPD (União Europeia, 2016) apresenta um painel único (*dashboard*) onde o titular pode gerir os consentimentos e acessos de forma clara e granular

Do ponto de vista técnico, o modelo facilita a transferência de dados entre as partes ao promover uma infraestrutura interoperável através de *Application Programming Interface (*API) padronizados e ainda da portabilidade entre os operadores e descentralizada, através da criação de contas *MyData*, cuja funcionalidade se assemelha a uma plataforma de gestão de consentimentos (Eskola et al., 2020; Langford et al., n.d.). Este modelo permite que os cidadãos controlem como seus dados são partilhados e utilizados, enquanto as organizações podem aceder aos dados de maneira eficiente, cumprindo a normas regulatória e o respeito pelo consentimento prestado. Além disso, a separação entre fluxo de consentimento e o fluxo de dados reais assegura a flexibilidade na transferência de informações e na interação entre diferentes serviços. O *MyData*, promove a transparência e devolve aos titulares dos dados o controlo sobre os mesmos, demonstrando a governança centrada no utilizador pode ser viabilizada por tecnologias avançadas.

Para ultrapassar as questões legais relativas ao RGPD, o *MyData* utiliza consentimentos explícitos e revogáveis, permitindo que os utilizadores controlem as autorizações concedidas e visualizem registos de uso. Para além do caso de estudo, a metodologia envolveu também a identificação de requisitos técnicos e jurídicos para o desenvolvimento de uma arquitetura computacional, baseada em *blockchain* que suporte a descentralização dos dados e a gestão eficiente dos consentimentos. Foram ainda consideradas as boas práticas das *guidelines*, com os princípios de UX (*user experience*) e UI (*user interface*), para desenvolver interfaces intuitivas, acessíveis e funcionais, garantindo uma boa experiência de utilização.

O *MyData* é um modelo alinhado com os princípios da transparência e limitação da finalidade (Art.. 5.º), portabilidade (Art.. 20.º), consentimento informado e granular (Art.. 7.º), do RGPG, contudo verifica-se que este modelo comporta também limitação jurídicas e tecnológicas.

Algumas das principais limitações prendem-se com a definição clara e precisa da responsabilidade das entidades envolvidas, quando se trata da efetivação dos direitos dos titulares dos dados.

Essa dificuldade verifica-se no exercício do direito ao esquecimento (Art.. 17.º do RGPD), uma vez que os dados podem ser partilhados dentro do mesmo ecossistema, com diversos operadores e plataformas, o que implicaria na prática, que o exercício desse direito obrigue a que todos os

operadores eliminem os dados em simultâneo, o que nem sempre ocorre, devido à inexistência de meios centrais de controlo e verificação.

A esta dificuldade acrescem ainda as questões relativas à responsabilização dos agentes, conforme resulta do Artigo 24.º do RGPD. Em muitas situações, verifica-se que os operadores aparecem como subcontratantes *(processors*), que executam as instruções de um responsável pelo tratamento de dados (*controller*), não tendo qualquer autonomia e controlo decisório, quanto ao tratamento e as suas finalidades, mostrando-se assim, fragilizado o princípio da responsabilidade *(accountability*), dificultando a identificação de quem deve ser responsabilizado, em última análise pela conformidade com o RGPD.

Na área tecnológica, a interoperabilidade em grande escala nunca foi testada, assim como a escalabilidade, que se encontra limitada à Europa, a isso acresce-se o custo de implementação por parte das organizações e o risco de se poder tornar numa solução apenas acessível a quem possa pagar por ela.

Consentua

O *Consentua* é um modelo CMP de origem britânica, criado para gerir consentimentos no meio digital, nas suas funcionalidades diferenciadores, destaca-se pelo consentimento continuo e revogável, com painéis personalizados (*dashboards*), que permitem ao utilizador configurar e alterar as suas preferências em tempo real.

Baseado no modelo *Dynamic Consent*[25]*,* no qual cada consentimento prestado é acompanhado da informação que permite compreender a finalidade, duração e o responsável pelo tratamento dos dados, desta forma permitindo que o titular dos dados tome decisões de forma consciente e informada Como características técnicas apresenta *API RESTful*, que a permite integrar em diferentes sistemas de gestão, assim permitindo a sua adaptação a fins comerciais diversos, como marketing, comércio digital ou outros. Por outro lado, permite ao utilizador dar o seu consentimento, revogar no todo ou em parte os consentimentos prestados. Este modelo garante o registo e auditabilidade dos consentimentos prestados, garantindo a rastreabilidade e ainda a exportação.

Desenhado para cumprir o RGPD, cumpre com a licitude e outros requisitos do consentimento, previstos no Artigo 6.º e 7.º do RGPD, bem como a transparência da informação, a que se refere o Artigo 12-º e por último, com a norma internacional ISO/IEC 29184, relativamente aos métodos para obtenção do consentimento online.

[25] O conceito *Dinamic Consent* tem origem no projecto *EnCoRe*, da Universidade de *Oxford*, pela mão de Kaye et al., (2015), definido como uma interface digital que facilita a gestão e revogação de consentimentos de forma continua e personaliza pelos titulares. Mais tarde Dankar et al., (2020), frisaram a importância deste conceito na resposta a questões éticas e biomédicas e Khalid et al., (2023), foi ainda mais longe e ampliou o conceito com a introdução de tecnologias descentralizadas como *Blockchain*.

Apesar de cumprir com os requisitos de obtenção do consentimento e com os fundamentos, denota-se ainda limitações como sucede com outras CMP nomeadamente, a interoperabilidade em larga escala e a sobrecarga da informação, que depende da configuração dada pela organização ou empresa, da qual pode resultar excesso de pedidos e em consequência, contribuir para a fadiga do utilizador e ainda a ausência de um acesso que permita ao titular verificar a rastreabilidade e a visualização do consentimento prestado(Utz et al., 2019).

***Solid Pods* (solidproject.org)**

O projeto *Solid Pods*, foi criado por *Tim Berners-lee*, e à semelhança do que acontece no *MyData*, a finalidade deste projeto é colocar o controlo dos dados pessoais nos seus titulares. O método utilizado por *Berners-Lee* é o uso de *pods*, que são espaços de armazenamento de dados pessoais, nas quais os titulares decidem a quem darão acesso, permitirão consultar ou modificar os seus dados (Verborgh et al., 2021). O *Solid* é um projeto de código aberto, que é criado para resolver a falta do controlo sobre as nossas informações pessoais na *web*. Trata-se de um serviço gratuito, no qual os *Pods* funcionam como servidores pessoais, acessíveis em qualquer lugar, permite a portabilidade pois pode ser guardado e usado em qualquer operador ou computador. Relativamente ao RGPD, o *Solid* cumpre com o direito de acesso (Art.. 15.º), retificação (Art.. 16.º), portabilidade (Art.. 20.º) e esquecimento (Art.. 17.º). Considerando a finalidade o *Solid,* revela algumas dificuldades na rastreabilidade e interoperabilidade ainda na auditabilidade, relativamente aos consentimentos prestados em tempo real e não menos importante, o cumprimento do princípio da responsabilidade pelo tratamento a que se reporta o Artigo 5.º, n.º 2 do RGPD

IBM Data Consent Manager

A IBM (DMC) é um modelo suportado por um ecossistema da IBM *Cloud*, esta solução nasceu pelas mãos da IBM, aquando da implementação do RGPD e da necessidade de apoiar as empresas na transição, permitindo gerir dados de forma central e escalável e o cumprimento do RGPD. Os pontos fortes esta plataforma é a escalabilidade e robustez, pois foi criada para organizações de grande dimensão e permite a gestão de dados em sistemas complexos, acrescendo aqui a outra vantagem que é a integração com *Cloud* e API, que permite a interoperabilidade com outras empresas e aplicações externas. Um pouco à semelhança das anterior apresenta um painel de preferências (*dashboard*) configurável, aproximando-o assim dos requisitos da transparência a que se reporta o Artigo 5.º, n.º 1, al. a) do RGPD.

Em termos técnicos o projeto distingue-se por utilizar a tokenização e pseudonomização, associado à utilização da *blockchain* e ainda a *OAuth 2.0*, UMA *(User managed Acess*) e *OpenID Connect*. À semelhança dos outros casos de estudo verificamos o cumprimento de diretrizes do RGPD, como da licitude, transparência e limitação da finalidade na recolha do consentimento, esta solução revela também fragilidades, como a extrema dependência da infraestrutural "mãe", por se trata de uma

plataforma para grandes organizações, o custo da aquisição torna-se mais onerosa e limita a escalabilidade e por conseguinte tem o foco no negócio e não no utilizado.

Esta análise comparativa permitiu-nos identificar os pontos fortes e fracos de cama uma das plataformas, assim como as limitações estruturais. Compreendemos que cada modelo procurou inovar e de certa forma implementar tecnologia que visava a transparência (*MyData)* e a descentralização (*Solid Pods*), ou a inclusão de tecnologias emergentes (*IBM*), continuam a padecer de notórias limitações que comprometem a pena funcionalidade.

Assim e em face da análise desenvolvida neste capítulo onde se verifique que, embora o enquadramento jurídico europeu em matéria de tratamento de dados pessoais se encontra consolidado, persistem ainda fragilidade conceptuais e práticas (Bygrave, 2014), que comprometem a aplicação efetiva em ecossistemas digitais contemporâneos. Em parte, pela dificuldade de as normas existentes acompanharem a velocidade e volatilidade das inovações tecnológicas e que se acresce a complexidade dos fluxos dos dados entre vários operadores(Lynskey, 2015).

A jurisprudência analisada, demonstra também um reforço da proteção dos titulares dos dados, como se verificou no acórdão *Planet49* (Processo C-673/17, 2017) *e Meta vs Bundeskartellamt* (Processo C-252/21, 2021)*,* contudo verificamos também a existência de lacunas quanto à harmonização entre interpretações nacionais e a efetivação de direitos como o esquecimento, portabilidade e a limitação do tratamento. De referir ainda, que se mostram em parte insuficientes, os pareceres técnicos da Comissão Europeia e orientações do Comité Europeu para a Proteção de Dados(EDPB, 2020; 2023), para sustentar a interoperabilidade técnica e jurídica efetiva entre sistemas de gestão de consentimento.

Outro desafio advém da fragmentação regulatória, devido à multiplicidade de instrumento legais que coexistem entre si, como os que atrás referimos, o RGPD, a Directiva *ePrivacy*, o *Data Governance Act*, o *Data Act* o regulamento *eIDAS,* da qual resulta uma sobreposição e lacunas na aplicação.

Esta circunstância, foi já evidenciado pela Comissão Europeia (European Commission, 2020; 2023) e acarreta problemas relativos à responsabilização e rastreabilidade dos agentes envolvidos no tratamento de dados. Existente, portanto, falta de uma infraestrutura comum, que garanta a transparência, auditabilidade e o controlo efetivo pelo titular, como defende (Poikola et al., 2020).

Neste contexto e convergindo com a literatura especializada (Cavoukian, n.d.; Giannopoulou, 2021; International Organization for Standardization, 2023), afigura-se necessário adotar modelos de consentimentos, que não os meramente declarativos, mas sim, modelos de arquitetura computacional de governação integrada, capazes de materializar, de forma mensurável, os princípios *privacy by design* e *accountability*.

É concretamente neste ponto, que se posiciona este trabalho, com uma proposta de arquitetura conceptual, que visa promover a implementação dos princípios do RGPD, nomeadamente os da licitude, transparência e responsabilização, em componentes lógicos.

O foco deste estudo não será o desenvolvimento de um artefacto técnico operacional, mas o desenho de um modelo de referência, que permita agregar as melhores práticas jurídicas e computacionais, e obedecendo ainda às orientações dos normativos como ISO/IEC 27560:2023(International Organization for Standardization, 2023) e as directrizes do EDBP(European Data Protection Board, 2025).

4. Proposta de solução - arquitetura computacional

O capítulo anterior permitiu constatar que existem ainda fragilidades e limitações significativas na aplicação prática dos princípios do RGPD e que apesar do consentimento constituir uma das fontes de licitude mais relevantes para o tratamento de dados pessoais, previsto no RGPD (União Europeia, 2016), padece ainda de fragilidades conceptuais e operacionais que põe em causa a sua efetividade (Bygrave, 2014; Lynskey, 2015).

A abordagem história permitiu-nos, compreender o contributo do direito privado e do direito biomédico, na evolução do conceito da autodeterminação e controlo individual dos dados pessoais (Bygrave, 2002; Pinheiro, 2015a) e evidenciou as fragilidades, como a assimetria da informação e a complexidade técnica das plataformas, cuja consequência é a redução do consentimento a um formalismo, desprovido de substância, que acarreta a falta de compreensão e a efetiva liberdade do titular dos dados (Giannopoulou, 2021; Zarsky, 2016).

No que concerne à jurisprudência do TJUE, concretamente nas decisões referentes ao caso do *Planet49*, (Processo C-673/17, 2017)*, Schrems II* ((Processo C-311/18, 2018), *Meta/Bundeskartellamt* (Processo C-252/21, 2021) ou ainda o *IAB Europe* (Processo C-604/22, 2022), dos quais verificamos que, as práticas atuais relativas às tecnologias da publicidade digital (*adtech),* não cumprem os princípios relativos à transparência e à granularidade dos consentimento, ao que se acresce, que o consentimento, em determinados meios pode ser uma condição de acesso ou resultar de padrões manipulativos (*dark patterns*), enfatizando o TJUE, a necessidade da revogação ocorrer com a mesma facilidade com a que foi dado e esta orientação extensível a todos os responsáveis pelo tratamento. Decorre da leitura e interpretação das decisões apresentadas, a existência de lacunas quanto à harmonização entre interpretações nacionais e a efetivação de direitos, como o direito ao esquecimento, que colocam em crise a efetivação dos direitos dos titulares.

Quanto aos normativos reguladores, tanto as orientações não vinculativas (*Soft law)*, como as normas internacionais ISO/IEC, a verdadeira fragilidade é sentida na operacionalidade, pela falta de perfis de implementação e formatos uniformes, que assegurem tanto a interoperabilidade, rastreabilidade, como a verificabilidade entre sistemas semelhantes, principalmente quando se trata de partilha de dados transfronteiriça (Internacional Organization for Standardization (ISO), 2023; 2019; 2020). De referir ainda que as *Guidelines 02/2025 on processing of personal data through blockchain technologie* (European Data Protection Board, 2025) reforçam a necessidade de uma plataforma técnica que agregue os princípios da *privacy by design* e *acoccountability* desde a criação dos sistemas. Na análise desenvolvida sobre os casos de estudo, verificamos que, apesar da evolução permitida pela implemen-

tação do *MyData, Consentua, Solid Pods e IBM Data Consentt Manager*, as fragilidades práticas, continuam evidentes quando falamos de interoperabilidade, portabilidade transfronteiriça, auditabilidade usabilidade (Poikola et al., 2020). A criação de soluções distintas e não uniformes, contribuem para o fenómeno da fadiga do consentimento (Solove, 2013).

Tendo por base as fragilidades analisadas no capitulo anterior e que acima resumimos, apresentamos o quarto capítulo, que versa sobre a solução proposta de arquitetura computacional conceptual de gestão de consentimentos, que é fruto da análise das fragilidade, interpretação e integração dos normativos legais, com ênfase nos problemas de investigação identificados, como a fadiga do consentimento, a opacidade dos atuais mecanismos de recolha do consentimento e ausência da rastreabilidade e da sua verificabilidade o paradoxo da privacidade.

Neste contexto, afigura-se necessária uma proposta de solução para estes desafios, que permita combinar fundamentos jurídicos e em mecanismos tecnológicos de forma coerente. A arquitetura aqui delineada constitui, uma resposta a estas fragilidades e que visa oferecer um modelo de gestão centralizada, que permita a recolha e verificação dos consentimentos, de forma transparente e segura. Ao longo deste capítulo iremos descrever os seus principais componentes técnicos e funcionais, a lógica de funcionamento e os mecanismos de segurança, pseudonimização, encriptação, anonimização e rastreabilidade. Incluímos ainda uma análise sobre a inclusão da inteligência artificial no apoio à gestão automatizada de consentimento e ainda uma análise jurídica da conformidade da arquitetura proposta, com base nos princípios e exigências do RGPD.

Este capítulo está dividido em seis secções que descrevem de forma sistemática, a arquitetura computacional proposta nomeadamente o ponto 4.1, onde apresentam a estrutura geral e principais componentes da arquitetura e a lógica modular entre componentes que permite o funcionamento do modelo proposto e a descrição técnica e funcional entre cada camada, o 4.2 que apresenta o ciclo de vida do consentimento, aqui se incluindo a revogação, com os fluxos da informação e os mecanismos de verificação automatizada, o 4.3 e 4.4 apresenta os modelos técnicos de pseudonimização, hashing , encriptação e articulação com as normas isso/IEC e as boas práticas de segurança e rastreabilidade. O 4.5 acerca-se da integração dos modelos de Inteligência Artificial para uma gestão mais dinâmica dos consentimentos e ainda para a deteção de inconformidades e por último o 4.6 no qual efetuamos uma análise jurídica sobre a arquitetura proposta, analisando a conformidade com o RGPD, e as questões legais do uso das tecnologias emergentes e os limites da automatização tendo por base a proteção de dados pessoais.

4.1. Paradigma Arquitetural e Visão Geral

A arquitetura computacional proposta para a plataforma de gestão centralizada de consentimentos adota um modelo híbrido que combina elementos de arquitetura de microserviços (Richardson, n.d.) com padrões de arquitetura orientada a eventos (Hohpe, n.d.) fundamentado nas exigências normativas do RGPD (União Europeia, 2016) e nas boas práticas técnicas estabelecidas por organismos internacionais de normalização.

4.1.1. Definição e Justificação do Paradigma Arquitetural Adotado

A escolha de uma arquitetura híbrida microserviços-eventos fundamenta-se em três pilares essenciais: a necessidade de modularidade imposta pelo princípio da proteção de dados desde a conceção e por defeito (Art. 25.º do RGPD); a exigência de auditabilidade independente de componentes para cumprimento do princípio da responsabilidade (Art. 5.º, n.º 2 do RGPD); e a escalabilidade horizontal necessária ao processamento de elevados volumes de consentimentos em ambientes empresariais complexos (Newman, 2021).

Conforme resumido na Tabela 1, a seleção deste paradigma resulta de uma análise comparativa rigorosa face a alternativas arquiteturais, considerando critérios técnicos e requisitos de conformidade regulatória. A arquitetura monolítica foi preterida pela rigidez estrutural que dificulta a conformidade granular com diferentes princípios do RGPD, enquanto a arquitetura exclusivamente orientada a eventos apresenta desafios de consistência transacional incompatíveis com os requisitos de prova documental exigidos pelo Art. 7.º, n.º 1 do RGPD (Bass, 2021).

Tabela 1 - Análise Comparativa de Paradigmas Arquiteturais para Gestão de Consentimentos[26]

Paradigma	**Modularidade**	**Auditabilidade**	**Escalabilidade**	**Conformidade RGPD**	**Complexidade**	**Decisão**
Monolítico	Baixa (acoplamento forte)	Difícil (*logs* centralizados)	Vertical (limitada)	Baixa (Art. 25.º)	Baixa	Rejeitado
Microserviços	Alta (serviços independentes)	Elevada (*logs* distribuídos)	Horizontal (ilimitada)	Alta (Art. 5.º n.º 2, 25.º)	Média-Alta	Parcial
Orientada a Eventos	Média (desacoplamento temporal)	Elevada (*event sourcing*)	Horizontal (assíncrona)	Média (desafios de consistência)	Alta	Parcial
Híbrida (Microserviços + Eventos)	Muito Alta	Muito Alta	Horizontal + assíncrona	Muito Alta (todos os artigos)	Alta	**Selecionado**
Serverless	Média (funções isoladas)	Média (*vendor lock-in*)	Automática	Média-Alta	Média	Considerado para component

[26] Análise baseada em Richardson, (n.d.), (Newman, 2021) e requisitos dos Art.s 5.º, n.º 2, 7.º, n.º 1, 25.º e 32.º do RGPD. A conformidade com o RGPD avalia a capacidade de materializar princípios normativos em mecanismos técnicos verificáveis.

						es específicos

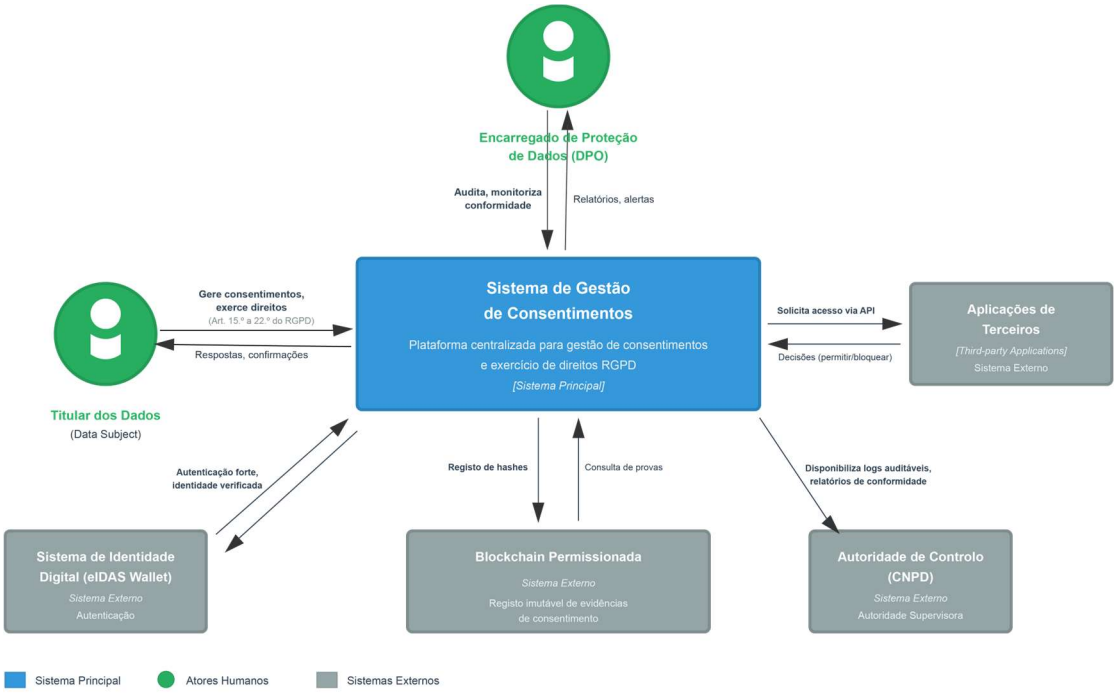
A arquitetura híbrida adotada materializa tecnicamente os seguintes princípios jurídicos:

Princípio da proteção de dados desde a conceção (Art. 25.º, n.º 1 do RGPD): A modularidade permite que cada componente implemente controlos de privacidade específicos sem dependências externas, assegurando pseudonimização, minimização de dados e encriptação como mecanismos nativos (*privacy by design*) e não como adições posteriores (Cavoukian, n.d.; European Data Protection Board, 2020b).

Princípio da responsabilidade (*accountability*) (Art. 5.º, n.º 2 do RGPD): A arquitetura orientada a eventos produz registos de auditoria imutáveis através de *event sourcing*, onde cada ação sobre o consentimento (concessão, revogação, acesso) gera evento rastreável e cronologicamente ordenado, conformando-se às orientações da ISO/IEC 27560:2023 sobre estruturas de registo de consentimento (International Organization for Standardization, 2023).

Requisito de demonstração de conformidade (Art. 7.º, n.º 1 do RGPD): A separação entre componentes de decisão (*Policy Decision Point*) e execução (*Policy Enforcement Point*) permite verificação independente da licitude do tratamento, respondendo à exigência de que "o responsável pelo tratamento tem de poder demonstrar que o titular dos dados deu consentimento" (União Europeia, 2016, Art. 7.º, n.º 1).

A Figura 4.1 apresenta a arquitetura no nível de contexto (modelo C4 - nível 1), evidenciando entidades externas, sistemas adjacentes e o perímetro da plataforma proposta.

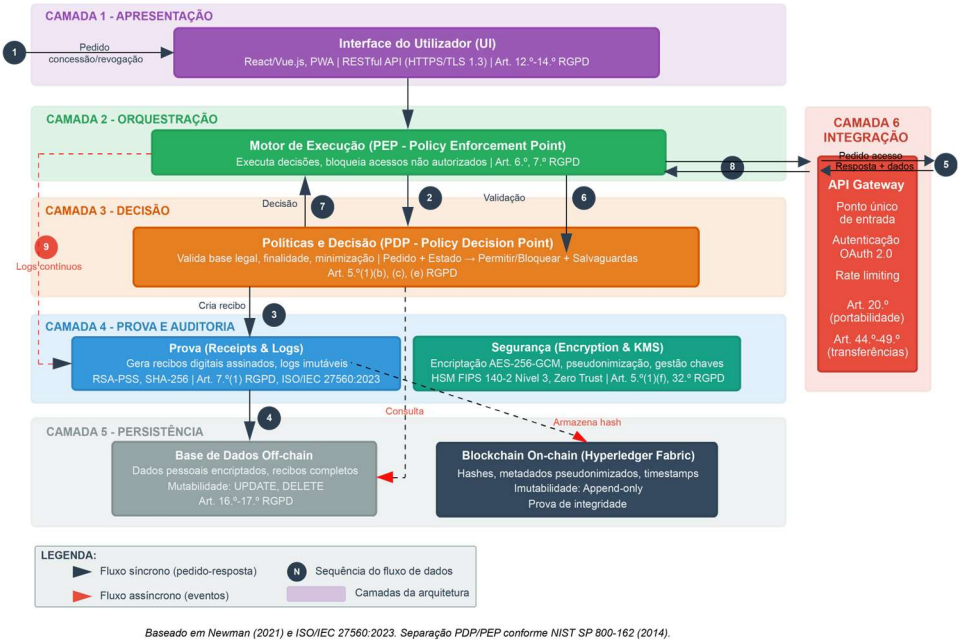


Adaptado de Brown (2018) - Modelo C4. Conformidade com Art. 5.º, n.º 2, 12.º a 14.º, 25.º do RGPD.

Figura 1 - Diagrama de Contexto da Plataforma de Gestão de Consentimentos (Modelo C4 - Nível 1)

4.1.2. Componentes Fundamentais e suas Interconexões

A arquitetura estrutura-se em sete componentes funcionais interdependentes, cada qual responsável por materializar requisitos específicos do RGPD através de mecanismos técnicos verificáveis. A Figura 4.2 detalha as interações entre componentes e os fluxos de dados, evidenciando a segregação de responsabilidades essencial à auditabilidade exigida pelo Art. 5.º, n.º 2 do RGPD.



Baseado em Newman (2021) e ISO/IEC 27560:2023. Separação PDP/PEP conforme NIST SP 800-162 (2014).
PEP = Policy Enforcement Point | PDP = Policy Decision Point | KMS = Key Management System | HSM = Hardware Security Module

Figura 2 - Arquitetura de Componentes e Fluxos de Dados da Plataforma

A figura 2 apresenta o modelo conceptual da arquitetura, organizada em camadas e apresentação a (Hu et al., 2014) separação entre ***Policy Decision Point*** (PDP) e ***Policy Enforcement Point*** (PEP), de forma seguir o modelo de referência de controlo de acesso estabelecido *pela National Institute of Standards and Technology* que recomenda a separação entre a lógica de decisão (PDP - avalia se o acesso deve ser concedido com base em políticas) e a lógica de execução (PEP - efetivamente permite ou bloqueia o acesso).

Esta separação é um ponto critico para a auditabilidade independente, que é exigida pelo RGPD, pois permite verificar separadamente se as regras de decisão refletem corretamente os princípios jurídicos (Art. 5.º do RGPD) e se a execução corresponde fielmente às decisões tomadas (European Union Agency for Cybersecurity., 2020).

A comunicação entre componentes opera através de dois padrões complementares, a **comunicação síncrona** via *RESTful APIs* para operações críticas que exigem resposta imediata (e.g., validação de consentimento antes de conceder acesso a dados), seguindo as especificações *OpenAPI 3.0* (Fielding, 2000)e (ii) **comunicação assíncrona** via eventos para operações de auditoria e registo, utilizando o padrão *publish-subscribe* para desacoplar temporalmente a execução do tratamento do registo probatório (Hohpe, n.d.). Esta dualidade assegura, simultaneamente, baixa latência nas interações do utilizador e completude dos registos de auditoria, sem comprometer o desempenho do sistema.

4.1.3. Decisões Arquiteturais Fundamentadas

As escolhas arquiteturais essenciais foram documentadas através de *Architecture Decision Records* (ADRs), metodologia proposta por Nygard, (2011) e recomendada para sistemas com requisitos de conformidade regulatória (Len Bass, 2021). A Tabela 2 sintetiza as cinco decisões arquiteturais mais críticas, apresentando para cada uma: (i) a alternativa rejeitada; (ii) a fundamentação técnico-jurídica da opção selecionada; e (iii) as consequências previsíveis dessa escolha.

Tabela 2 - Síntese de Decisões Arquiteturais Fundamentadas (Architecture Decision Records)[27]

ID	Decisão Tomada	Alternativa Rejeitada	Fundamentação Técnico-Jurídica	Consequências
ADR-01	Arquitetura híbrida microserviços-eventos	Arquitetura monolítica	Técnica: Necessidade de escalabilidade horizontal e independência de componentes para evolução (Richardson, n.d.) Jurídica: Art. 25.º do RGPD exige proteção desde	Facilita auditoria granular. Permite evolução independente. Aumenta complexidade operacional.

[27] Decisões baseadas em análise de *trade-offs* técnico-jurídicos. Alternativas rejeitadas não são inadequadas *per se*, mas subótimas face aos requisitos específicos de conformidade RGPD.

			conceção, impossível em sistemas monolíticos acoplados.	Exige competências *DevOps* avançadas.
ADR-02	Armazenamento híbrido *on-chain/off-chain*	Armazenamento exclusivo em blockchain	Técnica: *Blockchain* pública/permissionada [28] não permite *UPDATE/DELETE*, violando direitos titulares (Finck & Pallas, 2020). Jurídica: Art. 16.º e 17.º do RGPD impõem retificação e esquecimento, incompatíveis com imutabilidade absoluta.	Concilia imutabilidade (prova) com mutabilidade (direitos). Hashes *on-chain* + *dados off-chain*. Complexidade de sincronização. Risco de inconsistência.
ADR-03	*Hyperledger Fabric (blockchain* permissionada)	*Ethereum* (*blockchain* pública) ou bases de dados relacionais tradicionais	Técnica: *Fabric* oferece canais privados, controlo de identidade e consenso eficiente (Androulaki et al., 2018). Jurídica: Art. 32.º do RGPD exige controlo de acesso, impossível em *blockchains* públicas sem permissão. Bases de dados relacionais isoladas não oferecem imutabilidade requerida para prova (Art. 7.º n.º 1 do RGPD).	Controlo de acesso granular. Eficiência energética (não *PoW*). Conformidade Art. 32.º RGPD. Centralização relativa vs. blockchains públicas. Dependência de consórcio.
ADR-04	Pseudonimização via *HMAC-SHA256* com contexto	Anonimização irreversível ou identificadores diretos	Técnica: HMAC com chave secreta resiste a *rainbow tables*; contexto permite correlação controlada (NIST SP 800-107, 2012). Jurídica: Art. 4.º, n.º 5 do RGPD define pseudonimização como reversível com informação adicional; anonimização total impediria exercício de direitos (Art.s 15.º a 20.º). Identificadores diretos violam Art. 5.º, n.º 1, al. c) (minimização).	Protege identidade sem impedir direitos. Resistente a ataques conhecidos. Risco residual de re-identificação por *linkage*[29]. Gestão de chaves crítica (KMS).
ADR-05	Zero Trust Architecture	Modelo de segurança baseado em perímetro (firewall)	Técnica: Zero Trust assume breach inevitável, exige autenticação contínua e segmentação (Rose et al., 2020). Jurídica: Art. 32.º, n.º 1, al. b) do RGPD exige "capacidade	Defesa em profundidade. Deteção precoce de compromisso. Conformidade Art. 32.º do RGPD. Complexidade de implementação.

[28] O termo "permissionada" é um estrangeirismo técnico (do inglês *permissioned*).

[29] Técnica pela qual se consegue reidentificar indivíduos, aparentemente anónimos, com recurso à correlação de registos, com outro conjunto através de quase-identificadores. (e.g. data de nascimento, sexo, código postal) ou padrões comuns, que tem como consequência a reidentificação e a perda do anonimato.

			de assegurar [...] resiliência dos sistemas", não garantida por perímetro estático. Considerando (75) do RGPD enfatiza "estado da técnica" - *Zero Trust* é atual.	Possível impacto em latência.

A decisão ADR-01 (arquitetura híbrida) é a mais estruturante, pois determina todas as subsequentes. A não adoção do modelo de arquitetura monolítica fundamenta-se em três limitações técnicas incompatíveis com o RGPD: (i) impossibilidade de auditoria granular por princípio (Art. 5.º, n.º 2) exige demonstração de conformidade específica por finalidade); (ii) dificuldade de implementação de *privacy by design* em código acoplado (Art. 25.º); e (iii) risco de violação em cascata, onde compromisso de um módulo expõe todo o sistema, violando Art. 32.º, n.º 1, al. b) sobre resiliência (Newman, 2021).

A decisão ADR-02 (armazenamento híbrido) resolve a tensão mais crítica identificada pela doutrina: a incompatibilidade aparente entre imutabilidade da *blockchain* e direitos de retificação/esquecimento (Finck & Pallas, 2020; Godyn et al., 2022b).

A solução adotada, que compreende armazenar *hashes* criptográficos na *blockchain* (imutáveis, servem de prova) e dados pessoais completos em base de dados encriptada (mutáveis, permitem exercício de direitos), é reconhecida pela (European Parliamentary Research Service, 2019), como tecnicamente viável e juridicamente conforme, desde que os *hashes* não permitam, isoladamente, a identificação do titular.

A escolha da *Hyperledger Fabric*[30] *(*ADR-03) em detrimento de *blockchains* públicas (e.g*., Ethereum*) ou privadas com consenso *Proof-of-Work* justifica-se por três critérios cumulativos: (i) permissionamento, essencial ao controlo de acesso exigido pelo Art. 32.º do RGPD; (ii) eficiência energética, respondendo aos princípios de sustentabilidade do RGPD (Considerando 75 sobre "estado da técnica"); e (iii) modularidade, permitindo integração futura com sistemas de identidade digital europeus (eIDAS 2.0) sem alterações estruturais (Androulaki et al., 2018).

No que concerne a pseudonimização (ADR-04), a decisão tem por base três requisitos aparentemente contraditórios do RGPD: (i) minimização de dados (Art. 5.º, n.º 1, al. c)), que exige não tratar identificadores diretos desnecessariamente; (ii) exercício de direitos (Art. 15.º a 22.º), que exige capacidade de associar dados ao titular; e (iii) segurança (Art. 32.º), que exige resistência a re-identificação não autorizada. A técnica HMAC-SHA256 com contexto resolve esta tensão ao permitir reversibilidade controlada (apenas com chave secreta armazenada separadamente em Hardware Security Module (HSM) sem expor identificadores diretos.

[30] *Hyperledger Fabric* é uma *permissioned Blockchain* modular, direcionada a cenários empresariais, que diferencia validação de ordenação de transações e suporta canais privados para segregação lógica de dados entre participantes (Androulaki et al., 2018)

Por fim, a adoção de *Zero Trust Architecture*[31] (ADR-05) materializa o princípio de que "o responsável pelo tratamento [...] aplica as medidas técnicas e organizativas adequadas, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento" (Art. 32.º, n.º 1 do RGPD). O Considerando 75 do RGPD refere explicitamente, que as medidas devem ter em conta o "estado da técnica", e a arquitetura *Zero Trust* representa, à data, o paradigma mais avançado de segurança cibernética (Rose et al., 2020), tendo sido formalmente recomendada pela ENISA (European Union Agency for Cybersecurity., 2020), para sistemas que processem dados pessoais sensíveis.

A documentação e organização destas decisões através de ADRs cumpre duas funções essenciais: (i) conformidade com *accountability* (Art. 5.º, n.º 2 do RGPD), ao demonstrar que as escolhas técnicas resultaram de análise ponderada de alternativas, não de arbitrariedade; e (ii) facilitação de auditorias futuras, permitindo que autoridades de controlo (e.g., CNPD) compreendam a racionalidade técnico-jurídica da arquitetura sem necessidade de análise reversa do código-fonte (Len Bass, 2021).

4.2. Componentes funcionais da arquitetura

No presente capítulo apresentamos a descrição dos componentes funcionais que materializam a arquitetura conceptual proposta, descrevendo a forma como cada elemento operacionaliza os princípios jurídicos do RGPD, através de mecanismos técnicos verificáveis. Adotamos uma abordagem modular, por permitir a compreensão individual de cada componente, sem descartar a interligação sistemática.

4.2.1. Interface do utilizador

A interface do utilizador constitui o ponto de contacto primário entre o titular dos dados e a arquitetura proposta, desempenhando uma função crítica na concretização dos princípios da transparência e acessibilidade consagrados no RGPD. Este componente não se limita a apresentar informação, configura antes configura um instrumento de exercício efetivo dos direitos a que se reportam os artigos 15.º a 22.º do RGPD.

Tendo em conta o enquadramento normativo, a criação da interface deve observar rigorosamente os requisitos estabelecidos nos artigos 12.º a 14.º do RGPD, que determina que a informação seja apresentada de "forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples" (Art. 12.º, n.º 1). Esta exigência encontra eco nas orientações do European Data Protection Board, 2020), que reafirma a necessidade de interfaces que promovam decisões informadas, sem recorrer a padrões manipulativos. A este requisito acresce ainda o facto de que a

[31] *Zero Trust Architecture* (ZTA) – É um paradigma de segurança centrado na identidade e contexto, que utiliza a máxima "nunca confiar, verificar sempre", que exige a autenticação e autorizações granulares e acessos de menor privilégio a cada pedido (Rose et al., 2020).

interface deve cumprir os critérios de acessibilidade estabelecidos pelas *Web Content Accessibility Guidelines (WCAG) 2.1, (2018.)*, nível AA, assegurando a inclusão de utilizadores com necessidades especiais e concretizando o princípio da não discriminação no acesso à informação (Hardt, 2012)(Grassi, n.d.)(Parlamento Europeu e do Conselho, 2024a). A autenticação do utilizador constitui um elemento essencial desta camada, sendo implementada através de mecanismos que equilibram segurança e usabilidade. A arquitetura proposta suporta múltiplas modalidades de autenticação, incluindo *OAuth 2.0* para integração com fornecedores de identidade externos, autenticação multifator (Multi-Factor Authentication (MFA)) para contextos de risco elevado, e compatibilidade com a futura carteira europeia de identidade digital (eIDAS 2.0), conforme previsto no Regulamento (UE) 2024/1183. Esta panóplia de opções, permite ajustar o nível de segurança ao contexto específico de utilização, em conformidade com o princípio da gestão de risco previsto no artigo 32.º do RGPD.

A Tabela 3 sintetiza as funcionalidades principais da interface e a sua correspondência com os requisitos de conformidade do RGPD[32].

Tabela 3 - Funcionalidades da Interface do Utilizador e Conformidade com o RGP

Funcionalidade	**Descrição Técnica**	**Fundamento Jurídico RGPD**	**Normas Técnicas Aplicáveis**
Painel de consentimentos	Visualização histórica e gestão granular de consentimentos ativos	Art. 7.º, n.º 3 (revogabilidade)	ISO/IEC 27560:2023
Centro de informação	Apresentação estruturada de políticas de privacidade e finalidades	Art. 12.º-14.º (transparência)	WCAG 2.1 nível AA
Gestão de preferências	Configuração granular de finalidades e destinatários	Art. 6.º, n.º 1, al. a) (especificidade)	ISO/IEC 29184:2020
Exercício de direitos	Interface para pedidos de acesso, retificação, portabilidade e esquecimento	Art. 15.º-22.º (direitos dos titulares)	ISO/IEC 27018:2019
Histórico de operações	Registo cronológico de todas as interações e modificações	Art. 5.º, n. º2 (accountability)	ISO/IEC 27037:2012
Notificações proativas	Alertas sobre alterações de políticas, novos pedidos de consentimento ou eventos de segurança	Art. 13.º, n.º 3 e Art. 34.º	ISO/IEC 27035-1:2023

Para a implementação técnica privilegia-se as tecnologias *responsive design*, garantindo adaptabilidade a diferentes dispositivos (computadores, tablets, smartphones) sem comprometer a funcionalidade ou a segurança (Marcotte, 2010; Rescorla, n.d.). A comunicação entre a interface e os restantes componentes da arquitetura é assegurada através de *APIs RESTful* com encriptação *Transport Layer Security* (TLS) 1.3, prevenindo a intercetação ou manipulação de dados em trânsito.

[32] Adaptado de European Data Protection Board, (2020) e International Organization for Standardization, (2023).

É importante sublinhar que a eficácia desta interface, não este apenas depende da sua robustez técnica, mas também do equilíbrio entre a funcionalidade e segurança e a simplicidade de utilização. Como alerta Solove, (2013), interfaces excessivamente complexas podem paradoxalmente minar a autodeterminação informacional que pretendem promover, gerando novas formas de fadiga e consequente a perda de adesão por parte dos utilizadores. A arquitetura proposta procura mitigar este risco através de testes de usabilidade iterativos e da implementação de funcionalidades de apoio contextual, como *tooltips* explicativos e assistentes virtuais baseados em processamento de linguagem natural.

4.2.2. Motor de execução - Policy Enforcement Point

O Motor de Execução, tecnicamente designado como *Policy Enforcement Point* (PEP), representa o núcleo operacional da arquitetura, sendo responsável pela materialização das decisões de consentimento em ações técnicas concretas. Este componente desempenha função de organização crítica, coordenando a interação entre os diversos módulos e assegurando que apenas tratamentos legitimados são executados (Hu et al., 2014).

A função básica do PEP consiste em recolher todos os pedidos de acesso ou tratamento de dados pessoais, submetendo-os a um processo de validação antes da sua execução. Este processo envolve a consulta ao Componente de Políticas (PDP, descrito em 4.2.3), para obter uma decisão de autorização, seguida da aplicação dessa decisão através do bloqueio ou permissão do tratamento solicitado. A arquitetura conceptual do PEP segue o modelo de referência estabelecido pela norma ISO/IEC 10181-3:1996, (1996), adaptado ao contexto específico da proteção de dados.

Do ponto de vista jurídico, o Motor de Execução realiza e adapta diretamente os artigos 6.º e 7.º do RGPD, assegurando que todo o tratamento de dados pessoais se fundamenta numa base legal válida e verificável. A validação em tempo real impede que tratamentos ilegítimos sejam executados, mesmo que por erro ou má configuração, concretizando assim o princípio da licitude consagrado no artigo 5.º, n.º 1, alínea a) do RGPD. Como sublinha Menezes Cordeiro, (2022), que afirma que o consentimento não se esgota no momento da sua prestação, e que devem ser exigidos mecanismos de verificação da sua validade e implementação.

A implementação técnica do PEP, estrutura-se em três módulos funcionais interdependentes. O primeiro é o Módulo de Interceção, cuja função é a captura todos os pedidos de tratamento através de *hooks* no fluxo de dados, registando metadados essenciais (origem do pedido, tipo de operação, dados envolvidos, carimbo temporal). O segundo é o Módulo de Validação, que é responsável pela consulta o PDP para verificar a conformidade do pedido com as políticas vigentes, considerando não apenas a existência de consentimento, mas também a sua granularidade, período de validade e finalidade específica. O terceiro e último módulo, diz respeito ao Módulo de Execução, que aplica a

decisão recebida, permitindo ou bloqueando o tratamento, e regista a operação para efeitos de auditoria. Em caso de bloqueio, gera notificações. tanto para o solicitante como para o titular dos dados.

Este modelo implementa ainda mecanismos de resiliência (como por exemplo o *circuit breakers* e *fallback policies)*, que asseguram a continuidade do funcionamento da arquitetura, mesmo em situações em que exista indisponibilidade temporária de outros componentes. (Nygard, 2018).

Uma preocupação acrescida e legitima, resulta da latência que ocorre pelo processo de validação, que em contextos como o que aqui se apresenta de elevado volume de pedidos. A arquitetura proposta propõe a mitigação deste desafio através de mecanismos de *caching* inteligente, que armazenam temporariamente decisões de autorização para contextos frequentes, reduzindo a necessidade de consultas repetitivas ao PDP. Como forma de garantia do primado da vontade do titular dos dados, a implementação desta solução, possui limitações, que asseguram a invalidação imediata da *cache* sempre que ocorra revogação ou modificação de consentimento.

4.2.3. Componente de Políticas

O Componente de Políticas, ou *Policy Decision Point* (PDP), constitui o elemento decisório da arquitetura, sendo responsável pela transposição dos princípios normativos do RGPD em regras técnicas executáveis. Este componente não se limita a aplicar critérios pré-definidos, antes configurando um sistema interpretativo que avalia cada pedido de tratamento à luz dos requisitos jurídicos aplicáveis (Hu et al., 2014).

A função primária do PDP consiste em receber pedidos de autorização do Motor de Execução (PEP) e devolver decisões fundamentadas sobre a sua admissibilidade. Esta avaliação considera múltiplas dimensões jurídicas, incluindo a existência e validade do consentimento, a adequação da finalidade invocada, a proporcionalidade do tratamento solicitado e a verificação de eventuais restrições temporais ou geográficas. Bygrave, (2014), sustenta que a automatização de decisões de conformidade exige a tradução rigorosa de conceitos jurídicos abstratos em critérios verificáveis computacionalmente.

A implementação técnica do PDP é estruturada em torno de um motor de regras declarativas, que permite a especificação de políticas em linguagem de alto nível (e.g., XACML 3.0 ou equivalente), posteriormente interpretadas em tempo de execução (Godik & Moses, 2003). Esta abordagem possibilita a adaptação e flexibilidade para que se possa atualizar as políticas sem necessidade de recompilação ou reinicialização do sistema, permitindo celeridade na implementação de alterações legislativas ou jurisprudenciais.

4.2.4. Componente de Prova

O Componente de Prova constitui o elemento central para a concretização do princípio da responsabilização (*accountability*), previsto no artigo 5.º, n.º 2 do RGPD, sendo responsável pela geração, gestão e preservação de evidências técnicas que demonstram a conformidade do tratamento de dados. Este componente não se limita a registar eventos, mas também se destina a criar artefactos probatórios juridicamente válidos, que podem ser apresentados a autoridades de controlo ou em contexto judicial (Finck & Pallas, 2020).

A fundamentação técnica do Componente de Prova assenta em dois pilares criptográficos complementares: assinaturas digitais e *hashing* (Jonathan & Yehuda, n.d; Bertoni, 2013). As assinaturas digitais, (e.g., RSA-PSS ou curvas elípticas (ECDSA)), que garantem a autenticidade e não-repúdio dos recibos de consentimento, permitindo verificar inequivocamente a origem e integridade de cada documento. O *hashing* criptográfico, (e.g., como a família SHA-3 (*National Institute of Standards and Technology* (NIST) FIPS 202), gera identificadores únicos e irreversíveis para cada consentimento, possibilitando a verificação de alterações sem expor o conteúdo original.

A Figura 3 ilustra a estrutura de um recibo digital de consentimento conforme especificado pela norma ISO/IEC 27560:2023.

Figura 3 - Estrutura de Recibo Digital de Consentimento

A implementação de um sistema de registo híbrido *on-chain/off-chain,* constitui também uma inovação fundamental da arquitetura proposta, resolvendo a aparente contradição entre a imutabilidade da *blockchain* e os direitos de retificação e esquecimento previstos nos artigos 16.º e 17.º do RGPD. Como demonstram Matthias Berberich, (2016) e posteriormente Finck & Pallas, (2020), o armazenamento direto de dados pessoais em *blockchain* pública é incompatível com o RGPD, exigindo abordagens alternativas que preservem os benefícios da tecnologia sem comprometer os direitos fundamentais.

A Tabela 4 compara as características e finalidades do armazenamento *on-chain* (na *blockchain*) e *off-chain* (em base de dados convencional).

Tabela 4 - Comparação entre Armazenamento On-Chain e Off-ChainTabela[33]

Dimensão	**Armazenamento *On-Chain* (*Blockchain*)**	**Armazenamento *Off-Chain* (Base de Dados)**
Dados armazenados	*Hash* criptográfico (SHA3-256), Identificadores pseudonimizados, Carimbos temporais, Assinaturas digitais	Dados pessoais completos (encriptados com AES-256-GCM), Detalhes do consentimento, Metadados operacionais
Mutabilidade	Imutável após confirmação	Editável e eliminável mediante autorização
Finalidade principal	Prova de existência e integridade, Auditoria temporal, Não-repúdio	Gestão operacional, Exercício de direitos dos titulares, Portabilidade
Conformidade RGPD	Art. 5.º, n.º 2 (accountability), Art. 25.º (privacy by design)	Art. 16.º (retificação), Art. 17.º (esquecimento), Art. 20.º (portabilidade)
Tecnologia	*Hyperledger Fabric* v2.5 (permissionada), Algoritmo de consenso RAFT	*PostgreSQL 15* com encriptação TDE (*Transparent Data Encryption*)
Tempo de retenção	Indefinido (por natureza da tecnologia)	Conforme período especificado no consentimento + requisitos legais
Mecanismo de acesso	APIs de consulta via *chaincode*, restrito a participantes autorizados	*APIs RESTful* com autenticação *OAuth 2.0,* Interface de gestão para titular

O processo de criação de evidência probatória segue um fluxo rigoroso. Quando o titular presta consentimento, o sistema gera um recibo digital estruturado conforme a Figura 4.3, este recibo é encriptado com *Advanced Encryption Standard* (AES)-*256-GCM* e armazenado na base de dados *off-chain*; simultaneamente, é gerado o *hash* SHA3-256 do recibo e este identificador é registado na *blockchain* permissionada, juntamente com uma assinatura digital que atesta a autoria. O *smart contract* na *blockchain* regista o carimbo temporal fornecido por uma Autoridade de Carimbagem Temporal (TSA) conforme RFC 3161 (5), todas as operações subsequentes (modificação, revogação, acesso) geram novos *hashes* encadeados, criando uma cadeia probatória inviolável. (Chang et al., 2012)

Este modelo resolve a tensão entre imutabilidade técnica e flexibilidade jurídica, pois permite ao titular exercer o direito ao esquecimento eliminando os dados pessoais da base de dados *off-chain*, à entidade responsável demonstrar a existência prévia de consentimento válido através do registo *on-chain*, e às autoridades de controlo auditar a conformidade, sem acesso direto aos dados pessoais, e aos tribunais validar a autenticidade de evidências apresentadas em litígio (European Parliamentary Research Service, 2019; Politou et al., 2018).

Um aspeto técnico prende-se com a gestão de chaves criptográficas utilizadas nas assinaturas digitais. A arquitetura implementa uma hierarquia de chaves com rotação periódica (máximo 90 dias), onde

[33] Elaboração própria com base em Finck & Pallas, (2020), Godyn et al., (2022) e na ISO/IEC 27560:2023 - Security and Privacy, (2023).

uma chave raiz protegida em *Hardware Security Module* (HSM) certifica chaves operacionais de duração limitada, de acordo com as recomendações da NIST 800-57 *Recommendations for Key Management Requirements Analysis*, de forma a reduz o impacto de eventual comprometimento de chaves sem invalidar evidências históricas, que permanecem verificáveis através da cadeia de certificados preservada na *blockchain*.

4.2.5. Componente de segurança

O Componente de Segurança constitui a camada transversal que garante a confidencialidade, integridade e disponibilidade de todos os dados tratados pela arquitetura, transformando e operacionalizando as obrigações estabelecidas no artigo 32.º do RGPD, relativamente à implementação de "medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco" (Art. 32.º, n.º 1). Este componente não se limita a aplicar controlos de segurança de forma isolada, antes implementando uma estratégia de defesa em profundidade (*defense in depth*) que protege os dados em todas as fases do seu ciclo de vida (Stallings et al., 2012).

A proteção criptográfica dos dados assenta na utilização exclusiva de algoritmos validados por entidades reconhecidas internacionalmente (NIST, ISO/IEC, IETF) e considerados seguros, que têm por base três critérios cumulativos: primeiro, a ausência de vulnerabilidades conhecidas que comprometam a segurança (mínimo 10 anos), segundo, o suporte de implementações *open-source* auditadas (e.g., *OpenSSL 3.0+, BoringSSL*), e terceiro conformidade com certificação internacional (e.g., *Common Criteria EAL4+, FIPS 140-2 nível 3*).

O sistema de gestão de chaves (*Key Management System* (KMS)) constitui o elemento mais crítico da componente da segurança, pois o comprometimento das chaves criptográficas, invalida toda a proteção conferida pelos algoritmos, independentemente da sua robustez.

NIST 800-57 Recommendations for Key Management Requirements Analysis, (2020)(Barker & Kelsey, 2015)(Richard Kissel, 2017)A gestão operacional do KMS segue as recomendações da , de formar assegurar que as chaves são geradas em ambiente criptograficamente seguro (e.g., *Cryptographically Secure Pseudo-Random Number Generator* (CSPRNG) validado pela NIST SP 800-90A), assegurados e distribuídas através de canais autenticados (como o TLS 1.3 com *mutual authentication*), armazenadas em HSM, com rotação automática, revogação ou destruição segura .

A pseudonimização e anonimização, representam técnicas complementares de proteção de dados que, embora muito frequentemente confundidas, têm características e implicações jurídicas distintas. A pseudonimização, conforme definida no artigo 4.º, n.º 5 do RGPD, configura "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares", mantendo a possibilidade de reidentificação sob condições controladas. A anonimização, pelo contrário, remove de forma irreversível qualquer possibilidade de identificação,

fazendo com que os dados deixem de estar enquadrados no RGPD (European Data Protection Board, 2022).

A implementação destas técnicas na arquitetura segue uma abordagem em camadas, onde cada operação de tratamento é avaliada para determinar o nível mínimo de identificabilidade necessário.

Um desafio particular prende-se com a gestão do risco de reidentificação em contextos de análise combinada de múltiplos *datasets*.

Como demonstram Narayanan & Shmatikov, (2008), mesmo dados aparentemente anonimizados podem permitir reidentificação quando cruzados com fontes externas. A arquitetura mitiga este risco através da análise de risco de reidentificação, (com recurso a ferramentas como ARX *Data Anonymization Tool*) (Prasser, 2015) ou ainda a aplicação de múltiplas técnicas em cascata (e.g., *k*-anonimização, seguida de privacidade diferencial), e ainda a definição de cláusulas contratuais que proíbem tentativas de reidentificação em contratos de partilha de dados, acrescendo ainda a monitorização de publicações de *datasets* que possam facilitar ataques.

A reversibilidade da pseudonimização levanta questões jurídicas particulares, especialmente no contexto do exercício do direito ao esquecimento. A arquitetura resolve esta tensão mantendo as chaves de pseudonimização, separadas dos dados pseudonimizados, com períodos de retenção diferenciados. Quando o titular exerce o direito ao esquecimento, eliminam-se tanto os dados pessoais originais como as chaves de pseudonimização, tornando irreversível a reidentificação dos dados pseudonimizados remanescentes, que passam de forma efetiva para a categoria de dados anónimos.

4.2.6. Armazenamento e blockchain

O Componente de Armazenamento implementa uma arquitetura híbrida que combina uma base de dados relacional convencional (*off-chain*) com uma blockchain permissionada (*on-chain*), associa as vantagens de cada tecnologia enquanto mitiga as suas limitações, constituindo uma solução jurídica para a tensão existente entre a imutabilidade inerente à *blockchain* e os direitos de retificação e esquecimento consagrados no RGPD (Finck & Pallas, 2020; Politou et al., 2018).

A escolha de *Hyperledger Fabric* como plataforma de *blockchain,* fundamenta-se em considerações técnicas e jurídicas. Ao contrário de *blockchains* públicas como *Ethereum* ou *Bitcoin*, *Hyperledger Fabric* é uma *blockchain* privada, onde apenas entidades autorizadas podem participar na rede, ler transações ou submeter novos blocos (Androulaki et al., 2018). Esta característica é importante para cumprimento do artigo 32.º do RGPD, que exige controlo de acessos e confidencialidade dos dados pessoais.

O fluxo de armazenamento da arquitetura associa de forma sistemática uma base de dados relaciona (*PostpreSQL*) e uma *blockchain* permissionada (*Hyperledger Fabric),* que garantem simultaneamente eficiência e operacionalidade e prova imutável. Sempre que o titular presta o consentimento, o recibo

é encriptado (AES-256-GCM) e guardado na base de dados. Logo de seguida, é calculado o *hash* (*Secure Hash Algorithm)* (SHA-3)-256 do recibo, que posteriormente é registado na blockchain com metadados pseudonimizados. Antes de ser registada na *blockchain*, esta transação é validada por vários servidores (*peers)* da rede, que seguem uma "regra de Validação", previamente definida (*endorsement policy*), só após essa validação é que a transação é oficialmente confirmada e garantida através de um mecanismo de consenso (RAFT).

Esta solução responde às questões jurídicas sobre o uso da *blockchain* no RGPD, principalmente no que respeita ao direito ao esquecimento uma vez que, sempre que o titular exerce o artigo 17.º, o recibo é eliminado da base de dados, não permitindo qualquer acesso futuro aos dados pessoais. O *hash* permanece na *blockchain*, mas, sem informação identificável e desta forma não configurando a categoria de dado pessoal.

Um outro aspeto relevante, prende-se com transferências internacionais baseadas em consentimento explícito (artigo 49.º, n.º 1, al. a) do RGPD). Trata-se de uma exceção à regra geral, através da qual são autorizadas, transferências para jurisdições sem adequação ou garantias adequadas, desde que o titular seja informado clara e individualmente desses riscos específicos

Nesta arquitetura prevê-se uma interface própria, para este consentimento excecional, que é tratado como uma categoria especial, onde o titular recebe uma explicação clara, individualizada e compreensível, sobre os riscos da decisão. Este e mecanismos pela sua excecionalidade merece salvaguardas acrescidas, exigindo-se validação periódica (máximo anual) e sendo automaticamente revogado se a situação jurídica no país terceiro se deteriorar (e.g., aprovação de legislação de vigilância massiva), mediante monitorização automatizada de fontes oficiais (decisões da Comissão, relatórios do EDPB, jurisprudência do TJUE).

4.2.7. Integração e interoperabilidade (API Gateway)

O Componente de Integração materializa-se através de um *API Gateway,* que funciona como ponto de acesso único à plataforma para sistemas externos. Este desenho assegura a interoperabilidade técnica, segurança de perímetro e a visibilidade completa sobre cada transação.

O *API Gateway* não se limita a encaminhar pedidos, antes implementando funções avançadas de controlo e gestão, nele se incluindo a autenticação, autorização, conversão de protocolos, limitação chamadas para evitar abusos (*rate limiting*), e monitorização (Richardson, n.d.) ;(OpenAPI Specification v3.1.0, 2021). As funcionalidades principais do *API Gateway* estruturam-se em torno de três pilares fundamentais, primeiro, as APIs RESTful normalizadas, permitem a comunicação padronizada entre sistemas, garantindo a troca de informação segue um formato comum e compreensível, baseado em padrões internacionais, com a implementação de interfaces conformes com os princípios *Representational State Transfer* (REST) (*Representational State Transfer*), utilizando métodos *HTTP*

semânticos (*GET* para consulta, *POST* para criação, *PUT* para atualização, *DELETE* para eliminação), códigos de estado apropriados (2xx para sucesso, 4xx para erros do cliente, 5xx para erros do servidor), e negociação de conteúdo mediante *content-type negotiation* (suporte para *JSON, XML, Protocol Buffers*), bem como as especificações de API seguem o padrão *OpenAPI 3.0 (Swagger*), permitindo geração automática de documentação e *client SDKs* (Budin-Ljøsne et al., 2017; Hardt, 2012). Outo pilar da fundamental da *API Gateway,* é a verificação de identidade e permissões, uma vez que a *Gateway* confirma quem está a executar o pedido (autenticação) e o que essa entidade tem autorização para aceder (autorização). Estas funcionalidade são executáveis com implementação de mecanismos de autenticação modernos e seguros, como o OAuth 2.0, as autorizações realizadas mediante validação específica *JSON Web Tokens* (*JSON Web Token* (JWT), RFC 7519) e integração com fornecedores de identidade externos via *OpenID Connect* (OIDC), permite a integração com serviços externos de identidade, reduzindo a necessidade de gestão local de credenciais

O terceiro pilar, apresenta a segurança e a conformidade com o RGPD. O *Gateway* aplica de forma automática as regras relativas à proteção de dados e cibersegurança em todas as comunicações, através da rejeição de pedidos incorretos ou perigosos, da limitação do número de pedidos por segundo (por forma a prevenir ataques), impedindo que os dados sensíveis apareçam por engano em respostas, adicionando também cabeçalhos de segurança HTTP para evitar vulnerabilidades e ainda registando todas as operações para efeitos de auditoria e *accountability*

Para evitar falhas em cadeia, são aplicadas ainda funcionalidades avançadas de resiliência e observabilidade, como o circuit breakers que interrompem temporariamente pedidos a serviços que problemas, para prevenir propagação de falhas a outros componentes(Nygard, 2018). Além destes, implementam-se também mecanismos de observabilidade, que permitem rastrear cada pedido ao longo de vários serviços (*distributed tracing)*, medir o desempenho em tempo real (latência, erros, tráfego), e gerar alertas automático em caso de anomalias.

Outra vantagem do *Gateway*, advém da sua adaptabilidade permitindo tanto a integração com sistemas modernos, como a integração com sistemas legados (e.g., se um sistema só utiliza protocolos SOAP, o *Gateway* converte os pedidos automaticamente de *RESTful/JSON* para esse formato, e vice-versa), e por suportar integrações assíncronas, através de *webhooks* ou *message queues (RabbitMQ, Kafka*), permitindo notificações em tempo real (e.g., como revogações do consentimento)

A Figura 4 ilustra os fluxos de integração típicos mediante diagramas de sequência, nomeadamente: (1) autenticação inicial de aplicação externa e obtenção de *access token*, (2) submissão de pedido de consentimento pelo titular via aplicação terceira, (3) consulta de histórico de consentimentos por entidade auditora, e (4) notificação proativa de revogação de consentimento a sistemas integrados.

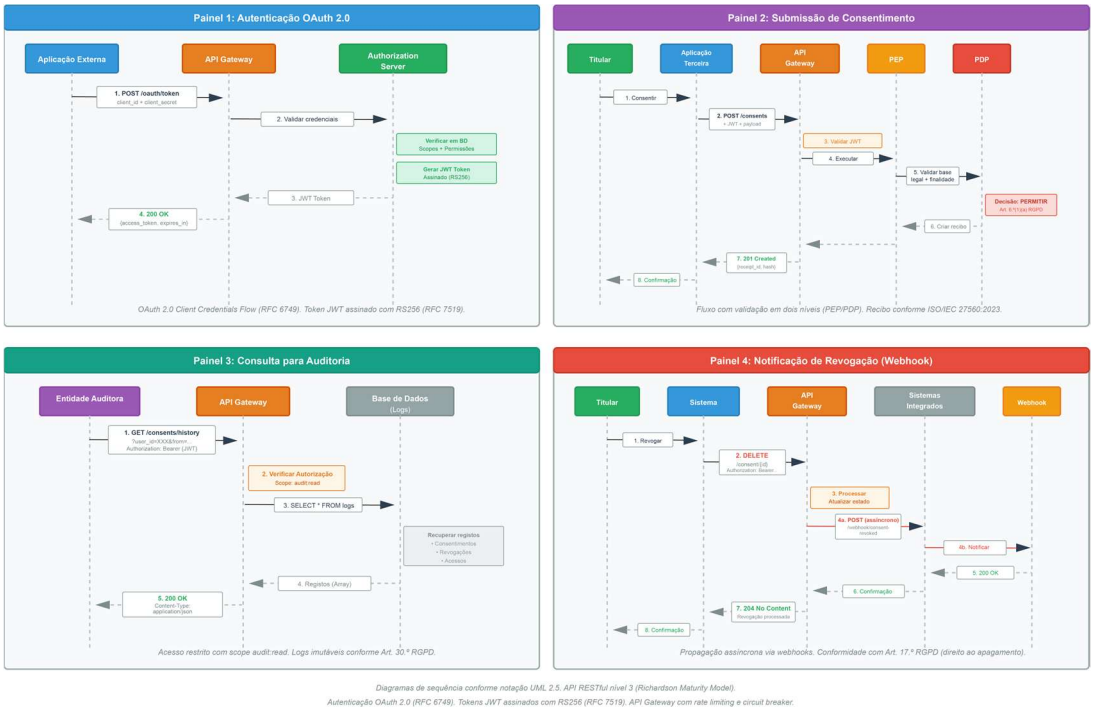


Figura 4 - Fluxos de integração do API Gateway

4.3. Ciclo de vida do consentimento (workflows)

A presente secção descreve os fluxos operacionais *(workflows*) que materializam o ciclo de vida completo do consentimento, desde a sua recolha inicial até à eventual revogação ou exportação. A documentação destes fluxos é essencial para demonstrar a conformidade da arquitetura com os requisitos do RGPD, permitindo tanto a auditoria técnica como a validação jurídica dos procedimentos implementados (ISO/IEC 27560:2023, 2023; Menezes Cordeiro, 2022).

4.3.1. Justificação Metodologica dos Workflows selecionados

A seleção dos *workflows* documentados nesta secção, fundamenta-se em critérios cumulativos de relevância jurídica, operacional e análise critica para a demonstração de conformidade. A norma ISO/IEC 27560:2023, (2023, p. 12) estabelece que "um sistema de gestão de consentimentos deve documentar minimamente os processos de recolha, atualização, consulta e eliminação de registos de consentimento", constituindo estes os fluxos essenciais para qualquer arquitetura neste domínio.

A literatura empírica sobre plataformas de gestão de consentimentos reforça a necessidade de transparência processual. Nouwens et al., (2020) concluiu após análise de 680 websites europeus, que “a opacidade dos mecanismos de recolha e revogação de consentimento constitui uma das principais causas de não conformidade com o RGPD", destacando a importância de fluxos claramente documentados e auditáveis. De igual forma, Utz et al., (2019) demonstraram que "a facilidade de revogação de consentimento influencia significativamente a perceção de controlo por parte dos titulares", justificando a inclusão deste fluxo como essencial.

Os quatro workflows selecionados abrangem quatro etapas críticas do ciclo de vida do consentimento, correspondendo diretamente a obrigações específicas do RGPD:

1. **Concessão de consentimento** – operacionaliza os artigos 6.º, n.º 1, al. a), 7.º e 12.º a 14.º, estabelecendo o momento inicial de legitimação do tratamento.
2. **Revogação e modificação** – Concretiza o artigo 7.º, n.º 3 ("o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento"), requisito de validade fundamental.
3. **Acesso por entidade externa** – materializa o princípio da *accountability* (Art. 5.º, n.º 2) e da limitação de finalidade (Art. 5.º, n.º 1, al. b)), assegurando que apenas tratamentos legitimados são executados.
4. **Portabilidade e exportação** – Implementa o direito à portabilidade consagrado no artigo 20.º do RGPD, permitindo ao titular transferir os seus consentimentos entre plataformas.

Esta seleção exclui intencionalmente *workflows* de manutenção interna (e.g., rotação de chaves criptográficas, sincronização entre réplicas de base de dados), que embora tecnicamente relevantes, não contribuem diretamente para a demonstração de conformidade com o RGPD do ponto de vista do titular dos dados. Como observa Bygrave, (2014), na análise do risco a documentação de conformidade deve centrar-se nas operações que possam ter impacto direto nos direitos fundamentais, remetendo-se os aspetos meramente operacionais para documentação técnica específica".

4.3.2. Workflow 1: concessão de consentimentos

O consentimento representa o ponto de partida da relação de tratamento de dados, constituindo a base legal que legitima operações que se seguem.

A Figura 5 ilustra o fluxo completo deste processo, desde o pedido inicial até à confirmação final.

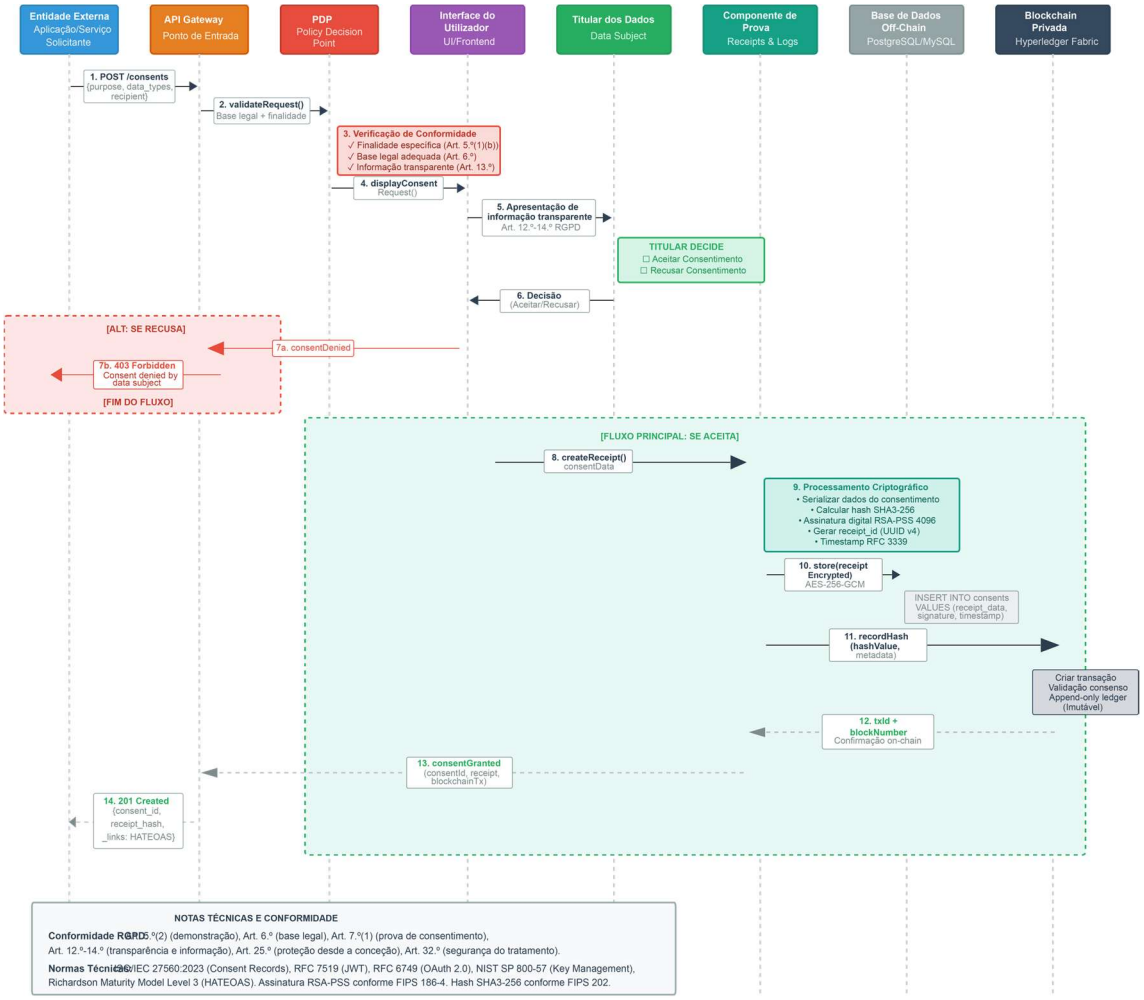


Figura 5 Workflow de Concessão de Consentimento

Fluxo descritivo: Uma entidade externa (e.g., serviço de *marketing* digital) submete um pedido de consentimento ao *API Gateway*, especificando a finalidade ("envio de comunicações comerciais") e categorias de dados necessários ("endereço de correio eletrónico"). O *API Gateway* encaminha o pedido ao PDP, que valida se a finalidade é específica e lícita (artigo 5.º, n.º 1, al. b) do RGPD). Após validação positiva, o pedido é apresentado ao titular através da Interface do Utilizador, em linguagem clara e com informação completa conforme artigos 12.º a 14.º do RGPD.

O titular, após leitura da informação, toma uma decisão autónoma. Em caso de recusa, o fluxo termina sem criação de registo, e a entidade solicitante é notificada da ausência de base legal. Em caso de aceitação, o Componente de Prova gera um recibo digital estruturado conforme ISO/IEC 27560:2023 (2023), incluindo todos os metadados relevantes (finalidade, prazo, destinatários, carimbo temporal). Este recibo é assinado digitalmente mediante RSA-PSS, garantindo autenticidade e não-repúdio (Jonathan & Yehuda, n.d.).

Simultaneamente, são executadas duas operações de armazenamento paralelas: (1) o recibo completo é encriptado com AES-256-GCM e armazenado na base de dados *off-chain*, permitindo futuras

operações de retificação ou esquecimento, e (2) o *hash* SHA3-256 do recibo, juntamente com metadados pseudonimizados, é registado na *blockchain* privada, criando prova imutável de existência (Finck & Pallas, 2020). A *blockchain* devolve o identificador da transação (*txId*) e número de bloco, que são incluídos na resposta final à entidade solicitante, permitindo verificação independente.

Conformidade RGPD: Este *workflow* operacionaliza cumulativamente os artigos 4.º, n.º 11 (definição de consentimento), 6.º, n.º 1, al. a) (licitude baseada em consentimento), 7.º (condições aplicáveis ao consentimento), 12.º (transparência), 13.º (informação a prestar), e 25.º (*privacy by design*). A arquitetura assegura que o consentimento é "livre, específico, informado e inequívoco", mediante validação automatizada no PDP e apresentação estruturada na interface.

4.3.3. Workflow 2: Revogação e Modificação de Consentimento

O direito de revogação constitui um elemento essencial da validade do consentimento, conforme estabelece o artigo 7.º, n.º 3 do RGPD: "deverá ser tão fácil retirar o consentimento como prestá-lo".

A Figura 6 ilustra o processo de revogação e modificação de consentimentos ativos.

Fluxo descritivo: O titular acede ao painel de gestão de consentimentos através de autenticação forte (*OAuth* 2.0 + MFA quando apropriado). A interface apresenta uma lista visual de todos os consentimentos ativos, com informação estruturada sobre finalidade, destinatários autorizados, período de validade e data de concessão. O titular seleciona um consentimento específico e escolhe a ação desejada: revogação completa, modificação de finalidades (se a arquitetura suportar consentimento granular), ou suspensão temporária.

No caso de revogação, o PDP valida que o pedido provém efetivamente do titular (mediante verificação do *JWT* e correlação com o *dataSubjectId* do consentimento). Após validação, o estado do consentimento na base de dados *off-chain* é alterado para "revogado", mas o registo não é eliminado, preservando-se para fins de *accountability* e eventual defesa em litígio (artigo 5.º, n.º 2 do RGPD). Simultaneamente, é gerado um novo recibo de revogação, assinado digitalmente, e o seu *hash* é registado na *blockchain*, criando prova temporal imutável da revogação (Politou et al., 2018).

Aspeto crítico deste *workflow* é a notificação proativa e imediata de todos os sistemas externos que anteriormente receberam autorização de acesso aos dados. O PEP envia notificações mediante *webhooks* a todos os destinatários registados no consentimento original, exigindo confirmação de cessação de tratamento. Sistemas que não confirmem receção dentro de um prazo configurável (e.g., 24 horas) são automaticamente bloqueados pelo PDP em acessos futuros, implementando assim uma política de "*fail-safe*" que privilegia a proteção dos direitos do titular sobre a conveniência operacional das entidades responsáveis.

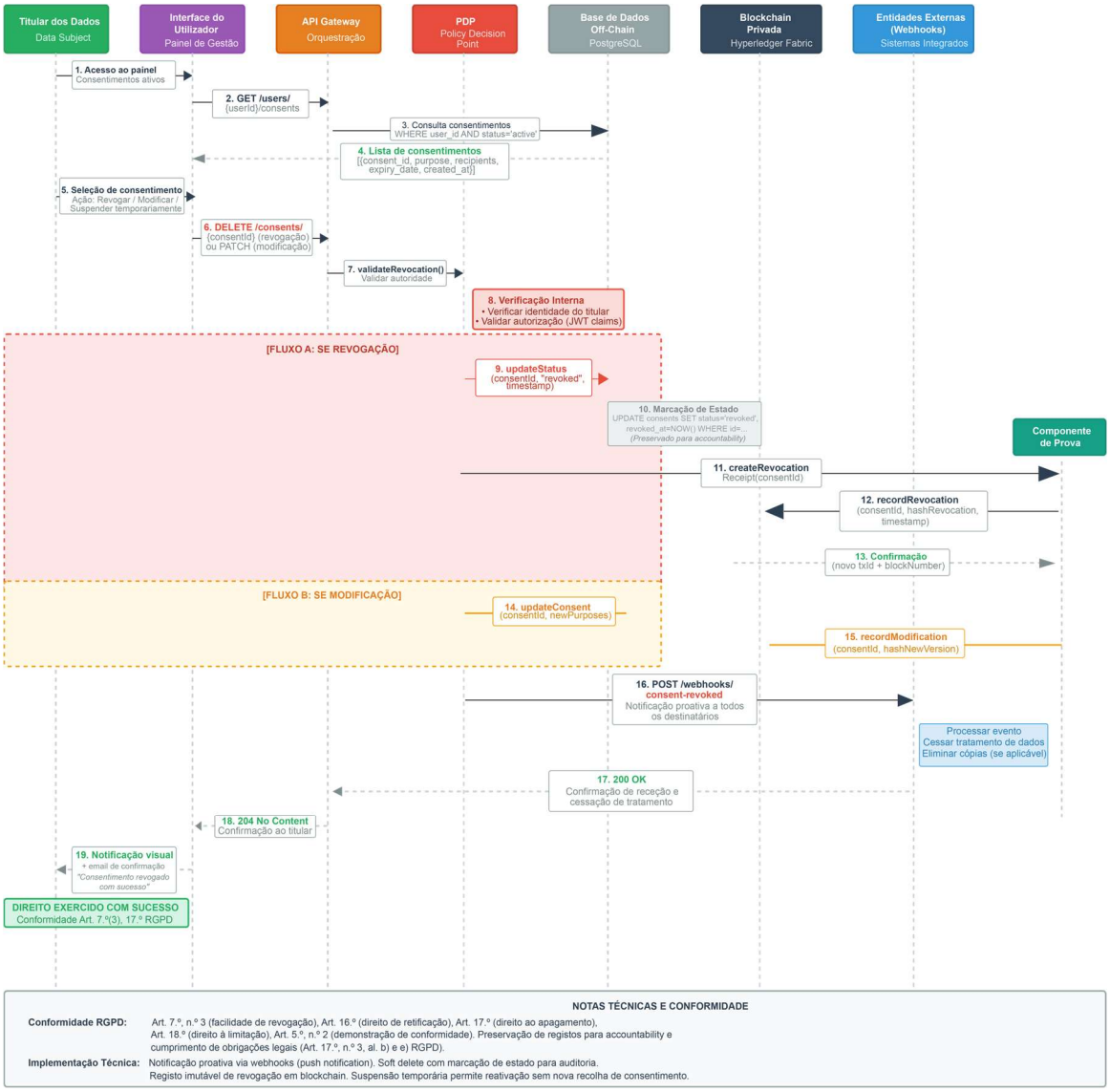


Figura 6 - Workflow de Revogação e Modificação de Consentimento

Conformidade RGPD: Implementação direta do artigo 7.º, n.º 3 (revogabilidade), artigo 17.º (quando aplicável o direito ao esquecimento), e artigo 21.º (direito de oposição). A facilidade de revogação é equivalente à de concessão, cumprindo as orientações do European Data Protection Board, (2020b), que determinam que a retirada do consentimento deve ser tão fácil, quanto a sua concessão.

4.3.4. Workflow 3: Acesso a Dados por Entidade Externa

Este *workflow* materializa o princípio da limitação de finalidade e o mecanismo de *Policy Enforcement Point (PEP)*, assegurando que apenas acessos legitimados por consentimento válido são executados. A Figura 7 ilustra o processo de validação e autorização.

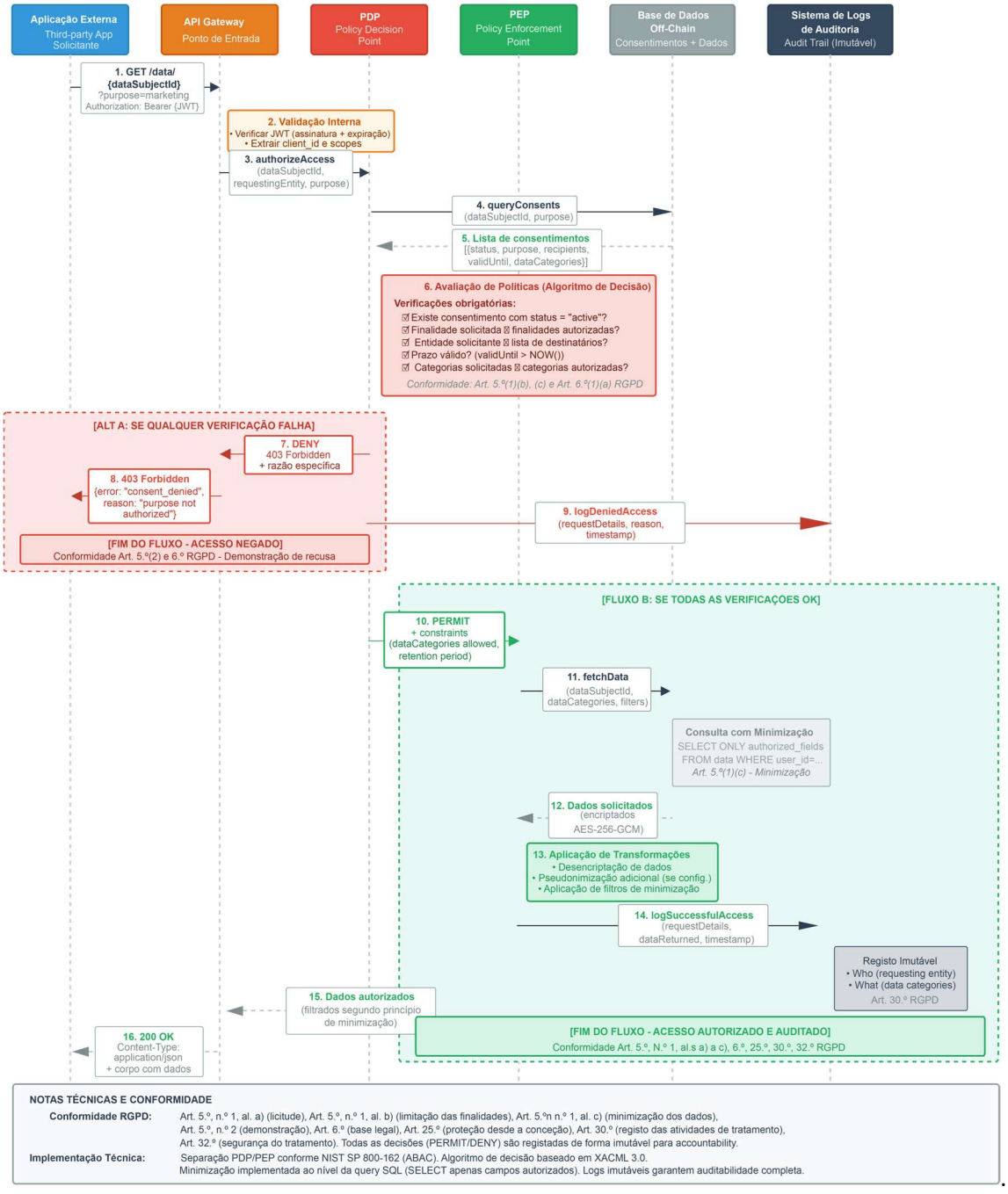


Figura 7 - Workflow de Acesso a Dados por Entidade Externa

Fluxo descritivo: Uma aplicação externa previamente registada na plataforma submete um pedido de acesso a dados de um titular específico, declarando a finalidade do tratamento (e.g.,"envio de campanha de marketing por email"). O *API Gateway* valida o *JWT* fornecido no cabeçalho *Authorization*, extraindo a identidade da entidade solicitante e os âmbitos (scopes) autorizados.

O pedido é encaminhado ao PDP, que executa uma série de verificações cumulativas: (1) consulta a base de dados para identificar consentimentos relacionados com o titular e a finalidade declarada, (2) verifica se existe pelo menos um consentimento no estado "ativo" (não revogado, não expirado), (3)

confirma que a finalidade solicitada corresponde *exatamorkflow* ente ou é subconjunto da finalidade autorizada no consentimento, (4) valida que a entidade solicitante consta na lista de destinatários autorizados, e (5) assegura que as categorias de dados solicitadas não excedem as autorizadas.

Se qualquer verificação falhar, o acesso é negado com código *HTTP 403 (Forbidden*), acompanhado de uma mensagem *JSON* estruturada que identifica a razão específica da recusa (e.g., "*consent revoked* on 2025-01-05", "*purpose 'profiling' not authorized*"). Esta transparência permite às entidades responsáveis diagnosticar problemas de configuração ou identificar necessidade de novo consentimento. Crucialmente, todos os acessos negados são registados no sistema de auditoria, permitindo deteção de tentativas de acesso não autorizado.

Em caso de autorização positiva, o PEP consulta a base de dados aplicando o princípio da minimização de dados: apenas os campos estritamente necessários para a finalidade declarada são recuperados, conforme matriz de necessidade pré-configurada (e.g., para finalidade "envio de email marketing" recupera-se apenas email e nome, excluindo-se morada, telefone ou histórico de navegação). Os dados podem ser sujeitos a pseudonimização adicional antes de entrega, se políticas de segurança o exigirem. Todo o acesso bem-sucedido é igualmente registado em *logs* de auditoria imutáveis, incluindo carimbo temporal, entidade solicitante, dados acedidos e finalidade declarada.

Conformidade RGPD: Implementação dos artigos 5.º, n.º 1, al. b) (limitação da finalidade), 5.º, n.º 1, al. c) (minimização dos dados), 6.º, n.º 1 (licitude do tratamento), e 32.º (segurança do tratamento). A arquitetura assegura que "os dados pessoais [...] são recolhidos para finalidades determinadas, explícitas e legítimas, e não podem ser posteriormente tratados de forma incompatível com essas finalidades".

4.3.5. *Workflow* 4: Portabilidade e Exportação de Consentimentos

O direito à portabilidade, consagrado no artigo 20.º do RGPD, permite ao titular "receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática"(União Europeia, 2016, Art. 20.º, n.º 1). A Figura 8 ilustra o processo de exportação de consentimentos.

Fluxo descritivo: O titular acede à funcionalidade de exportação através da interface, selecionando o formato desejado (*JSON* para interoperabilidade técnica, CSV para análise em folhas de cálculo, *XML* para compatibilidade com sistemas legados) e o âmbito da exportação (totalidade dos consentimentos, apenas ativos, apenas revogados, ou delimitados por período temporal específico).

O Serviço de Exportação, componente especializado, consulta a base de dados *off-chain* recuperando o conjunto completo de informação: consentimentos ativos e histórico de revogações, modificações e acessos. Cada registo exportado inclui todos os metadados estruturados conforme ISO/IEC 27560:2023, (2023) identificadores pseudonimizados, finalidades detalhadas, categorias de dados,

lista de destinatários, carimbos temporais de criação/modificação/revogação, método de recolha, versão da política de privacidade aplicável, e eventuais comprovantes de exercício de direitos.

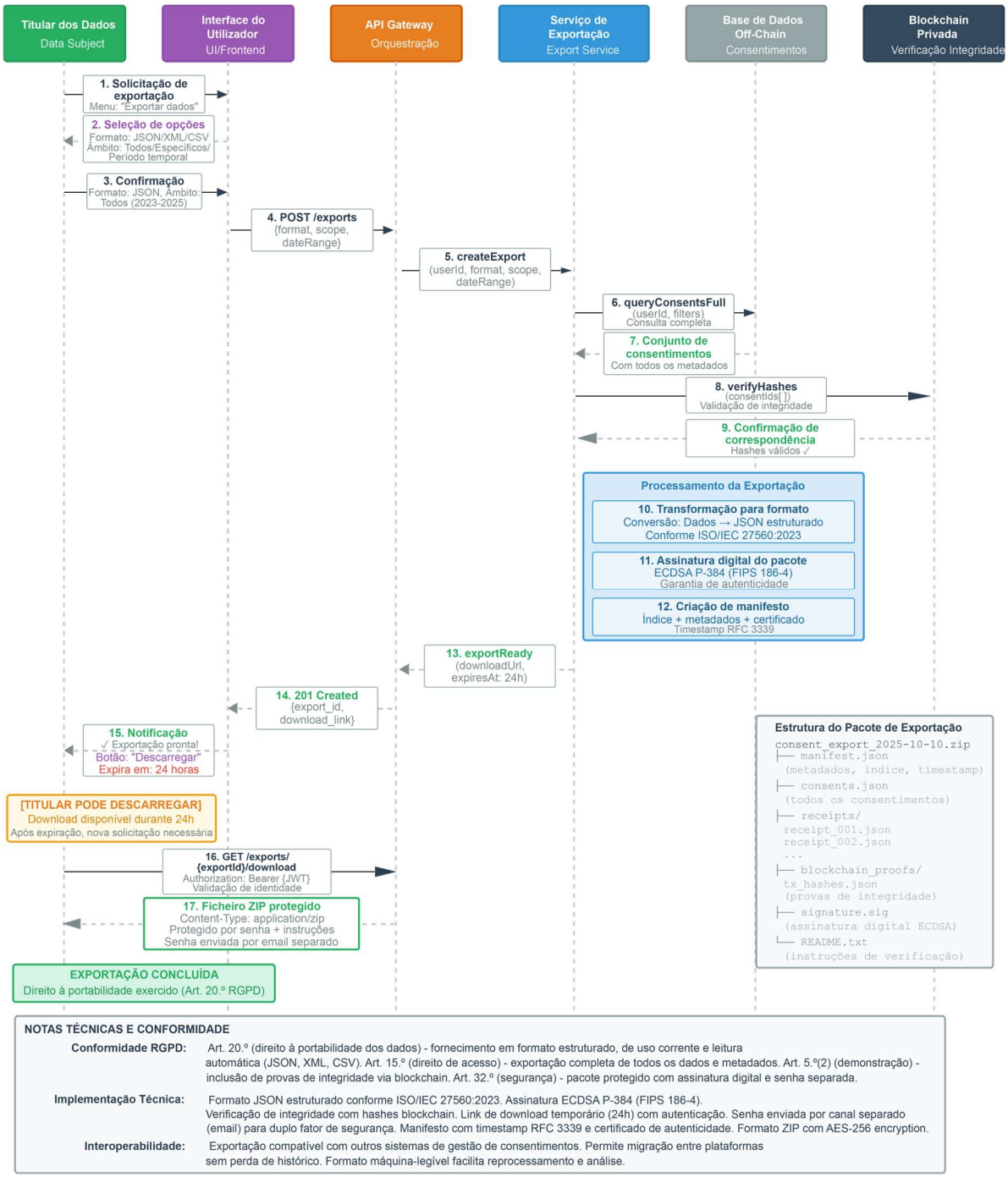


Figura 8 - Workflow de Portabilidade e Exportação

Aspeto crucial é a **verificação de integridade** mediante consulta à *blockchain*: para cada consentimento exportado, o serviço recupera o *hash* registado *on-chain* e valida que corresponde ao conteúdo atual na base de dados *off-chain*, detetando eventuais alterações não autorizadas ou corrupção de dados. Esta verificação confere ao pacote exportado um nível de certificação equivalente

a um documento notarialmente reconhecido, permitindo ao titular utilizar a exportação como prova em eventuais litígios (Finck & Pallas, 2020).

O pacote final é gerado em formato estruturado, assinado digitalmente mediante ECDSA (garantindo autenticidade e não-repúdio), e acompanhado de um manifesto JSON que documenta: (1) data e hora de geração, (2) âmbito da exportação, (3) formato utilizado, (4) assinatura digital, (5) cadeia de certificados para validação, e (6) instruções de verificação. O pacote é disponibilizado como ficheiro *ZIP* protegido por senha (comunicada ao titular por canal alternativo, e.g., SMS), com prazo de expiração configurável (tipicamente 72 horas), após o qual é eliminado dos servidores, reduzindo a superfície de risco.

Conformidade RGPD: Implementação direta do artigo 20.º (direito à portabilidade), artigo 15.º (direito de acesso), e artigo 12.º, n.º 3 (prazos de resposta). A arquitetura assegura que a exportação é fornecida "*num formato estruturado, de uso corrente e de leitura automática*", privilegiando *JSON* como formato *de facto* para interoperabilidade (Bray, 2017).

4.3.6. Tratamento de Exceções e Estratégias de Recuperação

A verdadeira robustez de uma arquitetura de sistemas críticos não se avalia apenas pelo funcionamento em condições normais, mas pela sua capacidade de desempenho em situações excecionais ou de uma falha, mantendo a conformidade legal e a integridade dos dados mesmo perante falhas (Nygard, 2018).

A arquitetura foi projetada para efetuar uma gestão de falhas de forma eficiente e segura, antecipando falhas e reagindo a estas de forma segura e conforme o RGDP. Quando ocorrem problemas, como indisponibilidade temporária de componentes essenciais (e.g., o módulo de decisão de políticas), o sistema entre num modo de segurança (*fail-safe*), no qual irá utilizar as decisões recentes em *cache* ou bloquear os acessos por precaução, notificando os administradores e desta forma garantindo a proteção do titular, existindo mecanismos específicos para lidar com cada tipo de falha operacional. Quando se trata de falhas escrita de consentimentos na *blockchain*, essa informação é colocada em fila de pendentes e reenviada automaticamente durante um período alargado, assegurando a *accountability* diferida, mas documentado, conforme o artigo 5.º, n.º 2 do RGPD. Se a revogação não for entregue à entidade externa, a plataforma efetua o bloqueio imediato do acesso dessa entidade aos dados e efetua várias tentativas de notificação, como garantia de efeito imediato do direito de revogação previsto no artigo 7.º, n.º 3 do RGPD.

Quando se trata de eventos pela sua natureza mais graves, como inconsistência entre dados *on-chain* e *off-chain* ou falhas de desencriptação, a arquitetura ativa alertas críticos, auditorias forenses automáticas e notificações obrigatórias ao Encarregado de Proteção de Dados e ao titular, tal como resulta do artigo 33.º e 34.º do RGPD.

Já em situações mais previsíveis, como é o caso da expiração de certificados digitais, são prevenidas com rotação automática e certificados de contingência, em linha com o artigo 32.º do RGPD (medidas técnicas adequadas). Durante picos de tráfego, o *API Gateway* faz o *auto-scaling*, priorizando as operações críticas (e.g., revogações e exercício de direitos), garantindo a resposta "sem demora injustificada", tal como previsto no artigo 13.º, n.º 3 do RGPD (Rescorla, n.d.; (União Europeia, 2016).
Quando se trata de falha do registo em *blockchain* do recibo de consentimento, a transação é colocada em *dead letter quele* e reenviada de forma assíncrona até 48H, mantendo o titular informado de esta "pendente", garantindo a transparência e evitando qualquer impressão de falsos consentimentos.
Abraçamos nesta arquitetura a implementação destas estratégias de recuperação assenta em princípios de engenharia de resiliência, que garantem a proteção dos direitos dos titulares perante as falhas técnicas e com assim adotando vários princípios fundamentais, como o princípio de precaução (em caso de dúvida, nega-se acesso privilegiando a proteção), monitorização proativa (alertas antes que exceções se tornem falhas graves), degradação graciosa (*graceful degradation* - sistema mantém funcionalidades essenciais mesmo quando alguns componentes falham), e transparência (titular e autoridades são notificados de situações relevantes).
Do ponto de vista jurídico, destaca-se a estratégia para notificação de revogação do consentimento. Mesmo que a comunicação à entidade externa falhe tecnicamente, a revogação produz efeitos imediatos mediante bloqueio no PDP, assegurando que o artigo 7.º, n.º 3 do RGPD é cumprido independentemente de cooperação de terceiros. Esta abordagem inverte o *burden of proof*, exigindo que entidades externas demonstrem receção de notificação para manterem acessos, em vez de presumir continuidade até confirmação explícita (Menezes Cordeiro, 2022).

4.4. Tecnologias Chave: Segurança, Criptografia e Inteligência Artificial

A segurança e a fiabilidade de uma arquitetura de gestão de consentimentos não dependem apenas da sua conformidade jurídica formal, da capacidade técnica de proteção dos dados em todas as fases do seu ciclo de vida

O presente capitulo analisa as tecnologias fundamentais que sustentam a segurança da arquitetura proposta, estruturando-se em quatro subcapítulos; primeiro, relativo a técnicas de pseudonimização e *hashing* que reduzem riscos de exposição de dados pessoais, segundo, especificações criptográficas e modelo de segurança *Zero Trust* que protegem dados em todas as fases do seu ciclo de vida, terceiro, integração conceptual de inteligência artificial como requisito funcional sujeito a salvaguardas específicas do AI Act , e quarto, sistemas de rastreabilidade e auditoria que materializam o princípio da responsabilização (*accountability*).

Esta abordagem reflete o entendimento de vários autores que defendem que a segurança da informação, não deve ser tratada como um complemento opcional ou implementada apenas numa fase mais tardia do seu desenvolvimento, mas sim incorporada desde a conceção do sistema *(security by design)*, alinhada como artigo 25.º do RGPD (Stallings et al., 2012). Este capítulo privilegia análise conceptual das tecnologias, conforme recomendação metodológica de Hart, (2018) para dissertações académicas que conjugam múltiplas disciplinas.

4.4.1. Pseudonimização e Hashing Criptográfico

A pseudonimização, definida no artigo 4.º, n.º 5 do RGPD como "*o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares*", constitui uma técnica essencial de proteção que mantém a utilidade analítica dos dados enquanto reduz drasticamente os riscos associados a acessos não autorizados ou violações de segurança. Ao contrário da anonimização, que torna a reidentificação irreversível (e consequentemente os dados deixam de estar enquadrdados pelo RGPD), a pseudonimização preserva a possibilidade controlada de reverter identificadores mediante informação suplementar armazenada separadamente (European Data Protection Board, 2022).

A arquitetura proposta aplica pseudonimização de forma estratégica em várias camadas, escolhendo a técnica mais ajustada de acordo com o nível de risco, finalidade do tratamento e a necessidade (ou não) de uma futura reidentificação. A escolha exige uma ponderação e avaliação equilibrada entre segurança, desempenho e reversibilidade, conjugadas com os outros fatores como a sensibilidade dos dados (artigo 9.º do RGPD), a finalidade (e.g., estatísticas *vs* auditorias), a necessidade de voltar a identificar titulares, ameaças prováveis e as exigências de desempenho do sistema. Apesar disso, a literatura revela que a pseudonimização por si não é suficiente. Estudos empíricos revelam que dados considerados anónimos, podem ser reidentificados, quando cruzados com outras fontes públicas (*linkage attacks*). Trabalhos como o de Narayanan & Shmatikov, (2008) revelou que 87,8% dos utilizadores da base de dados *Netflix Prize* foram reidentificados cruzando preferências de filmes com avaliações no *IMDb*. De igual forma, (Sweeney, 2013), que revelou 87% da população dos Estados Unidos pode ser identificada univocamente mediante combinação de apenas três atributos quasi-identificadores, como o código postal, data de nascimento e sexo. Em Portugal, dados do Censos 2021 sugerem que combinações equivalentes, permitem identificação única de 60-75% da população em áreas rurais com menor densidade populacional.

Tendo em consideração esses estudos, a arquitetura proposta adota a defesa em profundidade (*defense in depth*), combina várias medidas técnicas e organizativa de forma simultaneamente. Entre essas técnicas, destaca-se a pseudonimização em cascata que corresponde à aplicação e várias

técnicas em sequência, aumentando complexidade de reversão, também a separação física de chaves de reidentificação em HSM seguro, na qual as chaves de pseudonimização são armazenadas em HSM separado fisicamente da base de dados pseudonimizada, com controlos de acesso distintos e auditoria rigorosa. Outra técnica é a minimização de quasi-identificadores, que se traduz na redução de atributos de risco elevado (e.g., data de nascimento truncada para ano+mês, código postal reduzido a 4 dígitos) antes de pseudonimização, e também a análise de risco de reidentificação *ex ante***, que resulta da** utilização de ferramentas especializadas (e.g., *ARX Data Anonymization Tool*), que calcula estatisticamente qual a probabilidade de alguém ser reidentificado, permitindo estimar risco de reidentificação mediante métricas formas, (*Prosecutor Risk, Journalist Risk, Marketer Risk*), se o risco for alto os dados são anonimizados antes de sair. (Prasser, 2015)

Outra das técnicas que se aplicam são as Cláusulas contratuais anti-reidentificação, que se definem como contratos de partilha de dados com investigadores ou parceiros, onde se incluem proibições explícitas de tentativas de reidentificação, prevendo sanções contratuais e notificação à autoridade de controlo em caso de violação Por ultimo, a monitorização de publicações que sucede mesmo após a anonimização, o sistema continua alerta e vigia de forma automatia as bases públicas, como *Web scraping* automatizado de repositórios académicos (*arXiv, ResearchGate)* e bases de dados jornalísticas para detetar eventuais divulgações que possibilitem ataques de ligação.

Seguindo as orientações do European Data Protection Board, (2022), reconhecemos que na arquitetura proposta devemos também adotar a pseudonimização, e que esta não é uma solução isolada, mas que deve ser integrada num conjunto de medidas técnicas e organizativas, que acompanhem a evolução das técnicas de reidentiifcação.

4.4.2. Encriptação e Arquitetura Zero Trust

A encriptação constitui a última linha de defesa quando controlos de acesso falham, assegurando que mesmo em cenário de violação completa de segurança perimetral (comprometimento de servidores, roubo de dispositivos de armazenamento), os dados permanecem protegidos. A arquitetura proposta implementa encriptação ubíqua, dados são encriptados em todas as fases: em repouso (*data at rest*), em trânsito (*data in transit*), e idealmente durante processamento (*data in use*), assim dando cumprimento ao artigo 32.º do RGPD.

Em termos de especificação criptográficas, para dados armazenados, a arquitetura adota a AES-256-GCM (*Advanced Encryption Standard), padrão internacional definido no FIPS PUB 197: Advanced Encryption Standard (AES)., (2001); NIST, (2002)*, desta forma assegurando a confidencialidade e autenticação do texto encriptado (*FIPS PUB 197: Advanced Encryption Standard (AES).*, 2001), em modo GCM, que cifra e autêntica simultaneamente o conteúdo. A opção 256 *bits*, releva quanto à margem de segurança a longo prazo e o modo GCM acrescenta um *tag* de autenticação que denuncia

qualquer tentativa de alteração, desta forma preservando a integridade sem penalizar o desempenho. Esta configuração cumpre, na prática o determinado no artigo 32.º do RGPD, ao assegurar a confidencialidade e integridade de forma continua (União Europeia, 2016).

A arquitetura adota os princípios do modelo de segurança *Zero Trust,* que parte da premissa (*Never Trust, Always Verify*) de que nada é confiável por defeito. Foi desenvolvido inicialmente por Kindervag, (2010) e subsequentemente formalizado pela NIST SP 800-207 (Rose et al., 2020). Ao contrário de modelos tradicionais, onde entidades dentro da mesma rede são presumidamente confiáveis, o *Zero Trust* assume que nenhum utilizador, dispositivo ou sistema é por defeito confiável, exigindo validação contínua independentemente de localização na rede.

Este modelo obedece aos princípios do princípio de privilégio mínimo, no qual cada entidade (utilizador, serviço, processo) recebe apenas as permissões estritamente necessárias para as suas funções (Role-Based Access Control (RBAC)/ABAC e *just-in-time*,) revogadas imediatamente após conclusão da tarefa, o principio da microsegmentação, pelo qual a rede é dividida em múltiplas zonas isoladas, com *firewalls* interna entre componentes, outro principio é a autenticação multifator (MFA) universal, onde todos os acessos administrativos exigem MFA de dois ou mais fatores independentes para confirmar a identidade do utilizador (e.g., conhecimento + posse, e.g., senha + *token* TOTP). Outro princípio é a inspeção e *logging* contínuos de todo o tráfego de rede, para detetar anomalias, reconstituir incidentes e demonstrar conformidade. E por último a validação de integridade de software que significa que nenhum código é executado sem confirmação prévia de que é autêntico e não foi alterado. Para que isso seja possível, cada binário/contêiner é assinado digitalmente na fase *build* (com chave privada) e, antes de correr, a plataforma verifica a sua assinatura e a cadeia de confiança (certificado X.509). Se esta verificação falhar (assinatura inválida, certificado revogado/expirado ou *hash* diferente), a execução é bloqueada (*fail-closed*) e fica registo de auditoria do evento. Este controlo reduz o risco *de supply-chain attack*, concretizando o artigo 32.º do RGPD.

4.4.3. Inteligência Artificial: Posicionamento Conceptual e Requisitos

A presente arquitetura conceptual concebe a integração de sistemas de inteligência artificial (IA), não como uma implementação técnica concreta, mas sim como requisito funcional sujeito a especificações rigorosas.

Esta diferenciação é metodologicamente relevante uma vez que, este trabalho estabelece quais as funcionalidades necessárias e sob que condições normativas devem ser atingidas, remetendo *a* implementação (seleção de algoritmos específicos, treino de modelos, *hyperparameter tuning*) para trabalhos subsequentes de engenharia de *software*.

Esta abordagem encontra respaldo nas recomendações de Jobin et al., (2019) que defendem que, no contexto de sistemas críticos, antes da escolha ou conceção de modelos algorítmicos, os requisitos da

inteligência artificial, devem ser definidos com base nas funcionalidades necessárias e nas salvaguardas éticas a assegurar.

O recente Regulamento (UE) 2024/1689(Parlamento Europeu e do Conselho, 2024b) (*AI Act*) reforça também esta necessidade, impondo obrigações específicas para sistemas de IA conforme classificação de risco.

Esta arquitetura adota, portanto, a IA explicável (XAI) e supervisão humana efetiva, como requisitos de base, alinhando a tecnologia com a conformidade legal. Em sistemas que influenciam decisões com impacto em direitos, a explicabilidade e a transparência são exigidas pelo RGPD, como resulta do artigo 22.º do RGPD e pelo AI Act, no artigo 13.º, desta forma cada saída do modelo é acompanhada de uma explicação auditável (Goodman & Flaxman, 2016). Para que tal seja possível é necessária uma abordagem complementar ao modelo, a técnica SHAP e LIME.

A técnica SHAP atribui a cada variável de entrada, uma "quota de responsabilidade" pelo resultado, tanto ao conjunto de dados como de cada caso individual (Lundberg & Lee, 2017), a técnica LIME, cria, para cada caso, um modelo simples de proximidade que imita o comportamento do modelo vizinho, permitindo perceber de forma intuitiva porque saiu aquele resultado (M. Ribeiro et al., 2016). Sempre que se verifique risco elevado ou for detetado um *dark pattern*, o sistema gera fichas de explicação (*explanation cards*) com a decisão e o grau de confiança, as variáveis que mais pesaram, um contrafactual (o que se deve mudar para obter outro resultado), comparações com outros casos idênticos já auditados. Com isto, permite-se auditorias, contestação informada e supervisão humana efetiva.

As decisões sensíveis são automaticamente remetidas para revisão humana com poder de veto, assegurando a intervenção antecipada, informada e auditável (IA Act, artigo 14.º). Os revisores recebem a explicação XAI (SHAP/LIME) com grau de confiança variáveis determinates e contrafactuais, que permitem compreender, questionar e reverter o resultado necessário (AI Act, artigo 13.º; Lundberg & Lee, 2017; R. Ribeiro et al., n.d.)

A inclusão do modelo IA explicável (XAI), com supervisão humana significativa, assegura que as decisões automatizadas com o impacto direto nos direitos dos titulares são compreensíveis, transparentes e reversíveis, tal como decorre do artigo 13,º do IA Act e existe efetivo controlo humano, tal como resulta do artigo 14.º do mesmo diploma e reforçado pelo RGPD (artigo 22.º), que promove a proteção dos titulares contra as decisões baseadas exclusivamente em tratamento automatizado, sem as necessárias salvaguardas.

4.4.4. Rastreabilidade e Auditoria

A rastreabilidade constitui requisito essencial para operacionalização do princípio da responsabilização (*accountability*) consagrado no artigo 5.º, n.º 2 do RGPD: "*o responsável pelo tratamento deve poder*

demonstrar a conformidade" (União Europeia, 2016). Esta demonstração exige registos auditáveis que documentem todas as operações relevantes ao longo do ciclo de vida do consentimento, permitindo reconstrução forense de eventos passados e identificação de responsabilidades em caso de violação.
Para esse fim, a arquitetura adota um sistema de *logging* estruturado alinhado com especificações da NIST SP 800-92 (Kent, 2006) que estabelece requisitos para geração, armazenamento, análise e proteção de *logs* de segurança, no qual cada componente regista eventos em formato estruturado (JSON) com carimbo temporal normalizado, identificadores de evento, tipo de operação, atores, categorias de dados, resultado e contexto técnico (Kent, 2006).
Quanto à integridade e prova, são garantidas em duas camadas complementares: armazenamento *(Worm*) e a ancoragem periódica em *blockchain* privada, a primeira os *logs* são gravados em suporte que permite escrever uma vez e não alterar mais, o que impede de apagar/editar entradas e permite retenções conforme os prazos legais e "*legal holds*" e a segunda periodicamente calcula um *hash* agregado de todos os registos recentes, que fica gravado na *blockchain* que mais tarde pode ser consultado pelo auditor e servir de prova, que em determinada data o *log* existia e que não foi alterado (integridade + prova temporal).
De forma paralela, um SIEM (plataforma de correlação e monitorização), analisa continuamente os *logs* para detetar padrões anómalos (picos de acessos negados, volumes atípicos, ações fora do perfil) e emite alertas antecipadamente. No seu conjunto estas medidas contribuem e garantem a conformidade legal e estabelecem uma base robusta para auditorias e certificações. (*ISO_IEC 27701_2019*, 2019; Kent, 2006; União Europeia, 2016).

4.5. Análise Jurídica da Arquitetura

A presente secção procede a uma avaliação crítica da conformidade da arquitetura proposta com o quadro normativo aplicável, demonstrando que esta constitui uma solução não apenas tecnicamente sofisticada, mas juridicamente sólida (Menezes Cordeiro, 2022).

4.5.1. Conformidade com o RGPD

A arquitetura aplica e concretiza os requisitos fundamentais do RGPD através de mecanismos técnicos verificáveis e auditáveis, nomeadamente, os princípios fundamentais (Art. 5.º do RGPD).
Quanto à limitação da finalidade, esta é garantida através do motor de políticas (PDP) que valida a conformidade entre as finalidades invocadas para cada operação e as finalidades previamente autorizadas. Este mecanismo inibe tratamentos desviantes e previne o *function creep* mediante controlos automatizados e decisões de execução que bloqueiam solicitações incompatíveis. (Bygrave, 2014). A minimização dos dados concretiza-se através de matrizes de necessidade pré-configuradas e filtragem automática no PEP, implementando tecnicamente o princípio "*data protection by default*"

(Art. 25.º, n.º 2 do RGPD), limitando a recolha, o acesso e a divulgação ao mínimo indispensável para cada operação.

E ainda, o consentimento válido (Art. 4.º, n.º 11 do RGPD), que se materializa quando o sistema exige *opt-in* ativo obrigatório, com consentimento granular por finalidade, cumprindo as orientações EDPB Guidelines 05/2020 (European Data Protection Board, 2020b), prevendo ainda, que a revogabilidade (Art. 7.º, n.º 3 do RGPD) é assegurada através de revogação com efeito imediato e interface simétrica para concessão e revogação.

Quanto aos direitos dos titulares (Arts. 15.º-20.º do RGPD), o processamento automatizado de pedidos permite respostas em tempo real ou máximo 24 horas, contrastando com o máximo legal de um mês. A portabilidade é garantida mediante exportação em formatos interoperáveis (*JSON* primário, *XML/CSV* alternativos) conforme Art. 20.º, n.º 1 do RGPD e o princípio da responsabilização (Art. 5.º, n.º 2 do RGPD), materializa-se nos registos imutáveis na *blockchain* privada, recibos digitais assinados e rastreabilidade completa do ciclo de vida, que permitem demonstrar proativa de conformidade, conforme Considerando 82 do RGPD (União Europeia, 2016).

4.5.2. Tensões Normativas e Soluções Técnico-Jurídicas

A tensão mais relevante prende-se com a aparente incompatibilidade entre a imutabilidade técnica da *blockchain* e o direito ao esquecimento, uma vez que a impossibilidade técnica de eliminar dados inscritos numa *blockchain* pública constitui violação direta do artigo 17.º, pois o RGPD não admite exceções baseadas em limitações tecnológicas escolhidas voluntariamente pelo responsável (Finck & Pallas, 2020).

A arquitetura resolve esta tensão mediante modelo híbrido *on-chain/off-chain*, onde apenas h*ashes* criptográficos e metadados pseudonimizados são registados na *blockchain*, enquanto os dados pessoais completos residem em base de dados convencional. Quando exercido o direito ao esquecimento os dados pessoais são fisicamente eliminados mediante sobrescrita criptográfica conforme NIST SP 800-88r1 (Kissel, (2017), as chaves de pseudonimização são igualmente eliminadas e o *hash* permanece na *blockchain* mas transita efetivamente para o estatuto de dado anónimo (European Parliamentary Research Service, 2019).

Também a imutabilidade dos *smart contracts* pode conflituar com o princípio da proporcionalidade, que exige avaliação caso a caso e possibilidade de exceções em circunstâncias determinadas (European Parliamentary Research Service, 2019). A solução apresentada prevê incorpora a consulta ao PDP antes de execuções automatizadas, modo de pausa de emergência mediante *multi-signature*, registo detalhado das decisões tomadas e atualizações mediante padrão proxy. Esta abordagem alinha-se com as recomendações do EDPB, (n.d.), que vem reforçando que a automação de decisões não exonera o

responsável pelo tratamento de assegurar intervenção humana significativa quando necessário para salvaguardar direitos fundamentais.

No que diz respeito às transferências internacionais, o acórdão *Schrems II* (Processo C-311/18 -, 2018) estabeleceu que a mera existência de cláusulas contratuais-tipo é insuficiente, exigindo avaliação casuística e implementação de "medidas suplementares" (European Data Protection Board, 2021). A arquitetura implementa um sistema multicamadas: validação automática de decisões de adequação, exigência de CCTs aprovadas, aplicação automática de medidas suplementares conforme recomendações do EDBP (EDPB, n.d.) – incluindo pseudonimização reforçada, encriptação com chaves geridas exclusivamente no EEE e *split processing*, e bloqueio de jurisdições de alto risco.

4.5.3. Conformidade com Legislação Complementar

A arquitetura observa diplomas complementares: Diretiva 2002/58/CE (ePrivacy), mediante consentimento prévio para *cookies*; Regulamento (UE) 2022/2065 (DSA) através de interface concebida para evitar *dark patterns*; Regulamento (UE) 2022/868 (DGA) assegurando neutralidade e interoperabilidade; Regulamento (UE) 2023/2854 (Data Act) suportando exportação em formatos estruturados conforme ISO/IEC 27560:2023; Regulamento (UE) 2024/1183 (eIDAS 2.0) preparada para integração com a Carteira Europeia de Identidade Digital e Regulamento (UE) 2024/1689 (AI Act) limitando IA a funções de apoio explicável com supervisão humana obrigatória.

4.5.4. Limitações Reconhecidas

Uma análise jurídica rigorosa exige reconhecimento explícito de limitações (Solove, 2013). Desde logo a complexidade técnica e custos elevados (€500.000-€1.500.000 desenvolvimento; €100.000-€300.000 operacionais anuais), suscitando preocupações de equidade competitiva (Lynskey, 2015), as quais acrescem a escalabilidade limitada da *blockchain Hyperledger Fabric* (5.000 transações/segundo) (Androulaki et al., 2018), às quais se acrescem as incertezas interpretativas e dependência de evolução jurisprudencial do TJUE, e por último a dependência de componentes de terceiros com potenciais vulnerabilidades. As estratégias de mitigação incluem implementação modular faseada, *batching* e *sharding*, documentação exaustiva de decisões arquiteturais, e diversificação de fornecedores críticos.

O presente capítulo demonstrou que a gestão tecnicamente sofisticada e juridicamente sólida de consentimentos é viável mediante arquitetura modular que operacionaliza os requisitos abstratos do RGPD em mecanismos técnicos precisos e auditáveis. A solução proposta oferece contributos originais que refutam a perceção de que proteção de dados constitui mero formalismo (Bygrave, 2014; Menezes Cordeiro, 2022), resolvendo tensões técnico-jurídicas aparentemente insolúveis – nomeadamente a imutabilidade da *blockchain versus* o direito ao esquecimento – mediante modelo híbrido *on-chain/off-chain* fundamentado em literatura recente (Finck & Pallas, 2020; Godyn et al., 2022b). A

combinação de registos imutáveis, pseudonimização robusta e painel unificado para o titular responde às críticas deSolove, 2013) sobre dificuldade de fiscalização efetiva e de Nouwens et al., (2020) sobre fadiga do consentimento, criando cadeia probatória inviolável que beneficia titulares, responsáveis, autoridades de controlo e tribunais.

Não obstante os contributos identificados, a transição para implementação operacional enfrenta desafios significativos que não devem ser subestimados: custos elevados que constituem barreira para PME, escassez de competências multidisciplinares técnico-jurídicas, exigindo intensificação de formação em *LegalTech e Privacy Engineering* (Gellert & Gutwirth, 2013), complexidade de integração com sistemas legados, necessidade de gestão de mudança organizacional para transição de "*compliance* mínimo", meramente formal e reativo para "*compliance* substantivo", centrado em resultados e incerteza jurídica decorrente de múltiplos aspetos assentarem em interpretações doutrinárias não validadas judicialmente. Estes desafios exigem estratégias de mitigação cuidadosamente planeadas, incluindo implementação faseada, modelo *Consent Management* as a *Service (CMaaS*) para repartição de custos, e consulta prévia à CNPD conforme artigo 36.º RGPD para obtenção de segurança jurídica.

A validação definitiva da arquitetura depende de três vetores de trabalho futuro: desenvolvimento de *Minimum Viable Product (MVP)* para demonstração de viabilidade técnica e estimativa precisa de custos, realização de estudos de usabilidade conforme metodologia estabelecida para validar que interfaces não regeneram fadiga do consentimento (Nouwens et al., 2020) e certificação voluntária pela CNPD para redução de risco regulatório e criação de precedente orientador. Apenas mediante prototipagem, teste iterativo e investigação empírica rigorosa sobre métricas de eficácia – incluindo redução de fadiga do consentimento, aumento de exercício de direitos, melhoria de transparência percebida e redução de custos de conformidade – será possível validar se a arquitetura cumpre o objetivo fundamental a que se propõe: transformar o consentimento de formalismo burocrático em instrumento efetivo de autodeterminação informacional.

5. Implementação técnica e interoperabilidade

O capítulo cinco aborda, de forma clara e fundamentada, as principais linhas técnicas da arquitetura conceptual proposta, procurando descrever de forma rigorosa e compreensível os componentes essenciais da estrutura da arquitetura que permitem o seu funcionamento prático, conciliando as tecnologias emergentes com as exigências jurídicas do Regulamento Geral sobre a Proteção de Dados (RGPD). Como sublinha Hennessy & Patterson, (2019), a implementação de sistemas complexos exige uma abordagem sistemática que combine requisitos funcionais com restrições técnicas e normativas. Desta forma, serão analisadas a implementação do registo imutável em blockchain permissionada, a pseudonimização e encriptação de dados, e os mecanismos de interoperabilidade entre sistemas e entidades, com especial atenção aos direitos dos titulares dos dados. Com esta análise pretende-se apresentar uma visão aprofundada que responda às questões jurídicas e técnicas deste domínio, demonstrando a aplicabilidade prática do modelo proposto.

5.1. Especificações técnicas e registo imutável

A escolha das especificidades técnicas da arquitetura proposta revela-se fundamental, quando se pretende que não se fique apenas pelo plano conceptual, mas orientada para uma futura implementação prática, com respeito pela conformidade e os princípios do RGPD e orientada pelas boas praticas internacionais e normas técnicas internacionais em matérias de segurança e informação. No que diz respeito às linguagens e *frameworks*, privilegiamos soluções agnósticas, que tenham por base modelos de interoperabilidade.

Nesse sentido, para a comunicação entre módulos recorre-se a RESTful APIs e *frameworks* modulares (*Node,js, Spring Boot*), que seguram a coordenação eficiente entre das diferentes funcionalidades da arquitetura.

Quanto às bases de dados, elas serão concebidas em modelo híbrido no qual, existe uma base de dados relacional (SQL) encriptada (*off-chain*) e outra não relacional (*on-chain*) (*blockchain* permissionada [34] *)*. A primeira organiza e armazena os dados jurídicos fundamentais de cada consentimento (identificação do titular, data, finalidade) e a segunda, mais flexível permite articular um maior número de informação e pode ser usada para gerir *logs* de acesso, auditorias ou outras interações em tempo real. Assim, a base de dados relacional encriptada (*off-chain*), garante a confidencialidade e integridade dos dados, sendo o local onde se encontram armazenados os dados

[34] A escolha da *blockchain* permissionada, prende-se com o facto de estarmos perante a gestão de dados pessoais e da necessidade de garantir o controlo de acessos e de gestão compatível com o que é exigido pelo RGPD, diferente do que acontece com a redes públicas, expostas a riscos acrescidos de exposição de dados, anonimato entre outros (Giannopoulou, n.d.; Godyn et al., 2022a).

pessoais e os detalhes do consentimento, enquanto a *blockchain* permissionada, funciona como um registo imutável (Finck & Pallas, 2020; Giannopoulou, n.d.; International Organization for Standardization, 2023) e transparente com recurso a *hashes* criptográficos e metadados pseudonomizados, como identificadores, que garantem a prova da existência do consentimento, reforçando o principio da *accountability,* previsto no artigo 5.º do RGPD, conciliando assim a vantagem da imutabilidade da blockchain e a flexibilidade jurídica necessária, para assegurar o cumprimento da conformidade legal. Contudo, o exercício do direito ao esquecimento e retificação coloca um desafio à aplicação desta tecnologia, da qual nos acercaremos no próximo capítulo.

Os *smart contracts* também são preponderantes , tendo em conta que a sua programação permite automatizar o ciclo de vida do consentimento, como sucede com a limitação por finalidade, concedendo o acesso apenas dentro da finalidade para o qual foi consentimento e não outra que o responsável venha a considerar necessária, também a revogação imediata, quando o titular retira o consentimento e os *smart contracts* procedem ao bloqueio automáticos para prevenir futuros acessos, e ainda a expiração dos consentimentos, que acontece sempre que o prazo definido é atingido. Este mecanismo invalida o consentimento prestado e regista esta alteração na base de dado (*on- chain)* da blockchain. A automatização dos princípios jurídicos do RGPD, permite transformar normas jurídicas em regras técnicas exequíveis e verificáveis (European Parliamentary Research Service, 2019), também aqui reforçando o princípio da *accountability*.

A segurança encontra-se prevista na arquitetura de forma a assegurar que não configura apenas uma barreira técnica contra acessos não autorizados, mas que esta profundamente ligado às exigências do RGPD, normas internacionais e as boas práticas na matéria da segurança, como o *privacy by design* e *security by design*. O artigo 25.º do RGPD, impõe adoção de mecanismo técnicos que visem a proteção desde a conceção, princípio que é reforçado pelas normas Interational Organization for Standardization (ISO), (2011) e International Organization for Standardization (ISO), (2019), que determinam os requisitos específicos para a gestão da informação de privacidade. Neste domínio a solução mais relevante é a encriptação ponta-a-ponta (*end-to-end ecryptation* – E2EE) e de algoritmos de encriptação (como AES-256 ou RSA), que são verdadeiros requisitos de conformidade regulatória e não apenas escolhas técnicas (Godyn et al., 2022a). Importa referir que a segurança não deve ser concebida de forma isolada, mas de forma a incluir as diretrizes complementares como a Interational Organization for Standardization (ISO), (2011); Internacional Organization for Standardization (ISO), (2023), a proteção da privacidade e a interoperabilidade entre sistemas.

Desta forma, a definição técnica de mecanismos como linguagem, *frameworks*, bases de dados e APIs, normas de segurança, prepara a verificação e integração das tecnologias, como o registo imutável da *blockchain* e os *smart contracts*, a desenvolver no ponto seguinte.

5.2. Verificação automatizada e integração externa

A verificação automatizada dos consentimentos e a integração da arquitetura com outros sistemas representa o segundo pilar da implementação técnica, que assegura a conexão da arquitetura com ecossistemas digitais complexos e transfronteiriços.

Essencial por garantir que o tratamento dos dados pessoais é efetuado de acordo com a vontade manifesta do titular, a verificação automatizada é assegurada pelo motor de consentimentos (*consent engine*), cuja função consiste em analisar cada pedido de acesso em tempo real, cruzando-o com o estado atual do consentimento e as regras definidas pelo titular. Como defendem "a verificação automatizada de consentimentos mediante sistemas baseados em políticas permite reduzir significativamente a latência de resposta e aumentar a conformidade com requisitos de granularidade do RGPD".

Sempre que um terceiro solicita consentimento para o tratamento de dados, o motor verifica cumulativamente se existe base legal válida conforme artigo 6.º do RGPD, se a finalidade solicitada é compatível com a finalidade autorizada pelo titular, se o consentimento não foi revogado ou limitado temporalmente, e se as categorias de dados solicitadas não excedem as autorizadas. Cada acesso autorizado gera um artefacto de acesso (*access token*), registado com carimbo temporal (*timestamp*) certificado e prova criptográfica, que permite assegurar a sua rastreabilidade e integridade conforme ISO/IEC 27037:2012 (International Organization for Standardization, 2012).

A inteligência artificial (IA) representa um reforço da segurança e da transparência da arquitetura proposta. No entanto, como alertam Zhao et al., (2024) e a implementação de algoritmos de IA no contexto de gestão de consentimentos exige salvaguardas específicas para assegurar explicabilidade (*explainability*), supervisão humana e ausência de vieses discriminatórios.

A resposta ao direito de portabilidade consagrado no artigo 20.º do RGPD é operacionalizada através de APIs normalizadas que seguem especificações *OpenAPI 3.0* (anteriormente *Swagger*), permitindo que o titular exporte os seus consentimentos e preferências de forma estruturada e interoperável. (Richardson, 2007) defendem que a adoção de padrões abertos de *APIs RESTful* constitui requisito essencial para interoperabilidade técnica em ecossistemas heterogéneos".

A arquitetura suporta exportação em três formatos padronizados, conforme Tabela 5:

Tabela 5 - Formatos de Exportação de Dados Suportados pela Arquitetura[35]

Formato	Finalidade	Conformidade Normativa	Estrutura de Dados
JSON	Interoperabilidade técnica entre sistemas	ISO/IEC 21778:2017, RFC 8259	Estrutura hierárquica com metadados completos

[35] Todos os formatos incluem assinaturas digitais ECDSA para garantir autenticidade e integridade conforme NIST FIPS 186-4.

CSV	Análise em ferramentas de *spreadsheet*	RFC 4180	Tabela plana com cabeçalhos descritivos
XML	Compatibilidade com sistemas legados	W3C XML 1.1, ISO/IEC 27560:2023	Estrutura aninhada com *schema* validável

A exportação preserva integridade mediante verificação criptográfica: para cada consentimento exportado, o sistema recupera o *hash* registado *on-chain* na *blockchain* e valida que corresponde ao conteúdo atual na base de dados *off-chain*, detetando eventuais alterações não autorizadas ou corrupção de dados

5.3. Interoperabilidade, auditoria e conformidade

Outro eixo da implementação da arquitetura, é a interoperabilidade institucional e transfronteiriça e ainda os mecanismos de auditoria e conformidade, que funcionam como ele de ligação entre as exigências técnicas e a solidez do quando legal e normativo.

Esta interoperabilidade é viabilizada através de APIs normalizadas e seguras, implementadas mediante um *API Gateway* que funciona como ponto único de entrada (*single point of entry*) para todos os pedidos dirigidos à plataforma. O *Gateway* comunica com sistemas heterogéneos utilizando formatos padronizados conforme especificações ISO/IEC 27560:2023 (*Consent record information structure*), que define estruturas interoperáveis para registos de consentimento (ISO/IEC 27560:2023, (2023).

Nesta arquitetura, o modelo de *APIs RESTful* foi adotado por garantir interoperabilidade interna e externa mediante protocolos universalmente aceites baseados em *HTTP/HTTPS*. Como explicam Fielding & Taylor, (2002),"a arquitetura REST privilegia simplicidade, escalabilidade e independência de plataforma, características essenciais para sistemas distribuídos heterogéneos". A conformidade com princípios *REST,* incluindo interface uniforme, *statelessness*, *cacheability* e sistema em camadas - assegura que a plataforma pode integrar-se com qualquer sistema externo que suporte *HTTP*, independentemente da sua pilha tecnológica subjacente (Richardson, 2007).

No que toca às ligações externas, importa clarificar que as API permitem a ponte entre navegadores, aplicações e entidades terceiras com a plataforma, de forma segura e desta forma a interação de terceiros com a plataforma, independentemente da tecnologia utilizada, e ainda de forma transparente e compatível com o RGPD.

As auditorias são indispensáveis para assegurar a rastreabilidade e a transparência do tratamento de dados, materializando o princípio da *accountability* consagrado no artigo 5.º, n.º 2 do RGPD, que estabelece que o responsável pelo tratamento deve comprovar que o consentimento foi obtido, mantido e utilizado em conformidade com a lei (União Europeia, 2016).

A arquitetura implementa sistema de auditoria contínua estruturado em quatro componentes interdependentes. O primeiro componente é o de *Logs* Estruturados e Imutáveis, no qual todos os

eventos relevantes (concessão, revogação, cesso, modificação, exportação) são registados em formato *JSON* estruturado. Os *logs* são armazenados em sistema *Write Once, Read Many* (*WORM*) que impede alteração ou eliminação após escrita, conforme NIST SP 800-92 (Kent, 2006). O segundo Componente é a Ancoragem em Blockchain, onde periodicamente (a cada hora ou após acumulação de N eventos), o sistema calcula a impressão digital de todos os *logs* do período e regista este *hash* na *blockchain* privada *Hyperledger Fabric*, criando prova temporal inviolável. Esta técnica permite verificação de integridade de *logs* históricos, prova de existência temporal perante terceiros, e deteção de eliminação seletiva de registos (Androulaki et al., 2018; Nakamoto, 2008). O terceiro componente 3 é o SIEM e análise de anomalias, este sistema *Security Information and Event Management* (SIEM) ingere continuamente *logs* de todos os componentes, correlaciona eventos e gera alertas para padrões anómalos baseados em regras heurísticas e modelos de *machine learning* não supervisionado (Kent, 2006). O quarto componente, Relatórios de Conformidade, corresponde a Painéis (*dashboards*) interativos permitem visualização em tempo real de métricas de conformidade como a taxa de consentimentos ativos *vs*. revogados, distribuição de finalidades de tratamento, volume de exercício de direitos por categoria (acesso, retificação, portabilidade, eliminação), tempo médio de resposta a pedidos de titulares, taxa de deteção de *dark patterns* em interfaces externas. São gerados relatórios periódicos (mensais, trimestrais, anuais), automaticamente em formato PDF assinado digitalmente, incluindo análise estatística e recomendações de melhoria. Quando executadas com recurso a tecnologias como *blockchain*, viabilizadas por registos imutáveis e *logs* auditáveis, as auditorias permitem verificar em qualquer momento quem acedeu a que dados, com que finalidade e se o consentimento prestado permanecia válido no momento do acesso. Estes mecanismos podem ser consultados pelo titular, empresas, organizações e autoridades de controlo, funcionando como prova documental de conformidade. Bygrave, (2014), sublinha que a demonstração proativa de conformidade mediante sistemas de auditoria automatizada constitui requisito contemporâneo de governança de dados, transcendendo a mera reatividade a investigações regulatórias.

A conformidade regulatória representa a síntese dos componentes técnicos analisados. Tal como sublinhado por (Menezes Cordeiro, 2022), a proteção de dados desde a conceção exige que as garantias jurídicas sejam incorporadas na própria estrutura técnica dos sistemas, e não meramente sobrepostas como camada superficial. Quer a interoperabilidade quer a auditoria só adquirem relevância prática se acompanhadas do enquadramento jurídico que lhes é aplicável.

A arquitetura implementa conformidade com múltiplas camadas normativas, como o RGPD (União Europeia, 2016), de onde se destacam os princípios fundamentais (artigo 5.º), requisitos de consentimento (artigos 4.º, n.º 11 e 7.º), direitos dos titulares (artigos 15.º a 22.º), segurança do tratamento (artigo 32.º), e proteção desde a conceção (artigo 25.º).

Também a legislação complementar, como a Diretiva 2002/58/CE (ePrivacy),(União Europeia, 2002) relativa ao Consentimento prévio para *cookies* e comunicações eletrónicas, o Regulamento 2022/2065, (2022) (DSA), quanto à Proibição de *dark patterns* e transparência de recomendações algorítmicas, o Regulamento (UE) 2024/1689 (AI Act)(Parlamento Europeu e do Conselho, 2024b), quanto à classificação de sistemas de IA, requisitos de explicabilidade e supervisão humana e ainda o Regulamento (UE) 2024/1183 (eIDAS 2.0)(Parlamento Europeu e do Conselho, 2024a), quanto à Preparação para integração com Carteira Europeia de Identidade Digital.

Quanto à *Soft Law* e Orientações Regulatórias, a conformidade verificou-se pela incorporação das *Guidelines* do EDPB, nomeadamente *Guidelines* 05/2020 sobre consentimento, *Guidelines* 03/2022 sobre *dark patterns*, e *Recommendations* 01/2020 sobre medidas suplementares para transferências internacionais (European Data Protection Board, 2020b, 2022, 2023).

E por último as normas técnicas internacionais em conformidade com família ISO/IEC 27000 (gestão de segurança da informação), ISO/IEC 29100:2011 (*Privacy Framework*), ISO/IEC 27701:2019 (extensão de privacidade para ISO 27001), e ISO/IEC 27560:2023 (estrutura de registos de consentimento (International Organization for Standardization (2023); (2019); (2011).

Para além deste corpo regulatório, é necessária a adoção de práticas que evitem o comprometimento da validade do consentimento, como os *dark patterns* analisados anteriormente, garantindo que a arquitetura respeita plenamente o princípio da *privacy by design*. Este último princípio, como defendem Cavoukian,(2009) e Bygrave, (2027), exige que a proteção de dados seja considerada desde o início do ciclo de desenvolvimento de sistemas, e não adicionada a posteriori como funcionalidade complementar.

O ponto 5.3 permitiu compreender que os componentes analisados interoperabilidade técnica, auditoria contínua e conformidade regulatória multinível, não podem ser entendidos como realidades isoladas, mas como elementos interdependentes de um ecossistema técnico-jurídico coerente, e Apenas com as três componentes a funcionarem em sinergia é possível assegurar consentimentos tecnicamente exequíveis, juridicamente válidos e suscetíveis de demonstração perante autoridades de controlo a qualquer momento do seu ciclo de vida.

O capítulo cinco demonstrou que a implementação técnica da arquitetura proposta constitui uma ponte essencial entre os requisitos jurídicos abstratos do RGPD e a sua operacionalização em sistemas computacionais verificáveis e auditáveis.

Não obstante as soluções técnicas robustas apresentadas, o capítulo reconhece limitações inerentes à implementação proposta: a complexidade técnica e custos elevados constituem barreira à adoção por PME (Richardson, 2018); a escalabilidade da *blockchain Hyperledger Fabric* permanece limitada a aproximadamente 5.000 transações por segundo (Androulaki et al., 2018), subsistem incertezas interpretativas quanto à classificação jurídica de *hashes* como dados pessoais ou anónimos após

eliminação de chaves de pseudonimização (Finck & Pallas, 2020) e a implementação de módulos de IA, embora sujeita a salvaguardas rigorosas, introduz riscos residuais de vieses algorítmicos que exigem monitorização contínua (Mathur et al., 2019b). Estas limitações, conjugadas com as tensões normativas identificadas e os desafios operacionais de integração com sistemas legados, justificam a análise crítica aprofundada que será desenvolvida no capítulo seis, onde se procederá à avaliação sistemática da viabilidade jurídica, eficácia técnica e sustentabilidade

6. Análise Crítica da arquitetura proposta

Neste capítulo dedicamo-nos a una avaliação crítica da arquitetura conceptual proposta, nos capítulos anteriores e que visa identificar os pontos fortes, fragilidades e riscos que podem comprometer a sua aplicação. Na base da análise está a perspetiva interdisciplinar, que articula os requisitos jurídicos do RGPD, com a jurisprudência europeia e a exigências técnicas de segurança, interoperabilidade e usabilidade. Após a análise serão apresentadas as possíveis soluções para mitigar alguns dos problemas e limitações e ainda apresentadas as perspetivas futuras, que podem demostrar a evolução e a futura viabilidade prática deste modelo.

O capítulo estrutura-se em três secções principais. A secção 6.1, que identifica as potencialidades e s contributos da arquitetura, onde se evidenciam as inovações, a conformidade e a autodeterminação do titular dos dados. A secção 6.2, identifica as limitações, riscos e tensões normativas, com especial atenção para a aplicabilidade prática do princípio da proporcionalidade, minimização e do direito ao esquecimento em ecossistemas digitais imutáveis. A última secção corresponde ao 6.3, onde definimos as estratégias de mitigação e perspetivas futuras, onde se propõe medidas para colmatar as fragilidades e, novos caminhos em matéria regulatória e certificação e validação da arquitetura em contextos reais.

6.1. Potencialidade e contributos da arquitetura

O desenho da arquitetura que aqui propomos como forma de mitigar as limitações que encontramos ao longo deste trabalho, destaca-se pelas vantagens que a diferenciam das demais plataformas existentes e atualmente disponíveis no mercado, dentro das que se direcionam para o titular dos dados.

A primeira vantagem a que nos reportamos é o cumprimento da proteção de dados desde a conceção (*privacy by design*) e por defeito (*privacy by default*), como prevê o artigo 25.º do RGPD, que resulta da sua estrutura modular e de padrões de interoperabilidade, que facilitam a integração com outros sistemas e contextos transfronteiriços (Fielding & Taylor, 2002; ISO/IEC 27560:2023, 2023) e ainda, a minimização, rastreabilidade e a pseudonimização do tratamento dos dados desde o início do tratamento (Bygrave, 2027; Cavoukian, n.d.). Outra vantagem deste modelo adotado é a auditabidade e a transparência, desta forma respondendo a uma parte dos problemas relativos às plataformas existentes, acusadas de opacidade e manipulação (Nouwens et al., 2020) e a possibilidade que lhe é conferida de evolução para modelos de consentimento dinâmicos (Budin-Ljøsne et al., 2017; Kaye et al., 2015), oferecendo granularidade e revogação em tempo real ao mesmo tempo que previne os *dark patterns* (European Data Protection Board, 2022).

Outra vantagem decorre da introdução de um registo imutável de *blockchain* permissionada, combinado com *smart contracts*, cuja implementação neste contexto, acrescenta um valioso contributo para a prova do consentimento, da sua revogação ou modificação, permitindo a auditabilidade e a prova temporal (Androulaki et al., 2018; Godyn et al., 2022b).

Como refere Giannopoulou, (n.d.), a utilização de *blockchain* pode contribuir para reforçar a confiança no ecossistema digital, desde que na sua conceção não contrarie os direitos dos titulares dos dados e que tem reflexo enquanto prova para autoridades de controlo e tribunais.

A inteligência artificial explicável, emerge como uma camada transversal que permite a otimização e conformidade, enquanto mecanismo de suporte na deteção dos *dark patterns* e combate aos pedidos incoerentes ou com riscos acrescidos(European Data Protection Board, 2022; Nouwens et al., 2020) e promovendo as interfaces éticas. Tal como observamos com Solove, (2010), o consentimento não deve ser entendido como um mecanismo suficiente de autodeterminação informacional, ele carece de outros mecanismos de monitorização e controlo, o que resulta da intervenção desta tecnologia com a inclusão da monitorização e alertas inteligentes.

A última vantagem que aqui apresentamos é o empoderamento do titular, que se verifica com o acesso, num único painel, a um conjunto de ferramentas, que vão da consulta do histórico completo dos consentimentos, aos acessos efetuados aos seus dados, passando pelas operações de anonimização ou pseudonimização realizadas. Estas funcionalidades permitem cumprir com o exercício de direitos a que se reportam os artigos 12.º a 22.º do RGPD, permitindo ao titular dos dados, deixar a posição passiva e adotar um papel ativo na gestão da sua identidade informacional, o que representa também um reforço da confiança digital.

6.2. Limitações, risco e tensões normativas

Apesar das vantagens identificadas no ponto anterior, a arquitetura tem também limitações técnicas, riscos operacionais e tensões jurídicas. No que concerne às limitações técnicas, que advêm da complexidade técnica, que a adoção desta solução acarreta, como é o caso da implementação multicamadas, com a integração da tecnologia *blockchain*, IA, *smart contracts* e mecanismos de encriptação avançada, para além dos elevados custos de implementação, acrescem os manutenção, que podem ser aceitáveis para empresas de grande dimensão, mas não para as pequena e médias empresas, configurando um entrave à adesão plena e por conseguinte à escalabilidade em larga escala.

Ainda que se faça uso das técnicas de anonimização, subsiste o risco de reidentificação por *linkage*, quando os dados são correlacionados com bases externas ricas e esparsas (Narayanan & Shmatikov, 2008). Desta forma devemos considerar a anonimização como um processo continuo de gestão de risco, e não como um estado (*ISO_IEC 27555_2021*, 2021). As técnicas de pseudonimização (com *hash)*

os dados continuam a ser dados pessoais e correm o risco de ser revertidas pelo que devem sempre ser acompanhadas de medidas adicionais de segurança (e.g., hashing com segurança reforçada (SHA-256), encripção (AES-FIPS 197) (European Data Protection Board, 2020a).

No que às questões jurídicas dizem respeito, uma das tensões existentes pela contradição entre princípios é a relação entre imutabilidade da *blockchain* e o direito ao esquecimento do artigo 17.º do RGPD. Embora a solução apresentada por Godyn et al., (2022a), relativa ao modelo híbrido *on-chain/off-chain* pareça solucionar o problema, subsistem dúvidas quanto à aceitação desta solução por parte das autoridades de controlo e pelos tribunais, uma vez que apesar da eliminação dos dados do repositório *off-chain*, continuam a existir outros elementos (*hashes*, metadados, endereços), que podem permitir a identificação do titular, contrariando assim o disposto no artigo 17.º do RGPG, quanto ao esquecimento absoluto dos dados.

Outro desafio decorre da rigidez dos *smart contracts*, que embora permitam a automatização das regras jurídicas (como é caso da revogação imediata, expiração, limitação de finalidades), estes são pela sua natureza rígidos e após serem programados não permitem adaptação contextual para outras realidades que possam surgir, colidindo com situações em que é necessária a flexibilidade ou ponderação legal, como é o caso da suspensão provisória de um acesso por decisão judicial, levantando-se aqui a questão se a sua aplicação não poderá ser incompatível com o principio da proporcionalidade, consagrado no RGPD. Como sublinha European Parliamentary Research Service, (2019), a rigidez e a imutabilidade dos *smart contracts*, pode conflituar com os direitos fundamentais previstos no RGPD como acontece com o direito à retificação e ao pagamento, exigindo-se soluções híbridas e mecanismos de gestão que permitam flexibilidade.

No que se refere às transferências internacionais de dados, ainda que tendo considerado nesta abordagem o mecanismo de *geofencing* e restrições automatizadas, esta arquitetura continua sujeita a fragilidades jurídicas que advêm da fragilidade de decisões como *a Schrems II* (C-311/18), que invalidou o *Privacy shield* e demostrou a fragilidade das transferências para jurisdição sem garantias semelhantes às da União Europeia.

Devemos ainda considerar os riscos da inteligência artificial, que apesar de apoiar a conformidade, pode introduzir enviesamentos ou erros na sua classificação. O futuro Regulamento Europeu da Inteligência Artificial (IA Act), utiliza uma escala de classificação e risco, na qual os direitos fundamentais são classificados de alto risco e que necessitam de supervisão humana e explicabilidade, a adoção de uma plataforma, que prima pela ausência desses mecanismos pode representar um risco adicional.

Por último, a experiência de utilização (*user experience*) e a usabilidade do sistema podem, paradoxalmente, criar novas modalidades de fadiga, mesmo quando a arquitetura é tecnicamente robusta e juridicamente conforme. Esta tensão entre sofisticação técnica e simplicidade de uso

manifesta-se através de múltiplos fenómenos. Primeiro, a **fadiga de granularidade excessiva**: se o painel de gestão de consentimentos oferecer centenas de opções configuráveis individualmente (e.g., consentimento separado para cada finalidade específica, cada categoria de dados, cada destinatário terceiro), o utilizador pode sentir-se sobrecarregado pela quantidade de decisões a tomar, resultando em abandono ou aceitação indiscriminada por exaustão, reproduzindo o problema que se pretendia resolver (Machuletz & Böhme, 2020). Segundo, a **fadiga de notificação**: alertas excessivos sobre modificações de políticas, novos pedidos de consentimento, ou acessos aos dados podem dessensibilizar o utilizador, que passa a ignorá-los sistematicamente, como demonstrou o estudo de Utz et al. (2019) sobre *banner blindness* em avisos de privacidade. Terceiro, a **sobrecarga cognitiva por linguagem técnico-jurídica**: mesmo com interfaces graficamente apelativas, se a terminologia utilizada replicar a complexidade do RGPD sem mediação pedagógica (e.g., distinção entre "responsável pelo tratamento", "subcontratante", "interesse legítimo"), utilizadores com baixa literacia jurídico-digital podem sentir-se excluídos ou incapazes de exercer controlo efetivo (Solove, 2013). Quarto, a **fadiga de autenticação**: se cada operação sensível (revogação, exportação, modificação) exigir autenticação multifator sem avaliação contextual de risco, o processo torna-se penoso, desencorajando o exercício de direitos que deveriam ser facilitados pelo sistema (Grassi et al., 2017). Por fim, a **paralisia por excesso de transparência**: paradoxalmente, fornecer informação técnica demasiado detalhada (e.g., algoritmos de encriptação, especificações de *blockchain*, detalhes de pseudonimização) pode confundir em vez de esclarecer, violando o princípio da informação "concisa" e "inteligível" do artigo 12.º, n.º 1 do RGPD (European Data Protection Board, 2020b).

Para mitigar estes riscos, a arquitetura deve incorporar princípios de *design* centrado no utilizador: hierarquização de informação (detalhes técnicos disponíveis mas não impostos), configurações pré-definidas sensatas (*smart defaults*) que respeitem privacidade mas não exijam decisões imediatas, linguagem adaptativa ao perfil do utilizador (modo simplificado vs. modo avançado), e testes de usabilidade iterativos com amostras representativas da população, incluindo grupos vulneráveis (idosos, pessoas com deficiência, utilizadores com baixa literacia digital), conforme metodologia estabelecida por Nielsen (1994) e validada empiricamente por Nouwens et al. (2020) no contexto de consentimentos digitais.

6.3. Estratégias de mitigação e perspetivas futuras

Uma vez levantadas as limitações da arquitetura, devemos proceder à sua análise critica, com vista à identificação de estratégias que poderão permitir mitigar e garantir a eficácia prática e jurídica desta proposta. Os custos surgem como o entrave à implementação e manutenção desta proposta, que pode ser mitigada através da implementação faseada, permitindo que as organizações pequenas, adquiram

apenas o módulo essencial como a título de mero exemplo, uma empresa adquire o aceso ao painel unificado de verificação em tempo real, podendo mais tarde expandir para *blockchain* e *smart contracts*.

Quanto ao risco de reidentificação após a pseudonimização de dados, devem ser complementadas por outras técnicas de proteção como *differential privacy*, chaves efémeras e agregação estatística, como forma de mitigar esta limitação e na contradição dos princípios da imutabilidade da *blockchain* e o direito ao esquecimento, uma das soluções abordada por (Godyn et al., 2022a) para a incompatibilidade entre a imutabilidade da *blockchain* e o direito ao esquecimento previsto no RGPD, que sugere que em vez de os dados pessoais serem armazenados na cadeia, é gerado um identificado criptográfico (*hash*) que é registado de forma imutável na *blockchain*, enquanto os dados pessoais são guardados numa base de dados tradicionais (*off-chain*), desta forma o direito ao esquecimento, quando exercido é efetuado no armazenamento externo, sem comprometer a segurança e integridade da *blockchain*.

A tensão sobre *os smart contracts* e sua rigidez, pode encontrar solução através do uso de clausulas de exceção e mecanismos de "suspensão" ou reversibilidade, que permitam ao responsável pelo tratamento dos dados intervir, sempre que verifique existirem situações de abuso ou erro, dentro dos princípios da proporcionalidade e boa-fé. Esta proposta de mitigação da rigidez dos *smart contracts*, encontra acolhimento em propostas recentes e que indicam a necessidade de auditorias e design *human-centric* em mecanismos automatizados (Giannopoulou, n.d.; Zarsky, 2016).

No campo das transferências internacionais de dados e com vista a solucionar esta questão, a arquitetura devera prever o uso de mecanismos como, clausulas-tipo (Art. 46.º, n.º 2, c) do RGPD) ou as regras vinculativas aplicáveis às empresas (*biding corporate rules*, artigo 47.º RGPD).

E ainda, quanto ao risco de vieses da inteligência artificial, a intervenção pode ser obtida pela via da auditoria independente de algoritmos, da aplicação do princípio da transparência nos processos de decisão e a da adoção de metodologias de *explainable AI* (XAI) que tornem compreensíveis as decisões automatizadas, de acordo com o IA act e as orientações éticas mais recentes da Comissão Europeia.

Por último, para mitigar as limitações ligadas à experiência e usabilidade do utilizador de que são exemplo a fadiga do consentimento e os *dark patterns* (Nouwens et al., 2020) e afetam sistemas, que apesar de tecnicamente robustos, falham por não cumprirem com a clareza e a acessibilidade para com os titulares dos dados, propõe-se uma abordagem reforçada, como a adoção de interfaces intuitivas, painéis de controlo de fácil leitura e mecanismos de consentimento granular conforme as recomendações da European Data protetion Board, (2023).

7. Conclusões

A presente dissertação partiu da identificação do desafio central e contemporâneo relativo à gestão e do consentimento, no tratamento de dados pessoais, marcada pela fadiga dos titulares dos dados, pela opacidade dos mecanismos de recolha e pela falta de interoperabilidade e auditabilidade.

A revisão da literatura demonstrou que, o consentimento continua a ser a principal base legal para o tratamento de dados pessoais à luz do RGPD, a sua aplicabilidade prática no contexto digital, revelou as suas fragilidades (Nouwens et al., 2020; Solove, 2010).

A análise da doutrina e jurisprudência revelou que, o consentimento não deve ser visto como uma solução universal, mas como um ato jurídico, que carece de requisitos formais e materiais que lhe confiram validade como defendem Menezes Cordeiro, Lynskey, Bygrave, entre outros autores. A literatura mais recente (Mathur et al., 2019b; Nouwens et al., 2020), que a autenticidade do consentimento é afetada por práticas manipulativas e *dark patterns*, para os quais se deve diligenciar mecanismos técnicos e regulatórios, que promovam e fortaleçam a autodeterminação informacional do titular dos dados.

Neste contexto, o trabalho desenvolveu uma proposta de arquitetura conceptual para uma plataforma de gestão centralizada de consentimentos, concebida em camadas, conjuga princípios jurídicos e soluções tenológicas. A analise com detalhes dos componentes -- interface do utilizador, motor de consentimentos, camada de conformidade, registo imutável, segurança e interoperabilidade, demonstrou o potencial para responder às várias fragilidades dos modelos atuais, transformando desta forma, o consentimento num processo, verificável, transparente e auditável, desta forma correspondendo ao princípio da proteção de dados desde a conceção e por defeito (Art. 25.º do RGPD) e da prestação de contas (Art. 5, n.º 2 do RGPD).

Contudo, o estudo mostrou também que, a implementação deste modelo acarreta riscos e tensões, que foram identificados e analisados de forma critica que destacamos, desde a imutabilidade da *blockchain* em contradição com o direito ao esquecimento, a complexidade os custos associados à implementação, a possibilidade de reidentificação em contextos *big data*, a incerteza jurídica relativa ao uso da inteligência artificial e as transferências internacionais de dados. Estas fragilidades mostram que, apesar do possível sucesso da sua implementação, o modelo deve manter-se mutável as alterações técnicas e jurídicas e desta forma adaptável.

Como contributo académico, a dissertação oferece uma reflexão critica sobre a validade e os limites do consentimento, que articulada com a jurisprudência europeia (Processo C-252/21, (2021); Processo C-311/18, (2018); Processo C-604/22, (2022); Processo C-673/17, (2017)) e doutrinária. Na perspetiva

técnica, propõe uma solução baseada em tecnologia *blockchain* permissionada, *smart contracts*, pseudonimização e inteligência artificial explicável, alinhada com as normas internacionais e boas práticas de segurança da informação. Ao propor uma abordagem interdisciplinar, que combina direito, tecnologia e ética, como soluções para a proteção de dados pessoais, que não só é possível como essencial para dirimir os desafios futuros apresentados pela economia digital global.

As perspetivas futuras de investigação e aplicação prática, incluem aprofundar a coexistência e compatibilidade entre a *blockchain* e o exercício efetivo dos direitos fundamentais, bem como investigação dos limites das técnicas de pseudonimização e anonimização, para clarificação com rigor quando podemos afirmar, que deixam de ser considerados dados pessoais, após aplicação destas técnicas. No que concerne às transferências internacionais, torna-se imperativo avaliar a eficácia de mecanismos de proteção complementares e desenvolver abordagens que visem garantir estabilidade jurídica na transferência de dados para países terceiros. A jurisprudência *Schrems II* (Processo C-311/18, 2018) expôs as fragilidades dos acordos bilaterais, exigindo que investigações futuras se concentrem no desenvolvimento de quadros multilaterais robustos que incorporem: avaliação periódica e automatizada do nível de proteção nos países de destino, conforme recomendado pelo European Data Protection Board (2021); implementação sistemática de medidas suplementares técnicas, incluindo encriptação *end-to-end* com gestão de chaves no EEE e pseudonimização reforçada (Finck & Pallas, 2020) e criação de mecanismos de certificação transfronteiriços que permitam validação contínua de conformidade, ultrapassando a lógica estática das decisões de adequação da Comissão Europeia (Lynskey, 2015).

Outra integração futura passa por determinar qual o papel que terão as tecnologias emergentes, como a inteligência artificial explicável (XAI), na melhoria da gestão de consentimentos e no tratamento de dados pessoais. A XAI, definida por Goodman & Flaxman (2016) como o conjunto de técnicas que tornam os processos decisórios de sistemas de IA compreensíveis para humanos, assume relevância crescente no contexto da gestão de consentimentos por três razões fundamentais. Primeiro, permite operacionalizar o direito à explicação previsto no artigo 22.º do RGPD, fornecendo aos titulares informação inteligível sobre como as suas preferências de consentimento influenciam decisões automatizadas de tratamento de dados (Zarsky, 2017). Segundo, técnicas como SHAP (*SHapley Additive exPlanations*) e LIME (*Local Interpretable Model-agnostic Explanations*) possibilitam auditorias independentes dos algoritmos de recomendação de consentimentos, detetando vieses discriminatórios ou padrões manipulativos que violem o artigo 7.º do RGPD (Lundberg & Lee, 2017; M. Ribeiro et al., 2016). Terceiro, a XAI pode fundamentar intervenções humanas significativas em processos automatizados de alto risco, conforme exigido pelo Regulamento (UE) 2024/1689 (AI Act), nomeadamente quando sistemas de IA avaliam validade de consentimentos ou detetam tentativas de contorno dos direitos dos titulares (Parlamento Europeu e do Conselho, 2024b, Art. 14.º). Investigações futuras devem explorar a integração de modelos XAI na camada de validação (PDP) da arquitetura proposta, desenvolvendo *dashboards* de

transparência algorítmica que permitam ao titular compreender não apenas quais consentimentos prestou, mas também como esses consentimentos são interpretados e aplicados pelos sistemas automatizados (Jobin et al., 2019).

No plano técnico, passa pelo desenvolvimento de um produto mínimo viável (*minimum viable product* -- MVP), conceito introduzido por Ries (2011) no contexto da metodologia *Lean Startup*, que designa a versão mais simplificada de um produto que permite validar hipóteses fundamentais com utilizadores reais, minimizando tempo e recursos de desenvolvimento. No contexto desta investigação, um MVP da arquitetura proposta materializaria os componentes essenciais: interface do utilizador para gestão de consentimentos, motor de validação (PEP/PDP) com regras básicas do RGPD, base de dados encriptada para armazenamento *off-chain*, e registo simplificado em *blockchain* permissionada para prova de consentimentos. Este protótipo funcional, desenvolvido mediante metodologias ágeis e iterativas (Beck et al., 2001), permitiria testar a integração das tecnologias propostas em ambiente controlado, validar a usabilidade das interfaces através de estudos com utilizadores conforme recomendações de Nielsen (1994), e medir empiricamente métricas de eficácia como redução da fadiga do consentimento, tempo médio de resposta a pedidos de exercício de direitos, e taxa de conformidade com requisitos de auditoria. Com base na experiência prática adquirida, seria possível refinar o modelo conceptual, identificar gargalos de desempenho não antecipados, e fundamentar decisões sobre escalabilidade e interoperabilidade da plataforma definitiva (Richardson, 2018).

A validação empírica da arquitetura mediante desenvolvimento de MVP constitui contributo metodológico essencial, pois permite transitar do plano teórico-conceptual para a demonstração prática de viabilidade técnica e jurídica. Investigações subsequentes deveriam contemplar: implementação piloto em contexto organizacional real, mediante protocolo de investigação aprovado por comité de ética e autorizado pela CNPD; estudo longitudinal da adoção por utilizadores, avaliando evolução da perceção de controlo e confiança ao longo do tempo; e análise custo-benefício comparativa face a soluções CMP comerciais existentes, quantificando ganhos em conformidade, redução de risco regulatório, e satisfação dos titulares.

Considerando os recursos adicionais que permitiriam aprofundar significativamente esta investigação, três vetores principais emergem como prioritários. No plano temporal, a extensão do horizonte de investigação para três anos possibilitaria o desenvolvimento faseado e iterativo do MVP, incluindo ciclos completos de *design*-implementação-teste-refinamento, acompanhamento longitudinal de utilizadores para avaliar padrões de adoção e identificação de barreiras comportamentais, e validação em múltiplos contextos organizacionais (pequenas empresas, grandes corporações, setor público), permitindo generalização de resultados. No plano computacional, o acesso a infraestrutura de *cloud computing* escalável e a ambientes de teste em *blockchain* permissionadas empresariais (e.g., IBM Blockchain Platform, Azure Confidential Ledger) viabilizaria testes de desempenho sob carga realista,

simulando milhares de transações simultâneas de consentimento, experimentação com diferentes arquiteturas de consenso (RAFT, Kafka, BFT) para otimizar latência versus imutabilidade, e implementação de gémeos digitais (*digital twins*) da arquitetura para modelação de cenários de falha e recuperação sem impacto em dados reais (Androulaki et al., 2018). No plano financeiro, investimento estratégico permitiria constituição de equipa multidisciplinar incluindo programadores especializados em *blockchain* e segurança, juristas com experiência em litígios de proteção de dados, designers de experiência de utilizador (UX) para interfaces centradas no titular, e estatísticos para análise de dados dos estudos empíricos, aquisição de licenças de ferramentas comerciais de análise de risco de reidentificação (e.g., ARX Data Anonymization Tool) e auditoria algorítmica (e.g., AI Fairness 360), e financiamento de estudos de usabilidade com amostras representativas da população portuguesa, incluindo utilizadores com diferentes níveis de literacia digital e grupos vulneráveis, conforme recomendações metodológicas de Nouwens et al. (2020).

Estes recursos adicionais não apenas ampliariam o âmbito da investigação, mas possibilitariam contributos académicos de maior impacto: publicação em revistas internacionais de primeira linha (*tier 1*) nas interseções entre direito, tecnologia e sociedade; submissão de pedido de patente para componentes técnicos inovadores da arquitetura, protegendo propriedade intelectual para eventual comercialização; e desenvolvimento de *spin-off* académica para transferência de tecnologia, transformando a investigação em solução de mercado que democratize acesso a gestão de consentimentos conforme RGPD, particularmente para pequenas e médias empresas que atualmente enfrentam barreiras de custo e complexidade técnica (Lynskey, 2015).

Em suma, cremos que esta dissertação demonstrou que a abordagem conjugada pelo rigor jurídico e inovação tecnológica, pode contribuir para a construção de uma gestão de consentimentos verdadeiramente eficiente, capaz de proteger os direitos dos titulares dos dados, transformando a ideologia do ritual formal do consentimento, num processo transparente, continuo e verificável em tempo real, aliado à segurança e legalidade, permitindo o empoderamento do titular com o controlo efetivo sobre os seus dados, contribuindo para um ecossistema digital mais justo e confiável. A arquitetura proposta constitui avanço conceptual significativo face ao *status quo*, oferecendo resposta fundamentada aos desafios identificados na literatura sobre fadiga do consentimento, opacidade dos mecanismos de recolha, e ausência de rastreabilidade verificável. Contudo, reconhecemos que a transição da proposta conceptual para implementação operacional exige investigação complementar, validação empírica rigorosa, e recursos substanciais que ultrapassam o âmbito desta dissertação. As linhas de investigação futura identificadas -- aprofundamento da compatibilidade entre *blockchain* e direitos fundamentais, desenvolvimento de MVP funcional, integração de XAI para transparência algorítmica, e mecanismos robustos para transferências internacionais -- constituem agenda de investigação coerente e exequível

que, se prosseguida, poderá transformar as conclusões teóricas aqui apresentadas em contributo prático para o ecossistema digital europeu e global.

8. Referencias

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347.

Almeida Costa, M. J. (2010). Direito das Obrigações (12 .o Edição). Almedina.

Androulaki, E., … Yellick, J. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference. Association for Computing Machinery. https://doi.org/10.1145/3190508.3190538

Barker, E. B., & Kelsey, J. M. (2015). Recommendation for Random Number Generation Using Deterministic Random Bit Generators. https://doi.org/10.6028/NIST.SP.800-90Ar1

Berens, B. M., … Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. Computers & Security, 136, 103507. https://doi.org/https://doi.org/10.1016/j.cose.2023.103507

Bertoni, G. , D. J. , P. M. , & V. A. G. (2013). The Keccak sponge function family. Cryptology ePrint Archive.

Bray, T. (2017). The JavaScript Object Notation (JSON) Data Interchange Format. IETF.

Budin-Ljøsne, I., … Mascalzoni, D. (2017). Dynamic Consent… BMC Medical Ethics, 18(1). https://doi.org/10.1186/s12910-016-0162-9

Bygrave, L. A. (2002). Data protection law… Kluwer Law.

Bygrave, L. A. (2014). Data privacy law… Oxford University Press.

Bygrave, L. A. (2027, June 20). Data Protection by Design and by Default… Oslo Law Riview, 4. https://ssrn.com/abstract=3944535

Canaris, C.-W. (n.d.). Systemdenken und Systembegriff…

Canaris, C.-W. (2007). Larenz/Canaris, Lehrbuch des Schuldrechts… https://doi.org/10.17104/9783406731181-419

Cátia Rocha. (2021, July 30). Amazon recebe multa recorde… Jornal de Negócios. https://www.jornaldenegocios.pt/…

Cavoukian, A. (n.d.). What Is Privacy by Design? www.ipc.on.ca/index.asp?layid=86&fid1=328

Chang, S., … Bassham, L. E. (2012). Third-Round Report of the SHA-3… https://doi.org/10.6028/NIST.IR.7896

Comissão Europeia. (2020). Uma estratégia europeia para os dados. COM/2020/66 Final. https://eur-lex.europa.eu/…

Dankar, F. K., … Shuaib, K. (2020). Dynamic-informed consent… Computational and Structural Biotechnology Journal, 18, 913–921. https://doi.org/10.1016/j.csbj.2020.03.027

Donela, D. (2019). Da privacidade à proteção de dados pessoais… Thomson Reuters. https://www.amazon.com.br/…

Eskola, A., … Lehtiniemi, T. (2020). MyData – Um modelo nórdico…

European Commission. (2020). A European strategy for data.

European Data Protection Board. (2020a). Diretrizes 03/2020…

European Data Protection Board. (2020b). Guidelines 05/2020 on consent… https://edpb.europa.eu/…

European Data Protection Board. (2022). Guidelines 03/2022 on Deceptive design patterns…

European Data Protection Board. (2023). Report of the work undertaken by the Cookie Banner Taskforce.

European Data Protection Board. (2025). Guidelines 02/2025 on processing of personal data through blockchain technologies Version 1.1.

European Data Protection Board (EDPB). (2023). Guidelines 03/2022 on Deceptive design patterns… https://www.edpb.europa.eu/…

European Parliamentary Research Service. (2019). Blockchain and the GDPR… PE 634.445. https://www.europarl.europa.eu/…

European Union Agency for Cybersecurity. (2020). ENISA threat landscape 2020…

Faden, R. R., & Beauchamp, T. L. (1986). A history and theory of informed consent. Oxford University Press.

Fielding, R. (2000). Architectural Styles and the Design of Network-based Software Architectures.

Fielding, R. T., & Taylor, R. N. (2002). Principled design of the modern web architecture. 2, 115–150. https://doi.org/http://dx.doi.org/10.1145/514183.514185

Finck, M., & Pallas, F. (2020). They Who Must Not Be Identified… SSRN Electronic Journal, 10, 11–36. https://doi.org/10.1093/idpl/ipz026

FIPS PUB 197: Advanced Encryption Standard (AES). (2001).

Giannopoulou, A. (2021). PUTTING DATA PROTECTION BY DESIGN ON THE BLOCKCHAIN… EDPL, 7(3), 388–399. https://ssrn.com/abstract=3942392

Godik, S., & Moses, T. (2003). eXtensible Access Control Markup Language (XACML). ACM Standardview.

Godyn, M., … Song, H. (2022). Analysis of solutions for a blockchain compliance with GDPR. Scientific Reports, 12, 15021. https://doi.org/10.1038/s41598-022-19341-y

Gonçalves, M. E. (2024). Ciberdireito… Almedina.

Goodman, B., & Flaxman, S. (2016). European Union regulations on algorithmic decision-making… https://doi.org/10.1609/aimag.v38i3.2741

Grassi, P. A. , G. M. E. , F. J. L. (n.d.). Digital Identity Guidelines (NIST SP 800-63-3 e família…). NIST.

Habermas, J. (1999). Between Facts and Norms… MIT Press.

Hardt. (2012). The OAuth 2.0 Authorization Framework. http://www.rfc-editor.org/info/rfc6749.

Hart, C. (2018). Doing a Literature Review … SAGE.

Hijmans, H. (2016). The European Union as Guardian of Internet Privacy. Springer.

Hu, V. C., … Scarfone, K. (2014). NIST SP 800-162 - Guide to ABAC… https://doi.org/10.6028/NIST.SP.800-162

International Organization for Standardization. (2012). ISO/IEC 27037:2012 …

ISO_IEC 27002_2022. (2022). www.iso.org

ISO_IEC 27555_2021. (2021). www.iso.org

ISO/IEC 27560:2023 - Security and privacy — Consent record information structure (1.a ed.). (2023). www.iso.org

ISO_IEC 27701_2019. (2019). www.iso.org

ISO_IEC 29100_2011. (2011). www.iso.org

ISO_IEC 29184_2020. (2020). www.iso.org

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1. https://doi.org/10.1038/s42256-019-0088-2

Jornal de Negócios. (2022). Confirmada multa de 100 milhões à Google…

Kaye, J., … Melham, K. (2015). Dynamic consent… EJHG, 23(2), 141–146. https://doi.org/10.1038/ejhg.2014.71

Kent, K. ; S. M. (2006). Guide to Computer Security Log Management (NIST SP 800-92).

Khalid, M. I., … Kim, J. (2023). Privacy-First Paradigm for Dynamic Consent… Electronics, 12(24). https://doi.org/10.3390/electronics12244973

Kindervag, J. (2010). No More Chewy Centers: The Zero Trust Model… Forrester.

Kosta, E. (2013). Consent in European Data Protection Law. https://doi.org/10.1163/9789004232365

Kranenborg, H. (2016). O. Lynskey, The Foundations of EU Data Protection Law. IDPL, 6(4), 324–326. https://doi.org/10.1093/idpl/ipw017

Kyi, L., … Biega, A. J. (2023). Investigating Deceptive Design in GDPR's Legitimate Interest. CHI 2023. https://doi.org/10.1145/3544548.3580637

Langford, J., … Rikken, M. (2022). Understanding MyData Operators. https://mydata.org/organisation-members

Len Bass, P. C. R. K. (2021). Software architecture in practice (4.a ed.). Addison-Wesley.

Leslie K. John. (2018). Uninformed Consent. Harvard Business Review.

Lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making… CLSR, 50. https://doi.org/10.1016/j.clsr.2023.105848

Lundberg, S., & Lee, S.-I. (2017, October). A Unified Approach to Interpreting Model Predictions. https://doi.org/10.48550/arXiv.1705.07874

Lynskey, O. (2015). The Foundations of EU Data Protection Law. Oxford University.

Machuletz, D., & Böhme, R. (2020). Multiple Purposes, Multiple Problems… PoPETs, 2020, 481–498. https://doi.org/10.2478/popets-2020-0037

Mantelero, A. (2018). AI and Big Data… CLSR, 34(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

Marcotte, E. (2010). Responsive Web Design. A List Apart.

Mathur, A., … Narayanan, A. (2019a). Dark Patterns at Scale… Proc. ACM HCI, 3(CSCW). https://doi.org/10.1145/3359183

Mathur, A., … Narayanan, A. (2019b). Dark Patterns at Scale… PACMHCI, 3, 1–32. https://doi.org/10.1145/3359183

Matthias Berberich, M. S. (2016). Practitioner's Corner · Blockchain Technology and the GDPR… EDPL, 2, 422–426.

Menezes Cordeiro, A. B. (2018). O consentimento do titular dos dados no RGPD. In FinTech II… Almedina.

Menezes Cordeiro, A. B. (2021). Tratado de Direito Civil… (2.a). Almedina.

Menezes Cordeiro, A. B. (2022). Direito da Proteção de Dados. Almedina.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. In Proc IEEE Symp Sec Priv. https://doi.org/10.1109/SP.2008.33

Newman, S. (2021). Building Microservices… (2nd ed.). O'Reilly.

Nissenbaum, H. (2010). Privacy in Context… University of Chicago Press.

NIST. (2002). FIPS PUB 140-2: Security Requirements for Cryptographic Modules.

NIST 800-57 Recommendations for Key Management Requirements Analysis. (n.d.). https://nvlpubs.nist.gov/…

NIST Special Publication 800-107 Revision 1… (2012). https://doi.org/10.6028/NIST.CSWP.01162020

Norberg, P., Horne, D., & Horne, D. (2007). The Privacy Paradox… Journal of Consumer Affairs, 41, 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Nouwens, M., … Kagal, L. (2020). Dark Patterns after the GDPR… https://doi.org/10.1145/3313831.3376321

Pavlou, P. A. (2011). State of the information privacy literature… MISQ, 35(4), 977–988. https://doi.org/10.2307/41409969

Pinheiro, A. S. (2015a). Privacy e proteção de dados pessoais… Almedina.

Pinheiro, A. S. (2015b). Privacy e Protecção de Dados Pessoais… AAFDL.

Pinto Ramos, M. (2022). O consentimento do titular dos dados no contexto da Internet… Revista da FDUL, LXIII (1-2), 663–727.

Poikola, A., Kuikkaniemi, K. , K. O., … (2020). MyData – An Introduction… MyData Global. https://doi.org/https://mydata.org/publication

Poikola, A., Kuikkaniemi, K., & Honko, H. (n.d.). MyData.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent… Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy001

Prasser, F. , K. F. (2015). Putting Statistical Disclosure Control into Practice… In Medical Data Privacy Handbook (pp. 111–148). Springer. https://doi.org/10.1007/978-3-319-23633-9_6

Ribeiro, M., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?"… 1135–1144. https://doi.org/10.1145/2939672.2939778

Ribeiro, R., Da, G., & Organizador, S. (n.d.). Direito autoral, propriedade intelectual e plágio.

Richard Kissel, A. R. M. S. K. S. (2017). NIST SP 800-88 Rev. 1. NIST.

Richardson, L. ; R. S. (2007). RESTful Web Services.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST.

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent… Ethics and Information Technology, 16(2), 171–182. https://doi.org/10.1007/s10676-014-9343-8

Schwartz, P. M. (1989). The Computer in German and American Constitutional Law… AJCL, 37, 675–701.

Solove, D. J. (2010). Understanding Privacy. Harvard University Press.

Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. Havard Law Review, 126(7). http://bobgellman.com/rg-docs/rg-FIPPShistory.pdf.

Stallings, William., … Howard, Michael. (2012). Computer security : principles and practice. Pearson.

Sweeney, L. (2013). Discrimination in Online Ad Delivery. SSRN. https://ssrn.com/abstract=2208240 or http://dx.doi.org/10.2139/ssrn.2208240

Turow, J. (2011). How the New Advertising Industry Is Defining Your Identity and Your Worth. Yale University Press. http://www.jstor.org/stable/j.ctt5vkx84

Utz, C., … Holz, T. (2019). (Un)informed Consent… CCS, 973–990. https://doi.org/10.1145/3319535.3354212

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR), A Practical Guide. https://doi.org/10.1007/978-3-319-57959-7

Yin, R. K. (2018). Case Study Research and Applications… (6th ed.).

Zarsky, T. (2016). The Trouble with Algorithmic Decisions… STHV, 41(1), 118–132. http://www.jstor.org/stable/43671285

Zarsky, T. (2017). Big data: The end of privacy or a new beginning? IDPL, 3(2), 74–87. https://doi.org/10.1093/idpl/ips036

Zhao, Y., Li, Z., & Lv, S. (2024). Enhancing AI System Privacy… Computers, Materials and Continua, 80(1), 217–234. https://doi.org/10.32604/cmc.2024.052310

Legislação

Lei n.o 58/2019, 151/2019 Diário da República ___ (2019).

União Europeia. (2002). DIRECTIVA 2002/58/CE DO PARLAMENTO EUROPEU E DO CONSELHO. https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32002L0058

União Europeia. (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Jornal Oficial da União Europeia, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Parlamento Europeu e do Conselho. (2022, October 19). Regulamento (UE) 2022/868. Jornal Oficial Da União Europeia.

Regulamento 2022/2065 (October 19, 2022).

Parlamento Europeu e do Conselho. (2023). Regulamento (UE) 2023/2854. Jornal Oficial Da União Europeia.

Parlamento Europeu e do Conselho. (2024a). Regulamento (UE) 2024/1183.

Parlamento Europeu e do Conselho. (2024b). Regulamento (UE) 2024/1689. Jornal Oficial Da União Europeia, 1–144.

Jurisprudência

Processo C-252/21 – Bundeskartellamt v. Meta Platforms Inc. (2021).

Processo C-311/18 – Schrems II (2018). https://curia.europa.eu

Processo C-604/22 – IAB Europe (2022).

Processo C-673/17 – Planet49 GmbH/Bundesverband (2017-11-30).