I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL II

EUDES VITOR BEZERRA

CINTHIA OBLADEN DE ALMENDRA FREITAS

I61
Inteligência Artificial: Desafios da Era Digital II [Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Cinthia Obladen de Almendra Freitas, Eudes Vitor Bezerra. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-096-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Inteligência Artificial e Sustentabilidade na Era Transnacional

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Inteligência Artificial. 3. Desafios da Era Digital. I International Experience Perugia – Itália. (1: 2025 : Perugia, Itália).

CDU: 34

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

I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL II

Apresentação

O I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA, com temática “Inteligência Artificial e Sustentabilidade na Era Transnacional”, realizado no período de 28 a 30 de maio de 2025 na Universidade degli Studi di Perugia – Itália, reuniu centenas de pesquisadores, professores e estudantes de Programas de Pós-Graduação em Direito (PPGD) do Brasil, da Itália e de outras nações.

Com submissões de trabalhos, o GT - INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL surpreendeu pela quantidade de trabalhos submetidos, tendo sido subdividido em quatro subgrupos. Assim, esta apresentação refere-se aos trabalhos submetidos, selecionados e, efetivamente, apresentados e discutidos no GT - INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL II.

Os trabalhos apresentados foram organizados em dois blocos distintos pelas temáticas centrais dos artigos, permitindo uma unidade de discussões e reflexões. No primeiro bloco, os trabalhos trataram de temas referentes à aplicação de sistemas de IA em: Educação, Meio Ambiente, Planejamento Sustentável e Cidades Inteligentes, Trabalho, Poder Judiciário e Medicina e Saúde. As discussões envolveram de modo primordial os riscos advindos da aplicação de sistemas de IA nestas áreas, permitindo reflexões sobre: a) Educação: personalização do ensino, padronização excessiva do aprendizado, a mercantilização da educação e o uso inadequado de dados sensíveis de estudantes; b) Meio Ambiente: aplicações de sistemas de IA na governança ambiental, riscos e responsabilidade jurídica, regulação; c) Planejamento Sustentável e Cidades Inteligentes: sistemas de IA no planejamento urbano e mudanças climáticas e, também, viés adultocêntrico nas cidades inteligentes; d) Trabalho: plataformas digitais, subordinação algorítmica, precarização do trabalho humano, jornadas extensas, remuneração variável, ausência de direitos trabalhistas e ambiente de trabalho estressante devido à vigilância constante dos algoritmos; e) Poder Judiciário: democratização da justiça e exclusão digital, celeridade processual, transparência e explicabilidade, minutas automatizadas e dignidade humana, juízo humano versus decisão automatizada; f) Medicina e Saúde: formação médica, diagnósticos, simulações clínicas, desinformação em saúde. Percebeu-se que a temática de Inteligência Artificial desenvolverá cada vez mais um papel preponderante no desenvolvimento e na sustentabilidade de um ecossistema tecnológico, o qual precisa estar fundamentado em princípios jurídicos para que os desafios da Era Digital sejam enfrentados e os riscos mitigados. Deste modo,

considerando-se como premissa que a regulação de sistemas de IA deve ser guiada por quatro elementos fundamentais: transparência, não discriminação, responsabilidade e segurança jurídica; as discussões foram produtivas e permitiram compreender que tais elementos são essenciais para garantir que o uso de sistemas de IA respeite os direitos fundamentais e promova justiça social. E, ainda, há que se pontuar que os sistemas de IA não poderão apenas contemplar aspectos técnicos, mas também precisarão estar atentos aos aspectos jurídicos, éticos, sociais, culturais e ambientais.

No segundo bloco, os trabalhos trataram de aspectos relacionados à interação entre Inteligência Artificial e os direitos fundamentais, abordando questões como personalidade jurídica, proteção de dados, ética algorítmica, direitos da personalidade, inclusão social, reconhecimento facial e riscos processuais no uso de IA na advocacia e na pesquisa jurídica. Foram analisados os desafios da ausência de atribuição de personalidade jurídica à inteligência artificial na reforma do Código Civil brasileiro, bem como a proteção de dados em holdings familiares a partir de uma análise comparativa entre a LGPD e o GDPR. Discutiu-se a ética em IA, com foco em transparência e justiça algorítmica, além da proteção jurídica dos ciborguêses e as complexas inter-relações entre direitos da personalidade e desenvolvimento tecnológico.

As discussões também abordaram a regulamentação da inteligência artificial na União Europeia, com destaque para a garantia de acesso pleno e igualdade para pessoas com deficiência, segundo o AI Act. Questões relacionadas ao reconhecimento facial nos estádios de futebol brasileiros também foram objeto de estudo, com ênfase nos riscos de criminalização seletiva e nos impactos sobre os direitos humanos nas arenas esportivas.

Por fim, os trabalhos exploraram os riscos jurídicos associados ao uso da inteligência artificial na advocacia e os posicionamentos dos tribunais brasileiros sobre a matéria, além de proporem uma análise teórica e recomendações práticas para a utilização metodologicamente adequada da IA comercial na pesquisa jurídica.

Felizes pela variedade de temas de pesquisa, os coordenadores do GT - INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL II convidam a todas e todos para a leitura na íntegra dos artigos.

Cinthia Obladen de Almendra Freitas – Pontifícia Universidade Católica do Paraná (PUCPR) – cinthia.freitas@pucpr.br

Eudes Vitor Bezerra – Universidade Federal do Maranhão (UFMA) – eudesvitor@uol.com.br

INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS EM HOLDINGS FAMILIARES: UMA ANÁLISE COMPARATIVA ENTRE A LGPD E O GDPR

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION IN FAMILY HOLDINGS: A COMPARATIVE ANALYSIS BETWEEN LGPD AND GDPR

Rodrigo de Paula Zardini [1]
Laila Millene Silva Ribeiro [2]
Messias Henrique Vieira Silva [3]

Resumo

A transformação digital tem impactado significativamente a gestão corporativa, e a inteligência artificial (IA) emerge como uma ferramenta essencial para a otimização de processos, incluindo a administração de dados pessoais em holdings familiares. Essas estruturas empresariais lidam com um grande volume de informações sensíveis, tornando a proteção de dados um fator estratégico. Nesse contexto, a conformidade com normativas como a Lei Geral de Proteção de Dados (LGPD), no Brasil, e o Regulamento Geral sobre a Proteção de Dados (GDPR), na União Europeia, torna-se essencial para garantir segurança jurídica e governança eficaz. Este estudo tem como objetivo analisar comparativamente a LGPD e o GDPR no contexto das holdings familiares que utilizam IA na gestão de dados pessoais. Para isso, foi adotada uma abordagem qualitativa, baseada na análise documental e na revisão de literatura. Os resultados evidenciam que ambas as legislações possuem princípios comuns, como transparência e segurança, mas diferem em aspectos como bases legais para o tratamento de dados e aplicação de sanções. Conclui-se que, embora cada normativa apresente desafios específicos, a conformidade regulatória pode ser vista como uma oportunidade estratégica para as holdings familiares, promovendo maior proteção e confiabilidade na gestão de dados.

Palavras-chave: Inteligência artificial, Holdings familiares, Lgpd, Gdpr, Proteção de dados

Abstract/Resumen/Résumé

Digital transformation has significantly impacted corporate management, and artificial intelligence (AI) emerges as an essential tool for optimizing processes, including the management of personal data in family holdings. These business structures handle a large volume of sensitive information, making data protection a strategic factor. In this context,

[1] Doutor em Gestão Urbana (PUC-PR), Mestre em Contabilidade (Fucape), graduado em Direito (UFG), especialista em Direito Tributário e Empresarial, professor, pró-reitor da UniCerrado, empresário e advogado.

[2] Graduanda em Direito pelo Centro Universitário de Goiatuba - UniCerrado

[3] Graduado em Matemática (UEG), mestre em Matemática (UFG) e doutorando em Ciência da Computação (UFU), pesquisa em inteligência artificial e leciona no ensino superior desde 2004.

compliance with regulations such as the General Data Protection Law (LGPD) in Brazil and the General Data Protection Regulation (GDPR) in the European Union becomes crucial to ensure legal security and effective governance. This study aims to conduct a comparative analysis of LGPD and GDPR in the context of family holdings that use AI to manage personal data. A qualitative approach was adopted, based on documentary analysis and literature review. The results highlight that both regulations share common principles, such as transparency and security, but differ in aspects such as legal bases for data processing and the application of sanctions. It is concluded that, although each regulation presents specific challenges, regulatory compliance can be seen as a strategic opportunity for family holdings, promoting greater protection and reliability in data management.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Family holdings, Lgpd, Gdpr, Data protection

1 INTRODUÇÃO

Nos últimos anos, a transformação digital tem redefinido a dinâmica da gestão corporativa, impulsionando o uso de tecnologias emergentes, como a inteligência artificial (IA), para aprimorar processos, otimizar a tomada de decisão e garantir maior eficiência operacional (Soares, 2024). No contexto das holdings familiares, essa evolução assume um papel estratégico, sobretudo na administração de dados pessoais e empresariais, visto que essas estruturas concentram um volume significativo de informações sensíveis. Para além dos dados financeiros e societários, as holdings familiares lidam com informações pessoais de seus membros, muitas vezes abrangendo múltiplas gerações de uma mesma família, o que demanda um alto nível de proteção e conformidade regulatória (Bandeira; Schiavi; Momo, 2023).

Nesse cenário, a proteção de dados tornou-se um elemento essencial para garantir privacidade, segurança jurídica e continuidade dos negócios. A inteligência artificial, por sua vez, surge como uma aliada poderosa nesse processo, permitindo além da automação de tarefas e a análise preditiva, a implementação de sistemas mais robustos de monitoramento e governança de dados (Berno; Peixe; Balsan, 2024). No entanto, sua adoção também impõe desafios regulatórios e éticos, sobretudo no que diz respeito ao equilíbrio entre inovação tecnológica e o cumprimento das normas de proteção de dados pessoais. Afinal, como garantir que a IA contribua para a gestão eficiente de dados sem comprometer a privacidade e a conformidade com legislações específicas?

No cenário jurídico global, duas normativas se destacam como referências na regulamentação do tratamento de dados pessoais: a Lei Geral de Proteção de Dados (LGPD), vigente no Brasil, e o Regulamento Geral sobre a Proteção de Dados (GDPR), da União Europeia (Brasil, 2018; European Union, 2016). Ambas possuem diretrizes robustas para assegurar transparência, segurança e respeito aos direitos dos titulares, mas apresentam diferenças significativas devido a aspectos culturais, econômicos e jurídicos dos contextos em que foram desenvolvidas. Assim, compreender essas diferenças é fundamental para empresas que operam em múltiplas jurisdições ou que buscam adotar boas práticas internacionais em proteção de dados.

Diante disso, este artigo tem como objetivo analisar comparativamente a LGPD e o GDPR no contexto das holdings familiares que utilizam inteligência artificial para a gestão de dados pessoais. A investigação busca identificar pontos de convergência e divergência entre as duas legislações, destacando como suas particularidades impactam o uso da IA nesse tipo de estrutura empresarial. Ainda, pretende-se discutir a conformidade regulatória como um

diferencial estratégico, demonstrando que a adoção de boas práticas de proteção de dados evita sanções legais e fortalece a governança e a reputação das holdings familiares.

Para alcançar esse objetivo, a pesquisa adotará uma abordagem qualitativa, com ênfase na análise comparativa das legislações e na revisão de literatura sobre proteção de dados e governança corporativa. O estudo também discutirá os desafios e oportunidades da implementação de IA nesse contexto regulado, fornecendo subsídios para profissionais e gestores que buscam conciliar inovação tecnológica e segurança jurídica.

2 METODOLOGIA

Este estudo adota uma abordagem qualitativa, utilizando a análise comparativa como método central para examinar as semelhanças e diferenças entre a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR), com foco na aplicabilidade dessas normas no contexto das holdings familiares. A escolha dessa metodologia se justifica pela necessidade de compreender os aspectos normativos das legislações e os desafios e oportunidades que elas apresentam para as empresas que operam sob essas regulamentações.

A análise comparativa é um método amplamente utilizado em pesquisas jurídicas e administrativas, pois permite identificar padrões, divergências e pontos de convergência entre diferentes sistemas normativos e organizacionais. De acordo com Sartori (1995), a comparação é um instrumento essencial para o desenvolvimento de conhecimento teórico e aplicado, pois possibilita uma visão mais aprofundada sobre os fenômenos estudados. Da mesma forma, Ragin (2014) destaca que a análise comparativa descreve diferenças e semelhanças e permite compreender as razões por trás dessas variações e seus impactos práticos.

Neste artigo, a comparação entre a LGPD e o GDPR foi realizada a partir de uma análise documental, considerando o texto legal de ambas as normativas e documentos interpretativos emitidos por órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil e o *European Data Protection Board* (EDPB) na União Europeia. Ainda, foram analisados estudos acadêmicos e relatórios institucionais que discutem a aplicação dessas normas no ambiente corporativo, com ênfase nas peculiaridades das holdings familiares.

A metodologia adotada permitiu identificar pontos de convergência, como a centralidade do consentimento, a exigência de transparência no tratamento de dados e a necessidade de mecanismos de governança robustos. Também foram observadas diferenças estruturais, como o nível de detalhamento das bases legais e a obrigatoriedade da nomeação de

um Encarregado de Proteção de Dados (DPO). Esses elementos foram analisados sob a perspectiva da governança corporativa, buscando compreender como cada regulamentação pode impactar a gestão de dados dentro das holdings familiares.

Ao longo da pesquisa, buscou-se garantir a fidedignidade das informações por meio da consulta a fontes primárias e secundárias confiáveis. A revisão bibliográfica teve um papel fundamental na contextualização da problemática, fornecendo embasamento teórico para a discussão e interpretação dos dados comparativos. Assim, este estudo traça um paralelo entre as legislações e, simultaneamente, propõe uma reflexão crítica sobre os desafios e oportunidades que cada uma oferece no contexto das holdings familiares.

3 HOLDINGS FAMILIARES E DADOS PESSOAIS: CONCEITO E CARACTERÍSTICAS

As holdings familiares ocupam um lugar de destaque no panorama econômico global, assumindo uma função estratégica na gestão e preservação do patrimônio familiar ao longo das gerações.

> Uma holding familiar caracteriza-se pela proteção do patrimônio familiar, bem como pelo sucesso da empresa que, em última instância, pertence à família. Sabe-se que a herança hereditária, seja na família ou empresarial, geralmente representando uma questão espinhosa dentro do núcleo familiar. Como veículo de sucessão empresarial, a holding familiar é uma opção de solução de disputas sucessórias, pois protege a continuidade da empresa ao permitir que os fundadores da empresa identifiquem seus sucessores (Silva; Junior, 2022, p. 109).

Essas entidades, por definição, são constituídas com o objetivo de centralizar e administrar os ativos de uma família, sejam eles empresariais, financeiros ou imobiliários. Ao contrário de outras formas societárias, as holdings familiares não visam somente a obtenção de lucro imediato, mas também a organização, proteção e perpetuação do patrimônio, promovendo uma governança estruturada que minimize conflitos internos e garanta a sustentabilidade dos negócios familiares (Marçal, 2020).

Entre as principais características das holdings familiares, destaca-se sua capacidade de oferecer uma estrutura legal que facilite o planejamento sucessório. Ao transferir a titularidade dos ativos para uma entidade jurídica, as famílias conseguem evitar os desafios e as incertezas que podem surgir em processos de inventário e divisão de bens. Adicionalmente, a centralização patrimonial permite maior controle sobre os investimentos, redução de custos administrativos e eficiência na gestão dos negócios (Ribeiro; Barroso; De Castro Queiroz, 2023). Contudo, essa centralização também acarreta um elevado volume de informações sensíveis que precisam ser adequadamente geridas e protegidas.

Os dados pessoais presentes nas holdings familiares incluem informações financeiras, como valores de investimentos e participações societárias, além de dados sensíveis sobre os membros da família, como informações de saúde, histórico educacional, relações pessoais e até preferências de consumo. Esses dados são fundamentais para a gestão estratégica do patrimônio, pois permitem que a holding personalize sua abordagem às necessidades de cada membro, otimize a alocação de recursos e tome decisões informadas (Magalhães; Silva; Aguiar, 2022).

Entretanto, a relevância da gestão de dados vai além do aspecto operacional. Em um mundo cada vez mais conectado, as holdings familiares estão expostas a riscos como vazamentos de dados, ataques cibernéticos e uso indevido de informações. A perda ou comprometimento de dados sensíveis pode ter consequências devastadoras financeiras e reputacionais (Silva, 2024). Por isso, é imprescindível que as holdings adotem políticas rigorosas de proteção de dados, garantindo a segurança das informações sob sua responsabilidade.

Outro ponto importante é o caráter intergeracional das holdings familiares, que as torna especialmente sensíveis à dinâmica de transformação digital. A inclusão de membros mais jovens, que frequentemente trazem uma mentalidade voltada para a inovação, exige que a gestão de dados acompanhe as tendências tecnológicas, mantendo-se alinhada às melhores práticas de segurança e conformidade. Por outro lado, os membros mais experientes podem demandar maior clareza e controle sobre como seus dados são utilizados, o que reforça a necessidade de políticas transparentes e inclusivas (Demeyer; Da Cruz; Barbosa; Quiraque, 2023).

A gestão de dados nas holdings familiares também se relaciona diretamente com questões legais e fiscais. A complexidade das regulações tributárias, tanto em nível nacional quanto internacional, exige que as informações sejam organizadas de forma precisa e atualizada, minimizando riscos de penalidades e facilitando a tomada de decisões estratégicas. Nesse sentido, a proteção de dados acaba se tornando mais que uma obrigação legal, se caracterizando como uma ferramenta para assegurar a eficiência e a longevidade da organização.

É essencial reconhecer que as holdings familiares não operam isoladamente. Elas frequentemente interagem com bancos, consultorias, advogados e outros prestadores de serviços que também têm acesso a dados sensíveis. Esse ecossistema exige uma abordagem colaborativa para a proteção de dados, onde cada parte envolvida compreenda sua responsabilidade na segurança das informações compartilhadas. A relevância da gestão de

dados nesse contexto transcende a dimensão tecnológica, tornando-se uma peça-chave para garantir a continuidade, a proteção e o sucesso dos negócios familiares em um ambiente cada vez mais complexo e regulado.

4 INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS: IMPACTOS E DESAFIOS DA IA NA SEGURANÇA E PRIVACIDADE DE INFORMAÇÕES

A inteligência artificial (IA) tem se consolidado como uma das tecnologias mais transformadoras da era digital, influenciando significativamente a forma como os dados são gerados, analisados e utilizados em diversos setores (Ribeiro, 2023). No contexto da proteção de dados, a IA assume um papel paradoxal: ao mesmo tempo em que oferece ferramentas poderosas para a segurança e o gerenciamento de informações, também levanta preocupações éticas, legais e técnicas relacionadas à privacidade e ao uso responsável de dados pessoais.

A principal contribuição da IA na proteção de dados está na sua capacidade de processar grandes volumes de informações em alta velocidade, identificando padrões e anomalias que poderiam passar despercebidos por métodos tradicionais (Smith, 2019). Tecnologias baseadas em aprendizado de máquina é um exemplo viável para ilustrar a detecção de atividades suspeitas, como tentativas de invasão, acessos não autorizados e comportamentos anômalos em sistemas corporativos. Ainda, a IA permite a automação de processos relacionados à governança de dados, como a classificação e categorização de informações sensíveis, reduzindo erros humanos e otimizando a conformidade com regulamentações (Cardoso, 2024).

Apesar desses avanços, o uso da IA na proteção de dados traz desafios significativos. Um dos principais é o risco de decisões automatizadas baseadas em dados pessoais, muitas vezes sem o conhecimento ou consentimento dos titulares. Essas decisões podem impactar diretamente a vida das pessoas, como em processos de seleção de crédito, análises de risco e até mesmo no monitoramento de comportamentos. Quando essas decisões são tomadas sem transparência, os titulares perdem o controle sobre suas próprias informações, comprometendo a privacidade e os direitos individuais (Bioni; Luciano, 2019).

Outro desafio importante está relacionado ao treinamento dos algoritmos de IA. Para que esses sistemas sejam eficazes, é necessário alimentá-los com grandes volumes de dados, muitas vezes pessoais ou sensíveis (Segundo, 2022). Esse processo, conhecido como "aprendizado supervisionado", pode expor informações a riscos, especialmente se os dados utilizados não forem devidamente anonimizados ou protegidos. Além disso, a qualidade dos dados é um fator crítico: dados incompletos, enviesados ou imprecisos podem levar a resultados distorcidos, reforçando desigualdades ou perpetuando discriminações (Ludermir, 2019).

A questão da segurança cibernética também ganha destaque no uso da IA. Embora essa tecnologia possa fortalecer a proteção contra ataques, ela também pode ser explorada por agentes mal-intencionados para desenvolver técnicas mais sofisticadas de invasão e roubo de dados. Um exemplo é o uso de IA para criar ataques cibernéticos personalizados, baseados no comportamento e nas vulnerabilidades específicas de um sistema ou organização. Nesse sentido, a evolução constante da IA exige uma abordagem proativa, onde a proteção de dados seja continuamente atualizada para enfrentar novas ameaças (Belli et. al., 2019).

Adicionalmente, a IA levanta preocupações éticas relacionadas à privacidade e à autonomia dos indivíduos. A coleta massiva de dados para treinar algoritmos pode comprometer a confidencialidade das informações, especialmente em casos onde os titulares não estão cientes do uso de seus dados ou não têm controle sobre como eles são processados (De Teffé, 2022). Isso é especialmente preocupante em contextos como o de holdings familiares, onde os dados envolvem tanto informações pessoais quanto empresariais, muitas vezes com implicações financeiras e estratégicas de longo alcance.

A governança de dados em ambientes que utilizam IA também apresenta desafios de responsabilidade. Quando uma decisão é tomada por um sistema automatizado, quem é responsável por eventuais erros ou violações de direitos? Essa questão se torna ainda mais complexa em contextos onde a IA é desenvolvida e implementada por terceiros, como fornecedores de software ou consultorias especializadas. Estabelecer mecanismos claros de *accountability* (prestação de contas) é fundamental para mitigar riscos e garantir a proteção de dados (Abrusio; Tonin, 2024).

Por fim, o uso de IA na proteção de dados exige um equilíbrio entre inovação e conformidade regulatória dados (Abrusio; Tonin, 2024). A tecnologia tem o potencial de transformar a maneira como organizações, incluindo holdings familiares, gerenciam suas informações, mas sua implementação deve ser acompanhada por políticas claras de privacidade, transparência e segurança. Investir em soluções de IA que respeitem os princípios éticos e os direitos dos titulares não se limita a uma mera questão de adequação legal, como também se caracteriza como uma estratégia para fortalecer a confiança e a reputação das organizações em um mundo cada vez mais digitalizado.

Esse panorama evidencia que, embora a inteligência artificial represente um avanço significativo para a proteção de dados, sua aplicação deve ser cuidadosamente planejada e monitorada. Apenas assim será possível aproveitar os benefícios dessa tecnologia enquanto se enfrentam os desafios associados à segurança e à privacidade de informações.

5 PANORAMA GERAL DA LGPD E GDPR

A proteção de dados pessoais tornou-se uma preocupação central no cenário global, especialmente com o aumento exponencial do volume de informações digitais e a complexidade das tecnologias que as processam. Nesse contexto, legislações como a Lei Geral de Proteção de Dados (LGPD), no Brasil, e o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* - GDPR), na União Europeia, surgem como marcos regulatórios essenciais para garantir direitos fundamentais à privacidade e à proteção de informações pessoais (European Union, 2016; Brasil, 2018). Ambas as legislações estabeleceram padrões robustos e abrangentes para o tratamento de dados, representando respostas legislativas a uma realidade cada vez mais digitalizada e interconectada.

A LGPD, instituída pela Lei nº 13.709/2018, entrou em vigor no Brasil em setembro de 2020, com o objetivo de regulamentar o tratamento de dados pessoais por pessoas físicas e jurídicas, públicas ou privadas (Brasil, 2018). Inspirada em grande parte pelo GDPR, a LGPD trouxe ao país um arcabouço legal que visa garantir transparência, segurança e respeito aos direitos dos titulares de dados.

Entre os principais aspectos da LGPD, destaca-se a definição clara de conceitos fundamentais, como dados pessoais, dados sensíveis e anonimização. Dados pessoais referem-se a qualquer informação que permita identificar uma pessoa, como nome, CPF, endereço ou informações digitais, enquanto os dados sensíveis incluem categorias específicas, como origem racial ou étnica, convicções religiosas e dados de saúde (Minghelli; Garcia, 2024). A anonimização, por sua vez, trata do processo de desvincular os dados da identidade do titular, reduzindo os riscos de identificação (Bioni, 2020).

Outro ponto relevante da LGPD é a delimitação das bases legais para o tratamento de dados, que incluem o consentimento explícito do titular, a execução de contratos, o cumprimento de obrigações legais, entre outras. Além disso, a lei estabelece direitos fundamentais para os titulares, como acesso às informações, correção de dados incorretos, revogação do consentimento e portabilidade dos dados para outros controladores (Silva; Falcão, 2024).

A LGPD também instituiu a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar o cumprimento da lei, regulamentar normas específicas e orientar as organizações quanto às melhores práticas de proteção de dados. A criação dessa entidade reforça a governança e a implementação efetiva da LGPD, garantindo maior segurança jurídica às partes envolvidas (Autoridade Nacional de Proteção de Dados, 2019).

Já no que diz respeito a estrutura e princípios do GDPR, que entrou em vigor em maio de 2018, representa um marco regulatório pioneiro e abrangente na União Europeia, estabelecendo um padrão global para a proteção de dados pessoais. Aplicável a todas as organizações que tratam dados de cidadãos europeus, independentemente de sua localização geográfica, o GDPR tem como foco central a proteção dos direitos individuais, a transparência e a responsabilidade das organizações (European Union, 2016).

Entre os principais aspectos do GDPR, destaca-se a sua abordagem baseada nos princípios da privacidade desde a concepção ("*privacy by design*") e da privacidade por padrão ("*privacy by default*"). Esses conceitos exigem que as organizações considerem a proteção de dados desde o início de qualquer projeto ou processo, garantindo que apenas os dados estritamente necessários sejam coletados e processados (Bandeira; Ferreira, 2024).

Assim como a LGPD, o GDPR define bases legais para o tratamento de dados, incluindo o consentimento, o cumprimento de obrigações legais e o interesse legítimo. No entanto, o GDPR impõe requisitos que podem ser considerados mais rigorosos para a obtenção de consentimento, que deve ser dado de forma livre, informada e inequívoca, além de poder ser facilmente revogado (De Teffé; Tepedino, 2020).

O regulamento também introduziu sanções severas para violações, com multas que podem atingir até 20 milhões de euros ou 4% do faturamento global anual da organização, o que for maior. Essa medida reforça a seriedade do cumprimento da legislação e incentiva as organizações a adotarem políticas robustas de proteção de dados (Forbici; Soares, 2023).

Embora a LGPD e o GDPR compartilhem diversos princípios e objetivos, como a proteção dos direitos dos titulares, a transparência e a segurança no tratamento de dados, existem diferenças importantes em sua aplicação e estrutura. Uma diferença significativa é a abrangência territorial. Enquanto o GDPR aplica-se a organizações fora da União Europeia que tratam dados de cidadãos europeus, a LGPD tem uma abordagem mais limitada, abrangendo apenas operações realizadas em território brasileiro ou relacionadas a dados coletados no Brasil. Ainda, nota-se distinções no que diz respeito ao rigor das penalidades. Embora a LGPD também preveja multas e sanções, os valores máximos são mais baixos do que os estipulados pelo GDPR. Adicionalmente, a LGPD estabelece prazos diferenciados para a adaptação das organizações, enquanto o GDPR entrou em vigor com uma abordagem mais imediata (Brasil, 2018; European Union, 2016).

Por outro lado, ambas as legislações destacam a importância da transparência, da prestação de contas e da adoção de medidas de segurança adequadas para proteger os dados pessoais. A presença de autoridades reguladoras, como a ANPD no Brasil e as autoridades de

proteção de dados na União Europeia, também reflete a convergência entre os dois marcos no que diz respeito à governança (Sarlet; Rodriguez, 2022).

Diante desse contexto, o panorama geral da LGPD e do GDPR evidencia o esforço global para regulamentar o tratamento de dados pessoais em um ambiente cada vez mais digital. Ambas as legislações representam avanços significativos na proteção dos direitos dos titulares e na promoção de boas práticas organizacionais. No entanto, suas diferenças estruturais e de aplicação refletem as particularidades culturais, econômicas e legais de cada região, o que torna essencial uma análise detalhada e contextualizada para compreender suas implicações práticas.

6 ANÁLISE COMPARATIVA ENTRE LGPD E GDPR

A Lei Geral de Proteção de Dados (LGPD), do Brasil, e o Regulamento Geral de Proteção de Dados (GDPR), da União Europeia, representam marcos regulatórios robustos que buscam assegurar a privacidade e a proteção de dados pessoais em suas respectivas jurisdições. Apesar de compartilharem objetivos semelhantes, como a valorização do consentimento e a promoção da transparência, essas legislações possuem detalhes que refletem as especificidades culturais, econômicas e jurídicas de cada contexto. A seguir, é possível verificar uma análise comparativa que explora os principais pontos de convergência e divergência entre as duas normas, abordando temas como bases legais para o tratamento de dados, direitos dos titulares, nomeação de encarregados, transferência internacional de dados e transparência em decisões automatizadas.

QUADRO 1 - Quadro Comparativo: LGPD x GDPR

ASPECTO	LGPD (BRASIL)	GDPR (UNIÃO EUROPEIA)
BASES LEGAIS PARA TRATAMENTO	Art. 7º: Consentimento, execução de contrato, obrigação legal, proteção à vida, tutela da saúde, entre outras.	Art. 6º: Consentimento, execução de contrato, obrigação legal, proteção de interesses vitais, entre outras.
CONSENTIMENTO	Art. 7º, I e Art. 8º: Deve ser livre, informado, inequívoco e revogável a qualquer momento.	Art. 6º, 1(a) e Art. 7º: Deve ser livre, específico, informado e explícito (para dados sensíveis).
DIREITOS DOS TITULARES	Art. 18: Acesso, correção, portabilidade, eliminação, anonimização, e oposição ao tratamento.	Art. 15 a 22: Acesso, retificação, eliminação, restrição, portabilidade, e objeção ao uso de dados.
NOMEAÇÃO DE ENCARREGADOS (DPO)	Art. 41: Obrigatória para determinadas condições, com	Art. 37 a 39: Obrigatória para organizações que tratam dados em

	atribuições gerais definidas pela ANPD.	larga escala, com atribuições detalhadas.
TRANSFERÊNCIA INTERNACIONAL	Art. 33 a 35: Permitida para países com nível adequado de proteção ou mediante cláusulas contratuais específicas.	Art. 44 a 50: Exige nível adequado de proteção ou salvaguardas, como cláusulas padrão da UE.
TRANSPARÊNCIA EM DECISÕES AUTOMATIZADAS	Art. 20: Direito de revisão humana em decisões automatizadas que impactem o titular significativamente.	Art. 22: Direito de não ser submetido a decisões automatizadas sem salvaguardas adequadas, salvo exceções.

Fonte: Brasil (2018); European Union (2016).

Tanto a LGPD quanto o GDPR definem as bases legais que legitimam o tratamento de dados pessoais, embora apresentem algumas diferenças no número e no detalhamento dessas bases. A LGPD estabelece dez bases legais, entre elas o consentimento (Art. 7º, I), o cumprimento de obrigações legais (Art. 7º, II), a execução de contratos (Art. 7º, V) e o legítimo interesse (Art. 7º, IX). A inclusão do "legítimo interesse" na LGPD é uma inspiração direta do GDPR, permitindo que organizações tratem dados sem o consentimento do titular, desde que comprovem que o tratamento é necessário e que não viola os direitos dos titulares.

Por sua vez, o GDPR lista seis bases legais (Art. 6º), com destaque para o consentimento (Art. 6º, 1(a)), a execução de contratos (Art. 6º, 1(b)) e o cumprimento de obrigações legais (Art. 6º, 1(c)). A principal diferença está no nível de detalhamento e nas condições adicionais impostas pelo GDPR, como a necessidade de avaliar e documentar o impacto das bases legais em certas situações.

Já em relação ao consentimento é possível afirmar que se trata de um pilar fundamental em ambas as legislações, mas o GDPR exige um padrão mais elevado, especialmente para dados sensíveis. No GDPR, o consentimento deve ser específico e explícito (Art. 6º, 1(a); Art. 7º), enquanto a LGPD permite consentimento inequívoco para dados pessoais comuns (Art. 8º), sendo explícito apenas para dados sensíveis (Art. 11).

Quanto aos direitos dos titulares, ambos os marcos regulatórios garantem direitos como acesso, correção e eliminação de dados. Na LGPD, esses direitos estão listados no Art. 18, enquanto no GDPR, aparecem nos Arts. 15 a 22. No entanto, o GDPR adiciona o direito à restrição de tratamento (Art. 18) e enfatiza a possibilidade de objeção ao uso de dados para marketing direto ou perfis automatizados (Art. 21), aspectos que, embora presentes na LGPD, são menos detalhados.

Sobre a figura do Encarregado de Proteção de Dados (*Data Protection Officer - DPO*), é correto mencionar que possui caráter obrigatório nas duas legislações, mas com algumas

diferenças na aplicação. Na LGPD, a nomeação de um DPO é obrigatória para organizações públicas e privadas que realizam tratamento em larga escala (Art. 41), exceto em casos regulamentados pela Autoridade Nacional de Proteção de Dados (ANPD). Por outro lado, o GDPR impõe essa exigência para qualquer organização que processe dados pessoais em larga escala ou dados sensíveis (Arts. 37 a 39). Ainda, o GDPR detalha as responsabilidades do DPO, incluindo a comunicação direta com as autoridades de proteção de dados e a supervisão das políticas de privacidade da organização. A LGPD, embora mencione as atribuições do DPO, deixa espaço para a regulamentação adicional pela ANPD.

No que diz respeito a transferência de dados pessoais para outros países, configura-se como uma ação regulada em ambas as legislações, mas o GDPR estabelece critérios mais rigorosos. O GDPR permite transferências apenas para países que demonstrem um nível adequado de proteção (Art. 45) ou mediante salvaguardas específicas, como cláusulas contratuais padrão aprovadas pela Comissão Europeia (Art. 46).

A LGPD segue uma abordagem semelhante, exigindo que o país receptor tenha um nível de proteção de dados adequado, reconhecido pela ANPD (Art. 33, I), ou que sejam utilizadas salvaguardas contratuais ou normativas (Art. 33, II e III). No entanto, a LGPD ainda depende de regulamentações adicionais para detalhar esses mecanismos.

Mais um ponto relevante a ser mencionado é a transparência em decisões automatizadas, que por sua vez vem gerando uma preocupação crescente, especialmente com o avanço da inteligência artificial. Tanto a LGPD quanto o GDPR garantem o direito de revisão humana em decisões automatizadas que impactem significativamente os titulares.

No GDPR, esse direito é mais explícito (Art. 22), incluindo a possibilidade de contestação de decisões baseadas em perfis automatizados, salvo em situações excepcionais, como a execução de contratos. A LGPD aborda o tema de forma mais genérica (Art. 20), mencionando o direito à explicação sobre critérios adotados em decisões automatizadas, mas sem detalhar mecanismos específicos.

A principal distinção entre a LGPD e o GDPR em relação às bases legais reside na quantidade e no grau de detalhamento. Enquanto a LGPD apresenta um número maior de bases legais, o GDPR exige um processo mais rigoroso para justificar a escolha da base adequada. Adicionalmente, a abordagem europeia impõe diretrizes mais restritivas para o uso do consentimento e do legítimo interesse, garantindo uma proteção mais robusta aos titulares.

7 DISCUSSÃO

A comparação entre a LGPD e o GDPR evidencia diferenças normativas, bem como a forma como cada legislação reflete o contexto socioeconômico e jurídico em que foi concebida. Para holdings familiares, que lidam com um alto volume de dados sensíveis relacionados à gestão patrimonial e sucessória, compreender essas particularidades não se trata somente de uma questão de conformidade regulatória, mas de uma necessidade estratégica para a proteção dos interesses da família e a continuidade dos negócios (Tassinari; Teixeira, 2021). Enquanto o GDPR se destaca pela previsibilidade e robustez de suas diretrizes, a LGPD oferece um cenário mais flexível, mas ainda em desenvolvimento, o que pode gerar desafios na interpretação e aplicação das normas.

Um dos aspectos mais sensíveis para essas estruturas é a necessidade de equilibrar proteção de dados e eficiência operacional. O GDPR, ao impor um controle mais rígido sobre o uso de dados, pode representar um obstáculo para a agilidade dos processos internos, exigindo auditorias constantes, documentação extensa e uma abordagem cautelosa na implementação de novas tecnologias. Por outro lado, essa rigidez oferece um grau maior de segurança jurídica, pois suas regras são amplamente detalhadas e já foram testadas em diversas situações práticas. No Brasil, a LGPD adota um modelo menos prescritivo em algumas áreas, permitindo maior margem de interpretação e adaptação às particularidades das organizações (De Morais, 2023). No entanto, essa flexibilidade pode ser um desafio para holdings familiares que buscam um direcionamento claro sobre a melhor forma de estruturar sua governança de dados.

O tratamento de dados automatizado, impulsionado pelo avanço da inteligência artificial, acrescenta outra camada de complexidade a essa discussão. Sistemas que analisam investimentos, monitoram transações financeiras ou até mesmo auxiliam na tomada de decisões estratégicas podem esbarrar em limitações impostas pelas duas legislações (De Oliveira, 2023). O GDPR estabelece diretrizes mais rígidas sobre decisões automatizadas, exigindo transparência e possibilidade de revisão humana, o que pode restringir o uso de certas tecnologias em processos internos. A LGPD, embora mencione a necessidade de explicação sobre decisões automatizadas, não detalha de forma tão aprofundada os mecanismos necessários para garantir essa transparência, o que pode gerar incertezas sobre o nível de proteção esperado no Brasil.

Além da regulamentação, outro fator determinante para a eficácia das normas é a capacidade de fiscalização e aplicação das sanções. A União Europeia possui órgãos reguladores com atuação consolidada e poder efetivo para impor multas expressivas, o que torna o cumprimento do GDPR uma prioridade para empresas que operam na região. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) ainda está em processo de fortalecimento,

e sua capacidade de fiscalização e imposição de penalidades será um fator crucial para definir o real impacto da LGPD. Para holdings familiares, isso significa que, embora a adequação à LGPD seja essencial, sua aplicação prática pode variar conforme a evolução da regulamentação e a postura da ANPD diante de eventuais infrações (Paulo, 2021).

Diante desse cenário, a escolha entre um modelo mais rígido ou mais flexível de proteção de dados não se resume a uma questão de conformidade, mas à forma como cada holding enxerga a gestão de riscos e a governança de suas informações. Empresas que operam internacionalmente ou possuem parcerias com investidores estrangeiros podem se beneficiar de um alinhamento mais próximo ao GDPR, garantindo um padrão elevado de proteção e facilitando a interoperabilidade com mercados globais. Já aquelas que atuam predominantemente no Brasil podem encontrar na LGPD uma abordagem mais adaptável, desde que sejam estabelecidos mecanismos internos para suprir eventuais lacunas regulatórias. De qualquer forma, o desafio maior não se limita a adequação de normas, mas na criação de uma cultura organizacional que reconheça a proteção de dados como um pilar estratégico para a segurança e a longevidade da estrutura patrimonial.

8 CONCLUSÃO

A proteção de dados tem se tornado um eixo central na governança corporativa, e a comparação entre a LGPD e o GDPR evidencia como diferentes abordagens regulatórias podem impactar a forma como as organizações lidam com essa questão. No contexto das holdings familiares, que frequentemente administram grandes volumes de informações sensíveis sobre seus membros e negócios, a conformidade com essas normas representa tanto um desafio quanto uma oportunidade para aprimorar práticas de gestão e segurança da informação.

O GDPR, ao estabelecer regras mais detalhadas e mecanismos rigorosos de controle, oferece um nível de previsibilidade e uniformidade que pode beneficiar holdings que operam em múltiplos países da União Europeia. No entanto, essa rigidez pode ser um obstáculo para empresas que necessitam de maior flexibilidade para adaptar suas operações às exigências regulatórias. Já a LGPD, embora inspirada no GDPR, apresenta nuances que permitem um grau maior de adaptação à realidade empresarial brasileira, especialmente pela possibilidade de regulamentações complementares emitidas pela ANPD. No entanto, essa mesma flexibilidade pode gerar incertezas, exigindo que as holdings acompanhem de perto os desdobramentos normativos e adotem posturas preventivas para evitar riscos futuros.

A crescente adoção de inteligência artificial e outras tecnologias de automação no tratamento de dados adiciona camadas adicionais de complexidade a esse cenário. A exigência

de transparência em decisões automatizadas, presente tanto na LGPD quanto no GDPR, demonstra a preocupação com a proteção dos titulares, mas também desafia as empresas a equilibrarem inovação e conformidade. Holdings familiares, que muitas vezes dependem de algoritmos para otimizar processos de governança e investimentos, precisam estar atentas para garantir que o uso dessas ferramentas respeite os princípios de privacidade e proteção de dados, sem comprometer sua eficiência operacional.

Diante desse panorama, o maior desafio para as holdings familiares não se limita a atender aos requisitos formais de cada legislação, mas em desenvolver uma cultura organizacional voltada para a governança de dados, na qual a proteção da privacidade seja integrada às estratégias de longo prazo. As perceptivas e reflexões acerca do cumprimento das normas deve ultrapassar a barreira da mera obrigação regulatória, abrangendo a discussão referente ao diferencial competitivo que fortalece a confiança de investidores, clientes e demais *stakeholders*.

Portanto, mais do que simplesmente garantir a conformidade com a LGPD ou o GDPR, as holdings familiares devem enxergar a proteção de dados como um investimento na sustentabilidade e credibilidade do negócio. A adoção de práticas transparentes e responsáveis tende a reduzir os riscos regulatórios e contribuir diretamente para a construção de um ambiente corporativo mais seguro e ético, capaz de se adaptar às mudanças constantes do cenário digital e regulatório.

REFERÊNCIAS

ABRUSIO, Juliana; TONIN, Chiara. **Inteligência artificial: desafios, regulação e governança**. Editora Senac São Paulo, 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD); MENEZES, Aline; CAMPELLO, André; ARAÚJO JUNIOR, Antônio; VILELA, Camila; GUIMARÃES, Daniel. **O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados**. Coord. Paloma Mendes Saldanha. Recife: SerifaFina, 2019. Cap. 9, p. 86.

BANDEIRA, Amanda de Oliveira; SCHIAVI, Giovana Sordi; MOMO, Fernanda da Silva. Competências do Profissional Contábil para Atuação no Processo de Transformação Digital: Percepções de Contadores de uma Holding Familiar do Sul do Brasil. **Pensar Contábil**, v. 25, n. 86, 2023.

BANDEIRA, Antônia Ladymilla Tomaz Caracas; FERREIRA, Jussara Suzi Assis Borges Nasser. A ATUAÇÃO DO DIREITO NA PRIVACIDADE DOS DADOS PESSOAIS. **Revista Acadêmica Escola Superior do Ministério Público do Ceará**, v. 16, n. 1, 2024.

BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; DA HORA, Nina; GASPAR, Walter B. **Cibersegurança [recurso eletrônico]:** uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio, 2023. 118 p.

BERNO, Adriana; PEIXE, Adriana Maria Miguel; BALSAN, Jorge. O USO DA INTELIGÊNCIA ARTIFICIAL NA GESTÃO DE DOCUMENTOS E DE DADOS. **P2P E INOVAÇÃO**, v. 11, n. 1, 2024.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**. São Paulo, ano, v. 21, p. 191-201, 2020.

BIONI, Bruno; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada**. Inteligência Artificial e Direito. São Paulo:** Thomson Reuters Brasil, p. 207-231, 2019.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 jan. 2025.

CARDOSO, Oscar Valente. **Inteligência Artificial, Direito e Processo**. Editora Dialética, 2024.

DEMEYER, M. A. F.; DA CRUZ, A. P. C.; BARBOSA, M. A. G.; QUIRAQUE, E. H. Relação entre controles formais e informais, transformação digital e desempenho de empresas com gestão familiar. **Revista de Gestão e Secretariado**, [S. l.], v. 14, n. 9, p. 16228–16244, 2023. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/2867. Acesso em: 23 jan. 2025.

DE MORAIS, Celso. **Desmistificando a LGPD: entenda como a Lei Geral de Proteção de Dados Pessoais pode ser aplicada no dia a dia das empresas e das pessoas**. Editora Dialética, 2023.

DE OLIVEIRA, Marcella Vaz Guimarães. Tratamento De Dados Pela Inteligência Artificial. **Revista Foco**, v. 16, n. 8, p. e2662-e2662, 2023.

DE TEFFÉ, Chiara Spadaccini. **Dados pessoais sensíveis:** qualificação, tratamento e boas práticas. Editora Foco, 2022.

DE TEFFÉ, Chiara Spadaccini; TEPEDINO, Gustavo. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83-83, 2020.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.** General Data Protection Regulation. Official Journal of the European Union, L119, 4 May 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em: 20 jan. 2025.

FORBICI, Fernanda; SOARES, Francyne Dos Passos. Revisão Integrativa: Adequação Dos Sistemas De Recomendação Às Exigências Impostas Pelas Leis De Proteção De Dados. **Anais do Seminário de Desenvolvimento, Conhecimento e Tecnologia**, n. 1, 2023.

LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Estudos Avançados**, v. 35, p. 85-94, 2021.

MAGALHÃES, Danilo Rocha; SILVA, Lays Eduarda Capistrano da; AGUIAR, Nathan Emmanuel Rodrigues Ramos de. Herança digital: a aplicabilidade do direito sucessório na esfera do direito digital. **Revista de Estudos Jurídicos,** v. 2, n. 32, 2022.

MARÇAL, Alba Karoline Matos. Holding familiar: uma alternativa de planejamento tributário e sucessório. **Caderno de Administração**, v. 14, n. 1, 2020.

MINGHELLI, Marcelo; GARCIA, Bárbara Balbis. Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. **Em Questão**, v. 30, p. e-138249, 2024.

PAULO, Matheus Adriano. **Aspectos Destacados da Legislação Brasileira e Europeia sobre Proteção de Dados:** uma análise comparativa dos Institutos da Cooperação Internacional, das Sanções Administrativas e do Controle Judicial na Proteção de Dados na União Europeia e no Brasil. Editora Dialética, 2021.

RAGIN, Charles C. **The comparative method:** Moving beyond qualitative and quantitative strategies. Univ of California Press, 2014.

RIBEIRO, Lucas Gomes; BARROSO, Marcelly Eduarda; DE CASTRO QUEIROZ, Rachel Tavora. Holding familiar como forma de planejamento sucessório. **LIBERTAS DIREITO**, v. 4, n. 2, 2023.

RIBEIRO, Márcio Vinicius Machado. **Inteligência artificial no Poder Judiciário**: ética e eficiência em debate. Editora CRV, 2023.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD): elementos para uma estruturação independente e democrática na era da governança digital. **Revista Direitos Fundamentais & Democracia**, v. 27, n. 3, p. 217-253, 2022.

SARTORI, Giovanni. **Comparative Constitutional Engineering**. An Inquiry into Structures, Incentives and Outcomes. In: Legal Studies Forum. 1995.

SEGUNDO, Hugo de Brito Machado. **Direito e Inteligência Artificial**: O que os Algoritmos têm a ensinar sobre Interpretação, Valores e Justiça. Editora Foco, 2022.

SILVA, Caroline Lima e. Crimes cibernéticos: uma análise jurídica acerca. In: FONTINA, Aline Souto; FERNANDES, Carlos Marcel Ferrari Lima; RIBEIRO, Thaysa Navarro de Aquino (orgs.). **Direito em Transformação – v. 3, parte 1**. Belo Horizonte: Editora Expert, 2024. p. 135.

SILVA, Danyel Berk Castro Costa; FALCÃO, Eliane Carvalho. ANÁLISE CONSTRUTIVO DA LEI GERAL DE PROTEÇÃO DE DADOS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 10, p. 5042-5064, 2024.

SILVA, Kevin Tenório Soares; JUNIOR, Marcondes da Silveira Figueiredo. Holding familiar. **Facit Business and Technology Journal**, v. 1, n. 39, 2022.

SMITH, Brian Cantwell. **A promessa da inteligência artificial:** acerto de contas e julgamento. Mit Press, 2019.

SOARES, Marta. O poder da inteligência artificial no mundo empresarial. **The Trends Hub**, n. 4, 2024.

TASSINARI, Simone; TEIXEIRA, Ana Carolina Brochado. Futuros possíveis para o planejamento sucessório. **Revista Brasileira de Direito Civil**, v. 29, n. 03, p. 101-101, 2021.