Do consentimento formal ao consentimento verificável: contributos para uma arquitetura jurídico-digital de gestão de consentimentos no âmbito do RGPD

From formal consent to verifiable consent: contributions to a legal-digital signature management architecture under the GDPR

10.29073/j2.v8i1.1121

Recebido: 26 de fevereiro de 2026.
Aprovado: 28 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a 1 (Correspondente): Sílvia Catarina Ferreira, ESTG-IPP, Portugal, cfsolicitadora@gmail.com.

Autor/a 2: Patrícia Azevedo, ESTG-IPP, Portugal, pamv@estg.ipp.pt.
Autor/a 3: Marco Filipe Gomes, ESTG-IPP, Portugal, mfg@estg.ipp.pt.

Resumo

O consentimento constitui um dos fundamentos de licitude do tratamento de dados pessoais no quadro do Regulamento (UE) 2016/679, assumindo um papel central na tutela da autodeterminação informacional do titular dos dados. Todavia, a crescente digitalização das relações sociais, comerciais e administrativas revelou um desfasamento entre a construção normativa do consentimento e a forma como este é efetivamente recolhido nas plataformas digitais.

A repetição de pedidos de consentimento, a complexidade informacional, a utilização de interfaces manipulativas e a fragmentação dos mecanismos de escolha contribuem para a desmaterialização do consentimento enquanto ato jurídico livre, específico, informado e inequívoco. Como tem sido salientado pela doutrina e pela literatura especializada, a proteção de dados não pode ser reduzida a um formalismo procedimental, exigindo antes condições reais de controlo pelo titular dos dados (Bygrave, 2014; Menezes Cordeiro, 2022; Solove, 2010). A dissertação que está na base deste artigo parte precisamente desse problema e propõe uma reflexão jurídico-computacional sobre a necessidade de mecanismos mais transparentes, interoperáveis e auditáveis de gestão do consentimento.

Com base numa metodologia qualitativa, exploratória e descritiva, assente na análise jurídica, revisão técnico-científica e comparação de modelos existentes de gestão de consentimentos, sustenta-se que os mecanismos atualmente predominantes continuam excessivamente orientados para as necessidades de conformidade dos responsáveis pelo tratamento e insuficientemente centrados no titular dos dados.

Em resposta a estas limitações, propõe-se a reflexão sobre uma arquitetura jurídico-computacional orientada à gestão centralizada de consentimentos, alicerçada em princípios de *privacy by design*, interoperabilidade, segurança, rastreabilidade e auditabilidade, em linha com a literatura sobre proteção de dados desde a conceção e governação tecnológica da privacidade (Cavoukian, 2009; Giannopoulou, 2021; ISO/IEC 29100, 2011; ISO/IEC 27560, 2023). Tal proposta não visa substituir o regime jurídico do RGPD, mas antes contribuir para a sua efetivação material, reforçando a transparência, a prova do consentimento, a revogabilidade, a granularidade e a *accountability* no tratamento de dados pessoais.

Palavras-Chave: Arquitetura Computacional; Autodeterminação Informacional; Consentimento; Proteção de Dados Pessoais; RGPD.

Abstract

Consent constitutes one of the legal bases for the processing of personal data under Regulation (EU) 2016/679, playing a central role in protecting the informational self-determination of the data subject. However, the

increasing digitalization of social, commercial, and administrative relations has revealed a gap between the normative construction of consent and the way it is actually collected on digital platforms.

The repetition of consent requests, informational complexity, the use of manipulative interfaces, and the fragmentation of choice mechanisms contribute to the dematerialization of consent as a free, specific, informed, and unambiguous legal act. As has been highlighted by doctrine and specialized literature, data protection cannot be reduced to procedural formalism, but rather requires real conditions of control by the data subject (Bygrave, 2014; Menezes Cordeiro, 2022; Solove, 2010). The dissertation that forms the basis of this article stems precisely from this problem and proposes a legal-computational reflection on the need for more transparent, interoperable, and auditable consent management mechanisms.

Based on a qualitative, exploratory, and descriptive methodology, grounded in legal analysis, technical-scientific review, and comparison of existing consent management models, it is argued that the currently predominant mechanisms remain excessively oriented towards the compliance needs of data controllers and insufficiently focused on the data subject.

In response to these limitations, a reflection on a legal-computational architecture oriented towards the centralized management of consents is proposed, based on the principles of privacy by design, interoperability, security, traceability, and auditability, in line with the literature on data protection from the design stage and technological governance of privacy (Cavoukian, 2009; Giannopoulou, 2021; ISO/IEC 29100, 2011; ISO/IEC 27560, 2023). This proposal does not aim to replace the legal framework of the GDPR, but rather to contribute to its effective implementation, reinforcing transparency, proof of consent, revocability, granularity, and accountability in the processing of personal data.

Keywords: Computer Architecture; Consent; GDPR; Informational Self-Determination; Personal Data Protection.

1. Introdução

A proteção de dados pessoais constitui, hoje, um dos domínios mais relevantes da contemporaneidade jurídica, precisamente porque a intensificação das interações digitais veio transferir para o ambiente tecnológico uma parte substancial da vida privada, económica e relacional dos indivíduos. A recolha e o tratamento de dados pessoais deixaram de ser fenómenos marginais para se converterem em condição estrutural do funcionamento de plataformas, serviços digitais e modelos de negócio assentes na circulação informacional. Neste contexto, o Regulamento Geral sobre a Proteção de Dados surge como instrumento de harmonização normativa e de reforço da posição jurídica do titular dos dados, procurando assegurar que o tratamento seja realizado de forma lícita, transparente e respeitadora dos direitos fundamentais, numa linha já antecipada por autores como Bygrave (2014) e Lynskey (2015). A própria dissertação que serve de base a este artigo parte deste enquadramento, reconhecendo que a proteção de dados é simultaneamente um desafio jurídico e tecnológico e que a resposta regulatória europeia não pode ser dissociada das transformações técnicas que moldam o ecossistema digital.

Entre os vários fundamentos de licitude previstos no RGPD, o consentimento ocupa um lugar particularmente sensível. A sua centralidade decorre do facto de funcionar como expressão da vontade do titular dos dados e como mecanismo através do qual se pretende assegurar o controlo individual sobre o uso da informação pessoal. No plano normativo, o consentimento é configurado como manifestação de vontade livre, específica, informada e inequívoca. No plano prático, porém, o seu exercício tem vindo a ser progressivamente enfraquecido por mecanismos massificados de recolha, por interfaces desenhadas para induzir comportamentos rápidos e por um contexto de saturação cognitiva que reduz o ato de consentir a uma mera formalidade operacional, como assinalam Schermer et al. (2014), Utz et al. (2019) e Menezes Cordeiro (2018, 2022). É essa fratura entre forma jurídica e substância material que justifica a presente análise.

A questão central a que este artigo procura responder pode formular-se nos seguintes termos: pode o consentimento, tal como hoje é recolhido no ambiente digital, continuar a ser entendido como instrumento

idóneo de autodeterminação informacional? A dissertação de origem identifica como principais fatores críticos a fadiga do consentimento, o formalismo da recolha, os *dark patterns* e o paradoxo da privacidade, articulando estes fenómenos com a insuficiência das atuais plataformas de gestão de consentimento, sobretudo no que respeita à centralização, interoperabilidade, usabilidade e prova da validade do consentimento. Em consequência, o estudo não se limita à crítica do modelo vigente, antes avança para a formulação de uma proposta conceptual de arquitetura computacional juridicamente orientada, destinada a reforçar a posição do titular dos dados e a tornar mais efetivos os princípios estruturantes do RGPD.

2. O Consentimento no RGPD: Entre Fundamento de Licitude e Expressão da Autodeterminação Informacional

O consentimento não pode ser lido apenas como uma cláusula técnica de validação do tratamento de dados. A sua importância radica, antes de mais, na função que desempenha no sistema de proteção de dados: por um lado, constitui fundamento de licitude; por outro, representa a exteriorização jurídica do poder do titular sobre os seus próprios dados. Esta dupla dimensão é claramente compatível com a leitura proposta por Menezes Cordeiro (2018, 2022), Pinheiro (2015) e Bygrave (2014), para quem a proteção de dados deve ser compreendida como expressão de autonomia e controlo, e não apenas como disciplina formal de circulação informacional. A dissertação sublinha precisamente esta articulação, salientando que o consentimento funciona simultaneamente como requisito de licitude e como mecanismo de confiança nas relações digitais, na medida em que permite ao titular controlar a utilização da informação que lhe diz respeito.

O problema é que a força normativa desta construção se fragiliza quando o consentimento deixa de ser prestado num ambiente de verdadeira compreensão e liberdade. A exigência legal de que a vontade seja livre, específica, informada e inequívoca pressupõe um contexto relacional em que o titular conheça, em termos minimamente inteligíveis, a finalidade do tratamento, os intervenientes relevantes, o alcance da autorização conferida e a possibilidade real de recusar ou revogar. Ora, quando o consentimento se converte em gesto repetitivo, apressado e cognitivamente saturado, a preservação da sua substância torna-se altamente duvidosa. Como observam Schermer et al. (2014), uma maior proliferação formal do consentimento pode, paradoxalmente, conduzir a um consentimento materialmente mais fraco. O que se mantém é a aparência formal do ato; o que se perde é a sua densidade jurídica.

A erosão material do consentimento torna ainda mais evidente uma tensão estruturante do direito da proteção de dados contemporâneo: a de saber se a autonomia individual continua a ser adequadamente protegida por um modelo que, embora juridicamente exigente, é operacionalizado através de mecanismos digitais que não foram concebidos para favorecer reflexão, mas antes rapidez, adesão e fricção mínima para o acesso ao serviço. Por isso, autores como Solove (2010), Nissenbaum (2010) e Pavlou (2011) têm defendido que a privacidade e a autodeterminação não podem ser avaliadas apenas a partir da existência de uma escolha formal, mas antes da qualidade do contexto em que essa escolha ocorre.

3. A Crise do Consentimento no Ambiente Digital

Uma das principais contribuições da dissertação consiste em mostrar que o consentimento em ambiente digital atravessa uma crise de efetividade. Tal crise manifesta-se, desde logo, no fenómeno da fadiga do consentimento. O utilizador médio é permanentemente confrontado com *banners*, *pop-ups*, caixas de seleção, pedidos de aceitação de políticas de privacidade e múltiplos avisos de cookies, o que produz uma sobrecarga cognitiva incompatível com um processo decisório minimamente ponderado. O consentimento, em vez de representar uma escolha informada, transforma-se num reflexo de navegação. Esta crítica encontra eco em trabalhos como os de Utz et al. (2019), Nouwens et al. (2020) e Leslie John (2018), que mostram como os avisos e interfaces de consentimento falham frequentemente na promoção de decisões genuinamente esclarecidas.

A esta fadiga junta-se o formalismo da recolha. Em muitos contextos, o consentimento é apresentado não como expressão jurídica de autodeterminação, mas como simples etapa instrumental para aceder ao conteúdo, concluir uma compra ou continuar a utilizar uma plataforma. Tal realidade é agravada por práticas de agregação

e simplificação abusiva, em que diferentes finalidades, destinatários ou interesses de terceiros são colocados sob uma aparência de aceitação global, sem verdadeira granularidade. Trabalhos como os de Machuletz e Böhme (2020) e Budin-Ljøsne et al. (2017), ainda que em contextos distintos, sublinham a importância de modelos mais granulares, dinâmicos e compreensíveis de gestão do consentimento. A dissertação chama igualmente a atenção para o problema do consentimento prestado em favor de "fornecedores" ou "parceiros" não individualizados, sublinhando a incompatibilidade dessa prática com as exigências de especificidade, transparência e prova do consentimento.

Outro elemento central da crise é representado pelos *dark patterns*. A literatura recente tem demonstrado que as interfaces podem ser desenhadas de forma a influenciar decisões, desviando o utilizador da opção que melhor protege os seus interesses. Mathur et al. (2019a, 2019b), Nouwens et al. (2020), Kyi et al. (2023) e Berens et al. (2024) evidenciam que o design manipulativo não constitui um problema marginal, mas antes um padrão recorrente em *websites, banners* de *cookies* e ambientes digitais diversos. Em matéria de consentimento, isto traduz-se frequentemente na colocação em destaque de opções como "aceitar tudo", na ocultação da recusa em menus secundários, na assimetria visual entre aceitar e rejeitar, ou ainda na utilização de linguagem ambígua e percursos de decisão deliberadamente enviesados. Não se trata de um problema meramente estético ou ergonómico. Trata-se, antes, de um problema jurídico-material, porque a manipulação da interface afeta diretamente a liberdade da decisão e, por essa via, compromete a validade do consentimento. Também o EDPB tem vindo a advertir para esta realidade nas orientações sobre *dark patterns* e no relatório da *Cookie Banner Taskforce* (European Data Protection Board, 2022, 2023).

Finalmente, importa referir o paradoxo da privacidade, isto é, a contradição entre a preocupação declarada dos titulares relativamente à privacidade e o seu comportamento real de aceitação rápida e pouco refletida do tratamento dos seus dados. Norberg et al. (2007) identificaram este fenómeno de forma clássica, e Pavlou (2011) aprofundou a sua relevância na literatura sobre informação e privacidade. A dissertação mostra que esse paradoxo não significa falta de relevância da privacidade, mas antes evidencia as limitações do contexto em que a escolha é exercida. Políticas longas, linguagem técnica, desconhecimento do alcance dos riscos e confiança funcional no prestador do serviço contribuem para que o consentimento seja, muitas vezes, apenas formalmente válido, mas substancialmente deficiente.

4. Limites das Atuais Plataformas de Gestão de Consentimentos

O ambiente digital não é desprovido de mecanismos de gestão de consentimentos. Pelo contrário, a proliferação de *Consent Management Platforms* demonstra que o mercado reconheceu a necessidade de organizar a recolha e administração destes atos. Todavia, a dissertação evidencia que tais soluções se desenvolveram, em larga medida, sob uma lógica predominantemente empresarial, orientada para a demonstração de conformidade dos responsáveis pelo tratamento, e não prioritariamente para a capacitação do titular dos dados. Esta crítica é compatível com a leitura de Voigt e von dem Bussche (2017), segundo a qual a conformidade regulatória não deve ser confundida com efetiva proteção material dos direitos dos titulares.

É verdade que as CMP trouxeram ganhos relevantes ao nível da documentação do consentimento, da parametrização de preferências e da adaptação às exigências do RGPD. Porém, esses ganhos revelam-se insuficientes quando avaliados à luz de uma perspetiva verdadeiramente centrada no utilizador. A fragmentação permanece: cada plataforma gere consentimentos no seu próprio perímetro, com diferentes formatos, diferentes interfaces, diferentes níveis de detalhe e diferentes possibilidades de revogação. A prova também permanece dispersa, dificultando a reconstrução clara do percurso do consentimento ao longo do tempo. Acresce que, em muitos casos, a lógica de design dessas ferramentas continua a favorecer a aceitação em vez de promover uma decisão equilibrada. Assim, a mera existência de sistemas de gestão de consentimento não elimina a crise do consentimento; em certos casos, apenas a reorganiza sob uma aparência mais sofisticada de conformidade.

Foi precisamente a partir da identificação dessas lacunas que a investigação desenvolveu uma metodologia assente em três eixos complementares: a análise jurídico-dogmática do consentimento e do RGPD; a revisão técnico-científica de soluções e tecnologias relevantes; e a análise qualitativa-comparativa de modelos existentes, incluindo CMPs e sistemas alternativos como *MyData*, *Consentua*, *Solid Pods* e *IBM Data Consent Manager*. Esta aproximação metodológica é coerente com a utilização do estudo de caso e da comparação funcional como instrumentos de investigação jurídica e aplicada, em linha com Yin (2018) e com a literatura sobre ecossistemas de dados centrados no utilizador, como Verborgh et al. (2021) e Langford et al. (2022).

5. Para Além do Consentimento Formal: Proposta de Uma Arquitetura Jurídico-Computacional Orientada ao Titular

A originalidade da dissertação reside em não se limitar à crítica do modelo vigente, avançando antes com uma proposta conceptual de arquitetura computacional destinada a reforçar a autodeterminação informacional do titular dos dados. Essa proposta combina Direito e Computação como forma de repensar a recolha, gestão e validação do consentimento, partindo da premissa de que a efetividade do RGPD depende também da qualidade técnica das infraestruturas que sustentam o exercício dos direitos. Tal entendimento é compatível com a noção de *data protection by designand by default*, desenvolvida na doutrina e nas orientações regulatórias, segundo a qual as garantias jurídicas devem ser integradas na própria arquitetura dos sistemas e não apenas acrescentadas de forma posterior ou superficial (Bygrave, 2017; Cavoukian, 2009; Menezes Cordeiro, 2022). A própria dissertação afirma expressamente essa exigência de incorporação estrutural das garantias jurídicas.

A arquitetura proposta assenta em princípios de *privacy by design*, interoperabilidade e segurança, integrando mecanismos de pseudonimização, *hashing*, rastreabilidade e registo imutável. A sua lógica é eminentemente jurídico-funcional: criar condições para que o titular possa gerir os seus consentimentos de forma simplificada, transparente e segura, enquanto os responsáveis pelo tratamento dispõem de meios adequados para demonstrar a regularidade da recolha, da conservação da prova e do exercício dos direitos de modificação ou revogação. Neste plano, a ISO/IEC 29100 (2011), a ISO/IEC 27701 (2019) e a ISO/IEC 27560 (2023) oferecem enquadramentos particularmente relevantes para estruturar privacidade, gestão e registo do consentimento.

Do ponto de vista arquitetural, a investigação sustenta uma solução híbrida, articulando microserviços e eventos, com justificação ancorada na necessidade de escalabilidade, auditabilidade e adaptação dinâmica às operações associadas ao consentimento. Embora esta dimensão tenha um cariz mais técnico, ela pode ser juridicamente valorizada na medida em que suporta *accountability,* rastreabilidade e resposta eficiente aos direitos dos titulares. A literatura de arquitetura de *software*, como Bass et al. (2021) e Newman (2021), ajuda a compreender como estruturas modulares e orientadas a eventos favorecem controlo, separação de responsabilidades e flexibilidade evolutiva. O ponto essencial, porém, é jurídico: a arquitetura procura transformar a manifestação de vontade do titular em instruções operacionais verificáveis, suscetíveis de serem respeitadas por diferentes intervenientes e sistemas.

A componente de registo e prova pode igualmente beneficiar de mecanismos robustos de integridade e auditabilidade. Neste domínio, referências como Kent (2006), ISO/IEC 27037 (2012) e ISO/IEC 27560 (2023) são úteis para enquadrar requisitos de registo, preservação e estruturação da evidência digital. Já quanto ao eventual recurso a blockchain permissionada e registos imutáveis, importa adotar uma postura prudente. Trabalhos como os de Androulaki et al. (2018), Godyn et al. (2022) e Berberich (2016) mostram que estas tecnologias podem oferecer vantagens em matéria de integridade e rastreabilidade, mas levantam simultaneamente questões delicadas de conformidade com princípios como minimização, apagamento e limitação das finalidades. A dissertação reconhece essas tensões e, por isso, não apresenta a tecnologia como solução mágica, mas como instrumento a enquadrar juridicamente com cautela.

Acresce que uma arquitetura deste tipo deve ser pensada em coerência com os desafios contemporâneos colocados por sistemas automatizados e inteligência artificial. Autores como Mantelero (2018), Zarsky (2016, 2017), Giannopoulou (2021) e Lukács e Váradi (2023) mostram que a utilização de sistemas baseados em dados

exige padrões reforçados de explicabilidade, supervisão e conformidade. Isso é particularmente importante quando a gestão do consentimento deixa de ser apenas um registo passivo e passa a integrar componentes de automatização, verificação ou decisão.

6. Relevância Jurídico-Científica da Proposta

A passagem do consentimento formal ao consentimento verificável tem implicações dogmáticas relevantes. Em primeiro lugar, reforça a ideia de que a validade do consentimento não depende apenas da existência de um ato positivo, mas da qualidade do contexto em que esse ato é produzido, registado e subsequentemente gerido. Em segundo lugar, desloca o foco da mera recolha inicial para a governança integral do consentimento, compreendida como processo que inclui prova, revogabilidade, auditabilidade, portabilidade e interoperabilidade. Em terceiro lugar, contribui para reconduzir a proteção de dados à sua dimensão estrutural: a de uma tutela de direitos fundamentais que não se satisfaz com procedimentos formais, exigindo antes condições reais de exercício da autonomia informacional. Esta leitura é compatível com o pensamento de Bygrave (2014), Lynskey (2015), Menezes Cordeiro (2022) e Solove (2010), bem como com o enquadramento regulatório desenvolvido pelo EDPB.

Nesta perspetiva, a proposta de arquitetura jurídico-computacional tem valor não apenas instrumental, mas também hermenêutico. Ela permite ler o RGPD não como um conjunto de deveres abstratos desligados da realidade tecnológica, mas como um regime cuja aplicação prática depende de mecanismos de execução coerentes com os seus princípios. Assim, *privacy by design* deixa de ser mera cláusula programática e passa a exigir efetiva tradução técnica,*accountability* deixa de significar apenas dever de documentação e passa a implicar condições de reconstrução verificável do percurso do consentimento; transparência deixa de se esgotar em textos informativos extensos e passa a exigir inteligibilidade funcional. Tudo isto reforça a ideia de que a integração entre categorias jurídicas e estruturas computacionais é hoje condição da efetividade do direito da proteção de dados.

7. Conclusão

O consentimento continua a ocupar posição nuclear no regime da proteção de dados pessoais, mas a sua centralidade normativa não garante, por si só, a sua efetividade material. A análise desenvolvida demonstra que o ambiente digital contemporâneo favorece formas de consentimento apressadas, manipuladas, fragmentadas e insuficientemente compreendidas, comprometendo a liberdade e a informação que o RGPD exige. A fadiga do consentimento, o formalismo da recolha, os *dark patterns* e o paradoxo da privacidade revelam que o modelo vigente, embora juridicamente exigente, enfrenta sérias dificuldades de concretização prática, como assinalam Schermer et al. (2014), Nouwens et al. (2020), European Data Protection Board (2022, 2023) e Menezes Cordeiro (2022).

Todavia, a relevância do estudo não reside apenas nesse diagnóstico. O seu contributo decisivo está em demonstrar que a crise do consentimento não impõe necessariamente o abandono desta figura, mas antes a sua reconceptualização à luz das exigências do ambiente digital. Nesse sentido, a proposta de uma arquitetura jurídico-computacional de gestão de consentimentos apresenta-se como via promissora para reforçar a posição do titular, assegurar maior granularidade e revogabilidade, melhorar a prova da validade do consentimento e tornar mais efetivos os princípios de transparência, segurança, interoperabilidade e responsabilidade. Não se trata de substituir o Direito pela tecnologia, mas de reconhecer que, sem desenho técnico juridicamente orientado, o Direito corre o risco de permanecer apenas formalmente proclamado.

Em síntese, a passagem do consentimento formal ao consentimento verificável constitui não apenas uma possibilidade técnica, mas uma exigência jurídica coerente com a lógica do RGPD. A proteção de dados pessoais, numa era de ecossistemas digitais complexos, já não pode depender exclusivamente da repetição de cliques em interfaces opacas. Exige, antes, estruturas que devolvam ao titular controlo inteligível, escolha efetiva e capacidade de prova. É nesse ponto que a abordagem combinada entre Direito e Computação revela o seu maior mérito: o de contribuir para uma proteção de dados menos ritual e mais substantiva.

Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*.

Bass, L., Clements, P., & Kazman, R. (2021). *Software architecture in practice* (4.ª ed.). Addison-Wesley.

Berberich, M. S. (2016). Practitioner's corner: Blockchain technology and the GDPR. *European Data Protection Law Review, 2*, 422–426.

Berens, B. M., et al. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security, 136*, 103507.

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., Javaid, M. K., Jones, E., Katić, V., Simpson, A., Mascalzoni, D., & Hansson, M. G. (2017). Dynamic consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics, 18*(1).

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Bygrave, L. A. (2017). Data protection by design and by default. *Oslo Law Review, 4*.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*.

European Data Protection Board. (2022). *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them*.

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

Giannopoulou, A. (2021). Data protection by design in the era of artificial intelligence. *International Data Privacy Law*.

Godyn, J., Maček, N., & Pustisek, M. (2022). Blockchain and GDPR compliance: Opportunities and challenges for data protection. *Computer Law & Security Review*.

International Organization for Standardization. (2011). *ISO/IEC 29100:2011 — Information technology — Security techniques — Privacy framework*.

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence*.

International Organization for Standardization. (2019). *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*.

International Organization for Standardization. (2023). *ISO/IEC 27560:2023 — Privacy technologies — Consent record information structure*.

John, L. K. (2018). Uninformed consent. *Harvard Business Review*.

Kent, K. (2006). *Guide to computer security log management (NIST Special Publication 800-92)*. National Institute of Standards and Technology.

Kyi, L., et al. (2023). Investigating deceptive design in GDPR's legitimate interest. *CHI 2023*.

Langford, J., et al. (2022). Understanding MyData operators.

Lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making. *Computer Law & Security Review, 50*.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *PoPETs, 2020*, 481–498.

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review, 34*(4), 754–772.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019a). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1–32.

Mathur, A., Kshirsagar, M., Mayer, J., & Narayanan, A. (2019b). What makes a dark pattern dark? *Proceedings of the ACM on Human-Computer Interaction*.

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

Menezes Cordeiro, A. B. (2022). *Direito da proteção de dados*. Almedina.

Newman, S. (2021). *Building microservices* (2nd ed.). O'Reilly.

Nissenbaum, H. (2010). *Privacy in context*. University of Chicago Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988.

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

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology, 16*(2), 171–182.

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

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990.

Verborgh, R., Arndt, D., Vander Sande, M., Hartig, O., De Meester, B., Haesendonck, G., & Colpaert, P. (2021). Solid: Re-decentralizing the Web by giving users control over their data. *Proceedings of the Web Conference*.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.

Zarsky, T. (2016). The trouble with algorithmic decisions. *Science, Technology, & Human Values, 41*(1), 118–132.

Zarsky, T. (2017). Big data: The end of privacy or a new beginning? *International Data Privacy Law, 3*(2), 74–87.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Todo o conteúdo do ***J² — Jornal Jurídico*** é licenciado sob Creative Commons, a menos que especificado de outra forma e em conteúdo recuperado de outras fontes bibliográficas.