



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
CURSO DE LICENCIATURA EM COMPUTAÇÃO À DISTÂNCIA

Marcos Allan de Freitas Nunes

O impacto da inteligência artificial na gestão de dados: uma análise da proteção e
exploração de dados

Pau dos Ferros

2024

Marcos Allan de Freitas Nunes

**O impacto da inteligência artificial na gestão de dados: uma análise da proteção e
exploração de dados**

Monografia apresentada a Universidade
Federal Rural do Semi-Árido como requisito
para obtenção do título de Licenciado em
Computação.

Orientador: Prof. Dr. Paulo Henrique Lopes
Silva

Coorientadora: Prof.^a Dra. Amanda Gondim de
Oliveira

Pau dos Ferros

2024

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei nº 9.279/1996 e Direitos Autorais: Lei nº 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

N972i Nunes, Marcos Allan de Freitas.
O impacto da inteligência artificial na gestão de dados: uma análise da proteção e exploração de dados / Marcos Allan de Freitas Nunes. - 2024.
42 f. : il.

Orientador: Paulo Henrique Lopes Silva.
Coorientadora: Amanda Gondim de Oliveira.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Licenciatura em Computação, 2024.

1. inteligência artificial. 2. proteção de dados. 3. exploração de dados. I. Silva, Paulo Henrique Lopes, orient. II. Oliveira, Amanda Gondim de, co-orient. III. Título.

Ficha catalográfica elaborada por sistema gerador automático em conformidade com AACR2 e os dados fornecidos pelo(a) autor(a).

Biblioteca Campus Pau dos Ferros
Bibliotecária: Erlanda Maria Lopes da Silva
CRB: 15/966

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC's) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

Marcos Allan de Freitas Nunes

**O impacto da inteligência artificial na gestão de dados: uma análise da proteção e
exploração de dados**

Monografia apresentada a Universidade
Federal Rural do Semi-Árido como requisito
para obtenção do título de Licenciado em
Computação.

Defendida em: 05 / 12 / 2024.

BANCA EXAMINADORA

Prof. Dr. Paulo Henrique Lopes Silva
Presidente e Orientador

Prof.^a Dra. Amanda Gondim de Oliveira
Coorientadora

Prof.^a Dra. Angélica Felix de Castro
Membro Examinador

Prof. Dr. Leonardo Augusto Casillo
Membro Examinador

AGRADECIMENTOS

A Deus, pelo dom da vida.

Agradeço à minha família, em especial aos meus pais, Manoel e Zilmar, a quem devo tudo que sou. Foram eles que me educaram com amor e dedicação, guiando-me pelo caminho do bem. A minha irmã, Maria Emanuella, que sempre ofereceu seu apoio e incentivo.

À minha namorada, Roberta Milhomens, a pessoa que me ajuda todos os dias a ser melhor e me impulsiona a lutar pelos meus objetivos. Ela, juntamente com meus orientadores, me direcionou, mostrando que eu seria capaz e não deixando que eu desistisse.

Ao meu professor orientador, Dr. Paulo Henrique, e à coorientadora, Amanda Gondim, agradeço por acreditarem em minha capacidade e por todo o apoio ao longo dessa jornada, sempre me auxiliando e orientando com dedicação e carinho.

Aos professores do curso de Licenciatura em Computação, que, através de seus ensinamentos, me permitiram chegar até aqui e concluir este trabalho.

A todos os colegas de turma que, em algum momento, fizeram parte da minha formação.

À UFERSA, por todas as oportunidades e aprendizados que me foram proporcionados durante o curso, os quais levarei para toda a vida.

A todos que acreditaram e contribuíram de maneira somatória, direta ou indiretamente para a construção de minha formação, e que dirigiram suas orações a Deus em meu favor.

Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer.

Alan Turing

RESUMO

Este estudo aborda o impacto da inteligência artificial (IA) na gestão de dados, explorando a expansão exponencial das tecnologias de IA e destacando a importância de compreender os impactos desta tecnologia na proteção e exploração de grandes volumes de dados. O objetivo central é investigar como a IA se relaciona com a segurança e uso ético dos dados, analisando as áreas mais impactadas por sua aplicação, seus riscos e benefícios, além de seu relacionamento com a legislação em vigor. Para atingir esses objetivos, foi adotada uma metodologia que inclui a revisão bibliográfica de fontes confiáveis, utilizando livros, artigos científicos, legislação vigente e sites relevantes, totalizando 32 publicações selecionadas com base em critérios de relevância, atualidade e pertinência ao tema. A análise dos dados foi realizada por meio da técnica de Análise de Conteúdo de Bardin, seguindo etapas como leitura flutuante, codificação e categorização de informações, utilizando o Microsoft Excel para identificar padrões. Os resultados obtidos evidenciam a necessidade de promover o uso responsável das tecnologias de IA, equilibrando o avanço tecnológico e a proteção de dados, atentando ao contexto de economia digital vivenciado. Além disso, destacam o interesse em assegurar os princípios fundamentais individuais, com destaque para o direito à proteção de dados. Com base nos resultados, conclui-se que as abordagens sobre o tema derivam de variados campos de estudo, concentrando-se, em sua maioria, no cenário constitucionalista, aludindo a garantia dos direitos fundamentais. Desse modo, são sugeridas abordagens mais profundas em trabalhos futuros, que apresente detalhadamente como ocorre a coleta, proteção e uso dos dados pessoais, bem como a eficácia das legislações vigentes, identificando suas lacunas e suas oportunidades de evolução.

Palavras-chave: inteligência artificial; proteção de dados; exploração de dados.

ABSTRACT

This study addresses the impact of artificial intelligence (AI) on data management, exploring the exponential expansion of AI technologies and highlighting the importance of understanding the impacts of this technology on the protection and exploitation of large volumes of data. The main objective is to investigate how AI relates to the security and ethical use of data, analyzing the areas most impacted by its application, its risks and benefits, and its relationship with current legislation. To achieve these objectives, a methodology was adopted that includes a bibliographic review of reliable sources, using books, scientific articles, current legislation and relevant websites, totaling 32 publications selected based on criteria of relevance, timeliness and pertinence to the topic. Data analysis was performed using the Bardin Content Analysis technique, following steps such as skimming, coding and categorization of information, using Microsoft Excel to identify patterns. The results obtained highlight the need to promote the responsible use of AI technologies, balancing technological advancement and data protection, taking into account the context of the digital economy experienced. Furthermore, they highlight the interest in ensuring individual fundamental principles, with emphasis on the right to data protection. Based on the results, it is concluded that approaches on the subject derive from various fields of study, focusing mostly on the constitutionalist scenario, alluding to the guarantee of fundamental rights. Thus, more in-depth approaches are suggested in future works, which present in detail how the collection, protection and use of personal data occurs, as well as the effectiveness of current legislation, identifying its gaps and opportunities for evolution.

Palavras-chave: artificial intelligence; data protection; data exploration.

LISTA DE FIGURAS

Figura 1 – Esquema das etapas do processo de Análise de Conteúdo de Bardin.....	17
Figura 2 – Principais características da economia informacional	33

LISTA DE TABELAS

Tabela 1 – Categorias de análise	30
--	----

LISTA DE ABREVIATURAS E SIGLAS

GDPR	General Data Protection Regulation
IA	Inteligência Artificial
IoT	Internet of Things
LGPD	Lei Geral de Proteção de Dados
ML	Machine Learning
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico

LISTA DE SÍMBOLOS

® Marca registrada

SUMÁRIO

1	INTRODUÇÃO	13
1.1	Objetivos.....	16
1.1.1	Objetivo Geral	16
1.1.2	Objetivos específicos	16
2	MATERIAIS E MÉTODOS.....	17
3	REVISÃO DE LITERATURA	19
3.1	Legislação e ética.....	19
3.2	Cenário atual.....	23
3.3	Riscos e consequências.....	25
4	RESULTADOS E DISCUSSÕES	30
5	CONCLUSÃO	37
	REFERÊNCIAS	39

1 INTRODUÇÃO

Em 1950, Alan Turing, em seu artigo *Computing Machinery and Intelligence*, apresentou a ideia de uma máquina que pensasse. Neste artigo também foi apresentado o teste de Turing, originalmente conhecido como “Jogo da Imitação”. Turing propõe considerar a seguinte questão: “As máquinas podem pensar?”. Ademais, considera a existência de três pessoas: um homem (A), uma mulher (B) e um interrogador (C), ambos em salas separadas. Os participantes A e B devem confundir o interrogador, o qual deverá determinar qual é o homem e qual é a mulher. Quando Turing substitui um dos participantes por uma máquina, a dinâmica permanece inalterada, permitindo ao jogador C distinguir qual é a máquina e qual é o ser humano. O ponto significativo no teste de Turing é a capacidade de a máquina convencer o ser humano de sua inteligência, a ponto de confundi-la com a inteligência humana (Turing, 1950).

Para Sarlet, Sarlet e Bittar (2022), a inteligência é uma atividade mental que se baseia na aquisição e utilização dos dados para a construção e disseminação de informações, transformando-a em conhecimento. Em um primeiro momento, a inteligência esteve alinhada à perspectiva de um atributo exclusivamente humano, evoluindo no século XX com o avanço científico e tecnológico, passando a ser atribuída também a sistemas artificiais. Esses sistemas são capazes de simular as atividades mentais humanas, produzindo soluções de problemas de forma autônoma.

A inteligência artificial (IA) busca compreender, mas também, construir entidades inteligentes, ou seja, máquinas capazes de representar como agir de maneira eficaz e segura em diversas situações (Russel; Norvig, 2022). Para Kai-Fu Lee (2018 *apud* Russel; Norvig, 2022) a IA será o maior impacto já existente na história.

Segundo Russel e Norvig (2022), ao longo do tempo, pesquisadores têm buscado diferentes versões de IA. Enquanto alguns definiram inteligência com base no desempenho humano, outros preferem uma definição fundamentada na racionalidade, que se refere a fazer a “coisa certa”. A busca por inteligência que se assemelhe a humana deve ser considerada como uma ciência empírica; por outro lado, uma abordagem racionalista envolve uma combinação de matemática e engenharia. Existem, portanto, quatro linhas de pensamento que se relacionam com essas duas dimensões: os sistemas que agem humanamente, pensam humanamente, pensam racionalmente e agem racionalmente. É possível identificar projetos de pesquisa que se enquadram nas quatro dimensões, embora utilizem métodos diferentes.

De modo geral, o termo IA representa um software inteligente que visa fazer os computadores realizarem funções que eram exclusivamente dos seres humanos, por exemplo, praticar a linguagem escrita ou falada, aprender e reconhecer expressões faciais (Silva *et al.*, 2018).

Para tanto, destaca-se o machine learning (ML) como subárea da IA. Para Russel e Norvig (2022), ML é um campo da IA voltado ao desenvolvimento de programas capazes de aprender por meio da experiência, aprimorando seu desempenho ao longo do tempo. Assim, possibilita ensinar à máquina a identificar e reconhecer padrões que, muitas vezes, não seriam identificáveis aos olhos humanos, adquirindo conhecimento a partir de um conjunto de dados. De modo análogo, o aprendizado de máquina seria como um computador que observa alguns dados, baseado nisso, monta um modelo e, então, utiliza-o para a resolução de problemas.

Existem possibilidades ainda mais robustas no campo de IA, como o *deep learning*. Esses sistemas tornam-se autônomos, capazes de continuar a se desenvolver de maneira independente, para além da programação humana (Hoffmann-riem, 2019).

Os algoritmos de aprendizado devem ser capazes de se adaptar continuamente a mudanças no ambiente em que atuam, incluindo o seu próprio regime de funcionamento. Por outro lado, devem ter em conta as restrições impostas pelo tempo de resposta esperado, poder computacional, comunicações e bateria limitados. Agentes com capacidade de adaptação, atuando em ambientes dinâmicos sob condições adversas, deverão ser capazes de se autodiagnosticar e de tomar ações preventivas para a eventualidade de falhas (Faceli *et al.*, 2021, p. 359).

O princípio básico dessas tecnologias está no uso dos dados. Os sistemas de IA aprendem e aprimoram seu funcionamento por meio da exposição a uma grande quantidade de dados (*Big Data*), de forma semelhante ao processo de aprendizagem de um ser humano. Faceli *et al.* (2021) afirmam que entre os principais fatores que favoreceram os avanços da IA destacam-se a disponibilidade de infraestrutura de coleta, armazenamento, processamento e distribuição de grandes volumes de dados, além de avanços científicos e tecnológicos em diversas áreas.

Posto isso, Poeta (2020) ressalta as implicações do uso de *Big Data* para o desenvolvimento ou aprimoramento de tecnologias. Com o advento da internet e demais tecnologias, diversos serviços e setores se baseiam no tratamento de grandes conjuntos de dados. Soares (2022) aponta que a cada minuto são gerados mais dados do que foram produzidos desde o início da humanidade até o ano de 2003.

O maior crescimento ocorre nas empresas, com uma infinidade de possibilidades de uso. A *Netflix*, por exemplo, utiliza IA no sistema de recomendação e para identificação de padrões

de preferência dos seus usuários para a produção de conteúdo próprio. A *Google*, por sua vez, utiliza IA na organização de fotos do *Google Fotos*, geração de legendas automáticas para vídeos no *YouTube* e recomendações de respostas rápidas a mensagens de e-mail no *Gmail* (Faceli *et al.*, 2021).

O uso de *Big Data* tem beneficiado empresas e os governos, sendo-lhes possível compreender perspectivas e comportamentos de determinadas comunidades por meio da análise de dados digitais (Poeta, 2020). Botelho (*s.d*) destaca que redes sociais, aplicativos e empresas garantem os seus lucros através do tratamento dos dados dos seus usuários. Assim, passa a ser viável veicular publicidade personalizada para públicos específicos, criar perfis de consumidores e influenciar discussões amplas na esfera pública.

A IA desempenha um papel crucial nas áreas econômica, social, científica, médica, financeira e militar, entre diversas outras. Soares (2022) esclarece que o intuito primordial da implantação da IA em diversos setores é tornar o ser humano livre do trabalho repetitivo, tornando-o apto a desenvolver suas atividades principais de planejar, criar e inovar.

A utilização de IA em colaboração com grandes conjuntos de dados tem oportunizado que as empresas ofereçam serviços e funcionalidades que se adaptam melhor às necessidades e expectativas dos usuários. A IA, aplicada nesse contexto de *Big Data*, permite as empresas automatizarem tarefas e extraírem informações relevantes desse conjunto de dados as quais não podem ser percebidas pela mente humana devido à sua escala e complexidade.

Contudo, essa capacidade de coletar e analisar dados em larga escala coloca em risco a privacidade das pessoas, levantando preocupações éticas e legais que precisam ser cuidadosamente consideradas. Soares (2022) pressupõe que as novas tecnologias não podem ser vistas apenas por seus benefícios, é preciso que se considere também quais os riscos que trazem consigo.

Para Russel e Norvig (2022), temos a obrigação moral de usar bem as tecnologias de IA. Cada organização responsável pela sua criação têm a seriedade de assegurar que a tecnologia contribua sempre para o bem, não para o mal. É clara a necessidade de estabelecer uma compreensão sobre a proteção dos dados, identificando riscos e benefícios do uso destes por meio de ferramentas de IA. Desta forma, este trabalho justifica-se devido à necessidade em compreender os impactos da IA e o uso de grandes volumes de dados no desenvolvimento da tecnologia, permitindo identificar as implicações sociais, éticas e legais.

O interesse se deu em razão da crescente expansão da IA, notadamente de maneira global. Consequentemente, com o aumento exponencial, destaca-se a problemática dos limites éticos e jurídicos da utilização de máquinas autônomas (Sarlet; Sarlet; Bittar, 2022). Nesse

sentido, esses fatores despertaram o interesse sobre como se dá a proteção e exploração de dados pela IA.

1.1 Objetivos

1.1.1 Objetivo Geral

Analisar a relação da inteligência artificial com a proteção e exploração dos dados, considerando aspectos éticos e legais.

1.1.2 Objetivos específicos

- Apresentar as áreas mais impactadas pela aplicação da IA considerando a proteção de dados;
- Identificar os riscos e benefícios da IA no tratamento e uso dos dados;
- Investigar como as aplicações de IA se relacionam com a legislação vigente.

2 MATERIAIS E MÉTODOS

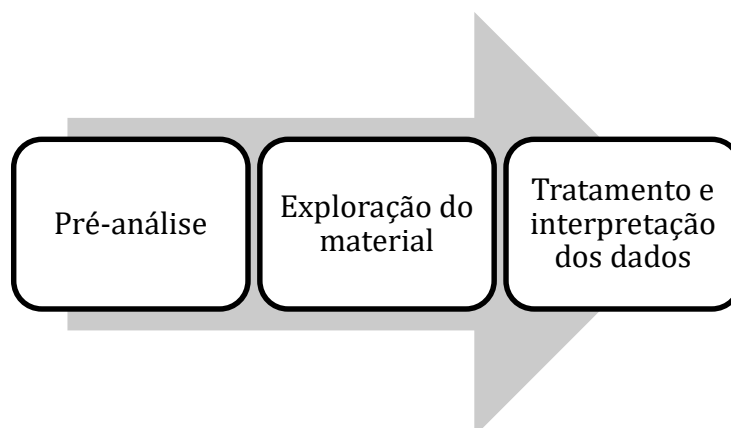
Trata-se de uma pesquisa de natureza exploratória com abordagem qualitativa, que consiste em uma revisão bibliográfica da literatura relacionada à temática da IA e a proteção e exploração de dados. A pesquisa bibliográfica consiste no levantamento de fontes confiáveis, exigindo dedicação à leitura de obras consultadas, por meio de uma leitura exploratória, seletiva e crítica (Guerra, 2023). Para a construção deste estudo, foram utilizados livros, artigos científicos, legislação vigente e sites relevantes, com foco em publicações realizadas no período de 2014 a 2024.

A busca por fontes foi realizada nas bases de dados eletrônicas Biblioteca Virtual da UFERSA, Google Acadêmico, SciELO e Portal de Periódicos CAPES, utilizando os descritores “inteligência artificial”, “proteção de dados” e “exploração dos dados”. Foram identificadas produções nacionais e internacionais, proporcionando uma visão ampla e diversificada sobre o tema.

Os critérios de inclusão dos estudos consideraram a relevância e atualidade das informações, com ênfase em abordagens que discutissem os impactos da IA na privacidade e segurança dos dados, a ética e a regulamentação para o uso de dados em IA, casos de uso da IA na exploração de dados em setores específicos, assim como estudos publicados nos últimos 10 anos, em Língua Portuguesa ou Língua Inglesa. Os critérios de exclusão dizem respeito à estudos que, apesar de tratar sobre a IA e proteção de dados, não discutem de forma relevante e explícita a proteção e exploração de dados. Assim, foram selecionadas 32 publicações.

Tratando-se da análise de dados, a Figura 1 demonstra o processo a partir da técnica de Análise de Conteúdo de Bardin (1997).

Figura 1 – Esquema das etapas do processo de Análise de Conteúdo de Bardin.



Fonte: Elaborada pelo autor (2024).

Na pré-análise, o autor destaca processos essenciais que consistem em: a) realizar leitura flutuante, sendo o primeiro contato com o material; b) fazer distinção do que será analisado; c) formular perguntas e objetivos; d) referência dos índices e elaboração de indicadores por meio de recortes de texto; e) preparação do material para análise.

A segunda fase, denominada exploração do material, caracteriza-se por uma etapa longa e meticulosa, envolvendo operações de codificação, desconto ou enumeração, visando transformar os dados brutos em informações mais compreensíveis e encontrar padrões.

Por conseguinte, os dados deverão ser processados para tornarem-se significativos e válidos, caracterizando a fase de tratamento e interpretação dos dados. A partir disso, objetiva-se a criação de quadros, gráficos, figuras e/ou modelos que representem as informações da análise para, assim, propor inferências e interpretações relacionadas ao objeto de estudo.

Nessa perspectiva, foi realizada a leitura do material e, em seguida, a codificação ocorreu por meio do programa *Microsoft Excel*, visando encontrar os padrões presentes nos textos. Em vista disso, estes padrões foram categorizados para facilitar a compreensão e possibilitar a discussão dos dados encontrados.

3 REVISÃO DE LITERATURA

O crescimento exponencial da IA levanta preocupações sobre a possibilidade de que essas tecnologias possam alcançar níveis superiores aos convencionais. Segundo Sarlet, Sarlet e Bittar (2022), o alicerce para o desenvolvimento da artificialização da inteligência está no uso de máquinas capazes de armazenar, tratar e compartilhar grandes volumes de dados. Com isso, se comparado a capacidade humana, o poder de processamento e aprendizado torna-se mais rápido e eficiente, ampliando o potencial disruptivo dessas tecnologias. Ademais, cabe assegurar que os direitos fundamentais dos indivíduos não sejam violados em função desse crescimento desmedido.

Nesse contexto, a fim de fundamentar esta pesquisa, serão abordados aspectos como legislação e ética, o cenário atual e os riscos e consequências dessas tecnologias.

3.1 Legislação e ética

Cada vez mais vem se discutindo a proteção e a exploração dos dados, visto que são a matéria prima principal para o avanço do campo da IA. Atualmente, há inúmeros serviços disponibilizados pela internet que coletam e utilizam dados. No nosso cotidiano, cedemos nossos dados pessoais para utilizar serviços, aplicativos e redes sociais. Assim, “vendemos” nossas informações em troca de facilidades.

Segundo Lima (2021), o intuito das aplicações de internet é transmitir ao usuário a concepção de serviços gratuitos, assim como ocorreu no início do WWW, onde a sua “gratuidade” estava ligada ao incentivo a utilização desses programas. Do mesmo modo, atualmente, muitos aplicativos oferecem suas vantagens e serviços de forma gratuita, conquistando mais usuários e, conseqüentemente, adquirindo acesso aos seus dados pessoais. O autor afirma que no contexto dessa economia informacional, a informação atua como um valor sobre si própria, logo, quanto maior for o número de informações nas mãos das grandes empresas, maior lucro e poder econômico elas terão.

Nesse contexto, Poeta (2020) compartilha que não se faz necessário aplicar limites excessivos para com a divulgação de dados pessoais, todavia, não se pode permitir que tais avanços ocorram e não seja colocado nenhuma barreira ou regulamentação. É fundamental garantir a privacidade e demais direitos dos cidadãos, reconhecendo os dados, no contexto atual, como recursos valiosos, comparados ao “novo petróleo”. Estes tornaram-se fundamentais para

o desenvolvimento de qualquer país, são os dados que ditam a economia global no mundo moderno.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709 de 14 de agosto de 2018, aborda o tratamento de dados pessoais, notadamente nos meios digitais, objetivando proteger os direitos fundamentais de liberdade e de privacidade, além de garantir o livre desenvolvimento da personalidade da pessoa natural. De modo complementar, o Marco Civil da Internet, Lei nº 12.965 de 23 de abril de 2014, em seu artigo 3º, já trazia consigo esses princípios, estabelecendo a proteção dos dados pessoais como um dos fundamentos essenciais para a regulação do uso da internet no país (Brasil, 2018; Brasil, 2014).

Em conformidade com a Constituição Federal de 1988, art. 5º, inc. X, são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Em suma, confirma-se o direito à privacidade e a proteção dos dados pessoais, ditos essenciais a vida digna das pessoas (Brasil, 1988).

Para compreensão do que é a privacidade, Poeta (2020, p. 77) dirá que,

No espaço virtual, isso ocorre normalmente quando um indivíduo se associa a uma rede social na Internet – trata-se de uma teia de conexão de um grupo de pessoas que se comunicam entre si, podendo ou não ter uma relação estreita de amizade. Nesse contexto, as pessoas costumam preencher perfis em que normalmente constam números de telefone, endereço de e-mail e outros dados pessoais que podem estar disponíveis apenas a um grupo fechado de indivíduos ou ser totalmente acessíveis ao público em geral.

Entende-se que os projetos de IA estão alicerçados na estruturação e processamento de dados e, conseqüentemente, envolvem a utilização de dados pessoais, por vezes coletados e manipulados sem o consentimento do titular dos dados (Leslei, 2019).

O dado pessoal pode ser definido, conforme a LGPD (2018), como qualquer informação relacionada a pessoa natural identificada ou identificável. Significa dizer que os dados pessoais podem ser representados nas diversas formas de informações, podendo identificar uma pessoa direta ou indiretamente. Poeta (2020) aponta que dados simplórios, se cruzados e tratados com outros, podem expor muitos detalhes da vida de uma pessoa. Em conformidade a isso, quando um usuário disponibiliza informações on-line está desistindo de sua privacidade e, de igual modo, de seus pais, amigos e outras pessoas, sem o devido conhecimento. O perigo encontra-se no fato de que o não conhecimento deste uso pode ser considerado como violação ao direito da privacidade, afetando diretamente no desenvolvimento da pessoa.

Por conseguinte, a lei caracteriza o dado pessoal sensível como os dados sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico. Botelho *et al.* (s.d) afirma que esse é o tipo de dado pessoal perigoso, passível de uso indevido e discriminatório.

Para isso, na União Europeia, a *General Data Protection Regulation* (GDPR) é a principal regulamentação quanto ao uso de dados pessoais. Fica estabelecido que os dados pessoais serão: 1) processados de forma lícita, leal e transparente em relação ao titular dos dados; 2) recolhidos para finalidades específicas, explícitas e legítimas; 3) adequados, relevantes e limitados ao que é necessário em relação às finalidades para as quais são tratados; 4) exatos e, quando necessário, atualizados; 5) mantidos num formato que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais os dados pessoais são processados; 6) processados de uma forma que garanta a segurança adequada dos dados pessoais.

No Brasil, o Marco Civil da Internet, em seu art. 5º, incisos VII, VIII e IX, prevê a segurança e a transparência em relação aos dados pessoais coletados. A norma veda o fornecimento a terceiros de seus dados pessoais, salvo mediante consentimento livre, exige informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção desses dados e, por fim, requer o consentimento expresso para a coleta, uso, armazenamento e tratamento de dados pessoais (Brasil, 2014).

Ante o exposto, Sarlet, Sarlet e Bittar (2022) destacam a necessidade de uma supervisão algorítmica mais transparente, que envolva uma constante avaliação dos seus impactos e de seus riscos. A já referida LGPD (2018), em seu artigo 20, traz ao titular dos dados o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, sejam elas, decisões que: tracem perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Além disso, no art. 2º, inciso II, da LGPD (2018), a autodeterminação informativa é um dos princípios à proteção de dados pessoais, representando o direito de cada indivíduo em controlar e proteger seus dados pessoais. Poeta (2020) dirá que sua finalidade primordial é permitir ao titular dos dados o direito de saber o intuito da utilização de suas informações pessoais e decidir sobre a autorização para os diversos fins. A coleta e o tratamento destes dados são inerentes ao funcionamento dos serviços e tecnologias que consumimos cotidianamente. Mas, é fundamental entendermos como nossas informações são utilizadas e como podemos mantê-las seguras.

Segundo Poeta (2020), esse direito torna ilegítima qualquer coleta de informações pessoais realizada sem o conhecimento e o consentimento explícito do titular. Ademais, considera que tais informações não podem ser compartilhadas além do contexto em que foram originalmente coletadas e utilizadas em fins que não sejam os inicialmente traçados, seja em uma instituição pública ou privada.

Por fim, os autores Sarlet, Sarlet e Bittar (2022) acrescentam a existência de esforços no legislativo para que se implemente um marco regulatório da IA no Brasil, firmando a adesão do país à Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), implicando em um novo padrão tecnológico. Isto posto, encontra-se em tramitação o Projeto de Lei nº 2338, de 2023, que dispõe sobre o uso da Inteligência Artificial. No texto original, a Lei estabelece normas para o desenvolvimento, implantação e uso responsável de sistemas de IA, com o intuito de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis (Brasil, 2023).

O texto determina fundamentos claros em seu artigo 2º para o desenvolvimento, a implementação e uso de sistemas de IA. Entre eles, estão princípios como a centralidade da pessoa humana, o respeito aos seus direitos e aos valores democráticos, a igualdade, a não discriminação e a pluralidade. Além disso, visa garantir o pleno desenvolvimento da tecnologia e sua inovação e, principalmente, estabelece a privacidade, a proteção de dados e a autodeterminação informativa como princípios norteadores para os sistemas de IA no país (Brasil, 2023).

Nessa perspectiva, Silva (2024) alude que as instituições responsáveis pelo uso dos dados devem implementar as legislações vigentes, do mesmo modo em que torna-se indispensável a supervisão de que estes estão sendo seguidos de forma eficaz. Outrossim, deve-se garantir que as legislações em vigor estabeleçam critérios e padrões claros que abordem uma coleta e tratamento de dados adequada, prevalecendo a segurança dos dados individuais.

Esses marcos regulatórios visam a promoção da proteção de informações sensíveis, mas também preocupa-se com a necessidade de integrar estes a princípios éticos no desenvolvimento tecnológico.

Para que ocorra o desenvolvimento de IA benéfica é necessário implantar a ética como uma de suas bases. A ética da IA, conforme Leslei (2019) representa um conjunto de valores, princípios e técnicas que orientam a conduta moral no desenvolvimento e uso de tecnologias de IA. Desse modo, esses valores, princípios e técnicas possuem como objetivo primordial motivar práticas moralmente aceitáveis e determinar encargos básicos para construir aplicações de IA éticas, justas e seguras.

Nesse sentido, a Declaração de Montreal (2018), indica princípios éticos que servem como guia para o desenvolvimento de IA em conformidade com os direitos humanos. Dentre os princípios, a declaração indica que a privacidade e a intimidade devem ser protegidas, assegurando que cada indivíduo deve ter amplo controle sobre seus dados pessoais, principalmente, no que diz respeito à sua coleta, uso e disseminação.

Mulholland e Frajhof (2021) destacam que a IA deve estar centrada na pessoa humana, no sentido de estar direcionada e supervisionada por ela. O objetivo central deve encontrar-se em servir a coletividade, garantindo a autonomia e poder de decisão das pessoas. Com isso, os autores refletem a necessidade de fortalecer os benefícios trazidos para a humanidade por meio da IA e esquivar-se dos riscos causados à sociedade.

Diante do exposto, e considerando a necessidade de desenvolver uma IA centrada no ser humano, é crucial adotar princípios éticos que estejam alinhados com a proteção dos direitos fundamentais assegurados por diversas regulamentações nacionais e internacionais. O desenvolvimento dessas tecnologias deve estar pautado não apenas na moralidade, mas também no respeito às normas jurídicas, garantindo a proteção da dignidade, liberdade e igualdade (Mulholland; Frajhof, 2021).

Lima e Sá (2021) consideram essencial que a construção de novas regulamentações seja conduzida com base no direito de proteger o pleno desenvolvimento das pessoas e suas convicções, garantindo que possam desenvolver-se livremente, sem a interferência ou vigilância das tecnologias em sua vida íntima.

3.2 Cenário atual

Sarlet, Sarlet e Bittar (2022) reafirmam que o principal *commodity* desta nova era tecnológica são os dados. Posto isso, o problema relacionado a proteção e exploração dos dados pessoais ganha mais relevância por ser intrínseco a proteção de outros direitos fundamentais a pessoa humana, seja no ambiente digital ou não.

Ainda que haja um enorme volume de dados produzidos e em expansão, considera-se que a grande maioria não é utilizada por não estar adequadamente estruturada. Contudo, o crescimento rápido e acelerado cria muitas oportunidades para a IA, pois essa depende dos dados produzidos por pessoas e dispositivos diariamente. À vista disso, a IA pode melhorar seu desempenho e ser usada em diferentes áreas (Sarlet; Sarlet; Bittar, 2022).

Compartilhando o pensamento de Russel e Norvig (2022), cada vez mais nota-se a presença da IA na economia, saúde, educação e segurança. Espera-se na próxima década um

acréscimo de trilhões de dólares à economia mundial a cada ano, representando um crescimento exponencial e sem precedentes.

Na saúde, a IA tem ganhado cada vez mais espaço no aprimoramento de diagnósticos e cuidados médicos. A pandemia da COVID-19 destacou a importância da tecnologia na análise diagnóstica de pacientes, devido a impossibilidade de realizar exames laboratoriais e testar a população em massa. Diversos países utilizaram aplicações de IA com a capacidade de diagnosticar a COVID-19 (Neto; Silva; Nogaroli, 2020). O Equador tornou-se o primeiro país da América Latina a utilizar um sistema auxiliar. O software permite, em até 3 minutos, analisar os resultados de tomografias de pacientes com suspeita da doença. O algoritmo contém milhares de imagens de pacientes ao redor do mundo com suspeita, confirmação e negativa de COVID-19, o que permite comparar os resultados e obter um diagnóstico mais preciso (TRT, 2020).

Na educação, as tecnologias digitais vêm conquistando o seu espaço nos últimos anos. A IA tem a possibilidade de modificar a educação de diversas maneiras, trazendo inúmeros benefícios. Cardoso *et al.* (2023) elencam alguns dos benefícios que a IA proporciona a educação: i) personalização da aprendizagem para as necessidades e habilidades de cada aluno; ii) automatização de tarefas tediosas e repetitivas, permitindo que os professores se concentrem em tarefas mais significativas; iii) análise de grandes quantidades de dados educacionais, permitindo a identificação de padrões e acelerando a identificação de áreas em que os alunos apresentam dificuldades.

Adicionalmente, as grandes empresas de tecnologia – *Facebook*®, *Amazon*®, *Apple*®, *Google*® e *Microsoft*® – estão ressignificando o campo econômico e exercendo um novo tipo de poder político. Essas empresas atuam mediante a coleta e utilização de imensas quantidades de dados, a qual pode ser considerada como a revolução de *big data* (Culpepper e Thelen, 2021).

Big data refere-se a grandes conjuntos de dados que crescem em velocidade exponencial. Russel e Norvig (2022) identificam que entre esses conjuntos de dados estão incluídos trilhões de palavras de texto, bilhões de imagens, bilhões de horas de áudio e vídeo, dados de rastreamento de veículos, redes sociais e até mesmo dados de sequências de cliques.

O termo é definido pela *TechAmerica Foundation* (2012, p. 9) como:

Big Data is not a technology, but rather a phenomenon resulting from the vast amount of raw information generated across society, and collected by commercial and government organizations. This phenomenon represents both a challenge in harnessing this volume of data, and an opportunity for government agencies who seek to enhance their effectiveness.

Para Ramidoff, Gonçalves e Menzel (2019), o termo *big data* diz respeito a coleta, armazenamento e organização de grande volume de informações, para que por meio de uma análise, obtenha-se conclusões, padrões, vínculos, comportamentos e tendências.

Silva (2023) complementa compartilhando que a *Internet of Things* (IoT) surge como um dos principais desafios em se tratando da privacidade dos usuários. A quantidade, multiplicidade e constância de dados gerados por esses dispositivos é incalculável.

Segundo Fornasier e Knebel (2021), a exploração de dados passa a ser algo necessário, influenciando no funcionamento dos serviços e da economia. Trata-se de um novo mercado lucrativo, o qual garante a estabilidade das empresas e impulsiona o surgimento de novas profissões. Neste cenário, as *big techs* são as principais detentoras dos recursos necessários para coletar, tratar e disseminar dados por meio de IA, enquanto os usuários, em sua vida cotidiana, são os grandes produtores desses dados.

Silva (2024) afirma que esses enormes bancos de dados auxiliam na classificação de perfis pessoais. Sistemas baseados em IA, em conjunto com grandes volumes de dados, são capazes de traçar preferências, hábitos, consumos e diversas outras características de uma pessoa. Após isso, estas informações são utilizadas como base no encaminhamento de publicidade direcionada, considerando as características de cada indivíduo, podendo ser chamado de *profiling*. O benefício do campo do *Big Data* expõe-se na possibilidade de exploração rápida, eficiente e pouco custosa.

Em 2018, o jornal britânico *The Guardian* divulgou o escândalo envolvendo a *Cambridge Analytica* em uma grande violação de dados. Trata-se de uma empresa de análise de dados que trabalhou com o time responsável pela campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos. A empresa teria comprado acesso a informações pessoais de milhares de usuários do *Facebook*, criando sistemas capazes de traçar o perfil de eleitores dos *EUA*, visando direcioná-los propaganda política personalizada (The Guardian, 2018).

Evidencia-se, portanto, a problemática da disseminação desenfreada de informações pessoais pela rede, não apenas comprometendo a segurança individual, mas também ampliando os riscos de manipulação em escala global. Assim, o crescimento acelerado dessas tecnologias acentua os riscos à privacidade e à autonomia dos indivíduos, abrindo caminho para as discussões sobre os riscos e consequências que a exploração desenfreada de dados pessoais pode gerar, o que será abordado na próxima seção.

3.3 Riscos e consequências

Russel e Norvig (2022) explicam que em conjunto com sua evolução, sistemas de IA podem assumir funções sociais que até pouco tempo eram desempenhadas apenas por humanos. Historicamente, os humanos utilizaram dessas funções para benefício próprio e não seria anormal que estes utilizassem os sistemas de IA para o mesmo fim, causando prejuízos individuais e coletivos.

O crescimento desmedido dessa tecnologia pode se tornar maléfico às pessoas, tornando-as mais vulneráveis e dependentes. Trata-se do uso de uma ferramenta poderosa, a qual não se tem total conhecimento sobre suas capacidades (Sarlet; Sarlet; Bittar, 2022). É perceptível, há algum tempo, a expansão das tecnologias digitais, não obstante, existem riscos e impactos negativos para a sociedade. O uso descontrolado de aplicações de IA, juntamente com o *Big Data*, intensifica os riscos à privacidade e autonomia dos indivíduos, à medida que sistemas de IA podem ser usados para explorar dados de maneiras cada vez mais intrusivas.

A economia digital contemporânea é marcada pelas grandes corporações de *Big Data*, por meio da coleta e análise dos dados para a manutenção dos seus negócios. Certamente, há benefícios claros quanto ao direcionamento eficaz do comércio ao consumidor final, mas também existem implicações, principalmente no que diz respeito as questões de autonomia e privacidade das pessoas. Portanto, se faz necessário buscar um equilíbrio entre os avanços gerados pelo *Big Data* e a proteção dos titulares dos dados, garantindo que o acúmulo de dados de diferentes fontes não represente um risco de exposição de dados indevida, primando a privacidade dos usuários e a segurança dos dados (Silva, 2024; Silva, 2023).

No entendimento de Lima (2021), a economia informacional forma-se a partir de tecnologias aplicadas para monetizar informações. Nesse contexto, as “pegadas digitais” são conceituadas como todos os tipos de rastros deixados pelos usuários das redes sociais e são utilizados na construção de perfis pessoais, objetivando otimizar o consumo de produtos e serviços, assim como de informações.

Santanna (2023) compartilha que a capacidade de análise de um grande conjunto de dados ultrapassa a aptidão humana, trazendo consigo efeitos relacionados às informações pessoais. A cada dia aumenta a quantidade de dados disponíveis sobre um indivíduo na internet, com o poder de impactar a sua vida. O autor afirma que uma simples busca na internet pelo próprio nome ou pelo nome de pessoas conhecidas pode revelar informações relevantes sobre o indivíduo.

A evolução das novas tecnologias proporciona inúmeros benefícios, todavia, assim como toda evolução, traz consigo riscos e consequências. As notícias falsas sempre existiram,

porém, sua disseminação aumenta proporcionalmente à evolução das novas tecnologias. Com isso, beneficia-se a criação de *deepfake*, que manipula imagens e vídeos, permitindo mesclar, combinar, substituir e sobrepor conteúdos visuais a fim de criar vídeos falsos que parecem autênticos. Esse tipo de uso aumenta o potencial de desinformação e confiança pública (Westerlund, 2019).

A IA generativa é um campo da IA que proporciona a criação de novos conteúdos como texto, imagens, áudios e vídeos, a partir de dados previamente usados para seu treinamento. Esse tipo de IA utiliza ML para gerar produções que simulam as criações humanas em diferentes contextos (Amazon Web Services, 2024).

O objetivo central de quem utiliza IA generativa de forma maliciosa diz respeito à manipulação da opinião popular. De acordo com o estudo realizado pelo *DeepMind*, pertencente a *Google*, a *deepfake* representa 27% dos casos de uso criminoso de IA, o que chega a ser maior do que ataques cibernéticos. Aplicações generativas se tornam cada vez mais utilizadas, por isso as empresas responsáveis começaram a monitorar a criação de conteúdos prejudiciais e antiéticos pelas suas ferramentas. Dentre os usos, destaca-se a geração de imagens pornográficas de pessoas reais e anúncios e notícias falsas (Exame, 2024).

Recentemente, o portal G1 (2024) publicou uma matéria afirmando o crescimento da pornografia *deepfake* em escolas da Coreia do Sul, envolvendo mais de 500 escolas e universidades. Nesses casos, os criminosos ameaçam as vítimas com imagens sexualmente explícitas e falsas, causando medo e repressão. Em janeiro deste ano, a cantora americana Taylor Swift foi vítima de falsos nudes criados por IA, conforme divulgou a CNN BRASIL (2024). Além disso, anúncios falsos com *deepfake* estão sendo usados para aplicar golpes milionários. A CNN WORLD (2024) relatou um caso em que a polícia de Hong Kong confirmou que golpistas usaram *deepfake* para se passar pelo diretor financeiro de uma multinacional em uma videoconferência, levando um de seus funcionários a transferir US\$ 25 milhões para fraudadores.

Os casos de uso indevido são variados, despertando preocupação entre autoridades de todo o mundo sobre o mau uso da IA. No Brasil, está em tramitação o Projeto de Lei 2.338/2023, que dispõe sobre o uso de IA, de autoria do Senador Rodrigo Pacheco. O texto inicial estabelece normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de IA no país, objetivando o desenvolvimento científico e tecnológico, mas assegurando os direitos fundamentais da pessoa humana.

Usos indevidos, como *deepfake*, são, por vezes, produtos de dados violados. Por isso, Eller e Santos (2024) destacam a necessidade de maiores investimentos em tecnologias de

segurança avançadas e eficazes, como monitoramento e avaliação, políticas e controle de dados, *firewalls*, autenticação, acesso e criptografia. De fato, as empresas ainda estarão sujeitas a violação dos dados, no entanto, é necessário tranquilizar os usuários de que medidas cabíveis serão tomadas e incidentes que coloquem sua privacidade em risco serão mitigados.

A maior preocupação por parte das empresas está direcionada ao retorno financeiro quanto ao investimento em segurança nas tecnologias da informação. Para Gouveia (2016), a Segurança da Informação (SI) objetiva proteger de forma apropriada os ativos informacionais, assegurando a continuidade das operações e minimizando eventuais perdas. Além disso, a segurança tende a maximizar o retorno sobre o investimento, dado que os esforços e custos na proteção dessas informações justificam-se pelo seu valor ou pelo valor que delas podem ser extraídos.

É crucial que as empresas compreendam a magnitude dos prejuízos associados aos vazamentos de dados. Em alguns dos casos, aplicam-se multas e penalidades que são estabelecidas nas regulamentações ora mencionadas. Contudo, é incomparável o impacto causado à imagem das empresas quando se tem um vazamento de dados exposto ao público, ou em redes clandestinas (Silva, 2023).

Por último, alguns autores também apontam como fundamental na busca por manter a segurança e privacidade dos dados que estes sejam anonimizados, dificultando a identificação dos titulares, deixando de serem considerados dados pessoais e, por fim, mitigando os riscos de vazamentos de dados. A ideia da anonimização é dificultar a associação dos dados a uma pessoa específica (Eller; Santos, 2024; Santanna, 2023; Silva, 2023).

As autoras Eller e Santos (2024) destacam a importância dos dados em diversos setores neste tempo tecnológico, muito em vista do seu valor para os seus titulares, para as empresas, para a economia e para a sociedade. As autoras afirmam que, para que os dados continuem a ser compartilhados contribuindo com o avanço da IA, é fundamental a adoção de uma postura transparente das empresas em relação aos titulares dos dados. Deixando o controle de compartilhamento em suas mãos, por exemplo, é possível minorar as percepções de vulnerabilidade, os dados do compartilhamento e os efeitos causados por possíveis violações.

Diante disso, é possível identificar várias técnicas e práticas recomendadas para promoção da proteção de dados. Dentre elas, Silva (2023) cita a anonimização e pseudonimização, criptografia, minimização de dados, acesso restrito, segurança de rede, treinamento em ambiente seguro, avaliação de riscos e impacto de privacidade, auditoria e monitoramento, conformidade com regulamentações e a educação e conscientização.

Nesse cenário, a educação e conscientização surgem como uma necessidade urgente, visando capacitar os usuários a interagirem de forma eficaz com as tecnologias emergentes. Educar os usuários envolve ensiná-los a usar ferramentas e sistemas de IA, mas também a desenvolver uma postura ética e responsável em sua aplicação. Dessa forma, a educação digital vai além do uso de ferramentas e sistemas de IA, envolvendo a compreensão das implicações éticas, legais e sociais do seu uso, tornando os usuários conhecedores de políticas públicas, regulamentações e práticas responsáveis no uso da IA, contribuindo para o fortalecimento de uma sociedade mais justa e segura diante do avanço tecnológico (Pereira; Moura, 2023).

4 RESULTADOS E DISCUSSÕES

A partir da análise realizada por meio da técnica de Análise de Conteúdo de Bardin (1997), foram identificadas 5 (cinco) categorias, que estão apresentadas na Tabela 1.

Tabela 1 – Categorias de análise

CATEGORIAS
1. Objetivo
2. Desafio
3. Princípios fundamentais
4. Economia informacional
5. Segurança de dados

Fonte: Elaborada pelo autor (2024).

A **categoria 1** aborda os objetivos principais para promoção do uso responsável das tecnologias de IA. Os autores enfatizam que o propósito maior se refere à busca pela garantia da proteção de dados e à privacidade da pessoa humana. Huang (2023) aborda a necessidade de posicionar os indivíduos à frente do desenvolvimento destas tecnologias, garantindo que sua individualidade não seja violada, bem como que a sua autonomia suficiente à proteção de seus direitos.

Nessa égide, Santanna (2023) e Huang (2023) versam sobre a necessidade do uso efetivo dos dados pessoais, visando permitir que as abordagens tecnológicas sejam utilizadas pensando em suas benéfices. É necessário, ao longo de todo o processo de desenvolvimento tecnológico, adotar uma postura que favoreça o aumento do nível de confiança pública na tecnologia.

Outro objetivo diz respeito à proteção dos princípios fundamentais, como liberdade, privacidade e livre desenvolvimento da personalidade. Esses princípios são abordados por Poeta (2020) ao destacar a LGPD (2018) como principal ordenamento jurídico brasileiro à proteção dos dados pessoais do indivíduo, trazendo consigo fundamentos que se relacionam com a personalidade, em especial ao respeito à privacidade, à autodeterminação informativa, ao livre desenvolvimento da personalidade, a dignidade e, assim, promover o exercício da cidadania pelas pessoas naturais.

Na **categoria 2** estão expostos os desafios inerentes à proteção de dados e suas implicações neste cenário. Em face do atual contexto, as tecnologias digitais viabilizam a coleta,

armazenamento e interpretação de um grande conjunto de dados por meio da aplicação de IA. Lima e Sá (2021) e Silva (2024) apresentam a certeza de que os sistemas inteligentes e autônomos podem afetar a esfera íntima do indivíduo. Portanto, torna-se oportuno impedir a interferência destas tecnologias no pleno desenvolvimento dos cidadãos e de suas opiniões.

Mediante a isso, impõe-se como maior desafio proteger os princípios fundamentais sem, no entanto, empatar o desenvolvimento tecnológico. Isso significa combater os excessos sem, ao mesmo tempo, incorrer no perigo de instituir censura. Na visão do autor, os dados podem ser considerados o “novo petróleo”, indispensáveis para o progresso de qualquer país, em vista desses estarem intrinsicamente ligados às tecnologias disruptivas do mundo atual (Poeta, 2020).

Adequar o crescimento exponencial das tecnologias e sua influência na sociedade à disciplina de proteção de dados é um grande desafio. Embora as tecnologias ofereçam benefícios significativos, é primordial atentar para o tratamento dos dados coletados e para a segurança dessas informações. A área de *Big Data* e os algoritmos usados para interpretá-los têm o poder de influenciar atividades e decisões humanas, desde relacionamentos até compras, medicina e educação (Eller; Santos, 2024).

Em consonância, Santanna (2023) reafirma o desafio imposto pela quantidade de informações disponíveis sobre um indivíduo pela rede. Essas informações podem se tornar benéficas para o desenvolvimento de uma identidade pessoal, mas, em outros casos, são utilizadas para propósitos prejudiciais, como manipulação de comportamentos, invasão de privacidade ou discriminação.

Concomitante, a segurança dos dados surge intimamente relacionada a ascensão na coleta, armazenamento e tratamento de dados. Assim, eclodem maiores incertezas e preocupações sobre como os dados estão sendo protegidos em projetos que compreendem a aplicação de *Big Data* e IA. Nesse cenário, a negligência no gerenciamento da segurança pode resultar em grandes vazamentos de dados, expondo informações pessoais, mas também sigilos corporativos, o que proporciona prejuízos à reputação das empresas, além de comprometer os direitos e a privacidade dos titulares dos dados (Silva, 2023).

Em consequência, Lima (2021) compreende que, para minimizar os impactos causados pelo crescimento exponencial dos dados e o uso de tecnologias de IA, as legislações de proteção de dados, como a LGPD no Brasil, devem ser constantemente atualizadas. Vale destacar a importância da LGPD como o principal ordenamento jurídico na luta contra os abusos na construção automatizada de perfis. Em suma, as leis vigentes devem estar alinhadas ao progresso tecnológico, a fim de garantir a eficácia de seus direitos fundamentais, promovendo o livre desenvolvimento da personalidade da pessoa natural.

A **categoria 3** discute os princípios e direitos fundamentais que deverão ser considerados na elaboração de projetos que envolvam a utilização de IA e o tratamento de dados. A proteção destes princípios apresenta-se como desafio abordado na categoria 2, com o intuito de que sua efetivação não incorra em risco ao desenvolvimento tecnológico.

Em conformidade com Silva (2023), é possível destacar legislações como a LGPD e a RGPD como primordiais na busca por proteger e efetivar os direitos fundamentais, tais como de liberdade e privacidade, além do livre desenvolvimento da pessoa natural. Essas regulamentações apresentam normas a serem cumpridas no uso e tratamento de dados individuais, para toda e qualquer finalidade.

Consoante a isso, salientam que o direito à proteção de dados se fundamenta em princípios e direitos fundamentais que o moldam. Dentre esses, destacam-se o princípio da dignidade humana, o direito ao livre desenvolvimento da personalidade, a liberdade, a privacidade, a intimidade e a autonomia sobre os próprios dados, constituindo o que se chama de autodeterminação informativa (Sarlet; Sarlet; Bittar, 2022).

O direito à proteção de dados foi verdadeiramente assegurado com a promulgação da Emenda Constitucional nº 115/22. Ao texto constitucional foi adicionado o inciso LXXIX ao artigo 5º, que dispõe sobre “o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 2022). Na visão de Sarlet, Sarlet e Bittar (2022), o direito à proteção de dados passa a vigorar assumindo uma maior importância, uma vez que, embora a LGPD represente um avanço, ainda possui lacunas a serem preenchidas, especialmente em áreas específicas não abrangidas pela legislação atual. Desse modo, com o reconhecimento do aludido direito, deixam de existir áreas onde os dados pessoais não estão protegidos.

As principais consequências do tratamento de dados sobre os direitos à proteção de dados e à privacidade manifestam-se, sobretudo, na limitação imposta pela imagem virtual em relação à liberdade real, restringindo a manifestação da personalidade do indivíduo. Para o autor, o direito à transparência ganha enorme relevância, pois garante aos indivíduos conhecimento e, principalmente, controle sobre a coleta e tratamento dos seus dados. O intuito é encorajar a aplicação de instrumentos capazes de se relacionarem com a proteção dos direitos fundamentais, viabilizando o controle de suas informações pessoais, garantindo o acesso, a veracidade, a segurança e o intuito de sua utilização (Santanna, 2023).

Huang (2023) acrescenta à discussão que com o intuito de garantir o consentimento informado para o uso de dados, as informações pessoais não podem ser coletadas, tratadas, ou ainda, compartilhadas, sem que o titular destes aprove. Com isso, assegurar o consentimento

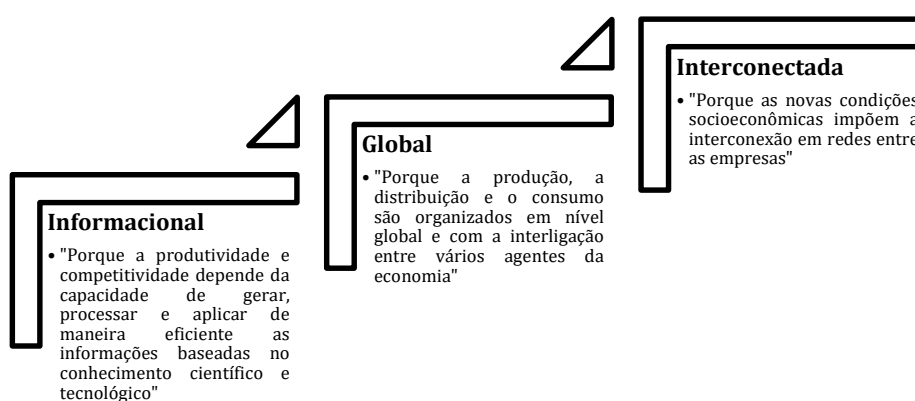
informado garante que os proprietários da informação tenham autonomia para determinar quem poderá utilizar seus dados e como o realizará.

Alguns autores apontam para a necessidade de equilibrar o desenvolvimento tecnológico com a proteção dos direitos dos tutelares. Como solução, sugere-se a implementação de políticas de governança de dados, em conformidade com as normas da LGPD e regulamentações que versam sobre os direitos fundamentais. Assim, como abordagem alternativa, mas fundamental, sugere-se a promoção de conscientização sobre a autoproteção. Essa abordagem abrange a explanação sobre a importância da privacidade de dados pessoais, os perigos de vazamento de dados e como proteger as informações pessoais (Huang, 2023; Lima; Sá, 2021; Silva, 2024).

A **categoria 4**, intitulada de economia informacional, explora o contexto econômico atual, estruturado em torno da utilização de tecnologias de IA para a monetização dos dados. Os dados se tornaram a matéria-prima principal desta nova era tecnológica. De fato, a interligação entre IA e dados resulta em uma ferramenta extremamente poderosa, capaz transformar a forma que os usuários tomam suas decisões e realizam seus consumos (Lima, 2021; Sarlet; Sarlet; Bittar, 2022).

A Figura 2 expõe as principais características da economia informacional, segundo Lima (2021, p.7).

Figura 2 - Principais características da economia informacional



Fonte: Elaborada pelo autor (2024).

Diante disso, Lima (2021) evidencia o aumento exponencial de informações no contexto econômico, ressaltando que algoritmos de personalização estão cada vez mais presentes,

levando os capitalistas a repensarem seus modelos de negócio em uma busca contínua por maior lucratividade. Esse fato incorre na premissa de que haverá uma maior vulnerabilidade e discordância entre esses capitalistas e os titulares quanto a utilização de seus dados.

Silva (2023) enfatiza a presença da tomada de decisões inteligentes em diversos setores da economia. Entre os benefícios oferecidos por essa prática, destaca-se a melhoria de processos, o controle de gastos, o aumento da produtividade, o desenvolvimento de produtos e soluções mais eficazes, além do impulso à inovação.

Nesse contexto, os rastros deixados pelos usuários na internet são elementos fundamentais para o favorecimento destes benefícios. A construção de perfis, por exemplo, é uma etapa primordial para o desenvolvimento do marketing comportamental, que objetiva a melhoria do consumo de produtos e serviços. Apesar disso, esta solução depende do tratamento de informações pessoais por algoritmos de personalização, possibilitando traçar o perfil de cada usuário e sugerir produtos e serviços alinhados à sua predileção (Lima, 2021).

Esses rastros podem ser coletados por meio de cliques, acessos e, principalmente, pelas informações que os usuários disponibilizam aos registrarem-se em páginas de internet para consumir algum serviço. Após isso, as aplicações de *big data* se encarregam de avaliar os perfis pessoais, verificando suas predileções, hábitos e até padrões de consumos. Com essa avaliação, as empresas possuem a capacidade de direcionar publicidades a públicos-alvo, baseada na análise comportamental (Silva, 2024).

A análise comportamental só é possível pela coleta de grandes volumes de dados, em uma ampla variedade de formatos. Para compreender a amplitude dessa coleta, consideram-se informações como horários e padrões financeiros, que servem como base para influenciar as decisões de compra *online*. Conforme demonstrado, as máquinas têm a capacidade de aprender com a exposição a dados, razão pela qual as empresas coletam cada vez mais dados, aumentando a capacidade dos seus sistemas de realizar previsões para aumentar seus lucros (Silva, 2024).

Para Eller e Santos (2024), o interesse em *big data* sucede mediante o seu potencial de valor comercial, em outras palavras, da capacidade de extrair valor dos dados de maneira que as habilidades humanas não permitem. A aplicação de *big data* resulta em *insights* mais rápidos, otimizando os serviços e produtos ofertados por corporações. Com isso, surgem desafios relevantes para o poder público, a sociedade e as organizações em relação a regulação, segurança e à proteção dos dados pessoais, devido à expansão exponencial das tecnologias digitais.

Notadamente, a prática de tomada de decisões inteligentes oferece diversos benefícios, contudo, não se deve ignorar o direito à proteção de dados. Evidencia-se, portanto, a relevância de compreender os limites da coleta e uso dos dados, além de implementar a ética em sua proteção e exploração. Proteger a pessoa humana passa, primeiramente, pela proteção de seus dados, o que reafirma os seus direitos constitucionais. Com a disseminação do uso comercial da internet, cresce as preocupações com a privacidade, coleta, uso e proteção de informações pessoais, visto que estão diretamente ligadas à influência da tecnologia no mundo atual (Eller; Santos, 2024).

Desse modo, compreende-se que a autonomia e privacidade das pessoas são postas em risco. É fundamental entender como os diversos tipos de dados relacionam-se, assegurando que sua obtenção não represente qualquer tipo de risco ao seu tutelar. Considerando a constante evolução das tecnologias digitais e o aumento nas violações de privacidade, considera-se indispensável efetivar normas que promovam a responsabilidade e a transparência. Deve-se buscar um equilíbrio que evite a censura ao desenvolvimento tecnológico, a fim de que seus benefícios sejam amplamente aproveitados (Poeta, 2020).

Por fim, a **categoria 5** destaca os mecanismos utilizados pelos responsáveis pela coleta, armazenamento e tratamento de dados para garantir a segurança dessas informações. Esses dados pessoais exigem proteção adequada para assegurar sua privacidade, bem como para garantir a segurança e o cumprimento das legislações vigentes à proteção de dados. Consoante a isso, torna-se relevante discutir as técnicas e práticas recomendadas para a proteção de dados sensíveis, a fim de minimizar riscos e intensificar a segurança. Assim, pode-se implementar técnicas robustas como anonimização e pseudonimização dos dados, criptografia e minimização dos dados (Silva, 2023).

A anonimização e pseudonimização consiste em remover ou substituir informações pessoais identificáveis, como nomes, endereços e números de identificação, por identificadores não pessoais, assegurando que esses dados não possam identificar uma pessoa específica. Portanto, ao aplicar técnicas de anonimização em dados pessoais, é possível utilizá-los em análises sem comprometer a privacidade dos indivíduos, reduzindo, assim, os riscos de vazamento de dados. Os dados anonimizados trazem a possibilidade de que modelos de IA possam ser treinados com dados sensíveis sem que a privacidade dos indivíduos seja violada (Eller; Santos, 2024; Santanna, 2023; Silva, 2023).

A criptografia, por sua vez, garante que apenas pessoas autorizadas tenham acesso aos dados. Esse processo protege as informações por meio de sistemas de codificação, de modo que apenas aqueles com a devida autorização e posse da chave de decodificação possam acessar e

compreender o conteúdo informativo. Embora a criptografia seja uma tecnologia avançada que aumenta o nível de segurança das comunicações, ela também impõe o desafio de dificultar investigações em casos em que essas trocas de informações possam ameaçar a segurança nacional ou global, como em situações de planejamento de ataques terroristas ou invasões cibernéticas (Poeta, 2020; Santanna, 2023).

É fundamental entender que a criptografia não consiste na eliminação de todos os problemas relacionados à proteção e privacidade dos dados, pois não assegura anonimização total. Em consequência, é necessário adotar abordagens que priorizem a criptografia eficaz, mas também considerem componentes como segurança, controle de acesso, monitoramento contínuo e políticas de gestão de dados. Estas preocupações garantem que incidentes de violações de segurança, investidas avançadas ou até incidentes de vazamento que possam revelar dados criptografados serão melhores gerenciados, com mínimas chances de acontecerem (Santanna, 2023).

Santanna (2023) e Silva (2023) também propõem a minimização dos dados como uma prática recomendada para promover a segurança de dados sensíveis. Em sistemas de IA que analisam grandes volumes de dados, é essencial coletar apenas as informações imprescindíveis para o propósito definido, evitando a coleta excessiva ou desnecessária. Assim, os autores ressaltam que a minimização de dados implica na coleta apenas dos dados necessários, reduzindo os riscos associados ao processamento excessivo e aumentando a proteção das informações.

5 CONCLUSÃO

As discussões acerca do uso de IA, retilínea à proteção e exploração dos dados, dedica-se, em grande parte, na análise das diretrizes impostas pela legislação vigente. Observa-se que os estudos estão concentrados no cenário constitucionalista, abordando a garantia dos direitos fundamentais, como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Nesse contexto, tais aspectos são essenciais ao desenvolvimento de tecnologias eficazes, mas também éticas e seguras. Portanto, torna-se indispensável uma rigorosa fiscalização na aplicação da legislação vigente, visando garantir uma IA benéfica. Além disso, é imprescindível propor melhorias constantes, considerando o rápido avanço das tecnologias digitais e a consequente necessidade de um contínuo aperfeiçoamento normativo.

Esta pesquisa atingiu os objetivos aos quais se propôs, haja vista que oportunizou a análise da relação entre a IA e a proteção e exploração dos dados, com destaque aos aspectos éticos e legais. Ao abordar as áreas mais impactadas pelo uso da IA no contexto da proteção de dados, foi possível identificar os riscos e os benefícios intrínsecos ao seu uso. Ademais, a investigação permitiu uma compreensão metódica sobre como as aplicações de IA se relacionam e interagem com a legislação vigente, apontando para desafios e diretrizes para o desenvolvimento ético e responsável da tecnologia.

Contudo, uma das principais limitações encontradas no desenvolvimento deste estudo refere-se ao fato de que existem poucas pesquisas sobre a proteção e exploração de dados em trabalhos provenientes de cursos de Tecnologia e Computação. Mediante a isso, conclui-se que a diversidade de abordagens nos campos de estudo representa um desafio considerável, pois exige a organização de materiais de áreas com ideias distintas.

Diante disso, sugere-se que estudos futuros abordem de forma mais aprofundada o desenvolvimento tecnológico relacionado à proteção e exploração de dados, detalhando o processo de coleta, proteção e uso dos dados pessoais. Além disso, esses estudos poderiam examinar a eficácia das legislações vigentes, identificando possíveis lacunas e revelando oportunidades para o aprimoramento de dispositivos legais, com o intuito de fortalecer o direito à proteção dos dados pessoais.

Por fim, a pesquisa oportunizou uma visão ampla sobre o impacto da IA na proteção de dados, destacando a crescente implementação dessa tecnologia em diversas áreas e sua presença cada vez mais forte no cotidiano das pessoas. A partir da análise das legislações vigentes, evidenciou-se a necessidade de uma governança robusta que assegure o desenvolvimento

tecnológico, assim como a proteção dos direitos fundamentais dos cidadãos. Do mesmo modo, este estudo traz enormes contribuições à esfera acadêmica, pois evidencia os desafios éticos e legais associados ao uso da IA, contribuindo para o desenvolvimento de tecnologias mais responsáveis e alinhadas a princípios como transparência e privacidade.

Em síntese, o desenvolvimento tecnológico, impulsionado pela IA, apresenta tanto oportunidades quanto desafios para a sociedade atual. Inegavelmente, aspectos como eficiência e automação de processos foram ressignificados. No entanto, é imperioso assegurar que as inovações tecnológicas estejam alinhadas às regulações que protejam os direitos fundamentais e assegurem uma exploração ética dos dados. Atingido o objetivo desta pesquisa, em analisar e relacionar a IA a proteção e exploração dos dados, espera-se que as óticas levantadas inspirem estudos futuros, aprofundando ainda mais as discussões e apoiando um desenvolvimento ético e eficaz da IA.

REFERÊNCIAS

AMAZON Web Services. **O que é IA generativa?** 2024. Disponível em: <https://aws.amazon.com/pt/what-is/generative-ai/>. Acesso em: 08 set. 2024.

BARDIN, L. **Análise de conteúdo** (L. de A. Rego & A. Pinheiro, Trans.). Lisboa: Edições 70, Presses Universitaires de France, 1977.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 16 set. 2024.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 03 set. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm. Acesso em: 03 set. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 set. 2024.

BRASIL. Senado Federal. **Projeto de nº 2338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 04 set. 2024.

BOTELHO, J. T. S.; KLAFKE, G. F.; LIMA, S. H. B.; GUIMARÃES, T. Proteção de dados. **Apostila do Curso Auto Instrucional da Fundação Getúlio Vargas**, s.d.

CARDOSO, F. S.; PEREIRA, N. S.; BRAGGION, R. C.; CHAVES, P.; ANDRIOLI, M. O uso da Inteligência Artificial na Educação e seus benefícios: uma revisão exploratória e bibliográfica. **Revista Ciência em Evidência**, [S. l.], v. 4, n. FC, p. e023002, 2023. Disponível em: <https://ojs.ifsp.edu.br/index.php/cienciaevidencia/article/view/2332>. Acesso em: 06 set. 2024.

CHEN, H.; MAGRAMO, K. Finance worker pays out \$25 million after video call with deepfake ‘chief financial officer’. **CNN WORLD**, 2024. Disponível em: <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>. Acesso em: 11 set. 2024.

CHOI, L.; MACKENZIE, J. Pornografia deepfake se espalha por escolas da Coreia do Sul e vítimas são jovens estudantes. **G1**, 2024. Disponível em:

<https://g1.globo.com/tecnologia/noticia/2024/09/03/pornografia-deepfake-se-espalha-por-escolas-da-coreia-do-sul-e-vitimas-sao-jovens-estudantes.ghtml>. Acesso em: 09 set. 2024.

CULLPEPPER, P. D.; THELEN, K. Are We All Amazon Primed? Consumers and the Politics of Platform Power. **Comparative Political Studies**, [S. l.], v. 53, n. 2, p. 288-318, 2019. Disponível em:

https://pure.mpg.de/rest/items/item_3070468_4/component/file_3289366/content. Acesso em: 06 set. 2024.

Declaração de Montreal pelo desenvolvimento responsável da inteligência artificial.

Universidade de Montreal, 2018. Disponível em:

https://declarationmontreal-iaresponsable.com/wp-content/uploads/2023/01/Portugues_-_UdeM_Decl_IA_Resp_LA_Declaration_vf.pdf. Acesso em: 05 de setembro de 2024.

ELLER, I. F. C.; SANTOS, G. V. dos. Coleta, proteção e uso de dados pessoais em negócios: a quem pertencem, como podem ser protegidos e explorados? **Revista de Gestão e Secretariado**, [S. l.], v. 15, n. 7, p. e3894, 2024. Disponível em:

<https://ojs.revistagesec.org.br/secretariado/article/view/3894>. Acesso em: 13 set. 2024.

Equador, pioneira na América Latina no uso de inteligência artificial para detectar COVID-19. **TRT**, 2020. Disponível em: <https://www.trt.net.tr/portuguese/america-latina/2020/04/01/equador-pioneira-na-america-latina-no-uso-de-inteligencia-artificial-para-detectar-covid-19-1389457>. Acesso em: 06 set. 2024.

FACELI, K.; LORENA, A. C.; GAMA, J.; ALMEIDA, T. A.; CARVALHO, A. C. L. F. **Inteligência Artificial - Uma Abordagem de Aprendizado de Máquina**. 2nd ed. Rio de Janeiro: LTC, 2021. *E-book*. p.1. ISBN 9788521637509. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788521637509/>. Acesso em: 30 ago. 2024.

FORNASIER, M. O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Praxis**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033. Disponível em: <https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/>. Acesso em: 08 set. 2024.

GOUVEIA, L. B. **Gestão da Segurança da Informação**. Disponível em: <http://hdl.handle.net/10284/5954>. Acesso em: 14 set. 2024.

GUERRA, A. de L. e R. Metodologia da pesquisa científica e acadêmica. **Revista OWL (OWL Journal) - REVISTA INTERDISCIPLINAR DE ENSINO E EDUCAÇÃO**, [S. l.], v. 1, n. 2, p. 149–159, 2023. DOI: 10.5281/zenodo.8240361. Disponível em: <https://www.revistaowl.com.br/index.php/owl/article/view/48>. Acesso em: 02 set. 2024.

HOFFMANN-RIEM, W. Big data e inteligência artificial: desafios para o Direito. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 431–506, 2020. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/484>. Acesso em: 02 set. 2024.

HUANG, L. Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. **Science Insights Education Frontiers**, [S. l.], v. 16, n. 2, p. 2577-2587, 2023. Disponível em:

<https://pdfs.semanticscholar.org/8755/8d5fd98f7428a79df46b056d9a532449f7c1.pdf>. Acesso em: 15 set. 2024.

LESLIE, D. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. **The Alan Turing Institute**, 2019. Disponível em: https://www.turing.ac.uk/sites/default/files/2019-08/understanding_artificial_intelligence_ethics_and_safety.pdf. Acesso em: 04 set. 2024.

LIMA, C. R. P. de. A proteção de dados pessoais no contexto da economia informacional: desafios regulatórios do marketing comportamental. **Revista Eletrônica do Curso de Direito da UFSM**, [S. l.], v. 16, n. 2, p. e64767, 2021. DOI: 10.5902/1981369464767. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/e64767>. Acesso em: 03 set. 2024.

LIMA, T. M. M.; SÁ, M. F. F. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, [S. l.], v. 26, n. 04, p. 227, 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 05 set. 2024.

LOPES, A. Deepfakes superam ataques cibernéticos como principal uso malicioso de IA, aponta DeepMind. **Exame**, 2024. Disponível em: <https://exame.com/inteligencia-artificial/deepfakes-superam-ataques-ciberneticos-como-principal-uso-malicioso-de-ia-aponta-deepmind/>. Acesso em: 09 set. 2024.

MULHOLLAND, C; FRAJHOF, I. Z. Entre as leis da robótica e a ética: regulação para o adequado desenvolvimento da Inteligência Artificial. In: JUNIOR, J. L. M. F.; BARBOSA, M. M.; NETTO, F. B.; SILVA, M. C. **Direito digital e inteligência artificial: diálogos entre Brasil e Europa**. Ed. São Paulo: Foco, 2021, p. 65-80. Disponível em: https://www.academia.edu/94013277/Entre_as_leis_da_rob%C3%B3tica_e_a_%C3%A9tica_regula%C3%A7%C3%A3o_para_o_adequado_deenvolvimento_da_Intelig%C3%Aancia_Artificial. Acesso em: 05 set. 2024.

NETO, M. K.; SILVA, R. D. G.; NOGAROLI, R. Inteligência artificial e big data no diagnóstico e tratamento da covid-19 na américa latina: novos desafios à proteção de dados pessoais. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 1, p. 149–178, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/974>. Acesso em: 05 set. 2024.

PEREIRA, I. S. D.; MOURA, S. A. **Explorações teóricas e oportunidades de integração curricular do letramento em inteligência artificial (IA) na educação básica**. **SciELO Preprints**, 2023. Disponível em: <https://preprints.scielo.org/index.php/scielo/preprint/view/7294>. Acesso em: 14 set. 2024.

PINOTTI, F. Taylor Swift é vítima de falsos nudes criados por IA; fãs pedem justiça. **CNN BRASIL**, 2024. Disponível em: <https://www.cnnbrasil.com.br/entretenimento/taylor-swift-e-vitima-de-falsos-nudes-criados-por-ia-fas-pedem-justica/>. Acesso em: 11 set. 2024.

POETA, V. S. **A inteligência artificial e a proteção de dados pessoais: reflexos do regulamento geral de proteção de dados europeu (RGPD) no âmbito da garantia de direitos fundamentais no direito brasileiro**. 2020. Dissertação (Mestrado em Ciência Jurídica) - Universidade do Vale do Itajaí, Itajaí, 2020.

RAMIDOFF, M. L.; GONÇALVES, F.; MENZEL, G. Uso de big data na formulação legislativa. **Revista de Relações Internacionais**, [S. l.], v. 1, n. 2, 2019. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3881>. Acesso em: 06 set. 2024.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. **General Data Protection Regulation**. Brussels, 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em: 04 set. 2024.

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 08 set. 2024.

RUSSELL, S. J.; NORVIG, P. **Inteligência Artificial: Uma Abordagem Moderna**. 4th ed. Rio de Janeiro: GEN LTC, 2022. E-book. p.839. ISBN 9788595159495. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788595159495/>. Acesso em: 30 ago. 2024.

SANTANNA, M. B. **O impacto da inteligência artificial na aplicabilidade da transparência e anonimização na proteção de dados**. 2023. Dissertação (Mestrado em Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2024. Disponível em: <https://dspace.mackenzie.br/handle/10899/38252>. Acesso em: 08 set. 2024.

SARLET, I. W.; SARLET, G. B. S.; BITTAR, E. C. B. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. Rio de Janeiro: Saraiva Jur, 2022. E-book. p.26. ISBN 9786555599527. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555599527/>. Acesso em: 30 ago. 2024.

SILVA, F. C. **Proteção de Dados Pessoais na Era da Inteligência Artificial**. 2023. Monografia (Especialista em Inteligência Artificial e Big Data) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2024. Disponível em: <https://dspace.mackenzie.br/handle/10899/38252>. Acesso em: 08 set. 2024.

SILVA, F. M.; LENZ, M. L.; FREITAS, P. H. C.; SANTOS, S. C. B. **Inteligência artificial**. Porto Alegre: SAGAH, 2018. *E-book*. p.17. ISBN 9788595029392. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788595029392/>. Acesso em: 30 ago. 2024.

SILVA, J. C. Proteção de dados pelas corporações na era do big data: uma análise entre a eficiência operacional e as questões da privacidade dos titulares. In: LEITE, F. P. A.; VITA, J. B.; CARMO, V. M.; FACHIN, J. A. **Direito, governança e novas tecnologias III**. Ed. Florianópolis: CONPEDI, 2024, p. 336-354. Disponível em: <http://site.conpedi.org.br/publicacoes/v38r977z/tb6u8a15/hnC3M6nHcT72UmTs.pdf>. Acesso em: 05 set. 2024.

SOARES, M. J. P. Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial. **Revista de Direito e as Novas Tecnologias [Recurso Eletrônico]**, São Paulo, n.15, abr./jun. 2022. Disponível em: https://mppr.mp.br/sites/default/arquivos_restritos/files/documento/2023-08/impacto_das_revolucoes_tecnologicas_no_reconhecimento_de_novos_direitos.pdf. Acesso em: 30 ago. 2024.

TECHAMERICA FOUNDATION. **Demystifying Big Data: A Practical Guide to Transforming the Business of Government**. [S. l.], 2012. Disponível em: https://bigdatawg.nist.gov/_uploadfiles/M0068_v1_3903747095.pdf. Acesso em: 06 set. 2024.

TURING, A. Computing Machinery and Intelligence. *Mind*, v. LIX, n. 236, p. 433–460, 1950.

WESTERLUND, M. The emergence of deepfake technology: a review. **Technology Innovation Management Review**, [S. l.], v. 9, n. 11, p. 39-52, 2023. Disponível em: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf. Acesso em: 08 set. 2024.