Inteligência Artificial e Privacidade: Os desafios do *Privacy by Design*

Tainã Dias da Silva[1]

Patrícia Martinez Domingues[2]

Resumo: o presente artigo visa abordar os desafios de garantir o *Privacy by Design* no desenvolvimento de sistemas com o uso de inteligência artificial, incluindo a IA generativa, tendo em vista o avanço crescente desta tecnologia e a necessidade de expandir as análises prezando pela garantia da privacidade e pelo fomento da inovação. A metodologia utilizada baseou-se na coleta de informações bibliográficas, de artigos científicos e legislações. Por meio desta metodologia, foi possível analisar a importância de se considerar aspectos de proteção de dados pessoais em IA, de forma a incorporar a privacidade no seu desenvolvimento e, assim, antecipar a aplicação de medidas mitigatórias de riscos aos titulares de dados, inclusive em relação a não-discriminação e à necessidade de transparência no tratamento dos dados. Portanto, o objetivo deste artigo é contribuir com reflexões necessárias para que o avanço tecnológico não represente um retrocesso, no que tange à previsão do direito à privacidade como um direito fundamental previsto na Constituição Federal Brasileira.

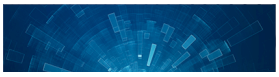
Palavras-chave: inteligência artificial; LGPD; privacidade; privacidade por design.

Artificial Intelligence and Privacy: The Challenges of Privacy by Design.

Abstract: This article aims to delve into the complexities of integrating Privacy by Design principles into the development of artificial intelligence systems, including generative AI. Driven by the rapid advancement of these technologies, this investigation underscores the necessity of enhancing evaluations that simultaneously promote the safeguarding of privacy and the encouragement of innovation. The investigative approach adopted herein is grounded in a compilation of bibliographical sources, encompassing both scholarly publications and pertinent legislative documents. Through this methodology, it was possible to analyze the importance of integrating personal data protection considerations into AI development processes. This integration aims to proactively embed privacy safeguards and implement risk mitigation strategies for data subjects, addressing potential issues of discrimination and necessitating transparency in data utilization practices. Therefore, this article aspires to foster pivotal discourse, ensuring that

[1] Graduada em Direito, advogada, pós-graduada em Compliance pelo Ibmec-SP, atua na área de Privacidade e Proteção de Dados Pessoais em projetos de diagnóstico, implantação e monitoramento de Programas de Privacidade em empresas com diferentes ramos de negócios. tainadiasds@gmail.com.br.

[2] Graduada em Direito, advogada, pós-graduada em Direito Administrativo pela PUC Minas, atua na área de Privacidade e Proteção de Dados Pessoais, em projetos de diagnóstico e adequação às legislações de privacidade. patricia.martinezdomingues@gmail.com.



technological progress does not undermine privacy rights, as enshrined in the Brazilian Federal Constitution, thereby affirming privacy as an inalienable fundamental right.

Keywords: artificial intelligence; LGPD; privacy; privacy by design.

1. INTRODUÇÃO

A Inteligência Artificial (IA) tem se estabelecido como uma das mais significativas revoluções tecnológicas do século XXI, redefinindo as fronteiras entre a capacidade humana e máquina. Com avanços contínuos em capacidade computacional, algoritmos e disponibilidade de grandes volumes de dados, a IA está sendo integrada em uma variedade crescente de setores, transformando profundamente o cenário econômico, social e tecnológico.

Atualmente, a IA permeia diversos setores, desde o financeiro e de saúde, até a educação e o entretenimento, demonstrando sua versatilidade e capacidade de adaptação a diferentes necessidades e contextos. Em finanças, por exemplo, algoritmos de IA são utilizados para detectar padrões de fraude em transações em tempo real, uma aplicação que se tornou indispensável no combate ao crime financeiro. No setor de saúde, a IA contribui para diagnósticos mais precisos e rápidos, através da análise de grandes volumes de dados médicos, melhorando o prognóstico e tratamento de doenças complexas como o câncer. No campo educacional, sistemas inteligentes oferecem personalização do aprendizado, adaptando conteúdos e métodos de ensino às necessidades individuais dos estudantes.

A adoção da IA não está restrita apenas a grandes corporações. Pequenas e médias empresas também estão implementando soluções baseadas em IA, para aumentar a eficiência e a competitividade. A capacidade da IA de processar e analisar grandes quantidades de dados, de forma mais célere em comparação aos humanos, amplia seu valor, não apenas em termos de eficiência operacional, mas também na geração de insights para inovação e estratégia.

Além disso, a IA está no centro da quarta revolução industrial, frequentemente referida como Indústria 4.0, integrando tecnologias digitais nas fábricas e automatizando processos que antes dependiam inteiramente de intervenção humana.

A onipresença da IA na vida cotidiana (SANTAELLA, 2023) levanta importantes questões sobre a ética e a privacidade, fundamentais para a aceitação e o sucesso contínuo desta tecnologia. A capacidade da IA de coletar, analisar e armazenar enormes quantidades de dados pessoais tem suscitado preocupações sobre como esses dados são usados, quem tem acesso a eles e como são protegidos.

O potencial de uso indevido de IA para vigilância, discriminação e outros fins prejudiciais destaca a necessidade de abordagens regulatórias e de desenvolvimento que priorizem a proteção dos direitos individuais. Nesse sentido, o compromisso com a privacidade e a proteção de dados pessoais é essencial para garantir que o desenvolvimento da IA não apenas avance tecnologicamente, mas que também esteja alinhado com os valores e normas sociais, assegurando um progresso equilibrado e justo.

A privacidade é um direito fundamental expressamente protegido por diversas legislações ao redor do mundo, incluindo a Constituição Federal Brasileira. Em um mundo cada vez mais digitalizado, onde informações pessoais são constantemente coletadas, processadas e armazenadas por sistemas de IA, a necessidade de proteger esses dados torna-se imperativa. A proteção de dados pessoais não apenas resguarda a privacidade individual, mas também fortalece a confiança na forma como as instituições gerenciam as informações.

A era da informação intensificou a exposição a riscos relacionados à privacidade, desde vazamentos de dados até usos indevidos que podem resultar em discriminação ou manipulação. Com a integração crescente da IA em serviços essenciais, como saúde, educação e segurança, a vulnerabilidade dos indivíduos aumenta, tornando premente a implementação de mecanismos robustos de proteção de dados.

Além de uma questão ética, a proteção de dados é também um imperativo estratégico para empresas e governos. Organizações que demonstram capacidade de proteger os dados de seus clientes e usuários não somente cumprem com suas obrigações legais, mas também ganham vantagem competitiva, aumentando a confiança do público em seus serviços. A conformidade com normativas de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, e o General Data Protection Regulation (GDPR) na União Europeia, consiste, atualmente, em componente crucial das estratégias de negócios e governança.

Este cenário impulsiona a discussão sobre a importância da implementação do conceito de *Privacy by Design* (PbD), que enfatiza a integração da privacidade desde o início do desenvolvimento tecnológico. Este artigo visa explorar os desafios de incorporar o PbD em sistemas de IA, buscando um equilíbrio entre inovação tecnológica e a proteção de direitos fundamentais, com foco particular na garantia da privacidade, conforme previsto na Constituição Federal Brasileira.

Sob esta perspectiva, o presente trabalho busca identificar os principais desafios técnicos e éticos relacionados à integração do conceito de *Privacy by Design* em tecnologias de IA; propor métodos e estratégias para a implementação efetiva de práticas de privacidade desde o início do desenvolvimento de sistemas baseados em IA; analisar o impacto das legislações de proteção de dados, como a LGPD e o GDPR, na conformidade e inovação tecnológica; e fomentar uma discussão sobre como a tecnologia de IA pode ser desenvolvida e utilizada de maneira responsável, assegurando a proteção dos direitos fundamentais dos indivíduos.

Com essa abordagem, o artigo busca contribuir para um entendimento mais aprofundado sobre como a privacidade pode ser incorporada ao processo inovativo, garantindo que o avanço tecnológico esteja harmonizado com a proteção de dados pessoais.

2. FUNDAMENTAÇÃO TEÓRICA

A compreensão dos conceitos basilares de Inteligência Artificial (IA), bem como das questões relacionadas à privacidade e proteção de dados pessoais, é essencial para avaliar os desafios impostos pelo *Privacy by Design* (PbD) no desenvolvimento de sistemas de IA. Esta seção explora as bases teóricas necessárias para uma análise criteriosa do tema.

Iniciaremos com uma revisão dos conceitos e evolução da IA, com ênfase especial na IA generativa, que representa uma das fronteiras mais avançadas e controversas da tecnologia atual. Em seguida, discutiremos os princípios fundamentais da privacidade e proteção de dados, essenciais para compreender as implicações legais e éticas associadas ao tratamento de dados pessoais. Por fim, abordaremos o conceito de *Privacy by Design*, detalhando sua origem, princípios e aplicação prática no contexto da IA.

Este arcabouço teórico fornecerá a base necessária para explorar como a privacidade pode ser integrada desde a concepção de sistemas automatizados, alinhando avanços tecnológicos com a proteção dos direitos fundamentais dos indivíduos.

2.1 CONCEITOS DE INTELIGÊNCIA ARTIFICIAL

No estudo da inteligência artificial (IA) é crucial entender as definições e a evolução histórica da tecnologia; suas classificações; e as metodologias específicas através das quais ela opera. Assim, este segmento do artigo explora as definições e a trajetória histórica da IA, estabelecendo uma base para a compreensão das diferentes categorias de IA: Focada, Generalizada e Superinteligente. Seguindo essa classificação, discutiremos as nuances do Aprendizado de Máquina, Aprendizado Profundo e IA Generativa.

2.1.1 DEFINIÇÕES E EVOLUÇÃO DO CONCEITO DE IA

A Inteligência Artificial (IA) tem sido definida e explorada de várias maneiras ao longo das décadas, refletindo seu desenvolvimento e evolução contínua. Faz parte

do campo da ciência da computação, dedicado ao desenvolvimento de sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana.

As raízes da IA remontam ao meio do século vinte, quando Alan Turing, um matemático britânico, propôs a ideia de uma máquina capaz de simular qualquer processo de raciocínio humano, que mais tarde evoluiu para o moderno conceito de computador. Turing sugeriu o conceito agora conhecido como "Teste de Turing", que se tornou um marco fundamental no campo da inteligência artificial. Este teste propõe o seguinte critério, para avaliar a inteligência de uma máquina: se ela conseguir convencer um humano de que é também um humano, então deve ser considerada "inteligente". (LUDERMIR, 2021).

Nos anos seguintes, em 1956, o termo "inteligência artificial" foi formalmente adotado na Conferência de Dartmouth, organizada por John McCarthy, Marvin Minsky, Allen Newell e Herbert A. Simon. (SANTAELLA, 2023). Esses pioneiros viam a IA não apenas como uma imitação da inteligência humana, mas como uma nova forma de inteligência que poderia ser construída e melhorada continuamente. Os trabalhos de Minsky e McCarthy, em particular, focavam em programas que podiam resolver problemas e raciocinar, estabelecendo a base para o que se conhece hoje como "IA clássica".

John Haugeland, em 1985, descreveu a IA como “O novo e interessante esforço para fazer os computadores pensarem... máquinas com mentes, no sentido total e literal” (HAUGELAND, 1985). Esta visão destaca a ambição inicial de equiparar a capacidade de processamento da máquina com a cognição humana.

Adicionalmente, Ray Kurzweil, em 1990, ofereceu uma definição mais pragmática da IA como “A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas.” (KURZWEIL, 1990). Esta descrição enfatiza a funcionalidade e a utilidade da IA, sugerindo uma abordagem focada em replicar e ampliar capacidades humanas específicas através de tecnologia.

A revolução do aprendizado de máquina começou nos anos 90, impulsionada pelos avanços em redes neurais, que foram fortemente influenciadas pelos trabalhos de

Geoffrey Hinton e Yann LeCun. Esses modelos, que imitam o funcionamento do cérebro humano para processar informações, representaram um avanço significativo, pois permitem que os sistemas de IA aprendam diretamente dos dados, ajustando-se e melhorando com a experiência.

No início do século 21, a ascensão de grandes volumes de dados e o aumento da capacidade de computação permitiram que a IA se desenvolvesse a uma velocidade sem precedentes. Autores como Andrew Ng e Pedro Domingos foram fundamentais na popularização de algoritmos de aprendizado de máquina e na exploração de suas aplicações práticas, de reconhecimento facial a sistemas autônomos de condução.

Hoje, a IA continua a evoluir, com pesquisas focadas em inteligência artificial geral (AGI), buscando criar sistemas que possam realizar qualquer tarefa intelectual que um ser humano faria.

Essas diversas perspectivas demonstram não apenas a complexidade da IA, mas também a profundidade de seu impacto potencial em diversos campos do conhecimento e da atividade humana.

2.1.2 TIPOS DE INTELIGÊNCIA ARTIFICIAL (IA FOCADA, IA GENERALIZADA E IA SUPERINTELIGENTE)

Após estabelecer as bases conceituais e históricas da Inteligência Artificial, torna-se fundamental explorar os diversos tipos de IA. A classificação da Inteligência Artificial pode ser entendida por meio de três categorias principais: IA Focada, IA Generalizada e IA Superinteligente. Essas categorias ajudam a ilustrar a evolução da tecnologia e suas potenciais capacidades.

A IA Focada, conhecida como IA Fraca, é caracterizada pelo uso de algoritmos especializados que são desenvolvidos para resolver problemas específicos em áreas bem definidas. Sistemas como os sistemas especialistas, que simulam o julgamento e o comportamento de um humano ou grupo de humanos com expertise específica em uma determinada área, e sistemas de recomendação, projetados para sugerir itens, produtos ou serviços aos usuários com base em suas preferências e

comportamentos anteriores, exemplificam essa categoria. Esses tipos de sistemas são dotados de uma grande quantidade de dados e são habilidosos na execução de tarefas complexas, mas restritas ao contexto para o qual foram criados. (LUDERMIR, 2021).

Por outro lado, a IA Generalizada, frequentemente referida como IA Forte, é conceitualmente definida como um tipo de IA que pode executar qualquer tarefa intelectual que um ser humano pode fazer. Esta definição implica que a IA Generalizada possui a capacidade de raciocínio, planejamento, aprendizado, percepção e comunicação em níveis humanos ou até superiores, em uma ampla gama de contextos, não apenas em tarefas específicas. (LUDERMIR, 2021).

Embora haja avanço em muitos campos específicos da IA, como processamento de linguagem natural e visão computacional, essas tecnologias ainda operam dentro de domínios restritos e são incapazes de exibir a flexibilidade e o amplo entendimento que caracterizariam a IA Generalizada. Em muitos casos, o que se observa são sistemas de IA altamente avançados que podem superar humanos em tarefas específicas, mas que ainda dependem fortemente de condições controladas e conjuntos de dados limitados para funcionar.

A categoria mais avançada, e ainda teórica, é a IA Superinteligente, que descreve uma futura geração de algoritmos que superariam significativamente as capacidades humanas em praticamente todas as tarefas. (LUDERMIR, 2021). Até o momento, a IA Superinteligente permanece um conceito hipotético, sem implementações reais, e está envolvida em debates intensos sobre sua viabilidade e as implicações éticas de sua possível existência.

As categorias expostas não apenas diferenciam os níveis de desenvolvimento e aplicabilidade da IA, mas também ajudam a moldar as discussões sobre as implicações éticas, os desafios regulatórios e as futuras direções de pesquisa e desenvolvimento no campo da Inteligência Artificial.

2.1.3 APRENDIZADO DE MÁQUINA, APRENDIZADO PROFUNDO E INTELIGÊNCIA ARTIFICIAL GENERATIVA

Após abordar os diferentes tipos de Inteligência Artificial, torna-se essencial explorar os subcampos específicos que estão definindo o curso atual da tecnologia: o aprendizado de máquina, o aprendizado profundo e a inteligência artificial generativa. Esses conceitos representam as fronteiras mais avançadas da tecnologia de IA e são fundamentais para compreender as capacidades e os desafios da aplicação prática da IA.

O aprendizado de máquina (machine learning) é um subcampo da IA que permite que sistemas aprendam e façam inferências ou decisões a partir de dados sem serem explicitamente programados para cada tarefa. Essa aprendizagem pode ocorrer de forma supervisionada, não supervisionada ou por reforço. Tal capacidade de aprendizado é realizada através de algoritmos que podem processar e aprender de grandes quantidades de dados. (SHARIFANI; AMINI, 2023).

Subcategoria do aprendizado de máquina, o aprendizado profundo (*deep learning*) utiliza redes neurais artificiais com muitas camadas – daí o termo "profundo". Esta tecnologia tem sido particularmente transformadora, pois as redes neurais profundas são capazes de captar padrões complexos e nuances em grandes conjuntos de dados, muito além do que é possível com técnicas mais tradicionais de aprendizado de máquina. O aprendizado profundo revolucionou campos como o processamento de linguagem natural e o reconhecimento visual, permitindo avanços significativos em aplicações como assistentes de voz e sistemas autônomos de condução. (SHARIFANI; AMINI, 2023).

A inteligência artificial generativa, por sua vez, representa uma fronteira avançada no campo da IA, em que sistemas são especificamente desenvolvidos para criar conteúdos novos que podem ser indistinguíveis dos criados por humanos. Esta capacidade de gerar dados inovadores abre um vasto leque de possibilidades em diversas áreas, citando-se como exemplo a criação de imagens artísticas, músicas, textos e vozes sintéticas.

Um dos exemplos mais notáveis da aplicação de IA generativa está na criação de obras de arte visuais. Programas equipados com essa tecnologia podem produzir

pinturas que refletem estilos de artistas reconhecidos, ou mesmo desenvolver estilos completamente novos, que desafiam as fronteiras tradicionais da expressão artística. Na música, algoritmos de IA generativa compõem peças que podem variar de simples melodias a complexas composições sinfônicas. No campo da escrita, a IA generativa pode produzir textos em uma variedade de gêneros.

Esses sistemas são treinados com vastas quantidades de textos humanos, para então emular estilos de escrita específicos ou produzir conteúdo inédito. Similarmente, as tecnologias de geração de voz sintética estão se tornando cada vez mais avançadas, permitindo a criação de vozes que não apenas soam naturalmente humanas, mas também carregam emoções e entonações variadas, adequadas para usos em assistentes virtuais e personagens de videogames.

Dentre as técnicas mais eficazes do subcampo da IA generativa estão as redes generativas adversariais (GANs). Este modelo inovador utiliza duas redes neurais em um arranjo de competição: uma rede geradora, que cria imagens, sons ou textos, e uma rede discriminadora, que avalia a autenticidade do conteúdo gerado. A rede geradora aprende continuamente a partir do feedback da discriminadora, refinando suas produções para torná-las cada vez mais convincentes. (BRUNO; GOMES, 2023). Este processo, em que a competição leva a melhorias contínuas através de um ciclo de tentativas e erros, simula uma forma de evolução natural dentro do ambiente de dados.

A capacidade de gerar conteúdo novo tem implicações profundas, não apenas em termos de potencial criativo, mas também nos aspectos éticos e de segurança. Questões sobre direitos autorais, autenticidade e a ética de criar conteúdos que podem influenciar opiniões ou comportamentos humanos são cada vez mais pertinentes. Conforme a tecnologia continua a evoluir, será crucial implementar diretrizes que garantam que essas ferramentas sejam usadas de maneira responsável e ética.

Os avanços na Inteligência Artificial ultrapassam as barreiras técnicas, levantando questões profundas e complexas sobre ética na IA e os riscos de seu mal uso. À medida em que as máquinas adquirem capacidades de “pensar”, de maneiras antes

vistas como exclusivamente humanas, intensificam-se os desafios de integrar essas tecnologias de maneira responsável.

A exploração desses conceitos de IA pavimenta o caminho para uma discussão mais aprofundada sobre privacidade de dados e como o *Privacy by Design* pode ser incorporado como uma salvaguarda e como um princípio orientador, desde o início do desenvolvimento tecnológico.

2.2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O crescimento da IA tem gerado discussões no que tange à privacidade e proteção de dados pessoais, tema este de relevância em um contexto Global de grande uso de informações que possuem características de dados pessoais e expansão tecnológica.

Dessa forma, com relação à privacidade e a proteção dos dados pessoais, algumas legislações surgiram com o objetivo de proteger o titular de dados, em destaque à legislação brasileira, Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018), que foi inspirada no Regulamento Geral de Proteção de Dados - RGPD (ou do inglês *General Data Protection* - GDPR) no contexto da União Europeia.

A LGPD, conforme dispõe no art. 1°, Lei 13.709/2018, tem por "objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", por meio da regulamentação do tratamento de dados pessoais. Ademais, a LGPD estabelece diretrizes para promover a transparência do tratamento aos titulares de dados e fomentar o tratamento responsável.

Para reforçar ainda mais a importância do direito à proteção de dados pessoais, este foi incluso no rol de direitos e garantias fundamentais através da Emenda Constitucional n° 115, de 2022, fixando a competência privativa da União para legislar sobre a proteção e tratamento de dados pessoais, além de reforçar a importância desta temática diante do avanço tecnológico.

Portanto, nesse contexto da privacidade e proteção de dados pessoais como direito fundamental e considerando os esforços legislativos para mitigar riscos relacionados à proteção dos dados, é importante ressaltar que o avanço da tecnologia não deve ocorrer em detrimento da proteção dos dados, e sim buscar equilíbrio, dada a importância de ambos os temas. Porém, a definição de equilíbrio dentro de um contexto de constante evolução de tecnologias e respeito à privacidade, além das responsabilidades envolvidas sob o viés social, representa um grande desafio (JIMENE, 2021).

Nesse contexto, é imperioso integrar o *privacy by design* no desenvolvimento de tecnologias, como na aplicação da IA, em busca de não haver conflitos que representem desiquilíbrio no tratamento dos dados frente à proteção ao titular do dado.

2.3. PRIVACY BY DESIGN

O *Privacy by design* é uma metodologia criada por Ann Cavoukian, nos anos 90, com o fim de proteger a privacidade do titular de dados pessoais, de forma a considerar padrões de proteção de dados desde o início do desenvolvimento de serviços e sistemas.

A criação dessa metodologia por Ann Cavoukian foi motivada, conforme citado por Jimene (2021):

> [...] pela convicção de que o avanço das tecnologias cada vez mais interconectadas permitiriam a coleta ilimitada de dados pessoais e que apenas a existência de leis não seria o suficiente para garantir a privacidade do usuário, sendo necessário encorajar as empresas que concebessem produtos e serviços a partir dessa metodologia, incorporando a privacidade em todos os seus projetos de tecnologia.

Dessa forma, a privacidade deve ser considerada desde o início do ciclo de vida do dado, ou seja, durante toda a jornada do tratamento de dados pessoais que, como bem conceitua a Lei 13.709/2028, em seu art. 5°, inciso X, o tratamento é:

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Em 2009, Ann Cavoukian escreveu um artigo consolidando o *privacy by design* com sete princípios, quais sejam: Proativo não reativo, preventivo não corretivo; Privacidade por padrão; Privacidade embarcada no Design; Funcionalidade integral; Segurança de ponta a ponta – proteção em todo ciclo de vida do dado; Visibilidade e Transparência; e Respeito à privacidade do usuário. Nesse artigo, Ann Cavoukian (2009) defende a incorporação por padrão da Privacidade em todo processo, conforme citado a seguir:

> Privacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives.

Dada a introdução sobre a metodologia do *privacy by design,* cabe elucidar cada um dos sete princípios.

2.3.1 Proativo não reativo, preventivo não corretivo

O objetivo do princípio Proativo não reativo, preventivo não corretivo, como o próprio nome prediz, é ser proativo, com o fim de evitar que ocorram eventos invasivos de privacidade, ou seja, prezar pela antecipação das ações necessárias para o fomento da privacidade e proteção dos dados (CAVOUKIAN, 2009).

Não se deve esperar que um risco de privacidade seja materializado e nem que uma infração ocorra, para que soluções sejam oferecidas (CAVOUKIAN, 2009). A privacidade desde a concepção de um serviço e/ou sistema é essencial para que a prevenção ocorra, assim considerar a avaliação de riscos dentro de uma organização é uma aliada na antecipação.

2.3.2 Privacidade por padrão

O princípio da privacidade por padrão também é conhecido como *Privacy by default* e preza pela ausência de necessidade de intervenção do usuário, para que a privacidade do titular seja configurada/considerada (CAVOUKIAN, 2009), assim deve haver transparência para o titular sobre o tratamento dos dados pessoais.

Como preceitua Ann Cavoukian (2009) "No action is required on the part of the individual to protect their privacy – it is built into the system, by default". Portanto, ações como a transparência, a minimização de dados e o alinhamento da coleta dos dados com a finalidade do tratamento são essenciais para a configuração padrão da privacidade.

2.3.3 Privacidade embarcada no Design

O princípio da privacidade embarcada no design considera que toda a arquitetura e design de um sistema e/ou serviço devem prever a privacidade (CAVOUKIAN, 2009), ou seja, todo ambiente do sistema e todo o desenvolvimento de um serviço deve refletir a segurança para que o tratamento seja realizado visando a proteção dos dados.

Práticas antes realizadas devem ser reinventadas em busca de alternativas aceitáveis ao contexto de privacidade, assim revisões e análises de riscos de privacidade em padrões e estruturas são fundamentais para a mitigação de riscos (CAVOUKIAN, 2009).

2.3.4 Funcionalidade integral

O princípio da funcionalidade integral considera que os interesses e objetivos legítimos devem ser considerados de forma que não haja um embate entre a privacidade e a segurança, pelo contrário, que ambos sejam considerados (CAVOUKIAN, 2009).

Nesse contexto, Jimene (2021) comenta que:

> O princípio da funcionalidade integral – também conhecido como princípio ganha-ganha – é baseado na premissa de que as funcionalidades da aplicação tecnológica não poderão ter suas capacidades reduzidas, pois, evidentemente, o usuário seria sobremaneira prejudicado.

Portanto, as funcionalidades não podem ser prejudicadas se aplicadas medidas técnicas de privacidade e vice-versa. As soluções devem buscar o equilíbrio para que o titular não tenha prejuízo com as escolhas.

2.3.5 Segurança de ponta a ponta – proteção em todo ciclo de vida do dado

Como o nome sugere, a segurança deve ser considerada em todo o ciclo de vida do dado, ou seja, desde a sua coleta até o seu fim (CAVOUKIAN, 2009). Assim, as melhores práticas de proteção aos dados pessoais devem ser aplicadas.

A ausência de medidas técnicas de Segurança é um impeditivo para que a privacidade seja fomentada, segundo Ann Cavoukian, 2009, “without strong security, there can be no privacy”. Portanto, segurança e privacidade devem andar juntas para assegurar a privacidade do titular.

2.3.6 Visibilidade e transparência

O princípio da visibilidade e transparência busca garantir que todo interessado em verificar se as operações estão ocorrendo da forma como foram descritas pela organização, tenha direito de fazer a verificação, estabelecendo assim uma relação de confiança, mas também de responsabilização (CAVOUKIAN, 2009).

A confiança em toda relação é primordial e é isso que o princípio da visibilidade e transparência promove. Portanto, esse princípio visa garantir que o titular de dados pessoais tenha clareza sobre o tratamento dos seus dados para que assim gere maior responsabilidade e confiança.

2.3.7 Respeito à privacidade do usuário

O princípio à privacidade do usuário fomenta que os interesses dos titulares de dados pessoais devem ser respeitados (CAVOUKIAN, 2009), ou seja, as expectativas dos titulares devem ser atendidas durante todo o processo de tratamento do dado.

A partir do momento que o interesse do titular é considerado, há a materialização do seu empoderamento. A capacidade do titular exercer de forma ativa os seus interesses e necessidades com a gestão dos seus próprios dados geram melhores resultados, conforme defendido por Ann Cavoukian (2009).

3. IA E DESAFIOS DA PRIVACIDADE

À medida em que a Inteligência Artificial se torna mais integrada em diversos setores da sociedade, emergem desafios significativos relacionados à privacidade e à proteção de dados pessoais. A capacidade das tecnologias de IA de coletar, analisar e utilizar grandes volumes de dados levanta questões críticas sobre a segurança e o uso ético dessas informações.

Enquanto a IA oferece oportunidades sem precedentes para melhorias em eficiência e inovação, ela também traz consigo a responsabilidade de gerenciar riscos potenciais que podem afetar a privacidade dos indivíduos e a integridade de suas informações pessoais.

Um dos riscos no uso de IA é a dificuldade em dar transparência sobre como a tecnologia gerou determinadas saídas de informações que por vezes podem estar contaminadas por viés discriminatório, fator gerador de impacto negativo ao titular. Ademais, a ausência de transparência dificulta com que os titulares tenham poder de controle sobre os seus dados, podendo ser um impeditivo no exercício de seus direitos. Nesse sentido, Patrícia Peck e Helen Batista (2022) dispõem que

> […] according to data protection laws, companies must provide specific information to data subjects relating to the logic behind automated decision-making that has a legal impact on them, which turns out to be a complex obligation to fulfil, as the decisions made by AI algorithms frequently cannot be anticipated.

Depreende-se que a imprevisibilidade de uma tomada de decisão por meio do uso de IA dificulta o cumprimento do direito previsto no art. 20, § 1°, da Lei 13.709/2018, qual seja, o fornecimento de informações claras sobre os critérios e procedimentos abarcados por uma decisão automatizada.

Outro aspecto relevante a ser analisado como um dos desafios da privacidade na IA é o fato de que a eficácia dos modelos de IA está diretamente relacionada à coleta de grandes volumes de dados, visto que quanto mais dados, mais "inteligente" o modelo se torna, entendendo os padrões comportamentais e gerando informações mais específicas em suas decisões. Dessa forma, para que o sistema de IA seja capaz de performar, este necessita ser treinado por meio de um grande conjunto de dados (CENTRE FOR INFORMATION POLICY LEADERSHIP; HUNTON ANDREWS KURTH, 2020) e, nesse contexto, o princípio da não discriminação dos dados deve ser respeitado.

O grande volume de dados é comumente utilizado por IA generativa para que novos dados sejam gerados. Nesse sentido, espera-se que até 2025 a IA generativa represente 10% de todo dado produzido, conforme estudo realizado pelo Gartner (2021). Porém, ao gerar novos dados, informações antes confidenciais podem vir a ser expostas, como, por exemplo, dados considerados sensíveis pela LGPD.

Neste contexto, é essencial explorar como a privacidade pode ser incorporada ao longo de todo o processo de desenvolvimento de sistemas baseados em IA. Assim, a adoção do conceito de *Privacy by Design* é crucial para assegurar que a privacidade seja considerada desde as fases iniciais de concepção de qualquer projeto de IA.

3.1 INCORPORAÇÃO DA PRIVACIDADE NO DESENVOLVIMENTO DE IA

A incorporação da privacidade no desenvolvimento de tecnologias de Inteligência Artificial é uma abordagem que exige atenção meticulosa, desde as primeiras etapas de design, até a implementação e operação dos sistemas. Este processo de *Privacy by Design* (PbD) envolve a integração de práticas de proteção de dados em todos os aspectos do ciclo de vida da tecnologia de IA.

Do ponto de vista regulatório, os desenvolvedores de IA devem estar em conformidade com leis de proteção de dados, como o GDPR, na União Europeia, e a LGPD, no Brasil. Conforme será visto adiante neste trabalho, essas legislações exigem que as práticas de privacidade sejam incorporadas nos sistemas de IA, demandando transparência nas operações, com o objetivo de proporcionar aos usuários maior controle sobre seus dados pessoais.

Sob a perspectiva técnica, um dos principais desafios na incorporação da privacidade em IA envolve a minimização de dados, ou seja, garantir que apenas os dados necessários para uma função específica sejam coletados e armazenados. Este conceito é enfatizado por autores como Daniel Solove e Woodrow Hartzog, que argumentam que a minimização de dados não apenas protege a privacidade dos usuários, mas também reduz potenciais danos em casos de vazamentos de dados. (HARTZOG; SOLOVE, 2022).

Os autores ponderam que a minimização de dados é crucial tanto para a proteção da privacidade quanto para a segurança dos dados. Além de impedir a criação desnecessária de dados, o princípio da minimização de dados exige sua destruição após o cumprimento de sua finalidade, alinhando-se, assim, com os requisitos regulatórios. Enquanto a segurança foca na proteção e integridade dos dados, garantindo, por exemplo, que apenas pessoas autorizadas tenham acesso aos dados, a privacidade lida com as políticas substanciais de retenção, uso e eliminação de dados. Sob este panorama, os escritores enfatizam que legislações deveriam priorizar a minimização de dados com a mesma intensidade dedicada às normas de segurança, visto que ambos os conceitos, embora distintos, convergem para fortalecer a proteção dos dados e alcançar objetivos comuns. (HARTZOG; SOLOVE, 2022).

Assim, a implementação prática dessa abordagem requer métodos sofisticados para determinar quais dados são realmente necessários e como eles podem ser processados de forma a manter sua utilidade para os sistemas de IA.

Além da minimização, a anonimização e a pseudonimização de dados representam estratégias cruciais para proteger informações pessoais. Essas técnicas alteram os dados de modo que a identidade do indivíduo não possa ser facilmente ligada às informações, mas sem comprometer a integridade dos dados para o processamento de IA. A anonimização remove definitivamente qualquer identificador que possa ser usado para rastrear a informação de volta ao usuário, enquanto a pseudonimização substitui identificadores pessoais por pseudônimos, permitindo uma análise mais segura.

O artigo 12, caput, e §1º, da Lei Geral de Proteção de Dados Pessoais (LGPD), trata da anonimização de dados pessoais e dispõe sobre os critérios que determinam quando esses dados deixam de ser considerados "pessoais" sob a lei, e, portanto, não estão sujeitos às obrigações da LGPD. O texto legal aponta que os dados anonimizados podem voltar a ser considerados dados pessoais se o processo de anonimização puder ser revertido. A reversão pode ocorrer de duas maneiras: usando meios próprios, ou seja, se a entidade que detém os dados pode reverter a anonimização usando suas próprias ferramentas e recursos, sem a necessidade de informações adicionais; ou com esforços razoáveis, que inclui considerar o custo, o tempo necessário e as tecnologias disponíveis para realizar a reversão.

O artigo 12, §1º, da LGPD, especifica que para determinar o que é considerado um "esforço razoável", deve-se levar em conta fatores objetivos, como o custo e o tempo necessários para reverter o processo de anonimização, utilizando as tecnologias disponíveis. A avaliação de "esforços razoáveis" é fundamental porque estabelece um limite prático entre dados verdadeiramente anonimizados e aqueles que ainda podem, de algum modo, ser ligados a indivíduos, se forem empregados recursos suficientes.

A relevância da anonimização é destacada na Lei nº 13.709/2018, pois esse processo exclui a aplicabilidade da legislação sobre dados pessoais aos dados tratados desta forma. Essencialmente, ao anonimizar dados, as obrigações e restrições legais que normalmente se aplicariam ao tratamento de dados pessoais deixam de ser exigíveis, removendo as proteções e responsabilidades previstas na lei.

José Luiz de Moura Faleiros Júnior e Guilherme Magalhães Martins (2021) expõem a problemática envolvendo a falta de clareza quanto à delimitação dos processos de anonimização, e destacam a necessidade de revisões periódicas das técnicas de ciência da computação, a fim de delimitar o que seria reversível ou não, em termos de aplicação do instituto:

> As conclusões fundamentais extraídas dessa análise, evidentemente, impõem considerar a diferença semântica entre "dados anônimos" e "dados anonimizados". Os primeiros sequer foram considerados pela lei; os segundos são o objeto deste estudo e revelam a importância do tema, na medida em que a disponibilidade cada vez mais crescente de grandes bancos de dados (Big Data) e o aprimoramento das técnicas de cruzamento de dados e reidentificação/repersonalização fazem com que até mesmo bancos de dados que estejam assegurados por técnicas de anonimização possam ter tais processos revertidos no futuro.
>
> Outrossim, o conceito legal de razoabilidade (artigo 12, §1º), se conjugado com a almejada entropia e, exigindo clareza quanto às técnicas empregadas no procedimento de anonimização para a coleta desse tipo de dado, pode contribuir para manter a utilidade desses dados para pesquisas e estatísticas internas sem enfraquecer a legislação. A adoção da heurística, compreendida como o rol de boas práticas aplicáveis aos processos computacionais, finalmente, deve perpassar por fortes e constantes atualizações para a anonimização, levando em conta os últimos avanços da matemática e da ciência da computação sobre o tema para, em um segundo momento, assegurar a almejada proteção a partir do respeito irrestrito à entropia de dados.

No contexto de desenvolvimento de sistemas de Inteligência Artificial, entender as nuances da anonimização é essencial à proteção da privacidade, no sentido de que os desenvolvedores devem garantir que os processos de anonimização sejam robustos o suficiente para impedir a reidentificação, mesmo com os avanços tecnológicos, para verdadeiramente proteger a privacidade dos indivíduos.

Portanto, a eficácia dessas técnicas deve ser continuamente avaliada à luz de avanços na capacidade de processamento e análise de dados. Em outros termos, a

conformidade com a LGPD exige que as técnicas de anonimização sejam revisadas regularmente, para assegurar que continuam sendo eficazes diante de novas tecnologias e métodos de análise de dados.

Pelo exposto, é evidente o desafio enfrentado pelos desenvolvedores de IA quanto à implementação de técnicas de anonimização e pseudonimização que, ao mesmo tempo, protejam a identidade dos indivíduos, enquanto permitem que os sistemas de IA realizem aprendizado efetivo.

Ademais, enquanto as técnicas de minimização, anonimização e pseudonimização formam a base para proteger a privacidade em sistemas de IA, a constante evolução das tecnologias de segurança e criptografia é essencial para enfrentar os desafios emergentes e garantir que a incorporação da privacidade seja efetiva e sustentável no longo prazo.

Para enfrentar os desafios de privacidade na inteligência artificial, é imprescindível adotar estratégias proativas, como a realização de Avaliações de Impacto à Proteção de Dados (DPIAs). Estas avaliações ajudam a identificar e mitigar riscos de privacidade desde as fases iniciais do desenvolvimento de sistemas de IA. Além disso, é fundamental incorporar tecnologias avançadas que garantam a proteção dos dados durante seu processamento e análise, como a encriptação de dados e o aprendizado federado.

Encriptação de dados refere-se ao processo de conversão de informações ou dados em um código secreto, o qual é difícil de decifrar sem a chave de descriptografia correspondente. A encriptação ajuda a garantir que mesmo se os dados forem interceptados durante a transferência ou acessados de forma não autorizada, eles não possam ser lidos ou utilizados por alguém que não possua a chave apropriada. (MACHADO; DONEDA, 2018). Isso é especialmente importante em ambientes de IA, onde dados sensíveis são frequentemente processados e armazenados.

Aprendizado federado, por outro lado, é uma técnica avançada de aprendizado de máquina que permite que modelos de IA sejam treinados de forma colaborativa sem que os dados saiam dos dispositivos locais dos usuários. Em vez de centralizar os

dados em um único servidor, o aprendizado federado envia o modelo de IA para os dispositivos, onde ele aprende utilizando os dados disponíveis localmente e apenas os parâmetros atualizados do modelo — e não os dados em si — são enviados de volta ao servidor central. Esse método não só melhora a privacidade e a segurança dos dados, mas também reduz a necessidade de transferência de grandes volumes de dados, o que pode ser benéfico em termos de eficiência e custos de transmissão de dados. (BOCHIE; SAMMARCO; DETYNIECKI; CAMPISTA, 2021).

Ambas as tecnologias, encriptação de dados e aprendizado federado, são fundamentais para proteger as informações enquanto são processadas e analisadas por sistemas de IA, assegurando que a privacidade dos dados seja mantida mesmo em ambientes complexos e distribuídos.

Igualmente crucial para a incorporação da privacidade no desenvolvimento de IA é cultivar uma cultura de privacidade dentro das organizações que desenvolvem essa tecnologia. Isso significa educar equipes de desenvolvimento sobre a importância da privacidade desde o início dos projetos de IA, e garantir que essas práticas sejam mantidas durante todas as fases de desenvolvimento, e depois de lançados os produtos.

Em suma, a adoção dessas práticas não apenas fortalece a confiança dos usuários nas soluções de IA, como também assegura que as inovações tecnológicas estejam alinhadas com normas éticas e legais de privacidade. Ao integrar a privacidade de maneira proativa nos sistemas de IA, as organizações podem antecipar e prevenir problemas legais e de reputação, enquanto promovem uma inovação responsável.

4. LEGISLAÇÃO APLICÁVEL

A evolução da Inteligência Artificial e a crescente capacidade de processamento de grandes volumes de dados pessoais têm levado a uma revisão das leis de proteção de dados em todo o mundo. Este capítulo aborda a legislação aplicável que rege o uso de dados pessoais, focando nas responsabilidades e obrigações que desenvolvedores e usuários de sistemas de IA devem observar.

À medida em que a tecnologia avança, é fundamental que as regulamentações se adaptem, não apenas para proteger os indivíduos contra possíveis abusos, mas também para promover clareza na promoção do desenvolvimento responsável de novas tecnologias.

4.1 LEGISLAÇÃO BRASILEIRA SOBRE PROTEÇÃO DE DADOS PESSOAIS

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco fundamental na regulamentação do tratamento de dados pessoais, tanto por entidades governamentais quanto privadas, estabelecendo diretrizes e requisitos para o tratamento de dados pessoais, incluindo sua coleta, armazenamento, tratamento e compartilhamento. Inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD tem como objetivo principal proteger os direitos fundamentais de liberdade e de privacidade, e promover a proteção dos dados pessoais dos cidadãos brasileiros.

A lei é fundamentada em uma série de princípios que devem orientar o tratamento de dados pessoais. Entre eles, destacam-se a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Esses princípios visam garantir que os dados pessoais sejam tratados de forma justa, transparente e com segurança, limitando seu tratamento ao mínimo necessário para atingir os objetivos legítimos propostos.

A LGPD garante aos titulares dos dados uma série de direitos, incluindo o direito de acesso, correção, anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a lei, bem como o direito de revogar o consentimento a qualquer momento. Isso confere aos indivíduos maior controle sobre seus dados pessoais, permitindo-lhes decidir como e por quem seus dados podem ser usados.

É importante destacar, no entanto, que o tratamento de dados pessoais pela LGPD não se limita apenas às situações em que há consentimento do titular. A lei prevê outras fundamentações legais para o tratamento de dados, como o cumprimento de

obrigação legal ou regulatória pelo controlador, a execução de políticas públicas, a realização de estudos por órgão de pesquisa, a proteção da vida ou da incolumidade física do titular ou de terceiros, entre outras. Assim, em certas circunstâncias, os dados pessoais podem ser tratados sem o consentimento do titular, sempre respeitando os princípios e garantias estabelecidos pela lei.

A legislação criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar o cumprimento da lei, aplicar sanções em caso de violações, e dirigir políticas públicas para a proteção de dados pessoais. A ANPD desempenha um papel crucial na interpretação da LGPD, orientando as organizações sobre como implementar as normas de forma eficaz.

A importância desta legislação e suas implicações para o desenvolvimento e aplicação de IA ilustram como o Brasil está alinhando suas diretrizes de privacidade com padrões globais, impactando o ambiente tecnológico e comercial do país. Para os desenvolvedores de tecnologia de IA no Brasil, a LGPD impõe a necessidade de integrar a proteção de dados desde o início do desenvolvimento dos sistemas (*Privacy by Design*). Este princípio acarreta a necessidade de revisão contínua e uma avaliação de riscos que podem surgir no tratamento de dados pessoais, garantindo que todas as operações de IA estejam em conformidade com os princípios estabelecidos pela LGPD, como a transparência, a finalidade e a necessidade.

Além disso, a LGPD incentiva uma cultura de responsabilidade, em que os desenvolvedores são obrigados a demonstrar, a qualquer momento, que seus sistemas estão operando de acordo com a lei e respeitando os direitos dos titulares dos dados. Isso inclui a implementação de medidas técnicas e administrativas apropriadas para proteger dados pessoais contra acessos não autorizados, por exemplo, e contra qualquer forma de tratamento inadequado. O foco está não apenas em adotar práticas de proteção de dados, mas também em manter uma postura proativa de verificação e demonstração de que tais medidas estão sendo efetivamente implementadas e mantidas ao longo do tempo.

O artigo 20 da LGPD aborda uma dimensão crucial da interação entre o titular dos dados e os sistemas de tratamento automatizados, incluindo aqueles baseados em

inteligência artificial. Este artigo assegura aos titulares o direito de solicitar a revisão de decisões que são tomadas unicamente por meios automatizados, as quais podem impactar significativamente diversos aspectos de suas vidas, como perfilamento profissional, de consumo, crédito ou personalidade. Essencialmente, este direito visa garantir que decisões importantes que afetem o titular dos dados não sejam deixadas exclusivamente a algoritmos, sem supervisão humana.

Adicionalmente, o controlador dos dados deve prover informações claras sobre os critérios e procedimentos empregados nessas decisões automatizadas, quando solicitado pelo titular, conforme o art. 20, §1º, da LGPD. Esta disposição é fundamental para manter a transparência, permitindo que os indivíduos entendam como e por qual motivo determinadas decisões são tomadas. Contudo, quando tais informações são retidas sob a alegação de proteger segredos comerciais ou industriais, o § 2º do mesmo dispositivo estipula que a Autoridade Nacional de Proteção de Dados (ANPD) pode realizar auditorias para verificar se há práticas discriminatórias no processamento automatizado dos dados. Esta medida reforça a proteção contra possíveis abusos e discriminações que possam surgir do uso de algoritmos na tomada de decisões.

Há autores que apontam, entretanto, ressalvas quanto ao previsto no art. 20, da LGPD. Veja-se as considerações realizadas por Caitlin Mulholland e Isabella Frajhof (2019):

> Merecem ser feitas duas notas importantes sobre este artigo. A primeira refere-se ao fato de que a lei autoriza o pedido de revisão, mas não significa que, após a análise do controlador, o resultado final necessariamente será alterado. A segunda reconhece, à primeira vista, a discricionariedade da autoridade nacional para realizar a auditoria apenas quando o controlador se negar a fornecer as informações elencadas no parágrafo primeiro.

Além dessas considerações, é essencial refletir sobre a natureza e a complexidade do que constitui uma "decisão automatizada", na era da inteligência artificial. Decisões automatizadas podem abranger desde simples escolhas algorítmicas, como recomendações de produtos, até decisões significativamente mais complexas que afetam o crédito, empregabilidade e outras áreas críticas.

Embora a LGPD ofereça uma base para o pedido de revisão de decisões automatizadas, a prática revela uma grande variação na interpretação e implementação desses pedidos, tendo em vista que esse direito pode variar significativamente de uma organização para outra. Isso porque os algoritmos e modelos de IA podem ser extremamente complexos, e nem sempre é claro para os controladores como as decisões estão sendo tomadas, o que pode dificultar a revisão efetiva dessas decisões de forma que satisfaça os requisitos da lei. Ademais, nem todas as organizações possuem a mesma capacidade técnica para analisar e revisar o processamento automatizado. Assim, é provável que grandes empresas tenham mais recursos e tecnologias avançadas para lidar com essas revisões, enquanto empresas menores enfrentem maiores dificuldades para atender às exigências legais, sem o suporte tecnológico adequado.

A LGPD fornece diretrizes gerais, mas é possível que ocorra ambiguidades em como essas diretrizes devem ser implementadas, o que pode levar a diferentes interpretações legais sobre o que exatamente é requerido para cumprir a lei, especialmente no que se refere a fornecer transparência sobre os critérios e procedimentos usados nas decisões automatizadas. Em alguns casos, ainda, os detalhes de como as decisões são automatizadas podem envolver segredos comerciais ou propriedade intelectual. Logo, as organizações podem se mostrar relutantes em divulgar essas informações, afetando a transparência e a capacidade de revisão.

Essas inconsistências sublinham a necessidade de diretrizes mais claras e robustas para assegurar que os titulares dos dados não apenas compreendam seus direitos, mas também possam exercê-los efetivamente. Uma abordagem consistente e transparente a esses desafios é essencial para manter a confiança do público no uso regulado e ético das tecnologias de IA no tratamento de dados pessoais.

Neste contexto, a LGPD transcende a mera imposição de obrigações e atua como um impulsionador de inovação no campo da inteligência artificial. Ao incentivar a adoção de práticas avançadas de privacidade, a legislação eleva os padrões de proteção de dados e oferece às empresas uma vantagem competitiva num mercado

global cada vez mais atento às questões de privacidade. Assim, a LGPD se torna um componente fundamental na estratégia das empresas que buscam não só competir, mas liderar na vanguarda tecnológica, destacando-se pelo compromisso com a privacidade e a inovação responsável.

4.2 MARCO REGULATÓRIO DA IA

No Brasil, o Projeto de Lei n° 2338, de 2023, que dispõe sobre normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial no país, representa um passo significativo na direção de estabelecer um marco regulatório específico para esta tecnologia. O projeto de lei busca criar diretrizes claras para o desenvolvimento e utilização de sistemas de IA, abordando as oportunidades e os riscos associados a essa tecnologia emergente.

O principal objetivo do PL é garantir que o desenvolvimento da IA no Brasil seja conduzido de maneira ética, segura e alinhada com os direitos humanos e liberdades civis. A legislação é estruturada em vários capítulos, oferecendo um quadro abrangente para o desenvolvimento ético e seguro da IA.

Inicialmente, o projeto de lei define os fundamentos para o desenvolvimento, a implementação e o uso de sistemas de inteligência artificial no Brasil, bem como o dever de observância a princípios como o da transparência, da não discriminação e da responsabilidade dos desenvolvedores e operadores de IA. Os princípios elencados no PL são vitais para garantir que as tecnologias de IA sejam desenvolvidas e utilizadas de maneira que respeite os direitos individuais e promova a confiança pública.

O Capítulo II, do PL 2338/2023, destaca os direitos dos titulares de dados, como o direito à informação e compreensão das decisões tomadas por sistemas de IA; o direito de contestar essas decisões e solicitar intervenção humana; o direito à não-discriminação, além de medidas para corrigir possíveis vieses discriminatórios diretos, indiretos, ilegais ou abusivos; e o direito à privacidade e à proteção de dados pessoais.

O projeto de lei também introduz uma categorização de riscos, diferenciando sistemas de IA com base em seu potencial de causar danos. Isso inclui protocolos específicos para sistemas considerados de "alto risco" e "risco excessivo". Para as empresas que desenvolvem ou utilizam IA, o projeto de lei impõe a obrigatoriedade de realizar uma avaliação preliminar, para classificação do seu grau de risco, antes de colocar no mercado produtos ou serviços atrelados a sistemas de IA, que possam ter efeitos significativos sobre os indivíduos ou a sociedade. Isso inclui uma análise detalhada dos riscos potenciais e das medidas de mitigação para prevenir danos ou abusos.

É possível interpretar que a implementação de avaliações para classificação do grau de risco de sistemas de inteligência artificial é uma incorporação direta, pelo PL 2338/2023, dos princípios de *Privacy by Design* (PbD). Essas avaliações são projetadas para proativamente identificar e mitigar riscos, incluindo os de privacidade, associados ao uso de IA, e para garantir que medidas de proteção sejam integradas no início do desenvolvimento do sistema.

Nesta linha, o PbD transcende a noção de uma mera prática recomendável e se estabelece como um requisito legal rigoroso, exigindo que as empresas implementem e documentem essas avaliações, submetendo-as à verificação por autoridades reguladoras. Portanto, as avaliações preliminares se refletem como extensão dos princípios de PbD, reforçando a seriedade com que a nova legislação brasileira trata a integração da ética e da privacidade no desenvolvimento e aplicação de tecnologias de IA.

Ademais, a Governança dos Sistemas de IA é tratada no capítulo IV do projeto de lei. Em suas disposições gerais, se estabelece o dever de implementar estruturas de governança e processos internos, como códigos de boas práticas, aptos a garantir a segurança dos sistemas e o atendimento dos direitos de pessoas afetadas por sistemas de IA, visando encorajar a adoção voluntária de padrões elevados de ética e segurança por parte das empresas que desenvolvem ou utilizam IA.

Em termos de responsabilidade civil, o projeto clarifica as responsabilidades legais dos fornecedores e operadores de sistemas de IA, estabelecendo a base para a

responsabilização em casos de danos patrimoniais, morais, individuais ou coletivos, impondo a obrigação de reparação integral da lesão causada, independentemente do grau de autonomia do sistema.

A supervisão e a fiscalização da lei são tratadas com a designação de uma autoridade competente para monitorar a conformidade com a legislação, e aplicar sanções quando necessário. As sanções administrativas previstas pelo PL são de advertência; multa simples; publicização da infração; proibição ou restrição para participar de regime de *sandbox* regulatório por até cinco anos; suspensão parcial ou total, temporária ou definitiva, do desenvolvimento, fornecimento ou operação do sistema de inteligência artificial; e proibição de tratamento de determinadas bases de dados.

Ao final do PL 2338/2023, há disposições que incentivam a inovação, como medidas de fomento e a criação de uma base de dados pública de IA de alto risco, acessível ao público, com documentos públicos das avaliações de impacto, que podem ajudar a estimular o desenvolvimento tecnológico, ao mesmo tempo em que se assegura a adesão aos princípios éticos.

A abordagem detalhada e estruturada do Projeto de Lei nº 2.338 reflete a consciência da complexidade e do potencial transformador da IA. Ao regulamentar proativamente essa tecnologia, o Brasil não apenas protege seus cidadãos, mas também posiciona sua indústria para competir de forma ética e inovadora no cenário global. Esta legislação é, portanto, um componente fundamental na estratégia nacional de integrar avanços tecnológicos com garantias de segurança, privacidade e justiça.

4.3 LEGISLAÇÃO SOBRE INTELIGÊNCIA ARTIFICIAL NA UNIÃO EUROPÉIA

O uso de Inteligência artificial tende ao crescimento cada vez mais acelerado e, diante dos desafios já abordados no presente artigo, como a falta de transparência, a possibilidade de discriminação, a exposição de dados e a inferência de dados, por exemplo, se faz necessária uma regulamentação. Como visto anteriormente, o Brasil

possui a LGPD como lei geral sobre privacidade e proteção de dados pessoais e tramita um projeto lei específico sobre IA. Porém, a União Europeia saiu na frente no que tange à aprovação do regulamento sobre IA, promovendo um marco regulatório importante no uso dessa tecnologia.

No dia 21 de maio de 2024, o Conselho Europeu aprovou o regulamento da inteligência artificial que segue o viés de análise de risco no que tange ao rigor da aplicação das regras. Este é um passo relevante no universo de IA e seus reflexos, bem como para a promoção do uso consciente e ético dessa tecnologia.

O regulamento se aplicará para prestadores que coloquem no mercado serviços ou sistemas de IA, responsáveis pela implementação desses sistemas em seu local de estabelecimento, ou mesmo estando em país terceiro, cujo resultado produzido pela IA seja utilizado na União. Também se aplica a fabricantes de produtos que integrem um sistema de IA, importadores e distribuidores de sistemas de IA, mandatários de prestadores não situados na União, e pessoas que sejam afetadas e estejam localizadas na União (Parlamento Europeu e Conselho da União Europeia, 2024).

O objetivo do regulamento é promover o uso de sistemas de IA de forma segura, além de garantir o respeito aos direitos fundamentais dos titulares de dados da União europeia, bem como estimular a inovação com responsabilidade (Conselho Europeu, 2024). No capítulo I, disposições gerais, artigo 1°, da minuta do regulamento é mencionada a sua finalidade, dando destaque ao intuito de proteger o titular e promover a inovação, conforme trecho a seguir:

> A finalidade do presente regulamento é melhorar o funcionamento do mercado interno e promover a adoção de uma inteligência artificial (IA) centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a proteção do ambiente, contra os efeitos nocivos dos sistemas de IA na União, bem como apoiar a inovação.

Nesse sentido, o regulamento estabelece regras para o fomento da IA no mercado com harmonia, requisitos necessários de atendimento para estar em compliance com a temática e proibição de práticas de IA.

O regulamento da União Europeia, ao valorizar o viés de riscos, trouxe a divisão dos tipos de IA de acordo com o risco a que estão sujeitos. Dessa forma, a classificação se dará desde uma avaliação de riscos mínimos até os riscos inaceitáveis.

A título de exemplo, o regulamento categoriza como inaceitável o uso de IA para realização de policiamento baseado em perfis categorizados pelo uso de dados biométricos e de acordo com o grupo que cada titular se enquadra, a depender da raça, religião ou orientação sexual (Conselho Europeu, 2024). Nesse sentido, conforme a graduação do risco, mais rigorosa será a aplicação das regras previstas.

Ao ser considerado um sistema de IA de alto risco, há previsão para que haja maior transparência sobre o seu desenvolvimento e utilização e até mesmo um registro na base de dados da União Europeia. Para além das medidas de proteção, o regulamento também prevê medidas de apoio à inovação, como a promoção de aprendizagem baseada em evidências (Conselho Europeu, 2024).

Portanto, a regulamentação de IA é de grande valia para que sejam respeitados os direitos fundamentais dos cidadãos e a privacidade de titulares de dados, sem que haja um avanço tecnológico acompanhado de retrocesso ético.

5. CONCLUSÃO

Com o avanço da Inteligência Artificial, a adoção de medidas técnicas de *Privacy by Design* é essencial para que a privacidade do titular de dados pessoais seja considerada desde o início do desenvolvimento de sistemas que usam essa tecnologia e assim não haja retrocesso em detrimento das conquistas de IA.

A adoção de práticas de *Privacy by Design* reflete na mitigação de riscos de privacidade e impulsiona a transparência sobre como ocorre o tratamento de dados pessoais. Consequentemente, essas práticas fortalecem a relação de confiança entre o usuário/titular e a tecnologia, fator de extrema importância para empresas que buscam vantagens competitivas.

Ademais, diante dos desafios enfrentados com o uso de IA e a crescente corrida para o desenvolvimento e uso dessa tecnologia, a adoção do *Privacy by Design,* além de se demonstrar como uma adequação a regulamentos de privacidade, tem se apresentado como uma tendência de medidas a serem consideradas e futuramente exigidas em legislação específica brasileira, que até então consiste no Projeto de Lei n° 2338, de 2023.

Em suma, pensar em IA sem considerar ações de *Privacy by Design* é inconcebível, dada a notória promoção do respeito à privacidade e da ética ao aplicá-las, e a valorização desses fatores como elementos primordiais para que essa tecnologia seja realmente considerada um avanço benéfico para a sociedade. Portanto, pensar em avanço da IA é pensar de forma colaborativa, buscando-se um equilíbrio entre a inovação, a segurança e a privacidade.

REFERÊNCIAS

BOCHIE, Kaylani; SAMMARCO, Matteo; DETYNIECKI, Marcin; e CAMPISTA, Miguel Elias M. *Análise do Aprendizado Federado em Redes Móveis*. 2021. Disponível em: https://sol.sbc.org.br/index.php/sbrc/article/view/16712/16554. Acesso em: 04 mai. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2019. Lei Geral de Proteção de Dados Pessoais (LGPD). In: *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 14 ago. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 mai. 2024.

BRASIL. Senado Federal. Projeto de Lei n° 2338/2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://legis.senado.leg.br/sdleg-

getter/documento?dm=9347622&ts=1714508324684&disposition=inline. Acesso em: 04 mai. 2024.

BRUNO, Diego Renan; GOMES, Julio Cesar. GANs – *Redes Adversarias Generativas: definições e aplicações*. Interface Tecnológica – v. 20 n. 2, 2023, p. 182-194. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1800/949. Acesso em abril/2024. Acesso em: 04 mai. 2024.

CAVOUKIAN, Ann. *Privacy by Design The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Information & Privacy Commissioner, Ontario, Canada, 2009. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 19 mai. 2024.

CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL); HUNTON ANDREWS KURTH. *Artificial Intelligence and Data Protection How the GDPR Regulates AI*. Mar. 2020. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf. Acesso em: 20 mai. 2024.

CONSELHO EUROPEU. *Lei sobre inteligência artificial (IA): Conselho dá luz verde final às primeiras regras mundiais sobre IA*. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/. Acesso em: 21 mai. 2024.

FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. *Proteção de Dados e Anonimização: Perspectivas à Luz da Lei nº 13.709/2018*. Revista Estudos Institucionais, v. 7, n. 1, p. 376-397, jan./abr. 2021. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/476/681. Acesso em: 04 mai. 2024.

GARTNER. *Gartner Identifies the Top Strategic Technology Trends for 2022*. Stamford, Connecticut, 18 de outubro de 2021. Disponível em:https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022#:~:text=By%202025%2C%20Gartner%20expects%20generative%20AI%20to%20account%20for%2010%25%20of%20all%20data%20produced%2C%20up%20from%20less%20than%201%25%20today. Acesso em: 21 mai. 2024.

HAUGELAND, John. *Artificial Intelligence: The Very Idea*. Massachusetts: The MIT Press, 1985.

HARTZOG, Woodrow; SOLOVE, Daniel, *Breached!: Why Data Security Law Fails and How to Improve It* (2022). Books. 333. p. 156. Disponível em: https://scholarship.law.bu.edu/books/333. Acesso em: 04 mai. 2024.

JIMENE, Camilla do Vale. *Reflexões sobre o privacy by design e privacy by default: da idealização à positivação*. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). Comentários do GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo (SP: Editora Revista dos Tribunais. 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/6-reflexoes-sobre-privacy-by-design-e-privacy-by-default-da-idealizacao-a-positivacao-comentarios-ao-gdpr-regulamento-geral-de-protecao-de-dados-da-uniao-europeia/1339455450#a-269738949. Acesso em: 19 mai. 2024.

JÚNIOR, Marcos Ehrardt; NETTO, Milton Pereira De França. *O marco regulatório da Inteligência Artificial no Brasil: Entre avanços e retrocessos*. JURISMAT, n. 16, p. 20-20, 2023.

KURZWEIL, Ray. *The Age of Spiritual Machines*. Massachusetts: The MIT Press, 1990.

LUDERMIR, Teresa Bernarda. *Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências*. Scielo Brasil. Inteligência Artificial. Estud. av. 35 (101). Jan-Apr 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.007. Acesso em: 04 mai. 2024.

MACHADO, Diego; DONEDA, Danilo. *Proteção de Dados Pessoais e Criptografia: Tecnologias Criptográficas entre Anonimização e Pseudonimização de Dados*. Revista dos Tribunais - Caderno Especial - A Regulação da Criptografia. 2018. p. 100-125. Disponível em: https://profmatheus.com/wp-content/uploads/2019/12/0.pdf. 2018. Acesso em: 04 mai. 2024.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. *Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning*. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. p. 272.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. PE-CONS 24/24. 19 de maio de 2024. Disponível em: https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/pt/pdf. Acesso em: 19 mai. 2024.

PINHEIRO, Patricia Peck; BATTAGLINI, Helen Batista. *Artificial Intelligence and Data Protection: A Comparative Analysis of AI Regulation through the Lens of Data Protection in the EU and Brazil*. GRUR International, Volume 71, Outubro de 2022, Páginas 924–932. Disponível em: https://academic.oup.com/grurint/article/71/10/924/6613160?guestAccessKey=ed380cb9-1fe9-4b4f-9930-8677c9797819&login=false. Acesso em 19 mai. 2024.

SANTAELLA, Lucia. *A inteligência artificial é inteligente*? São Paulo: Edições 70, 2023.

SHARIFANI, Koosha e AMINI, Mahyar. *Machine Learning and Deep Learning: A Review of Methods and Applications* (2023). World Information Technology and Engineering Journal, Volume 10, Issue 07, pp. 3897-3904, 2023, Disponível em: https://ssrn.com/abstract=4458723. Acesso em: 04 mai. 2024.