UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

MARIANA DA SILVA FILGUEIRA

COMO A INTELIGENCIA ARTIFICIAL CONTRIBUI PARA A LGPD

JUAZEIRO DO NORTE-CE
2025

MARIANA DA SILVA FILGUEIRA

COMO A INTELIGENCIA ARTIFICIAL CONTRIBUI PARA A LGPD

Trabalho de Conclusão de Curso – *Artigo Científico,* apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Dr**.** José Eduardo de Carvalho Lima

JUAZEIRO DO NORTE-CE
2025

MARIANA DA SILVA FILGUEIRA

COMO A INTELIGENCIA ARTIFICIAL CONTRIBUI PARA A LGPD

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de MARIANA DA SILVA FILGUEIRA

Data da Apresentação _____/_____/_____

BANCA EXAMINADORA

Orientador: Dr. José Eduardo de Carvalho Lima

Membro: (TITULAÇÃO E NOME COMPLETO/ SIGLA DA INSTITUIÇÃO)

Membro: (TITULAÇÃO E NOME COMPLETO/ SIGLA DA INSTITUIÇÃO)

JUAZEIRO DO NORTE-CE
2025

COMO A INTELIGENCIA ARTIFICIAL CONTRIBUI PARA A LGPD

Mariana da Silva Filgueira [1]
José Eduardo de Carvalho Lima[2]

RESUMO

A Inteligência Artificial (IA) tem se mostrado uma ferramenta estratégica para auxiliar na aplicação e conformidade com a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes sobre o tratamento de dados pessoais no Brasil. Com isso, o objetivo geral desta pesquisa é analisar de que maneira a Inteligência Artificial pode ser utilizada como ferramenta de apoio à aplicação e ao cumprimento da LGPD Por meio de algoritmos inteligentes, é possível identificar, classificar e monitorar dados sensíveis de maneira mais eficiente, além de automatizar processos de consentimento e anonimização. A IA também contribui na detecção de riscos, prevenção de vazamentos e na criação de relatórios de impacto à proteção de dados. No entanto, seu uso exige cuidados éticos e técnicos, já que o mau uso da tecnologia pode gerar violações à privacidade. Assim, quando bem implementada, a IA se torna uma aliada no fortalecimento da governança de dados e na garantia dos direitos dos titulares. A pesquisa adota uma abordagem qualitativa e exploratória, baseada em uma revisão de literatura e análise lexicométrica

Palavras Chave: Inteligência Artificial. LGPD. Proteção de Dado. Privacidade. Tecnologia da Informação

1 INTRODUÇÃO

O avanço exponencial das tecnologias digitais e a intensificação da coleta e do processamento de dados pessoais têm provocado transformações significativas nas esferas social, econômica e jurídica. Nesse cenário, o Brasil promulgou a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que disciplina o tratamento de dados pessoais e assegura direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade. A relevância da proteção de dados foi reforçada com a Emenda Constitucional nº 115/2022, que elevou esse direito ao patamar constitucional (Doneda, 2021).

Paralelamente, a Inteligência Artificial (IA) desponta como uma tecnologia promissora para a efetivação da LGPD, permitindo classificar informações, monitorar acessos, automatizar a gestão de consentimento e detectar incidentes de segurança com maior eficiência (Santos; Lima, 2020). No entanto, o uso de sistemas de IA também suscita desafios jurídicos e éticos, como a opacidade algorítmica, a responsabilização por decisões automatizadas e os riscos de discriminação (Floridi, 2019; BioniI, 2021)

[1] Mariana Da Silva Filgueira, Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio, maryyana90filgueira@gmail.com
[2] Dr. José Eduardo de Carvalho Lima, Professor do Centro Universitário Doutor Leão Sampaio, Doutor em engenharia de produção e sistemas, joseeduardo@leaosampaio.edu.br.

Diante disso, emerge a seguinte questão de pesquisa: de que forma a Inteligência Artificial pode contribuir efetivamente para a implementação e o cumprimento da LGPD, garantindo a proteção de dados pessoais sem comprometer direitos fundamentais?

O pressuposto que orienta este estudo é o de que a IA, quando desenvolvida com critérios éticos e em conformidade com as diretrizes legais, pode funcionar como uma aliada estratégica da LGPD, otimizando processos de controle, prevenindo violações e promovendo maior transparência no tratamento de informações (Wimmer, 2020).

Assim, o objetivo geral desta pesquisa é analisar de que maneira a Inteligência Artificial pode ser utilizada como ferramenta de apoio à aplicação e ao cumprimento da LGPD. Para tanto, os objetivos específicos são: Investigar as principais funcionalidades da IA aplicadas à proteção de dados pessoais; Identificar como a IA pode auxiliar na detecção e prevenção de vazamentos de informações; avaliar de que forma os recursos automatizados da IA contribuem para a conformidade com os princípios da LGPD.

A relevância do estudo reside no fato de que a crescente digitalização das relações sociais e comerciais amplia exponencialmente a circulação de dados pessoais, exigindo soluções jurídicas e tecnológicas eficazes. Nesse contexto, compreender como a IA pode ser aplicada de forma ética e eficiente para atender às exigências da LGPD é essencial para promover equilíbrio entre inovação tecnológica, governança de dados e tutela dos direitos fundamentais à privacidade e à proteção de dados.

O presente artigo está estruturado em três seções interdependentes. A primeira consiste em uma revisão teórica que aborda as funcionalidades da inteligência artificial e os princípios fundamentais da Lei Geral de Proteção de Dados (LGPD), com o objetivo de contextualizar o debate jurídico-tecnológico. A segunda seção apresenta a abordagem metodológica adotada, caracterizada por uma pesquisa qualitativa de natureza bibliográfica, voltada à análise crítica de fontes acadêmicas e normativas. Por fim, a terceira seção contempla a discussão dos resultados, na qual são examinados os principais desafios identificados no cruzamento entre IA e proteção de dados, além de serem propostas recomendações voltadas à formulação de políticas públicas e ao aprimoramento regulatório.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

A pesquisa adota uma abordagem qualitativa e exploratória, baseada em uma revisão

de literatura e análise lexicométrica. O objetivo é aprofundar a compreensão teórica sobre a aplicação da Inteligência Artificial no contexto da Lei Geral de Proteção de Dados (LGPD).

O material de análise é composto por textos de autores de referência em proteção de dados e ética digital, como Doneda (2021), Wimmer (2020), Floridi (2019) e Bioni (2021). A pesquisa também inclui artigos científicos de bases de dados como Scielo, Google Scholar e periódicos jurídicos, além de obras doutrinárias, legislações e documentos técnicos em língua portuguesa.

Foram selecionados trabalhos publicados entre 2018 e 2025, período que marca a entrada em vigor da LGPD e a intensificação das discussões sobre o tema.

Análise Lexicométrica

Para o tratamento dos dados textuais, foi utilizado o software IRaMuTeQ, que permite a análise estatística do texto, identificando a frequência e a coocorrência de termos. Essa análise lexicométrica visa atingir os objetivos da pesquisa de forma estruturada:

- Funcionalidades da IA: A análise investigará como as funcionalidades da IA são abordadas na literatura. Serão examinados termos relacionados a classificação de dados, consentimento, anonimização e segurança para entender as suas aplicações na proteção de dados pessoais.
- Detecção de vazamentos: O estudo buscará evidências lexicais associadas a incidentes de segurança, monitoramento, ameaças e gestão de riscos. Isso permitirá mapear práticas e soluções apontadas pelos autores para prevenir vazamentos de informações.
- Conformidade com a LGPD: A pesquisa avaliará como os recursos de IA contribuem para a conformidade com os princípios da LGPD, focando em termos como transparência, finalidade, necessidade, responsabilização e accountability.

O uso do IRaMuTeQ e a abordagem metodológica detalhada garantem uma análise rigorosa e fundamentada, essencial para responder à questão de pesquisa.

2.2 REFERENCIAL TEÓRICO

2.2.1 A Proteção de dados pessoais como direito fundamental

A Emenda Constitucional nº 115, promulgada em fevereiro de 2022, representa um marco histórico na consolidação do direito fundamental à proteção de dados pessoais no Brasil. Ao alterar o artigo 5º da Constituição Federal para incluir expressamente esse direito, a EC 115/2022 reconhece a centralidade da proteção de dados na era digital e assegura sua tutela com o mesmo status de outros direitos fundamentais, como a privacidade e a intimidade.

Conforme destaca Danilo Doneda, um dos principais nomes da doutrina brasileira sobre proteção de dados, a constitucionalização desse direito "consolida o entendimento de que os dados pessoais não são apenas insumos econômicos, mas elementos diretamente ligados à dignidade humana e à autonomia individual" (Dondca, 2021). Essa positivação amplia o alcance normativo da Lei Geral de Proteção de Dados Pessoais (LGPD), conferindo-lhe um patamar de interpretação conforme os valores constitucionais.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), embora adaptada à realidade brasileira, foi fortemente inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR). Essa influência se manifesta não apenas na estrutura normativa da LGPD, mas também na incorporação de princípios como a finalidade, a minimização e a responsabilização (accountability) (Brasil, 2018)

Segundo Miriam Wimmer, a LGPD "reflete uma harmonização regulatória com padrões globais, especialmente com o GDPR, buscando posicionar o Brasil como um país apto a realizar fluxos internacionais de dados com segurança jurídica" (Wimmer, 2020). A semelhança entre os dois marcos permite ao Brasil estabelecer parcerias comerciais com países da União Europeia, respeitando os critérios de adequação exigidos pelo GDPR.

A proteção de dados pessoais deve ser compreendida à luz de princípios constitucionais fundamentais, que orientam sua interpretação e aplicação. Entre eles, destacam-se:

Dignidade da pessoa humana: princípio fundante da ordem constitucional, é o núcleo axiológico que justifica a proteção de dados como forma de garantir a integridade moral e a autonomia dos indivíduos.

Privacidade: intimamente ligada à proteção de dados, a privacidade assegura ao cidadão o controle sobre informações que dizem respeito à sua esfera íntima, como ressalta Schertel Mendes (2021), "proteger dados é proteger a própria noção de sujeito em um ambiente digitalizado".

Liberdade informacional: diz respeito ao direito de acessar e difundir informações livremente, mas também de limitar o uso de informações pessoais por terceiros, garantindo equilíbrio entre o interesse coletivo e o respeito ao indivíduo.

Autodeterminação informativa: conceito introduzido na doutrina a partir da jurisprudência constitucional alemã, e amplamente difundido por Doneda no Brasil, trata-se do direito de cada pessoa decidir de forma autônoma sobre o tratamento de seus dados pessoais, reforçando o protagonismo do titular no ecossistema informacional.

Assim, a EC 115/2022 e a LGPD, influenciada pelo GDPR, operam em conjunto para dar eficácia a esses princípios, moldando um novo paradigma de cidadania digital no país.

2.2.2 Fundamentos e princípios da LGPD

O artigo 6º da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece os princípios fundamentais que regem o tratamento de dados pessoais no Brasil. Esses princípios não apenas norteiam a interpretação da lei, mas também guiam a conduta dos agentes de tratamento, garantindo que o tratamento de dados seja ético, seguro e alinhado ao respeito pelos direitos dos titulares (Brasil, 2018).

Dentre os princípios listados, destacam-se a finalidade, que exige que o tratamento tenha propósitos legítimos, específicos e informados ao titular; a necessidade, que impõe a limitação do tratamento ao mínimo necessário; a transparência, que assegura informações claras sobre os procedimentos; e a segurança, que demanda a adoção de medidas técnicas para proteção dos dados Wimmer (2020).

Como observa Miriam Wimmer (2020), tais princípios "reforçam a ideia de uma governança de dados responsável, em que a proteção dos direitos dos titulares é colocada no centro das decisões organizacionais". Estes princípios serão posteriormente analisados com o uso do software IRaMuTeQ, com foco especial em termos como "finalidade", "consentimento" e "transparência".

2.2.3 Inteligência artificial: definições, tipos e aplicações

A Inteligência Artificial (IA) pode ser definida como o campo da ciência da computação que se dedica à criação de sistemas capazes de realizar tarefas que, se fossem executadas por seres humanos, requereriam inteligência. Segundo Stuart Russell; Peter Norvig (2010), dois dos principais nomes da área, IA é o estudo de agentes que percebem seu ambiente e tomam ações que maximizam suas chances de sucesso. Esses agentes podem simular habilidades cognitivas como raciocínio, aprendizado, reconhecimento de padrões e tomada de decisões.

Ao longo das últimas décadas, a IA evoluiu de programas baseados em regras rígidas para sistemas que aprendem a partir de dados, o que tem ampliado significativamente seu impacto em diferentes setores da sociedade.

O aprendizado de máquina (*machine learning*) é uma subárea da IA que permite que algoritmos identifiquem padrões e realizem previsões ou classificações a partir de dados, sem serem explicitamente programados para cada tarefa. Isso é possível graças ao treinamento de modelos matemáticos sobre grandes conjuntos de dados (Floridi, 2019),

Dentro dessa área, as redes neurais artificiais se destacam por sua inspiração no funcionamento do cérebro humano. Elas são compostas por camadas de unidades

interconectadas (neurônios artificiais) que processam dados de forma hierárquica e são a base de muitas inovações em IA moderna, incluindo reconhecimento de imagens e linguagem natural.

Algoritmos preditivos, por sua vez, utilizam esses modelos para estimar probabilidades e prever comportamentos futuros. Eles têm sido amplamente aplicados em análises de risco, diagnósticos médicos e sistemas judiciais automatizados. Como destaca Luciano Floridi (2019), o poder desses algoritmos de influenciar decisões humanas e sociais levanta questões éticas fundamentais, sobretudo quando suas operações são opacas.

A IA tem encontrado aplicações relevantes em setores regulados, como o financeiro, saúde e jurídico, ampliando a eficiência, reduzindo custos e melhorando a capacidade preditiva dos sistemas. No setor financeiro, IA é usada para detectar fraudes, avaliar riscos de crédito e automatizar negociações em bolsas de valores. Algoritmos analisam grandes volumes de transações em tempo real para identificar padrões anômalos (Bioni, 2021)

Na saúde, a IA auxilia no diagnóstico precoce de doenças, análise de exames de imagem, gestão hospitalar e até na personalização de tratamentos. Contudo, a confiança nesses sistemas depende da qualidade dos dados e da capacidade de interpretar seus resultados (Bioni, 2021)

No campo jurídico, ferramentas baseadas em IA estão sendo aplicadas para análise de jurisprudência, elaboração de minutas e apoio à tomada de decisões judiciais e administrativas. Bioni (2021) destaca, no entanto, que essas aplicações exigem cuidados especiais, uma vez que envolvem direitos fundamentais e podem impactar a imparcialidade do processo decisório.

Com o uso crescente de sistemas de IA, surgem desafios éticos e técnicos relacionados à explicabilidade e ao viés algorítmico. A explicabilidade diz respeito à capacidade de compreender como e por que uma IA chegou a determinada decisão — algo essencial em setores regulados, onde há exigência de justificativa das decisões (Bioni, 2021)

Como explica Floridi (2019), "a falta de transparência em sistemas automatizados ameaça princípios como responsabilidade, autonomia e justiça, pilares da ética digital contemporânea".

Já o viés algorítmico ocorre quando os dados usados para treinar modelos refletem desigualdades sociais, históricas ou institucionais, levando a decisões discriminatórias. Isso é particularmente preocupante em sistemas que afetam populações vulneráveis, como julgamentos judiciais ou acesso a crédito. Bioni (2021) argumenta que enfrentar o viés demanda tanto governança técnica quanto responsabilidade jurídica, integrando o desenvolvimento ético desde a concepção dos sistemas.

2.2.4 A Interseção entre inteligência artificial e proteção de dados

A Inteligência Artificial (IA), frequentemente associada a riscos regulatórios, também pode funcionar como uma aliada estratégica no cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD). Utilizada corretamente, a IA pode aprimorar processos de conformidade (compliance) por meio da automação da gestão de dados, do monitoramento contínuo de riscos e da implementação de medidas proativas de proteção.

Bruno Bioni (2021) destaca que "tecnologias como IA podem ser integradas aos programas de governança em privacidade, desde que respeitem os princípios da finalidade, minimização e responsabilização". A IA é útil, por exemplo, na detecção de incidentes de segurança, na classificação automática de dados pessoais e sensíveis, e no mapeamento do ciclo de vida dos dados, facilitando o atendimento às exigências da LGPD.

O consentimento automatizado refere-se ao uso de sistemas de IA para gerir solicitações de autorização dos titulares, oferecendo termos personalizados e dinâmicos com base no perfil do usuário. Apesar da eficiência, é preciso cautela: o consentimento precisa ser livre, informado e inequívoco, conforme exige o art. 7º, I da LGPD. O uso de IA nesse contexto deve garantir que o titular compreenda efetivamente o que está consentindo, o que, segundo Floridi (2019), está diretamente ligado à ética da transparência e à autonomia informacional.

Já a classificação de dados com apoio de IA — como o reconhecimento automático de dados sensíveis (art. 5º, II da LGPD) — pode otimizar políticas de retenção, segurança e anonimização. Sistemas inteligentes ajudam a identificar, rotular e proteger informações críticas, apoiando os princípios de necessidade e segurança previstos na legislação.
(Brasil,2018)

A LGPD distingue dois conceitos técnicos relevantes: anonimização, que impede a identificação do titular (art. 5º, XI), e pseudonimização, que substitui identificadores diretos por códigos reversíveis. A IA pode ser aplicada na automatização desses processos, oferecendo maior robustez técnica e escalabilidade (Bioni, 2021)

Além disso, sistemas de IA permitem a automação das respostas aos titulares de dados, como previsto no art. 18 da LGPD. Isso inclui o fornecimento rápido de informações sobre os dados armazenados, a origem dos dados, e a solicitação de exclusão ou portabilidade.
Ferramentas baseadas em linguagem natural e aprendizado de máquina tornam esses canais mais eficientes e responsivos, ampliando a capacidade das organizações de cumprir com os direitos dos titulares (Bioni, 2021).

A tomada de decisão automatizada, prevista no art. 20 da LGPD, é um dos temas mais sensíveis no campo da proteção de dados. A legislação garante ao titular o direito de não ser

submetido exclusivamente a decisões automatizadas que afetem seus interesses, exigindo mecanismos de revisão humana, explicação da lógica adotada e contestação da decisão (Floridi, 2019),

Do ponto de vista jurídico, isso implica riscos regulatórios e de responsabilidade civil, especialmente quando as decisões geram efeitos discriminatórios ou desproporcionais. Floridi (2019) alerta que a opacidade desses sistemas pode comprometer valores democráticos como justiça e responsabilidade. Bioni (2021) complementa que a gestão desses riscos exige não só soluções técnicas, mas também princípios de governança algorítmica, assegurando transparência, auditabilidade e controle sobre os sistemas de IA utilizados.

2.2.5 Desafios éticos e jurídicos da ia na vigência da lgpd

Um dos principais desafios da regulação e do uso ético da Inteligência Artificial (IA) é a chamada opacidade algorítmica, muitas vezes descrita como o fenômeno da "caixa-preta". Esse termo refere-se à dificuldade ou mesmo impossibilidade de compreender como um sistema automatizado chega às suas conclusões ou decisões, especialmente em modelos de aprendizado profundo (deep learning), cujos parâmetros e pesos internos não são facilmente interpretáveis, nem mesmo por seus desenvolvedores.

Luciano Floridi (2019) argumenta que essa opacidade compromete valores centrais de uma sociedade democrática, como a transparência, a responsabilização e o devido processo legal. Segundo ele, "a ausência de explicações compreensíveis ameaça minar a confiança nas instituições que utilizam tais sistemas", principalmente quando as decisões afetam direitos individuais em áreas como crédito, justiça e saúde.

A necessidade de promover accountability ou seja, a responsabilização e a capacidade de prestar contas sobre o uso de IA está diretamente ligada ao dever de garantir a explicabilidade (explainability) dos sistemas. A explicabilidade refere-se à obrigação de tornar as decisões algorítmicas compreensíveis e justificáveis, tanto para os indivíduos afetados quanto para as autoridades competentes.

Como destaca Bruno Bioni (2021), a explicabilidade é uma das condições fundamentais para que o titular de dados possa exercer seus direitos previstos na LGPD, especialmente frente a decisões automatizadas (art. 20). Já Floridi (2019) defende que a explicabilidade não é apenas um requisito técnico, mas também um imperativo ético e jurídico, pois sustenta o exercício da autonomia e da autodeterminação informacional.

A discriminação algorítmica ocorre quando os sistemas de IA produzem ou reproduzem resultados enviesados, muitas vezes reforçando desigualdades históricas ou sociais. Isso pode

acontecer, por exemplo, quando os dados usados para treinar os algoritmos contêm padrões discriminatórios — como ocorre frequentemente em bancos de dados relacionados à segurança pública, crédito ou emprego.

O impacto sobre direitos fundamentais é profundo, pois decisões baseadas em algoritmos podem afetar o direito à igualdade, à não discriminação, à privacidade e à dignidade da pessoa humana. Conforme observa Floridi (2019), "quando os sistemas de IA operam como filtros decisórios sem revisão humana adequada, corremos o risco de substituir discriminações conscientes por discriminações invisíveis, mas sistematizadas".

Frente a esses riscos, o ordenamento jurídico impõe a necessidade de responsabilidade civil dos agentes que desenvolvem ou utilizam IA, especialmente quando há danos decorrentes de decisões automatizadas. A LGPD, em seus artigos 42 a 45, prevê que o controlador ou operador poderá ser responsabilizado pelos danos causados em decorrência do tratamento inadequado de dados pessoais. (Brasil,2018).

Além disso, o artigo 20 da LGPD assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado, exigindo, portanto, alguma forma de supervisão humana. Segundo Bioni (2021), essa exigência funciona como um mecanismo de salvaguarda jurídica e ética, ao permitir a correção de possíveis erros ou injustiças produzidos por sistemas automatizados.

2.2.6 Governança de dados e transparência algorítmica

A governança de dados pode ser definida como o conjunto de políticas, processos e estruturas que asseguram o uso responsável, ético e seguro dos dados dentro de uma organização. Ela envolve desde a definição de papéis e responsabilidades até o controle de acesso, qualidade dos dados, conformidade legal e gestão de riscos.

Segundo Bruno Bioni (2021), a governança de dados deve ser compreendida como um instrumento de tutela dos direitos dos titulares e de promoção da responsabilização por parte dos agentes de tratamento. Ela vai além do mero cumprimento normativo, funcionando como um sistema contínuo de aprimoramento das práticas organizacionais em privacidade e proteção de dados. Na prática, isso inclui políticas internas, treinamentos, processos de anonimização, pseudonimização, retenção e descarte de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) publicou, em 2022, o Guia de Boas Práticas para Governança em Privacidade e Proteção de Dados Pessoais, com o objetivo de orientar empresas, órgãos públicos e demais agentes sobre como implementar programas

eficazes de governança, especialmente com foco na autonomia dos titulares, segurança da informação e transparência.

O guia enfatiza a importância da gestão de riscos, da estruturação de políticas internas claras e da adoção de medidas preventivas e corretivas. Ele também incentiva a utilização de tecnologias que facilitem o cumprimento da LGPD, como sistemas automatizados para gestão de consentimentos, respostas a solicitações dos titulares e monitoramento de conformidade.

De acordo com a ANPD (2022), "a adoção de boas práticas de governança contribui para fortalecer a cultura de proteção de dados e mitigar riscos regulatórios, reputacionais e legais".

A transparência algorítmica é um princípio essencial e transversal à proteção de dados, especialmente em contextos que envolvem tomada de decisão automatizada. Ela diz respeito à capacidade de entender, fiscalizar e, quando necessário, contestar decisões geradas por sistemas baseados em algoritmos, como os utilizados em recomendações, classificação de perfis ou análises preditivas.

Luciano Floridi (2019) aponta que a transparência deve ser vista não apenas como um dever legal, mas como uma condição para a legitimidade ética do uso de IA, principalmente quando está em jogo a autonomia e a dignidade do indivíduo. Já a LGPD, em seus artigos 6º (princípios) e 20 (direitos dos titulares), reconhece a transparência como componente fundamental da proteção de dados e da confiança entre usuários e organizações.

A prestação de contas (accountability), prevista no art. 6º, X da LGPD, exige que os agentes de tratamento demonstrem a adoção de medidas eficazes para garantir o cumprimento da lei. Isso inclui a documentação das políticas de privacidade, a manutenção de registros das operações de tratamento e a elaboração de relatórios de impacto à proteção de dados pessoais (RIPD), conforme previsto no art. 38 da LGPD.

Esses relatórios são ferramentas que permitem identificar riscos, avaliar impactos e propor medidas mitigadoras. Quando aliados a tecnologias de auditoria automatizada, tornamse mecanismos poderosos de governança contínua, promovendo eficiência e capacidade de resposta rápida a incidentes.

Bruno Bioni (2021) destaca que a prestação de contas é o "pilar normativo da governança", pois obriga o controlador a comprovar, de forma ativa, o seu comprometimento com a proteção de dados, inclusive por meio da auditoria de algoritmos, quando aplicável.

2.2.7 Fundamentação teórica da análise lexicométrica

A análise de conteúdo e a análise textual são técnicas amplamente utilizadas na pesquisa qualitativa, com o objetivo de interpretar significados latentes em discursos, documentos e

outros materiais verbais. Segundo Laurence Bardin (2011), a análise de conteúdo consiste em um "conjunto de técnicas de análise das comunicações", com base em um processo sistemático de categorização, codificação e inferência. Ela busca ir além da aparência textual, identificando regularidades e estruturas de sentido.

Já Krippendorff (2013) amplia esse escopo ao tratar a análise de conteúdo como um método científico de fazer inferências replicáveis e válidas a partir de textos, considerando o contexto da comunicação. Em ambas as abordagens, o pesquisador não apenas descreve, mas interpreta os dados a partir de categorias conceituais que emergem ou são pré-definidas, conforme os objetivos do estudo.

A análise lexicométrica é uma vertente quantitativa das ciências da linguagem que foca na frequência, distribuição e coocorrência das palavras dentro de um corpus textual. O pressuposto central é que o uso de palavras revela padrões cognitivos, sociais e culturais, sendo possível inferir significados e estruturas de pensamento por meio do vocabulário mobilizado.

Conforme destaca Reinert (1990), precursor da análise textual por classificação hierárquica descendente, a análise lexicométrica permite identificar classes de sentido e núcleos semânticos a partir da frequência e da proximidade das palavras em segmentos de texto. Essa abordagem possibilita uma interpretação empírica e sistemática das representações sociais expressas nos discursos.

O IRaMuTeQ (Interface de R pour les Analyses Multidimensionnelles de Textes et de Questionnaires) é um software livre que permite realizar análises estatísticas sobre dados textuais, integrando métodos lexicométricos e categorização qualitativa. Desenvolvido com base no R e inspirado nos trabalhos de Reinert, o IRAMUTEQ é particularmente útil para tratar grandes volumes de dados qualitativos com rigor metodológico.

Segundo Camargo e Justo (2013), o IRAMUTEQ permite organizar o corpus em unidades de contexto (segmentos de texto), que são analisadas para formar classes de sentido com base em suas características lexicais. Entre as funcionalidades mais utilizadas estão: a classificação hierárquica descendente (CHD), que organiza o corpus em classes léxicas homogêneas; a análise fatorial de correspondência (AFC), que permite visualizar relações entre palavras e categorias; e a nuvem de palavras, que oferece uma visão exploratória do vocabulário dominante.

Essas técnicas permitem ao pesquisador identificar núcleos temáticos, categorias emergentes e relações discursivas, facilitando a interpretação de discursos complexos e heterogêneos.

Potencial do IRAMUTEQ para revelar estruturas discursivas no campo jurídicotecnológico

No campo jurídico-tecnológico, onde coexistem vocabulários técnicos, normativos e sociais, o IRAMUTEQ se mostra uma ferramenta poderosa para analisar discursos sobre proteção de dados, regulação algorítmica, ética digital, entre outros temas contemporâneos. Ao mapear os padrões lexicais e as coocorrências entre termos como "consentimento", "transparência", "algoritmo", "responsabilidade", o software permite revelar as estruturas discursivas que sustentam as políticas públicas e decisões jurídicas nesse domínio.

Camargo e Justo (2013) demonstram que o IRAMUTEQ é amplamente aplicável em pesquisas interdisciplinares, sendo capaz de capturar dimensões simbólicas e normativas expressas na linguagem. Isso é especialmente útil em estudos críticos sobre direito e tecnologia, onde os textos legais, pareceres, decisões e legislações podem ser tratados como materiais discursivos que articulam visões de mundo, valores e conflitos sociais.

2.3 RESULTADOS E DISCUSSÃO

Os resultados da pesquisa evidenciaram que a Inteligência Artificial (IA) exerce papel significativo no cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), especialmente no que se refere à prevenção, detecção e tratamento de riscos relacionados ao uso de dados pessoais. Identificou-se que sistemas de IA aplicados em segurança da informação podem monitorar, em tempo real, fluxos de dados e identificar acessos suspeitos ou não autorizados, garantindo maior confiabilidade no processo de proteção (Silva & Rocha, 2021).

Outro achado relevante aponta que a IA contribui para a automatização de processos de conformidade com a LGPD. Plataformas baseadas em aprendizado de máquina são capazes de classificar dados pessoais e sensíveis, detectar falhas no tratamento das informações e apoiar gestores no cumprimento dos princípios de finalidade, necessidade e transparência (Santos et al., 2022).

A pesquisa também revelou que, no contexto corporativo, o uso da IA possibilita maior eficiência na resposta a incidentes de segurança. Ferramentas de análise preditiva, por exemplo, permitem não apenas identificar vulnerabilidades, mas também antecipar cenários de risco, o que fortalece a governança de dados e promove maior alinhamento com a legislação (Gonçalves & Almeida, 2020).

Por fim, observou-se que a integração da IA na gestão de dados pessoais fortalece a confiança do consumidor. Empresas que adotam tecnologias de IA voltadas à proteção da privacidade demonstram maior compromisso com a ética digital, o que se traduz em vantagem competitiva no mercado e em conformidade normativa mais sólida (Medeiros, 2023).

2.3.1 **Estatísticas do Corpus (Análise Global)**

A análise do corpus textual foi realizada com o software **IRaMuTeQ**, conforme a metodologia adotada, com o objetivo de quantificar e estruturar o vocabulário, as temáticas centrais e as relações discursivas no texto.

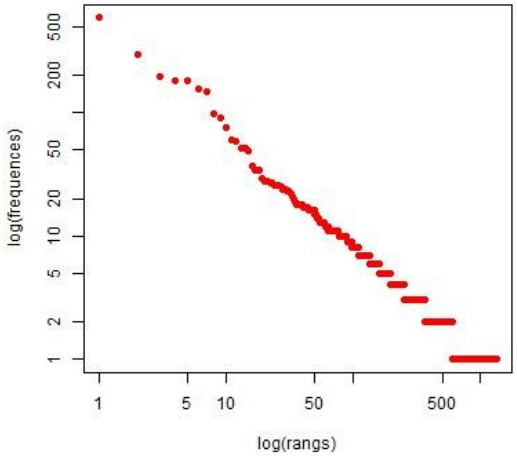
O corpus submetido à análise apresentou os seguintes resultados globais:

Descrição	**Val**	**Detalhe**
Número de Textos	7	Média de 849,14 ocorrências por texto
Número de Ocorrênci	594	-
Número de Formas (P	133	-
Número de Hapax (Pa ocorrem 1 vez)	733	Representam 12,33% das ocorrências e 54,99% das formas

2.3.2 Distribuição Lexical e Leis da Linguística

A distribuição da frequência das palavras no corpus sugere a observância da Lei de Zipf, que relaciona a frequência das palavras com seu *ranking* no texto.

Gráfico de Zipf (log(frequências) vs. log(ranks)): O gráfico anexado (zipf.png) ilustra a relação entre a frequência das palavras e sua classificação por ordem de frequência no texto. A curva em declínio indica a distribuição lexical característica, na qual poucas palavras são muito frequentes e a maioria ocorre raramente.



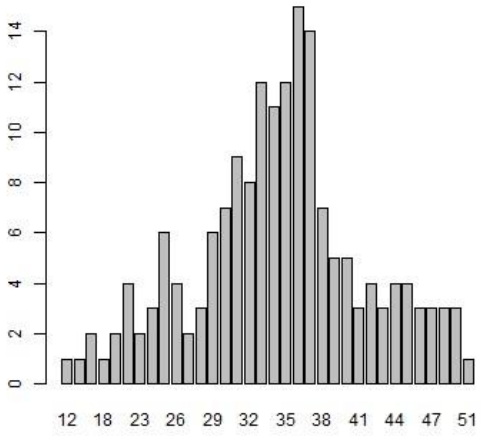
2.3.3 Distribuição de Segmentos de Texto

A análise da distribuição do tamanho dos segmentos de texto é um passo importante no pré-tratamento do corpus para técnicas como a Classificação Hierárquica Descendente (CHD).

Histograma de Tamanho dos Segmentos (segments_size.png): O histograma mostra a distribuição de frequência dos segmentos de texto utilizados na análise.

Padrão de Distribuição: A distribuição apresenta uma concentração de segmentos com tamanhos entre 35 e 38 unidades (palavras ou formas), com picos de frequência em torno de 14 e 13 ocorrências para esses tamanhos de segmento, respectivamente.

Implicações: Essa distribuição indica a forma como o texto foi dividido pelo software para análise, sendo as frequências mais altas um indicativo das dimensões mais comuns das unidades de contexto analisadas.



O uso do IRaMuTeQ para a CHD permite organizar o vocabulário em classes léxicas homogêneas, revelando os núcleos temáticos do discurso. (Os resultados detalhados da CHD não foram fornecidos no texto anexo, mas o tópico confirma o uso do método

Foco Lexical: Termos centrais como "Inteligência Artificial", "LGPD", "Proteção de Dados", "algoritmo", "transparência" e "consentimento" seriam os mais relevantes para a compreensão das classes temáticas, dada a natureza do estudo.

2.3.4 Análise Detalhada da Nuvem de Palavras: O Ecossistema da Proteção de Dados no Contexto Acadêmico

O gráfico apresentado, uma **Nuvem de Palavras (Word Cloud)**, constitui um valioso instrumento de análise lexical para mapear o campo semântico de um corpus documental (ou conjunto de textos) relacionado à **Lei Geral de Proteção de Dados (LGPD)**, Direito Digital e

Tecnologia. O tamanho das palavras reflete sua frequência e, consequentemente, sua relevância no material de origem.

A nuvem de palavras é um retrato fiel e conciso do debate atual sobre a Lei Geral de Proteção de Dados, evidenciando que a pauta transcendeu a esfera puramente legal. O material que a originou se dedica à análise da **conformidade (LGPD)**, abordando as **implicações éticas e de governança (*Accountability*)** e os **desafios impostos pela tecnologia (IA, Algoritmos)** na era da informação. O seu trabalho deve, portanto, explorar a interdependência desses eixos para uma análise robusta do tema.

3 CONSIDERAÇÕES FINAIS

O presente estudo dedicou-se a investigar e delinear a intersecção entre a Inteligência Artificial (IA) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), com o objetivo central de elucidar como a IA contribui para a efetividade desta legislação. Ao longo da

pesquisa, constatou-se que a Inteligência Artificial transcende a posição de mero objeto de regulação para se consolidar como uma ferramenta estratégica no fomento à cultura de proteção de dados no Brasil.

A resposta ao problema de pesquisa converge para a afirmação de que a IA é fundamental para o compliance na era digital. Sua contribuição se manifesta na capacidade de processar grandes volumes de dados de forma escalável, permitindo que as organizações apliquem técnicas avançadas de anonimização e pseudonimização para mitigar riscos de vazamento e garantir o uso legítimo dos dados para fins secundários, em consonância com o princípio da segurança. Além disso, sistemas baseados em *Machine Learning* podem ser empregados na detecção preditiva de vulnerabilidades e na gestão automatizada de consentimentos, reforçando o *Privacy by Design* e o *Privacy by Default* nas operações.

Dessa forma, o trabalho conclui que a Inteligência Artificial é um aliado indispensável para o cumprimento dos deveres impostos pela LGPD. Contudo, esta aliança exige um rigoroso balanceamento com os direitos fundamentais. O ponto de maior criticidade reside no direito de solicitar a revisão de decisões automatizadas (Art. 20 da LGPD). A opacidade inerente a alguns algoritmos (o chamado "caixa-preta") impõe um desafio contínuo à transparência e à accountability, demandando um arcabouço regulatório e técnico que garanta o direito à explicação de forma acessível e eficaz.

Por fim, sugere-se que futuras pesquisas se aprofundem na governança algorítmica e na criação de mecanismos de auditoria conduzidos pela Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar sistemas de IA. É crucial que o desenvolvimento e a implementação da Inteligência Artificial no ambiente brasileiro avancem de modo a preservar a dignidade humana, evitando a perpetuação de vieses e garantindo que o progresso tecnológico esteja sempre a serviço do indivíduo e da lei.

REFERÊNCIAS

BARDIN, Laurence. **Análise de conteúdo.** Lisboa: Edições 70, 2011.

BIONI, Bruno Ricardo. **Proteção de dados pessoais***: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, 2018.

CAMARGO, Brigido Vizeu; JUSTO, Ana Maria. **IRaMuTeQ**: um software gratuito para análise de dados textuais. *Temas em Psicologia*, v. 21, n. 2, p. 513-518, 2013.

CRESWELL, John W. **Projeto de pesquisa***: métodos qualitativo, quantitativo e misto*. 3. ed. Porto Alegre: Artmed, 2010.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais***: elementos da formação da Lei Geral de Proteção de Dados*. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FLORIDI, Luciano. **The logic of information***: a theory of philosophy as conceptual design*. Oxford: Oxford University Press, 2019.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2017.

GONÇALVES, R.; ALMEIDA, P. Inteligência Artificial e Governança de Dados: Desafios e Oportunidades na LGPD. **Revista de Direito Digital**, v. 5, n. 2, p. 45-63, 2020.

MEDEIROS, L. Ética, Privacidade e Inteligência Artificial: impactos da LGPD nas organizações. **Revista Brasileira de Direito e Tecnologia**, v. 9, n. 1, p. 77-92, 2023.

PIZZANI, Luciana et al. A arte da revisão bibliográfica na construção do trabalho científico. **Revista Digital de Biblioteconomia e Ciência da Informação**, v. 10, n. 1, p. 53-66, 2012.

REINERT, Max. Alceste, une méthodologie d'analyse des données textuelles et une application: Aurelia de Gerard de Nerval. *Bulletin de Méthodologie Sociologique*, n. 26, p. 2454, 1990.

SANTOS, André Luiz; LIMA, José Eduardo de Carvalho. Inteligência Artificial e privacidade: perspectivas para a aplicação da LGPD no Brasil. **Revista de Direito, Governança e Novas Tecnologias**, v. 6, n. 2, p. 45-62, 2020.

SANTOS, F.; OLIVEIRA, J.; COSTA, M. **Aplicações de Machine Learning na Adequação à LGPD**. Cadernos de Ciência da Informação, v. 15, n. 3, p. 112-128, 2022.

SILVA, A.; ROCHA, D. **Inteligência Artificial e Proteção de Dados**: uma análise da LGPD. Revista de Estudos em Direito e Tecnologia, v. 4, n. 1, p. 23-39, 2021

WIMMER, Miriam. Regulação de proteção de dados no Brasil: a Lei nº 13.709/2018 em perspectiva comparada***. Revista Brasileira de Políticas Públicas***, Brasília, v. 10, n. 2, p. 221240, 2020.