2025

CAROLINA
LOPES VENTURA

AS PREOCUPAÇÕES DE PRIVACIDADE COM O USO DA INTELIGÊNCIA ARTIFICIAL E DA ANÁLISE PREDITIVA NO COMPORTAMENTO DE COMPRA DO CONSUMIDOR ONLINE

2025

CAROLINA LOPES VENTURA

AS PREOCUPAÇÕES DE PRIVACIDADE COM O USO DA INTELIGÊNCIA ARTIFICIAL E DA ANÁLISE PREDITIVA NO COMPORTAMENTO DE COMPRA DO CONSUMIDOR ONLINE

Dissertação apresentada à Faculdade de Ciências da Universidade Europeia, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão realizada sob a orientação científica da Professora Doutora Paula Rita Brito Vitorino de Carvalho, Professora Auxiliar da Universidade Europeia.

Agradecimentos

Gostaria de começar por expressar a maior gratidão aos meus pais, pois sem o apoio incondicional deles, a entrega e o desenvolvimento desta dissertação não teriam sido possíveis. Obrigada, por me terem apoiado sempre ao longo de todo o meu percurso académico e por me terem permitido desenvolver e crescer como pessoa, sempre com amor, carinho, sacrifício e paciência. Sou bastante grata por tudo o que me conseguiram proporcionar, ao longo da minha vida pessoal e académica.

Ao meu namorado, que foi o meu maior e melhor apoio ao longo desta etapa desafiante, o meu muito obrigada. Agradeço-lhe por todo o amor, motivação e ajuda constante, e por estar sempre disponível para partilhar as suas opiniões, sugestões e conselhos. Estarei sempre grata por ter sido o meu pilar desde o início ao fim deste percurso e por me ter incentivado nos momentos de maior dificuldade. Um obrigada não é suficiente.

À minha orientadora, Professora Doutora Paula Rita Brito Vitorino de Carvalho, estou bastante agradecida por toda a disponibilidade, paciência e ajuda que me deu ao longo deste ano. Agradeço pela partilha de conhecimentos, recomendações e ideias, que conseguiram tornar este estudo bastante valioso.

Aos meus amigos e restantes familiares, o meu sincero agradecimento por me acompanharem neste processo e por compreenderem os meus momentos de felicidade, frustração, ansiedade e determinação. O vosso apoio foi essencial para que conseguisse chegar até aqui.

Por fim, agradeço a todas as pessoas que, de alguma forma, estiveram envolvidas neste projeto, seja a nível pessoal ou académico. Sem o vosso apoio, este processo teria sido muito mais difícil.

Resumo

O avanço das tecnologias digitais, em particular da Inteligência Artificial (IA) e da análise preditiva, tem transformado a forma como as empresas interagem com os consumidores e influenciam as suas decisões de compra. Estas ferramentas potenciam a personalização e a eficácia das estratégias de marketing, mas levantam questões éticas relevantes, sobretudo no que diz respeito à privacidade e ao uso de dados pessoais. Neste contexto, a presente dissertação tem como objetivo analisar as preocupações de privacidade dos consumidores online, relativamente à conduta das empresas que usam IA e análise preditiva para influenciar o comportamento do consumidor.

Para alcançar este propósito, foi elaborado um estudo quantitativo, baseado num questionário que recolheu 394 respostas válidas. Os dados foram tratados estatisticamente com recurso ao *software IBM SPSS Statistics*, de modo a testar hipóteses específicas e avaliar relações entre variáveis demográficas, comportamentais e cognitivas.

Os resultados revelaram que o nível de escolaridade exerce influência na perceção dos riscos de privacidade, enquanto a idade demonstrou ter um impacto reduzido. Verificou-se também que a frequência de compras online não está diretamente associada às preocupações com a privacidade. Por outro lado, a familiaridade com conceitos de IA e análise preditiva mostrou-se determinante para uma compreensão mais profunda sobre o uso de dados pessoais. Constatou-se ainda que a confiança nas empresas pode aumentar a disposição para partilhar determinados dados, embora persista uma resistência significativa relativamente à divulgação de informações consideradas altamente sensíveis.

Em termos de contributos, este estudo reforça a importância da privacidade como dimensão estratégica da Gestão, ao destacar que as organizações que investem em transparência, comunicação clara e práticas éticas de utilização de dados, estão mais bem posicionadas para conquistar a confiança dos consumidores e criar relações de longo prazo.

Em suma, esta investigação acrescenta valor académico e prático ao debate sobre o equilíbrio entre inovação tecnológica e ética empresarial, ao sublinhar a importância de alinhar a utilização da IA e da análise preditiva com os direitos fundamentais e as expectativas de privacidade dos consumidores.

Palavras-Chave: Inteligência Artificial; Análise Preditiva; Privacidade de Dados; Ética; Comportamento do Consumidor Online; Políticas de Privacidade

Abstract

The advancement of digital technologies, particularly Artificial Intelligence (AI) and predictive analytics, has transformed the way companies interact with consumers and influence their purchasing decisions. These tools enhance the personalization and effectiveness of marketing strategies, but they also raise significant ethical concerns, especially regarding privacy and the use of personal data. In this context, the present dissertation aims to analyse online consumers privacy concerns in relation to the conduct of companies that use AI and predictive analytics to influence consumer behaviour.

To achieve this goal, a quantitative study was conducted, based on a questionnaire that collected 394 valid responses. The data were statistically processed using IBM SPSS Statistics software, in order to test specific hypotheses and assess relationships between demographic, behavioural, and cognitive variables.

The results revealed that educational level influences the perception of privacy risks, whereas age was found to have a reduced impact. It was also observed that the frequency of online purchases is not directly associated with privacy concerns. On the other hand, familiarity with concepts of Artificial Intelligence and predictive analytics proved to be a determining factor for a deeper understanding of the use of personal data. Furthermore, it was found that trust in companies may increase the willingness to share certain data, although significant resistance remains regarding the disclosure of information considered highly sensitive.

In terms of contributions, this study reinforces the importance of privacy as a strategic dimension of Management, by highlighting that organizations investing in transparency, clear communication, and ethical data practices are better positioned to earn consumer trust and build long-term relationships.

In summary, this research adds academic and practical value to the debate on the balance between technological innovation and business ethics, by emphasizing the importance of aligning the use of AI and predictive analytics with consumers fundamental rights and privacy expectations.

Keywords: Artificial Intelligence; Predictive Analytics; Data Privacy; Ethics; Online Consumer Behaviour; Privacy Policies

Glossário

AP- Análise Preditiva

BA - *Business Analytics*

CC - Comportamento do Consumidor

CRP - Constituição da República Portuguesa

IA - Inteligência Artificial

ID - *Identity*

IP - *Internet Protocol*

RGPD - Regulamento Geral de Proteção de Dados

UE - União Europeia

Índice de Conteúdos

Índice de Tabelas

Índice de Gráficos

Índice de Apêndices

Capítulo 1 – Introdução

1.1 Contextualização

O avanço das tecnologias digitais, especialmente da Inteligência Artificial (IA) e da Análise Preditiva, tem transformado profundamente a forma como as organizações interagem com os consumidores, processam informações e tomam decisões estratégicas (Dias, Gonçalves, Costa, Pereira, & Dias, 2023). No contexto do marketing, estas ferramentas revelam-se particularmente poderosas, pois possibilitam a previsão de comportamentos e a personalização de ofertas. No entanto, o seu potencial vem acompanhado de dilemas éticos significativos, sobretudo no que diz respeito à privacidade, à proteção de dados e à possibilidade de manipulação e discriminação algorítmica (Mühlhoff, 2021).

A análise preditiva, entendida como o uso de dados históricos, métodos estatísticos e algoritmos de *machine learning* para antecipar eventos ou comportamentos futuros, tornou-se um dos principais recursos de apoio à tomada de decisão em diversos setores. No marketing, a sua aplicação tem como objetivo compreender padrões de consumo e antecipar necessidades individuais. Contudo, a recolha e o processamento de grandes volumes de dados pessoais suscitam preocupações legítimas sobre a transparência, segurança e uso ético dessas informações, exposição dos consumidores a potenciais riscos de vigilância, perda de autonomia e exploração comportamental (Belen-Saglam, Nurse, & Hodges, 2022).

Neste contexto, a ética aplicada à Inteligência Artificial emerge como um campo de estudo fundamental. Inserida na ética digital, esta área procura refletir criticamente sobre os impactos sociais, políticos e económicos da utilização da IA e do *Big Data*, ao articular princípios como justiça, transparência, responsabilidade, autonomia, privacidade e segurança.

Assim, esta dissertação tem como objetivo analisar, com uma abordagem quantitativa, a conduta ética no uso da Inteligência Artificial e da análise preditiva no marketing, com particular atenção aos dilemas relacionados com a privacidade, a proteção de dados e a discriminação algorítmica. Pretende-se, deste modo, contribuir para a consciencialização da sociedade sobre as noções e riscos éticos do uso destas tecnologias, por parte das empresas.

1.2 Motivação

A escolha deste tema resulta de uma combinação de motivações pessoais e sociais que refletem tanto o interesse individual como a relevância coletiva da investigação. A nível pessoal, sempre houve um especial interesse em compreender como as empresas utilizam tecnologias como a Inteligência Artificial e a análise preditiva para prever e influenciar o comportamento dos consumidores, o que motivou a exploração crítica deste fenómeno.

No contexto social, este estudo é impulsionado pela necessidade de promover a sensibilização da sociedade sobre os riscos e desafios associados à utilização de dados pessoais em ambientes digitais, bem como pela relevância social e a proteção dos direitos fundamentais. Ao analisar as preocupações de privacidade relacionadas com a aplicação da IA e da análise preditiva no comportamento de compra online, pretende-se contribuir para o debate social, sobre a necessidade de práticas mais transparentes, éticas e centradas no respeito pelos indivíduos, ao reforçar a importância de alinhar a inovação tecnológica com os valores fundamentais que regem a sociedade.

1.3 Objetivos de Investigação

Neste contexto, a presente dissertação tem como objetivo geral, analisar as preocupações de privacidade dos consumidores online, em relação à conduta das empresas que utilizam Inteligência Artificial e análise preditiva, para influenciar o comportamento de compra. Este objetivo parte do reconhecimento de que, no contexto digital atual, as organizações recorrem a estas tecnologias de forma cada vez mais sofisticada para recolher, tratar e interpretar grandes volumes de dados, com o intuito de prever padrões de consumo e influenciar decisões de compra. Contudo, esta prática levanta questões éticas, especialmente no que diz respeito à forma como os dados são obtidos, ao grau de transparência dos processos e aos riscos percebidos pelos consumidores quanto à utilização das suas informações pessoais.

Para uma melhor compreensão desta investigação, a problemática será analisada através de diferentes vertentes, estruturadas em objetivos específicos. Em primeiro lugar, pretende-se analisar as diferenças na perceção sobre privacidade online e no grau de confiança nas empresas entre diferentes grupos demográficos, nomeadamente variáveis como a idade e o nível de escolaridade. Com esta abordagem, pretende-se compreender de que forma os fatores socioeconómicos e

culturais podem influenciar a forma como os consumidores percebem os riscos e benefícios associados à utilização dos seus dados pessoais pelas organizações.

Além disso, procura-se investigar a correlação entre as preocupações com a privacidade online e a frequência de compras online, de modo a avaliar se os receios relacionados com o tratamento dos dados têm impacto nas decisões de consumo. Este objetivo é particularmente relevante para compreender se existe uma relação entre o grau de confiança digital e o comportamento de compra. Outro aspeto fundamental é estudar o nível de conhecimento dos consumidores sobre Inteligência Artificial e análise preditiva, bem como a sua compreensão sobre como estas tecnologias utilizam os seus dados. Trata-se de perceber até que ponto os consumidores têm consciência das práticas adotadas pelas empresas e de que forma essa consciência (ou a sua ausência) pode influenciar as suas perceções sobre privacidade, confiança e segurança digital.

Complementarmente, pretende-se explorar a relação entre a frequência de compras online e a disposição para partilhar diferentes tipos de dados pessoais, ao analisar se consumidores mais habituados a comprar em ambientes digitais apresentam maior abertura à partilha de informações, ou, pelo contrário, se desenvolvem um comportamento mais cauteloso e protetor. Esta análise permitirá identificar tendências e padrões associados à confiança e ao uso continuado de plataformas digitais. A investigação inclui ainda o objetivo de analisar a relação entre a leitura de políticas de privacidade e o conhecimento sobre os riscos associados à utilização de dados pessoais, partindo do pressuposto que o consumo destas informações pode contribuir para decisões mais conscientes e informadas sobre a partilha de dados.

Finalmente, procura-se analisar as diferenças na compreensão sobre o uso de dados por IA entre diferentes faixas etárias, bem como examinar a relação entre a familiaridade com essa tecnologia e análise preditiva e a leitura de políticas de privacidade. Estes dois objetivos permitem identificar possíveis lacunas geracionais no conhecimento das tecnologias digitais e avaliar se o grau de literacia digital está associado a um comportamento mais proativo na procura de informações sobre a utilização dos dados.

Em suma, estes objetivos permitem obter uma visão abrangente sobre as perceções, os receios e os comportamentos dos consumidores relativamente ao uso de IA e análise preditiva no comércio eletrónico, pois contribui para um debate mais informado sobre a necessidade de práticas empresariais que conciliem inovação, ética e respeito pelos direitos fundamentais dos indivíduos.

1.4 Estrutura da Investigação

A presente dissertação encontra-se organizada de forma lógica e coerente, de modo a permitir uma compreensão aprofundada do tema em análise, as preocupações de privacidade associadas ao uso da inteligência artificial e da análise preditiva no comportamento de compra do consumidor online.

O capítulo 2 é constituído pela Revisão da Literatura. Esta apresenta a base teórica da investigação, que reúne e analisa criticamente os principais contributos científicos relevantes para o tema. São discutidos conceitos como inteligência artificial, análise preditiva, comportamento do consumidor digital, privacidade de dados e ética tecnológica. Este capítulo permite não só contextualizar teoricamente o objeto de estudo, como também sustentar as relações entre as variáveis analisadas, ao oferecer suporte à formulação das hipóteses de investigação.

No capítulo 3, onde se encontra a Metodologia de Investigação, é detalhado o percurso metodológico adotado. Descreve-se, também, o modelo conceptual que representa as relações entre as variáveis, de acordo com as hipóteses formuladas, a abordagem quantitativa, a caracterização da amostra e o instrumento, e procedimento de recolha de dados.

Em relação ao capítulo 4, referente aos Resultados, este é dedicado à exposição e interpretação dos dados recolhidos. São apresentados os resultados estatísticos obtidos através da análise com recurso ao *software SPSS*. Este capítulo procura responder aos objetivos de investigação, ao verificar a validade das hipóteses formuladas.

Já no capítulo 5 sobre a Discussão dos Resultados, este procura compreender o que os resultados significam no contexto do tema em estudo, ao relacioná-los com as hipóteses de investigação e com os contributos de outros autores. A discussão permite identificar pontos de convergência e de divergência com estudos prévios, ao refletir sobre as implicações que as preocupações de privacidade e o recurso à inteligência artificial no comércio eletrónico podem ter, tanto para a confiança e comportamento dos consumidores, como para as estratégias adotadas pelas empresas.

Por fim, o capítulo 6, Conclusão, reúne as principais conclusões do estudo, que reflete os seus contributos teóricos e práticos. É apresentado a importância do desenvolvimento deste estudo, para a área de gestão. E são também identificadas as limitações da investigação e sugestões para estudos futuros que queiram aprofundar esta temática, cada vez mais relevante no contexto do comércio eletrónico e da proteção dos dados pessoais dos consumidores.

A estrutura adotada reflete uma preocupação em apresentar coerentemente as diversas etapas da investigação, ao promover uma leitura fluida, com o objetivo de oferecer um contributo relevante para o debate atual sobre a utilização ética e transparente das tecnologias preditivas no ambiente digital.

Capítulo 2 – Revisão da Literatura

2.1 Inteligência Artificial e Análise Preditiva

2.1.1 A origem da Inteligência Artificial

A Inteligência Artificial (IA), começou a desenvolver-se a partir dos meados do século XX e tem provocado mudanças profundas na tecnologia e na sociedade. Um dos marcos inaugurais foi o trabalho de McCullhoch e Pitts (1943), que apresentaram um modelo computacional inspirado no funcionamento dos neurónios, que demonstrou como circuitos lógicos poderiam representar processos mentais básicos e abriu caminho à simulação de raciocínio em máquinas.

Devido ao crescente desenvolvimento sobre o tópico da IA, tornou-se necessário criar uma metodologia sistemática para avaliar a inteligência de um sistema artificial. Com isto, Alan Turing (1950) publicou um dos primeiros trabalhos que abordava o tema da inteligência de um modelo, intitulado de "Computing Machinery and Intelligence". Este estudo tinha como objetivo perceber se as máquinas conseguiriam imitar a inteligência humana e tomar decisões baseadas em informação. O teste, intitulado de *Turing Test* ou Jogo da Imitação, envolvia três personagens, dois interrogados, um ser humano e um computador, e um interrogador, que estaria numa sala separada, onde realizava questões a um e a outro. Se o interrogador não fosse capaz de distinguir as respostas da pessoa e da máquina isto significava que esta tinha passado no *Turing Test*.

Foi então, em 1956, que os pioneiros da inteligência artificial, John McCarthy e Marvin Minsky e os investigadores Claude Shannon, pai da teoria da informação, e Nathaniel Rochester, arquiteto do primeiro computador científico, organizaram a conferência de *Darmouth Summer Research Project on AI*. Esta convenção marcou a primeira abordagem do conceito de IA onde este foi considerado uma nova área de estudo (Dick, 2019).

À medida que a investigação avançava, novos ramos e especializações começaram a emergir dentro deste campo. Uma das componentes que foi considerada a mais importante, por vários

autores, denominou-se de *machine learning*. Este conceito foi introduzido por Samuel (1959). A sua ideia consistia em criar um programa de computador que jogasse damas, um jogo de tabuleiro de estratégia, e que fizesse com que a máquina aprendesse através da experiência e autoaperfeiçoamento. Este provou que era possível criar sistemas que não só realizavam tarefas predeterminadas, mas também tinham a capacidade de aprender e de se aperfeiçoar com base nas experiências passadas.

Durante a década de 1970, a área da inteligência artificial enfrentou diversos desafios. O avanço contínuo desta tecnologia foi prejudicado por limitações no poder computacional, pois os computadores da época possuíam baixa capacidade de armazenamento e processamento rápido de informações. Além disso, os custos elevados associados ao desenvolvimento desta área levaram a uma redução no financiamento por parte das entidades financeiras, o que dificultou o avanço nas pesquisas (Jones, 2025).

Foi então, em 1997, que um computador da IBM (*International Business Machines Corporation*) conseguiu vencer o campeão mundial de xadrez. Este algoritmo armazenava jogadas, combinações e estratégias concebidas por humanos e, com a sua rapidez e capacidade de examinar diferentes alternativas, conseguiu vencer o homem. Com este acontecimento, a área de estudo da IA passou a ser mais credível para os investidores, o que levou a um aumento gradual dos fundos (Campbell, Hoane & Hsu, 2002).

Entre os anos de 2000 e 2010 surgiram duas componentes, da IA, consideradas as mais importantes nos dias de hoje: o *Deep Learning* e o *Big Data*. De acordo com Manyika, Chui, Brown, Bughin, Dobbs, Roxburgh e Byers (2011) o *Big Data* refere-se a conjuntos de dados extremamente grandes e complexos que não podem ser geridos, processados ou analisados através de métodos tradicionais de gestão de bases de dados, mas que através do uso desta ferramenta as organizações podem descobrir padrões, tendências e associações, especialmente no comportamento humano e nas suas interações, o que pode ser usado para tomar decisões mais estratégicas. E o *deep learning* é um conjunto de algoritmos baseados em redes neurais profundas, capazes de aprender representações complexas de dados por meio de múltiplas camadas de processamento (Shrestha, Krishna & Krogh, 2021).

No ano de 2011, a empresa *Apple* criou uma assistente virtual denominada de *Siri*, esta era capaz de responder a uma ampla variedade de perguntas feitas pelo usuário, ao combinar o raciocínio

humano com o da máquina, revolucionando assim a interação entre o humano e a tecnologia. Nos anos seguintes surgiram outros assistentes virtuais como a *Alexa*, em 2014, criada pela *Amazon* e o *Google Duplex*, em 2018, criada pela *Google* (Carter, 2018). "A inteligência artificial, ao contrário de um robot normal, tem a capacidade de tomar decisões independentes com base nos dados obtidos, (…) também é capaz de analisar as suas próprias decisões anteriores e alterá-las, ou seja, de agir de forma alternativa" (Evstratov & Guchenkov, 2020, p.14).

De acordo com publicações de caráter profissional, como a *Supply Chain Magazine* (2024), o ecossistema de Inteligência Artificial é atualmente moldado por tendências como a automatização aprimorada e autónoma, a IA generativa e multimodal, a crescente regulamentação e os debates éticos, bem como os desafios relacionados com *deepfakes* e desinformação. Estas dinâmicas, já visíveis em *smartphones* e em diversas aplicações do quotidiano, exercem um impacto direto no marketing orientado por dados, onde a IA e a análise preditiva suportam a personalização, a segmentação e a tomada de decisão em tempo real.

Em síntese, a trajetória histórica da IA, dos modelos lógicos iniciais à adoção massiva em produtos e serviços, explica a maturidade atual das técnicas preditivas que serão mobilizadas nesta dissertação para compreender o marketing, a privacidade e a confiança do consumidor no ambiente digital.

2.1.2 Introdução da Análise Preditiva

O conceito de análise preditiva não é recente. A sua utilização remonta a 1689, quando a *Lloyd Company*, responsável pela emissão de seguros marítimos, começou a analisar registos de viagens anteriores para estimar riscos e prever padrões de responsabilidade. Esta prática primitiva já evidenciava o princípio central da análise preditiva: aprender com dados passados para antecipar eventos futuros (Predictive Sucess Corporation, 2019).

Séculos depois, com a invenção do computador, iniciou-se a chamada fase descritiva. A introdução deste tipo de tecnologia facilitou a criação de modelos e algoritmos que previam o futuro a partir de dados históricos. Um dos modelos mais utilizados era denominado de modelo preditivo. De acordo com Strickland (2014), os modelos preditivos procuram estimar a probabilidade de que uma unidade com características semelhantes, em diferentes amostras, exiba um desempenho equivalente. Com os avanços da computação, estes sistemas evoluíram para além da simples

previsão estatística, tornando-se capazes de simular comportamentos humanos e até de reproduzir reações a determinados estímulos. Com isto, houve uma melhoria considerável nas funções e capacidades das máquinas, o que levou a um maior armazenamento e melhor análise de grandes quantidades de dados (Schwecke, 2021).

2.1.3 Definição de Análise Preditiva

A análise preditiva é uma área integrante da inteligência artificial (IA), que utiliza técnicas de *machine learning* e metodologias estatísticas para examinar dados e prever resultados futuros. Estas ferramentas permitem que as máquinas aprendam a partir de dados, identifiquem padrões e tomem decisões de forma autónoma, constituindo-se como elementos centrais da IA.

Com os avanços tecnológicos, a análise preditiva deixou de se basear exclusivamente em modelos estatísticos, passando a incorporar técnicas sofisticadas de inteligência artificial. Segundo Bracanovic (2019), trata-se da prática de analisar grandes volumes de dados, recorrendo a métodos como *data mining* e *machine learning*, com o objetivo de prever eventos futuros, incluindo comportamentos e preferências humanas.

Desde então, a análise preditiva consolidou-se como um método robusto para a exploração detalhada de dados e algoritmos, evoluindo juntamente com o *machine learning* para detetar padrões e antecipar acontecimentos. Bishop (2006) descreve o *machine learning* como o processo de aprender automaticamente relações e padrões significativos a partir de exemplos e observações. De forma complementar, Shrestha, Krishna e Von Krogh (2021) destacam que os avanços nesta área têm permitido o desenvolvimento de sistemas inteligentes capazes de exibir competências cognitivas comparáveis às humanas.

Contudo, os benefícios e o potencial da análise preditiva só foram apreciados, recentemente, devido ao fenómeno do *Big Data*. O conceito de *Big Data* refere-se a volumes massivos de informação que requerem arquiteturas e tecnologias avançadas para a sua recolha e processamento, permitindo assim extrair valor e apoiar uma compreensão mais aprofundada dos fenómenos, bem como uma tomada de decisão mais eficiente (Hajjaji, Boulila, Farah, Romdhani & Hussain, 2021)

A análise preditiva é um dos três tipos de análise, utilizada no *Business Analytics* (BA). BA é uma combinação de métodos, ferramentas tecnológicas e aplicações, empregadas na análise de dados e do desempenho de uma empresa, com o objetivo de extrair *insights* fundamentados em dados, para

orientar as decisões futuras e investimentos de uma organização (Lee, Cheang & Moslehpour, 2022).

O período que se vive, atualmente, é definido pela presença dominante da tecnologia, das suas evoluções e descobertas notáveis. Esta realidade culmina na geração com vasta quantidade de dados. Este volume de dados, em constante expansão, amplamente acessível e de proporções gigantes, caracteriza a época da informação. Para navegar eficazmente neste cenário, são necessárias ferramentas robustas e flexíveis que possam extrair, automaticamente, *insights* valiosos de grandes conjuntos de dados, convertendo-os num conhecimento estruturado. O *data mining* corresponde ao processo de identificar padrões, modelos e informações relevantes em grandes volumes de dados, transformando-os em conhecimento útil para a tomada de decisão (Han, Pei & Tong, 2022).

De acordo com Wolniak e Grebski (2023, p.2) "A análise preditiva é uma ferramenta poderosa que permite às organizações antecipar resultados, comportamentos e tendências futuras (…), a sua adoção pode conduzir a uma maior eficiência operacional, a melhores experiências para os clientes e a uma maior competitividade." Para estes autores a aplicação da análise preditiva divide-se em várias etapas. Primeiro, as organizações devem clarificar o problema que desejam resolver e encontrar as fontes de dados pertinentes. De seguida, é crucial escolher os modelos e algoritmos de previsão apropriados, adaptados à natureza do problema e aos dados disponíveis. Estes modelos são então treinados, através da utilização de dados históricos e testados, para verificar a sua precisão e eficácia (Wolniak & Grebski, 2023).

A metodologia da análise preditiva possibilita que as empresas atuem de forma proativa e focada no futuro, o que antecipa resultados e comportamentos a partir da análise de dados concretos, em vez de se basearem apenas em hipóteses ou suposições não fundamentadas (Lee et al., 2022). De acordo com Kumar e Garg (2018) o processo de análise preditiva é dividido em seis fases, a recolha de requisitos; recolha de dados; análise e tratamento de dados; estatísticas e *machine learning*; modelação preditiva e por fim, as previsões e monitorização.

A primeira fase concentra-se na compreensão da necessidade que uma empresa tem em desenvolver um modelo preditivo, sendo imprescindível esclarecer o objetivo da previsão e definir o tipo de conhecimento que se pretende obter com a mesma. De seguida, a segunda fase da análise foca-se na recolha de dados necessários para o desenvolvimento do modelo preditivo, que pode

incluir uma lista exaustiva das empresas que utilizam ou consultam os produtos de uma determinada organização. Na terceira fase é quando os dados recolhidos são examinados e preparados para a análise e utilização do modelo, pois a eficácia do mesmo está inteiramente dependente da qualidade dos dados.

Depois, através das técnicas de estatística, que envolvem a teoria das probabilidades e a análise de regressão, assim como os métodos de aprendizagem automática, que englobam as redes neuronais artificias e as árvores de decisão, é que os modelos preditivos são desenvolvidos. Na fase da modelação preditiva é quando o modelo já está concebido e é avaliado através de um conjunto de dados de teste, constituído por uma parte dos dados previamente recolhidos para verificar a sua validade, se for aceite, o modelo é capaz de fornecer previsões precisas para novos dados que sejam introduzidos no sistema. Na fase final, quando o modelo preditivo passa nos testes de previsão, este é implementado no sistema do cliente, com o objetivo de fornecer previsões diárias e apoiar o processo de tomadas de decisão, sendo monitorizado de forma contínua (Kumar & Garg, 2018).

2.1.4 Aplicações da Análise Preditiva e Inteligência Artificial no marketing

A aplicação da Análise Preditiva (AP) no marketing remonta às décadas de 1950 e 1960, quando as ferramentas estatísticas começaram a ser utilizadas para segmentar mercados e identificar tendências de consumo. A estatística desempenhou um papel essencial nesse desenvolvimento, ao permitir a padronização e organização dos dados recolhidos, com vista à modelação de fenómenos de consumo e previsão de comportamentos futuros. Segundo Mercante (2023), a aplicação de técnicas estatísticas permite padronizar e organizar os dados recolhidos, possibilitando, a partir dessa análise, a construção de modelos que representem o fenómeno em estudo.

Nos últimos anos, a AP tornou-se uma ferramenta central na definição de estratégias de marketing orientadas por dados. A análise preditiva é amplamente aplicada no marketing, sobretudo na previsão do comportamento dos clientes. Para tal, as empresas registam e analisam as respostas e transações dos consumidores, utilizando esses dados como base para definir e orientar as suas campanhas de marketing (Asniar & Surendro, 2019).

Com a evolução da Inteligência Artificial, o marketing preditivo sofreu uma transformação significativa. A IA foi identificada como uma das cinco principais áreas de inovação no marketing

contemporâneo, (Shaik, 2023), o que levou ao aumento do uso de tecnologias como o *machine learning* e o *deep learning* na previsão de comportamentos e preferências dos consumidores. Estas ferramentas permitem às empresas antecipar necessidades dos clientes, personalizar ofertas em tempo real e otimizar as suas estratégias de comunicação (Belk, Belanche & Flavian., 2023). O marketing preditivo tem atraído um interesse crescente, por parte das empresas, devido aos seus benefícios, como o aumento das receitas, personalização das interações e retenção de clientes, resultante de comunicações nas redes sociais, transações digitais e dispositivos móveis. (Verma et al, 2021). O uso da análise preditiva pode ser muito vantajoso na ótica das empresas, pois ajuda as organizações a otimizar o envolvimento dos clientes, a direcionar audiências com precisão e a aumentar a eficiência geral do marketing. Estes avanços, no ramo da inteligência artificial, têm aberto novas possibilidades para que as empresas mantenham a sua competitividade, num painel de negócios cada vez mais orientado por dados.

Embora a AP e a IA ofereçam vantagens competitivas significativas, também levantam importantes questões éticas. Os sistemas de marketing baseados em IA podem amplificar preconceitos existentes, o que conduz a decisões discriminatórias e injustas. Além disso, a capacidade destas tecnologias para manipular comportamentos de consumo levanta preocupações legítimas sobre privacidade e consentimento. A utilização deste tipo de tecnologias no marketing pode originar desequilíbrios de poder entre empresas e consumidores, especialmente quando os dados pessoais são explorados sem transparência ou controlo adequado por parte dos indivíduos (Chintalapati & Pandey, 2022).

Neste sentido, Naz e Kashif (2023) reforçam a importância de um equilíbrio entre inovação e responsabilidade, alertando para a necessidade de práticas éticas e reguladas na aplicação da IA no marketing. As empresas devem, assim, desenvolver estratégias orientadas por dados que respeitem os princípios de justiça, transparência e proteção da privacidade dos consumidores.

Em suma, o marketing preditivo, impulsionado pela IA, tornou-se uma componente central das estratégias empresariais modernas, permitindo não apenas compreender o comportamento do consumidor, mas também antecipar tendências futuras. Contudo, a sua aplicação exige um olhar crítico e ético, assegurando que os avanços tecnológicos não comprometam os direitos fundamentais dos indivíduos.

2.2 Conduta de ética no uso da Inteligência Artificial e Dados Pessoais

O uso da análise preditiva e da IA no marketing constitui uma ferramenta poderosa, capaz de originar vantagens competitivas significativas. No entanto, o seu uso levanta preocupações éticas relevantes, principalmente no que diz respeito à recolha, tratamento e uso de dados pessoais dos consumidores. Estas preocupações incluem a criação de preconceitos e desigualdades, práticas de recolha pouco transparentes, riscos à privacidade e até a possibilidade de manipulação do comportamento dos consumidores (Fassiaux, 2023).

2.2.1 Definição de Ética aplicada à IA

De acordo com Kazim e Koshiyama (2021) a ética é o estudo racional e sistemático dos princípios que distinguem o certo do errado. Já a moralidade refere-se, de forma mais comum na língua portuguesa, às noções de bem e mal no comportamento humano do dia a dia.

A ética da Inteligência Artificial consolidou-se como um campo de estudo emergente, impulsionado pelas crescentes preocupações relativas ao impacto social, económico e tecnológico da IA. Inserida no domínio mais amplo da ética digital, esta área tem como finalidade refletir de forma crítica sobre os desafios éticos associados ao uso de tecnologias digitais, como a Inteligência Artificial e o *Big Data*. A ética aplicada a estas tecnologias abrange questões morais, sociais e políticas, analisando aspetos como a autonomia, a justiça, a responsabilidade, a transparência e até os impactos ambientais decorrentes do seu desenvolvimento e aplicação (Kazim & Koshiyama, 2021).

Na adoção da IA, as organizações deparam-se com preocupações éticas que envolvem a privacidade, segurança e conformidade regulatória, exigindo uma abordagem cuidadosa e responsável. (Naz & Kashif, 2023).

2.2.2 Dilemas éticos

O avanço da Inteligência Artificial tem trazido inúmeras oportunidades para a inovação e a eficiência em diversos setores, mas também tem colocado em evidência uma série de dilemas éticos que desafiam os limites da responsabilidade tecnológica. Entre os mais debatidos estão a privacidade e a proteção de dados pessoais, frequentemente comprometidas por práticas de recolha massiva de dados, bem como os riscos associados à manipulação de comportamentos e à discriminação algorítmica. Estes dilemas representam as realidades no impacto direto sobre os

direitos, a dignidade e a autonomia dos indivíduos. Neste capítulo, são analisadas estas duas dimensões críticas, onde é destacado os riscos éticos e sociais associados à utilização da IA sem uma regulação adequada, e sublinhar a importância de princípios como a transparência, a equidade e a responsabilidade no seu desenvolvimento e aplicação.

Privacidade e Proteção de Dados

A *Internet* é um fator fundamental no debate sobre a privacidade da informação devido às suas capacidades incomparáveis de recolher uma larga escala de dados pessoais (nome; endereço residencial; endereço de e-mail; endereço de IP[1]; nº do cartão de identificação; ID[2] de cookie;) sobre indivíduos e as suas atividades online, o que pode comprometer as suas liberdades. Com isto, nos últimos anos foram criadas algumas legislações, com o fim de proteger os direitos e a liberdade dos indivíduos no que diz respeito à privacidade da informação.

O direito à privacidade, relativo à proteção da vida íntima, e o direito à proteção de dados, embora pareçam ter a mesma definição, são distintos. O direito à proteção de dados é mais amplo do que o direito à privacidade, pois não se limita à salvaguarda desta, pois abrange outros direitos, como a liberdade de expressão, a liberdade de informação, a saúde e a não discriminação (Regulamento UE 2016/679, 2016, art. 1.º, n.º 2; Carta dos Direitos Fundamentais da União Europeia, 2000, arts. 7.º- 8.º; Constituição da República Portuguesa, 1976, arts. 26.º e 35.º). Já o direito à privacidade é considerado um direito fundamental, consagrado no artigo 8.º da Convenção Europeia dos Direitos Humanos (1950) e no artigo 12.º da Declaração Universal dos Direitos Humanos (1948), podendo ser restringido apenas quando necessário para proteger um interesse coletivo relevante.

De acordo com a Constituição da República Portuguesa (CRP) (1976, art. 26, n.º 1) refere "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação." No artigo 35º, alínea 1, sobre a utilização da informática, diz que os cidadãos têm o direito de retificação, atualização e conhecer a finalidade e a que se destinam, todos os seus dados que são informatizados. Ainda no artigo 35º, alínea 3, a CRP refere que "a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação

[1] IP – *Internet Protocol*
[2] ID – Identity

partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis."

A proteção de dados surgiu como uma resposta à crescente digitalização e ao aumento da recolha e processamento de informações pessoais, que levantaram preocupações quanto à privacidade e segurança dos dados individuais.

Segundo o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, no artigo 4, alínea nº1 estabelece que a definição de dados pessoais é "informação relativa a uma pessoa singular identificada ou identificável (…), como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."

Manipulação e discriminação algorítmica

A integração da IA no marketing suscita preocupações relativas à manipulação do comportamento dos consumidores. Sistemas de marketing preditivo, ao utilizarem técnicas avançadas, têm a capacidade de influenciar as decisões dos clientes, levantando questões éticas sobre os limites entre persuasão legítima e manipulação indevida (Verma, 2019).

Segundo Mühlhoff (2021, p.685) "Existe um significado negativo e um significado neutro para "discriminação": a conotação negativa implica o tratamento injusto de certos grupos sociais ou demográficos, enquanto o significado etimologicamente mais original e neutro refere-se ao ato de distinguir casos e possibilidades entre si.". No que diz respeito à análise preditiva, esta é feita para discriminar, no sentido neutro do conceito. O objetivo é realizar distinções, com base em dados, e ser parcial em relação aos atributos que se correlacionam como uma variável alvo fixa. A análise preditiva tem tendência para compilar indivíduos em grupos baseados nas semelhanças e diferenças, de acordo com categorias como o género, origem étnica, classe social, nível de capital, estatuto social ou nível de habilitações literárias. Este sistema pode levar à criação de padrões discriminatórios e à intensificação de desigualdades sociais, principalmente quando tais práticas são "desenhadas" com o objetivo de tratar estes grupos de forma diferente no acesso a recursos e informações.

2.2.3 Regulamentos e Legislações

Regulamento Geral de Proteção de Dados (RGPD)

O Regulamento Geral de Proteção de Dados é uma lei da União Europeia criada em 2016, que entrou em vigor no dia 25 de maio de 2018. Enquanto regulamento, o RGPD procura harmonizar a legislação de proteção de dados. Aplica-se tanto aos controladores como aos processadores de dados pessoais que tratam dos dados de cidadãos da UE (Niebel, 2021). Este regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados contidos em ficheiros. A sua finalidade é estabelecer um regime regulatório de circulação e tratamento de dados pessoais, de forma complexa, o que assegura um maior controlo e proteção desses dados (Tamburri, 2020).

"O espírito do RGPD é destacado através de sete princípios: licitude, lealdade e transparência, limitação de finalidades, minimização de dados, exatidão, limitação da conservação, integridade e confidencialidade, e responsabilidade." (ICO, 2019). Uma das características notáveis deste regulamento é a gama de direitos individuais que são fornecidos aos consumidores. Estes incluem o direito de ser informado, de acesso à informação, de retificação, de extinção, de limitar tratamento de portabilidade de dados, de oposição ao tratamento, incluindo a oposição à tomada de decisão automatizada quanto exclusivamente realizadas por algoritmos (Parlamento Europeu & Conselho da União Europeia, 2016).

De acordo com o Regulamento Geral sobre a Proteção de Dados (União Europeia, 2016), o titular dos dados tem o direito de não ser sujeito a decisões exclusivamente automatizadas, incluindo a definição de perfis, que produzam efeitos na sua esfera jurídica ou que os afetem de forma significativa. Isto abrange, por exemplo, decisões automatizadas sobre preços personalizados, recusa de crédito, segmentação de marketing ou exclusão de benefícios.

Para além disso, esta lei impõe a obrigação de transparência algorítmica, o que implica que as organizações devem explicar, de forma clara e compreensível, como funcionam os modelos de IA que tratam dados pessoais. Esta exigência choca, muitas vezes, com a complexidade dos algoritmos de *machine learning* e *deep learning*, que nem sempre permitem uma explicação direta ou acessível.

O artigo 5º, estabelece que o princípio da minimização de dados obriga a que apenas sejam recolhidos os dados estritamente necessários para o fim pretendido. Contudo, muitos sistemas de IA funcionam melhor com grandes volumes de dados. A conformidade com o RGPD, nestes casos, exige um equilíbrio entre desempenho tecnológico e respeito pelos direitos fundamentais dos titulares de dados.

2.3 Comportamento de compra do consumidor no online

O comportamento do consumidor (CC) reflete o conjunto de decisões dos consumidores relacionados com a compra, o consumo e a disposição de produtos e serviços. Este é influenciado por alguns fatores externos como a cultura, a sociedade, as necessidades, o estilo de vida e a situação económica (Olan, Suklan, Arakpogun & Robson, 2024). Os profissionais de marketing consideram o CC como um processo contínuo pois, se através da obtenção de um produto ou serviço, as expectativas dos consumidores forem satisfeitas ou ultrapassadas, a probabilidade de estes repetirem a compra, aumenta.

Nesta nova era digital, a tecnologia tem vindo a desempenhar um papel crucial no estabelecimento de estratégias de marketing e na evolução da economia. Consequentemente, originou uma mudança no comportamento do consumidor e nas suas atitudes, em relação à decisão de compra (Robbins, 2020). Certas redes de IA estabelecem relações entre os produtos e serviços com as respostas emocionais dos consumidores, enquanto analisam padrões de compras e atitudes dos clientes, em diversas localidades geográficas. Para além disto, essas mesmas redes utilizam ferramentas de marketing analíticas, com o objetivo de visar estrategicamente produtos e serviços, que correspondem aos interesses e necessidades dos consumidores.

Desde a crise pandémica originada pela Covid-19, registou-se um crescimento significativo nas compras realizadas nas plataformas online, o que originou uma mutação na perceção e nos hábitos dos consumidores. O conhecimento sobre ferramentas digitais tornou-se uma necessidade, tornando o uso da tecnologia digital e dos serviços online como parte integrante da nova realidade. Para se adaptarem a este novo contexto, os consumidores começaram a utilizar serviços que nunca tinham explorado, e descobriram as vantagens e a segurança da entrega ao domicílio. Desde então, pode-se afirmar que a internet se tornou o principal meio para adquirir produtos e serviços essenciais, sendo este método de compra amplamente considerado indispensável (Dias, Gonçalves, Pereira & Dias, 2023).

A pandemia do Covid-19 originou mudanças significativas no comportamento dos consumidores, incluindo o aumento da atividade de compras *online*, a evolução dos fatores de influências, o fortalecimento das relações, a mudança nas prioridades dos mesmos e a adaptação às compras *online* (Gu, Slusarczyc, Kovalyona & Sakhbieva, 2021). Alguns determinantes que influenciam o comportamento de compras dos consumidores online, são a conveniência, recomendações e avaliações digitais, impacto dos influenciadores, descontos, experiência do utilizador, design do site e interação nas redes sociais. As variáveis que não alteraram, nos últimos 15 anos, foram o preço, a qualidade e a necessidade de compra (Antosova, Psurny & Stavkova, 2023).

2.4 Perceção do Consumidor sobre Inteligência Artificial e Análise Preditiva, Privacidade e Confiança online

2.4.1 Perceção do consumidor sobre Inteligência Artificial e Análise Preditiva

A perceção dos consumidores em relação a estas tecnologias é ambivalente, existe aprovação no que toca à melhoria na experiência de compra e suporte, mas existem receios relacionados à privacidade, segurança e impacto social no uso da IA e da Análise Preditiva.

De acordo com Ozturk (2024, p. 8) a perceção dos consumidores em relação à IA e à AP ainda apresenta alguns elementos de preocupação, nomeadamente no que diz respeito à confiança, privacidade e ética. Estas inquietações surgem devido à possibilidade de uso inadequado das informações pessoais, à não transparência das decisões tomadas pelos sistemas baseados nesta tecnologia e à ameaça aos direitos dos indivíduos, através de discriminação, Ozturk (2024, p. 8). Além disso, muitos consumidores encaram estas ferramentas como uma ameaça ao mercado de trabalho, o que contribui para a resistência à sua adoção e utilização. Perante este cenário, torna-se bastante importante que as empresas reforcem a transparência e comuniquem de forma clara os benefícios e limitações associados a estas tecnologias.

Por outro lado, quando estas ferramentas são aplicadas com o objetivo de melhorar a experiência do cliente, há uma perceção mais favorável. Este resultado é especialmente favorável quando existe um atendimento contínuo, respostas rápidas e soluções personalizadas que vão ao encontro das necessidades e preferências dos consumidores. No entanto essa aceitação está fortemente condicionada pela confiança na proteção da privacidade e utilização ética dos dados pessoais. (Ozturk, 2024).

2.4.2 Preocupações de Privacidade e Confiança do Consumidor Online

Apesar das plataformas, baseadas em IA, promoverem benefícios para os utilizadores, ao terem acesso às suas informações, persistem preocupações entre os mesmos, relativamente à proteção da sua privacidade. A preocupação com a privacidade, pode ser definida como o conjunto de receios que os utilizadores têm em relação à forma como as organizações recolhem, utilizam e processam as suas informações pessoais. No contexto digital, esta preocupação pode ser influenciada pelas experiências prévias dos consumidores com invasões de privacidade, bem como por aspetos individuais como a sexualidade, a idade e a cultura (Cheng, Mei Zhong & Gao, 2021).

Os quatro fatores principais que influenciam as preocupações gerais dos utilizadores, em relação à privacidade, são a recolha de dados, os erros nos dados, a utilização secundária não autorizada dos dados e o acesso inadequado aos dados. (Smith, Milberg & Burke, 1996). Cheng et al referem (2021, p.811) "Na era da informação, os dados de privacidade dos consumidores são frequentemente recolhidos, e os investigadores descobriram que as preocupações com a privacidade e as atividades relacionadas com a proteção da mesma, como o risco de segurança da informação, podem influenciar o comportamento de compra dos consumidores.". O valor e a confiança percecionados pelos consumidores em relação às empresas, especialmente no que diz respeito à segurança no uso dos seus dados, possuem uma influência significativa na intenção de compra.

Capítulo 3 – Metodologia de Investigação

3.1 Modelo Conceptual e Hipóteses de Investigação

O modelo conceptual proposto para esta investigação procura explorar a relação entre diversas variáveis individuais e percecionais no contexto da confiança e privacidade em ambientes de comércio eletrónico. As variáveis independentes analisadas incluem a idade, o nível de escolaridade, experiências prévias com violações de privacidade, reputação da empresa e conhecimento sobre Inteligência Artificial (IA) e bem como, a Análise Preditiva (AP). Estas variáveis são estudadas em relação à variável mediadora, a preocupação com a privacidade, e às variáveis dependentes, como a intenção de compra online e a disposição para partilhar dados pessoais Este modelo foi delineado com o objetivo de compreender que fatores influenciam a confiança dos consumidores, a sua preocupação com a privacidade, e em que medida estas

influenciam a decisão de partilhar dados pessoais com empresas que utilizam tecnologias baseadas em IA e AP.

As hipóteses formuladas para testar este modelo são as seguintes:

Tabela 1

	Hipóteses
Hipótese 1 a)	Consumidores mais jovens percebem melhor os riscos de privacidade do que os consumidores mais velhos
Hipótese 1 b)	Consumidores com maior nível de escolaridade percebem melhor os riscos de privacidade.
Hipótese 2 a)	Indivíduos mais velhos tendem a confiar menos nas empresas em relação à proteção dos seus dados pessoais.
Hipótese 2 b)	Indivíduos com maior nível de escolaridade tendem a confiar menos nas empresas em relação à proteção dos seus dados pessoais.
Hipótese 3	Existe uma associação negativa entre a preocupação com privacidade e a frequência de compras online.
Hipótese 4	As frequências de compra online são diferentes se o consumidor sofreu ou não violações de privacidade.
Hipótese 5	Existe associação entre o nível de conhecimento dos consumidores com Inteligência Artificial e Análise Preditiva e a sua compreensão sobre como estas tecnologias utilizam os seus dados.
Hipótese 6	Existe uma associação positiva entre o grau de confiança dos consumidores nas empresas e a sua frequência de realizar compras online.
Hipótese 7	Consumidores que realizam compras online com maior frequência estão mais dispostos a partilhar dados pessoais sensíveis.
Hipótese 8	Consumidores que leem políticas de privacidade com maior frequência apresentam níveis mais elevados de conhecimento sobre riscos de privacidade.
Hipótese 9	Consumidores de menor faixa etária apresentam maior compreensão sobre como a IA e a Análise Preditiva utilizam os seus dados.
Hipótese 10	Consumidores com maior familiaridade com IA e Análise Preditiva leem políticas de privacidade com maior frequência.

A Tabela 2 recorda os objetivos definidos no início desta investigação enquanto a Tabela 3 apresenta a relação entre as hipóteses, a secção do questionário, e os objetivos de investigação.

Tabela 2

	Objetivos de Investigação
Objetivo 1	Comparar perceções de privacidade e confiança entre grupos demográficos (idade e escolaridade).
Objetivo 2	Avaliar se as preocupações com a privacidade influenciam a frequência de compras online.
Objetivo 3	Medir o nível de conhecimento dos consumidores sobre IA e análise preditiva e a sua compreensão do uso de dados.
Objetivo 4	Explorar a relação entre a frequência de compras online e a disposição para partilhar dados pessoais.
Objetivo 5	Analisar o impacto da leitura de políticas de privacidade no conhecimento dos riscos associados ao uso de dados.
Objetivo 6	Identificar diferenças geracionais na compreensão do uso de dados por IA.
Objetivo 7	Examinar se a familiaridade com IA e análise preditiva está associada a maior leitura de políticas de privacidade.

Tabela 3

Tabela de relação entre Hipóteses, Secção do Questionário e Objetivos de Investigação

Hipóteses	Secção do Questionário	Objetivos de Investigação
H1	Secção 1 e 6	O1
H2	Secção 2 e 6	O1
H3	Secção 1 e 6	O2
H4	Secção 3 e 6	O2
H5	Secção 4	O3
H6	Secção 2 e 6	O2
H7	Secção 5 e 6	O4
H8	Secção 1 e 5	O5

H9	Secção 4 e 6	O6
H10	Secção 1 e 4	O7

3.2 Metodologia

O presente estudo adota uma abordagem quantitativa, com a finalidade de analisar as preocupações de privacidade dos consumidores online, em relação à conduta das empresas, quando utilizam Inteligência Artificial e Análise Preditiva, para influenciar o comportamento de compra.

A escolha da abordagem quantitativa justifica-se pela necessidade de recolher dados generalizáveis que permitam testar hipóteses, identificar padrões de comportamento e relações estatisticamente significativas entre variáveis. Este tipo de abordagem permite, ainda, avaliar o impacto de fatores demográficos e comportamentais nas atitudes dos consumidores, por meio de técnicas estatísticas rigorosas.

A análise quantitativa envolve o uso de métodos estatísticos, para descrever, sintetizar, comparar e identificar ligações entre variáveis. Esta possibilita testar hipóteses e realizar previsões com base em dados (Slater & Hasson, 2025). Para tal, recorreu-se à aplicação de um questionário estruturado como instrumento de recolha de dados.

3.3 Instrumento de Recolha de Dados

Os dados foram recolhidos através de um questionário *online*, que foi criado na plataforma *Google Forms*. A sua partilha foi feita através de redes sociais, como o *Instagram*, *Whatsapp* e *Facebook*, com a intenção de alcançar o maior número de indivíduos possíveis, para suportarem a veracidade deste estudo.

Os participantes foram informados sobre a natureza voluntária da sua participação, garantindo-se o anonimato e confidencialidade das respostas, de acordo com o Regulamento Geral sobre a Proteção de Dados (RGPD). Um termo de consentimento informado foi incluído no início do questionário, onde se detalhou os objetivos do estudo, o tempo estimado de resposta e os direitos dos inquiridos.

O questionário foi composto por 18 perguntas, divididas em 6 secções principais:

1. Conhecimento e comportamento relacionados à privacidade online: questões sobre a perceção de riscos de privacidade, hábitos de leitura de políticas de privacidade e avaliação da possibilidade de uso indevido de dados pessoais.
2. Confiança nas empresas e partilha de dados pessoais: perguntas sobre experiências de desconfiança em plataformas digitais, motivos para evitar fornecer informações e perceção da segurança oferecida pelas empresas.
3. Impacto das preocupações e experiências na compra online: avaliação de situações em que receios ou violações de privacidade influenciaram a decisão de compra e alteração da intenção de compra após experiências negativas.
4. Conhecimento sobre IA e Análise Preditiva: análise do nível de familiaridade e compreensão sobre estas tecnologias, bem como da perceção dos tipos de dados recolhidos para personalização.
5. Reputação e confiança na partilha de dados: questões sobre a influência da reputação das empresas na confiança do consumidor e sobre a predisposição em fornecer diferentes tipos de dados pessoais (nome, contacto, localização, informação financeira).
6. Perfil do respondente: recolha de dados sociodemográficos, incluindo género, faixa etária, nível de escolaridade e frequência de compras online.

A maioria das questões foram de escolha fechada, com escalas de *Likert* de 5 pontos (1 = discordo totalmente, 5 = concordo totalmente), permitindo mensurar atitudes e perceções de forma objetiva. O tempo estimado para preenchimento foi de 5 a 7 minutos.

3.4 Procedimento de Análise de Dados

No final do período de recolha, foram obtidas 394 respostas completas e válidas, que constituíram a base para a análise estatística desta investigação. Após a conclusão desta fase, os dados foram cuidadosamente exportados e preparados para tratamento no software *IBM SPSS Statistics*, reconhecido pela sua fiabilidade e robustez na análise quantitativa em contextos científicos.

Numa primeira etapa, procedeu-se à codificação das variáveis, adaptando-as à estrutura necessária para análise no SPSS. As variáveis foram classificadas de acordo com a sua natureza, nominais ou ordinais, que assegura que, na fase subsequente, fossem aplicados os testes estatísticos mais adequados. No caso das questões com escalas de *Likert*, cada categoria de resposta foi convertida

em valores numéricos, o que preservou a ordem lógica da escala. Já as questões de múltipla escolha foram recodificadas em variáveis binárias, que assumiram o valor 0 quando a opção não foi assinalada e 1 quando foi selecionada, o que permitiu uma a análise individual de cada item.

A análise estatística iniciou-se com uma abordagem descritiva, de forma a caracterizar a amostra e fornecer um enquadramento inicial sobre as tendências de resposta. Foram calculadas frequências absolutas e relativas. Esta etapa permitiu obter um retrato global da distribuição das respostas e do perfil dos participantes.

Numa fase posterior, passou-se à análise inferencial, com o intuito de testar as hipóteses de investigação previamente formuladas. Para identificar associações e diferenças significativas entre grupos, foram aplicados testes estatísticos não paramétricos adequados à natureza das variáveis em estudo. Assim, para variáveis categóricas, recorreu-se ao teste do Qui-quadrado de independência, o que permitiu avaliar relações entre diferentes categorias de resposta. Quando o objetivo foi comparar medianas entre dois ou mais grupos independentes em variáveis ordinais, utilizaram-se os testes *Mann-Whitney* U *e Kruskal-Wallis*, respetivamente.

No caso da análise de relações uniformes entre variáveis ordinais, optou-se pelo coeficiente de correlação de *Spearman*, apropriado para avaliar a intensidade e direção da associação entre duas variáveis não paramétricas. Em todos os testes realizados, foi adotado um nível de significância de 5% (α= 0,05), considerando-se estatisticamente significativos os resultados com valores de p inferiores a este limiar.

Esta metodologia de análise, cuidadosamente estruturada e alinhada com os objetivos e hipóteses da investigação, permitiu extrair conclusões fundamentadas e estatisticamente robustas, garantindo a coerência entre a recolha de dados, o tratamento aplicado e a interpretação dos resultados obtidos.

3.5 Caracterização da Amostra

A amostra deste estudo é composta por 394 participantes, selecionados através de métodos de amostra não probabilísticos por conveniência e por bola de neve.

A amostragem por conveniência é um método de recrutamento de participantes que se baseia na facilidade de acesso e disponibilidade do investigador. O método de seleção utilizado, neste estudo, foi por meio de anúncios nas redes sociais onde se conseguiu alcançar membros da

população de interesse. A técnica de bola de neve é uma estratégia na qual um ou vários participantes iniciais, escolhidos de uma forma não aleatória, indicam ou convidam os seus contactos, que por sua vez fazem o mesmo com outras pessoas, criando assim uma sequência de referências. (Morris & Wesson, 2022).

Embora estas técnicas não permitam generalização estatística para toda a população, proporcionam uma amostra suficientemente diversa para explorar padrões relevantes no comportamento do consumidor digital. A amostra abrangeu diferentes faixas etárias, níveis de escolaridade e níveis de familiaridade com tecnologias digitais.

3.5.1 Estatística Descritiva

De forma a aprofundar a compreensão sobre o perfil dos participantes, recorreu-se à aplicação de estatística descritiva e estatística descritiva bivariada na caracterização da amostra. A estatística descritiva permitiu resumir e apresentar de forma clara as principais variáveis sociodemográficas e comportamentais, utilizando medidas como frequências e percentagens. Já a estatística descritiva bivariada possibilitou a análise das relações entre pares de variáveis, o que fornece uma visão mais detalhada sobre possíveis associações e padrões no grupo estudado.

Esta combinação de métodos ajudou a enquadrar melhor as etapas seguintes da investigação, o que permitiu que a interpretação dos resultados fosse feita com base no contexto real e nas características concretas da amostra. De seguinte, apresentam-se as tabelas e gráficos resultantes destas análises, que evidenciam o perfil e a diversidade dos participantes envolvidos no estudo.

Este estudo contou com 394 respostas válidas, das quais 169 (42,9%) correspondem a indivíduos do sexo masculino e 225 (57,1%) ao sexo feminino, como representa a Tabela 4.

Tabela 4

Estatística Descritiva da variável Género

Género	Frequência	Percentagem
Masculino	169	42,9
Feminino	225	57,1
Total	394	100,0

Nota: dados da pesquisa do autor (2025)

Relativamente à faixa etária, a maioria dos participantes situa-se entre os 18 e os 24 anos (29,4%), seguida pelas faixas dos 45-54 anos (19,3%) e dos 55-64 anos (18,5%). Outras faixas etárias representadas incluem os 25-34 anos (17,8%), 35-44 anos (9,1%), e mais de 65 anos (5,1%). A faixa etária com menor representação foi a dos menores de 18 anos, com apenas 0,8% da amostra, indicado na Tabela 5.

Tabela 5

Estatística Descritiva da variável Faixa Etária

Faixa Etária	Frequência	Percentagem
Menos de 18 anos	3	0,8
18 – 24 anos	116	29,4
25 – 34 anos	70	17,8
35 – 44 anos	36	9,1
45 – 54 anos	76	19,3
55 – 64 anos	73	18,5
Mais de 65 anos	20	5,1
Total	394	100,0

Nota: dados da pesquisa do autor (2025)

No que diz respeito ao nível de escolaridade, a maior parte dos participantes possui licenciatura (40,9%), seguida do ensino secundário (33,5%). Participantes com mestrado representam 17,3%, enquanto 5,6% possuem pós-graduação e 1,3% possuem doutoramento. Apenas 1,5% dos respondentes indicaram ter o ensino básico como nível de escolaridade, conforme demonstrado na tabela seguinte.

Tabela 6

Estatística Descritiva da variável Nível de Escolaridade

Nível Escolaridade	Frequência	Percentagem
Ensino básico	6	1,5
Ensino secundário	132	33,5

Licenciatura	161	40,9
Pós-Graduação	22	5,6
Mestrado	68	17,3
Doutoramento	5	1,3
Total	394	100,0

Nota: dados da pesquisa do autor (2025)

Observa-se que a maioria dos participantes indicou realizar compras online "Às vezes" (41,6%), seguida de "Frequentemente" (29,2%). Uma proporção menor declarou comprar "Raramente" (22,1%), enquanto 5,1% afirmaram "Nunca" efetuar compras online. Apenas 2,0% reportaram realizar compras online "Sempre". (vide tabela 7) Estes resultados sugerem que, embora a compra online seja uma prática comum entre os respondentes, a frequência varia consideravelmente, com predominância de um comportamento moderado.

Tabela 7

Estatística Descritiva da variável Frequência de Compras *Online*

Freq compras online	Frequência	Percentagem
Nunca	20	5,1
Raramente	87	22,1
Às vezes	164	41,6
Frequentemente	115	29,2
Sempre	8	2,0
Total	394	100,0

Nota: dados da pesquisa do autor (2025)

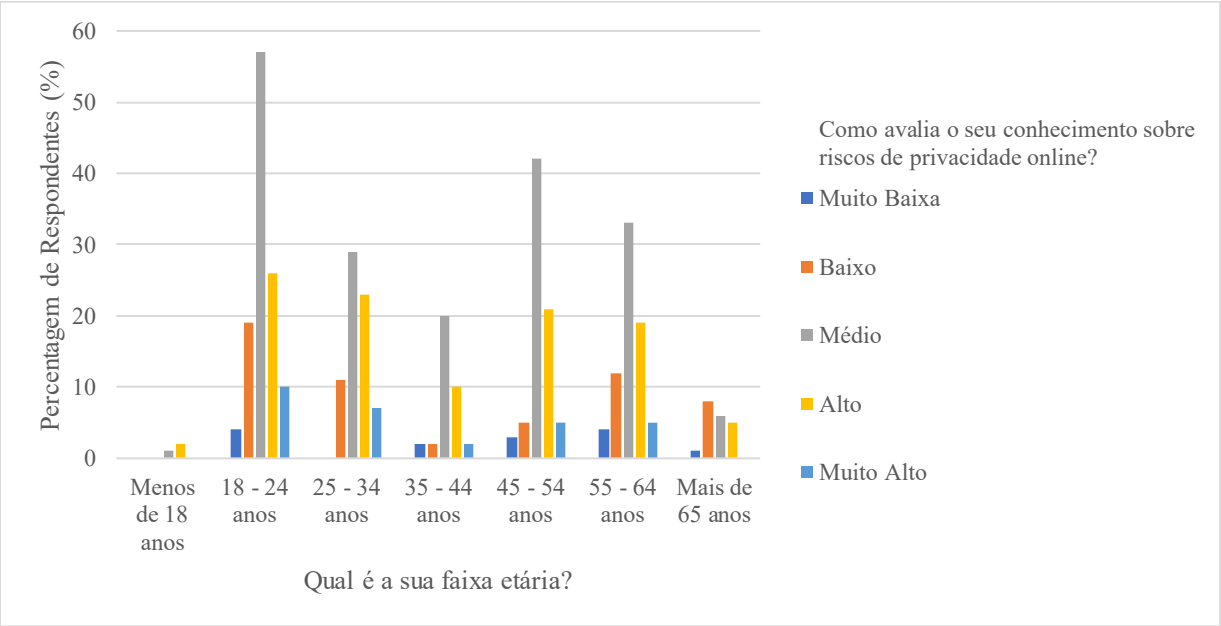
A análise dos dados por faixa etária revela padrões interessantes na perceção sobre riscos de privacidade online. Os indivíduos entre os 18 e 24 anos destacam-se com as maiores percentagens nos níveis "Médio" (cerca de 57%) e "Alto" (26%), o que evidencia uma perceção consideravelmente elevada. Já nas faixas etárias superiores, como 55-64 anos e mais de 65 anos, observa-se uma distribuição mais equilibrada, com ligeira predominância dos níveis "Médio" e "Baixo", que indica uma perceção mais moderada, como se observa no Gráfico 1. No geral, os

dados sugerem que os participantes mais jovens demonstram uma perceção mais elevada dos riscos de privacidade online, o que pode refletir uma maior exposição ou sensibilização a temas digitais.

Estes resultados parecem apoiar a hipótese de que os consumidores mais jovens têm uma maior perceção sobre os riscos de privacidade online quando comparados com os consumidores mais velhos, o que pode estar relacionado com uma maior familiaridade com o ambiente digital e com o uso frequente de plataformas online que envolvem partilha de dados pessoais.

Gráfico 1

Distribuição percentual da perceção sobre riscos de privacidade online por faixa etária



Nota: dados da pesquisa do autor (2025)

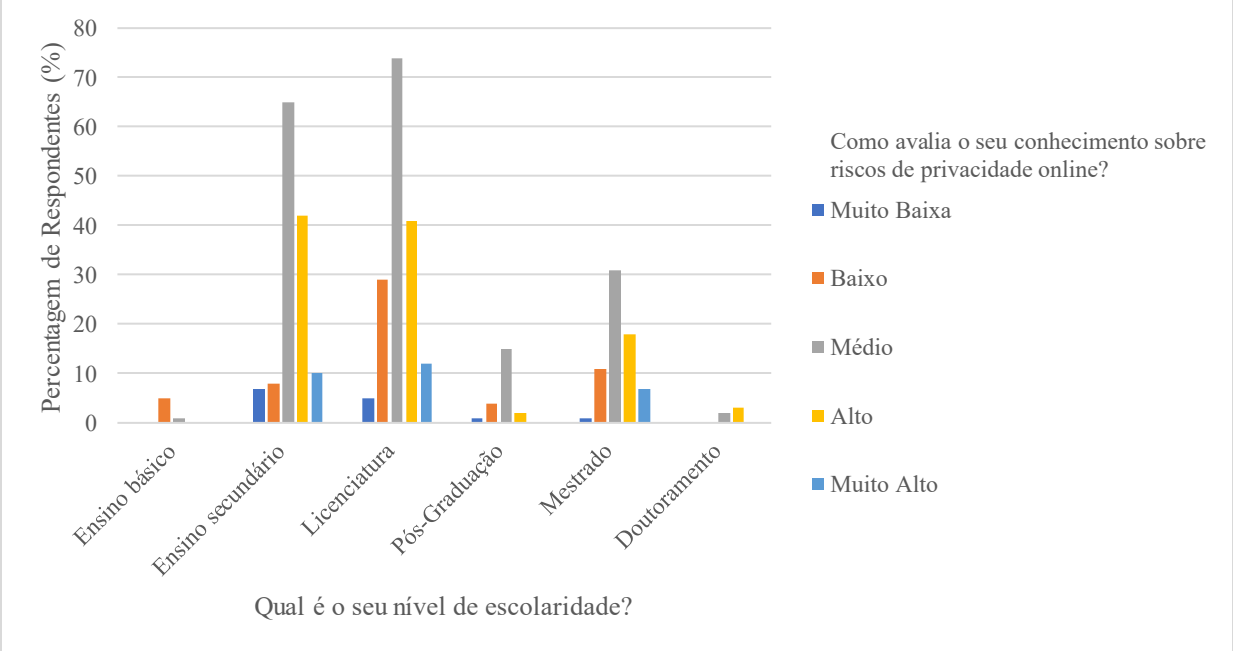
No que respeita ao nível de escolaridade, os dados mostram que a perceção dos riscos de privacidade online varia de forma significativa. Os participantes com ensino secundário e licenciatura representam os maiores grupos, sendo nestes que se concentra a maioria das perceções classificadas como "Médio" (66% e 74%, respetivamente). Curiosamente, no ensino secundário também se destaca uma elevada percentagem no nível "Alto" (38%). Já nos níveis mais altos de escolaridade, como mestrado e doutoramento, a distribuição torna-se mais uniforme, mas com tendência para os níveis "Médio" e "Alto". O grupo com ensino básico, apesar de pequeno, revela sobretudo perceções "Baixas". Estes resultados indicam que a perceção dos riscos de privacidade

tende a aumentar ligeiramente com a escolaridade, embora não de forma linear, sendo o nível "Médio" o mais comum em quase todos os graus de ensino, constatado no gráfico 2.

Em suma, os dados parecem confirmar parcialmente a hipótese de que níveis mais altos de escolaridade estão associados a uma maior perceção dos riscos de privacidade. No entanto, a relação não é absoluta: também se encontram perceções elevadas entre indivíduos com ensino secundário, e perceções baixas entre licenciados. Isto sugere que a escolaridade é um fator relevante, mas não o único a influenciar esta perceção, havendo provavelmente o contributo de outras variáveis como experiência digital, interesse pelo tema, ou exposição a situações de risco.

Gráfico 2

Distribuição percentual da perceção sobre riscos de privacidade online segundo o nível de escolaridade



Nota: dados da pesquisa do autor (2025)

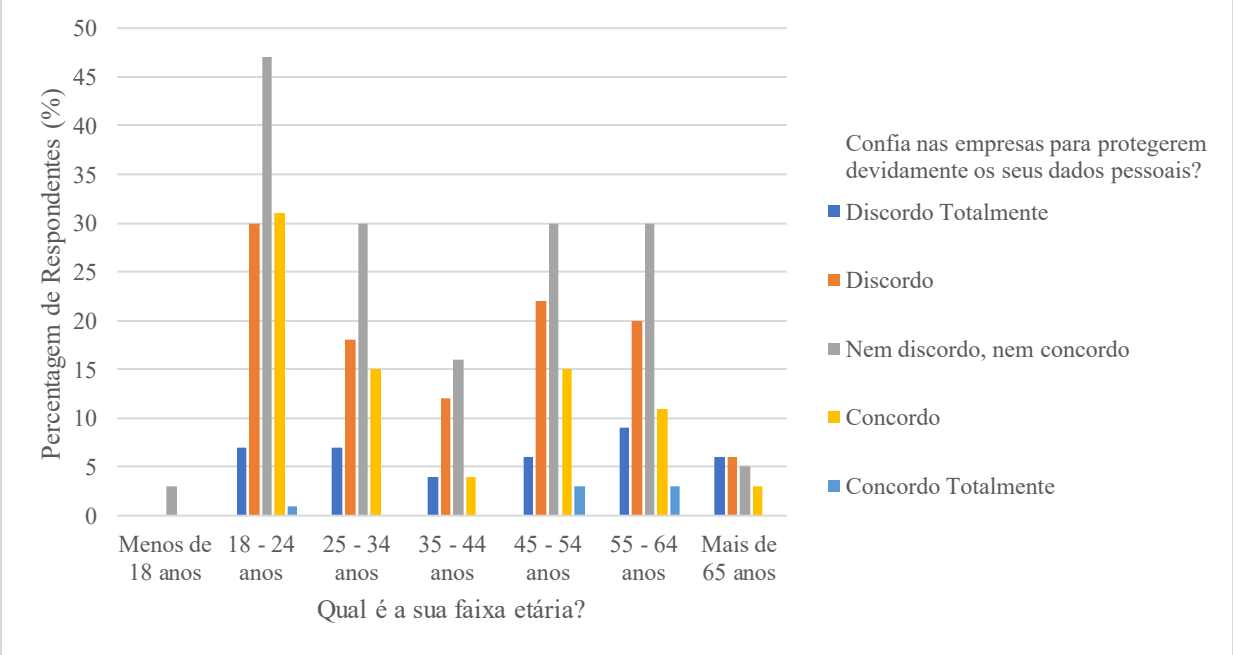
A análise da relação entre faixa etária e nível de confiança nas empresas na proteção de dados pessoais permite observar tendências importantes. De forma geral, verifica-se que os indivíduos mais jovens, especialmente do grupo 18–24 anos, são os que mais expressam níveis mais elevados de confiança: cerca de 30% concordam e aproximadamente 2% concordam totalmente com a afirmação de que as empresas protegem adequadamente os seus dados. À medida que a faixa etária

aumenta, observa-se uma redução gradual nos níveis mais elevados de concordância. Por exemplo, nas faixas 45–54 e 55–64 anos, os níveis de concordância são inferiores, com destaque para o aumento das respostas neutras ("Nem concordo, nem discordo") e discordantes, como está representado no Gráfico 3.

Esta distribuição parece sustentar a hipótese formulada: indivíduos mais velhos tendem a confiar menos nas empresas no que diz respeito à proteção dos seus dados pessoais. Ainda que o grupo mais idoso seja numericamente menor, o padrão de respostas é consistente com um maior ceticismo associado à idade.

Gráfico 3

Distribuição percentual do nível de confiança nas empresas para proteção dos dados pessoais, segundo a faixa etária



Nota: dados da pesquisa do autor (2025)

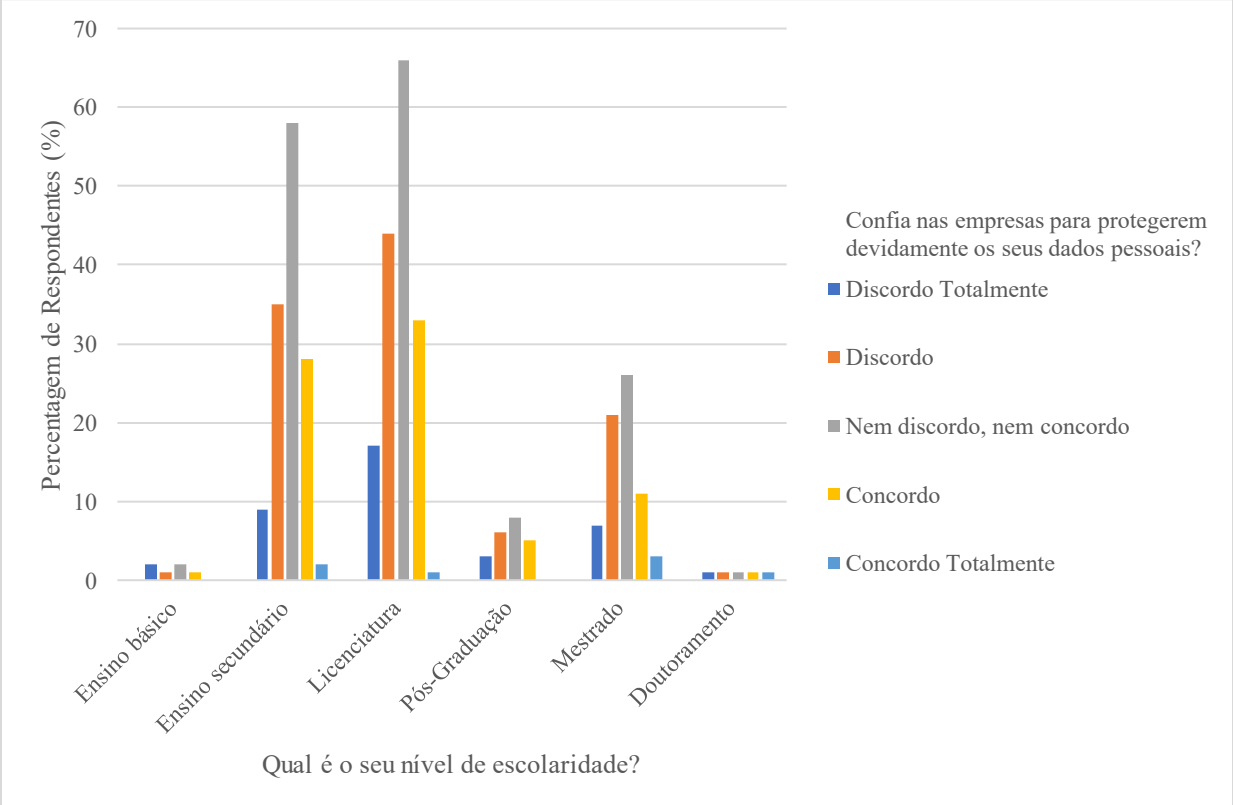
A análise da distribuição percentual da confiança nas empresas quanto à proteção de dados pessoais em função do nível de escolaridade revela uma tendência interessante, onde os indivíduos com níveis mais elevados de escolaridade, como mestrado e doutoramento, tendem a manifestar menor confiança nas empresas. Observa-se que, apesar da licenciatura representar uma grande parte da amostra, existe uma percentagem significativa de respondentes que referem níveis baixos

de confiança, particularmente aqueles que escolheram as opções “discordo” e “discordo totalmente”. Já os indivíduos com ensino secundário apresentam uma elevada neutralidade, sendo a opção “nem discordo, nem concordo” a mais selecionada. No entanto, à medida que o nível de escolaridade aumenta, nota-se uma diminuição nas respostas que expressam concordância, sendo os níveis de confiança mais baixos nos graus de pós-graduação, mestrado e doutoramento (vide gráfico 4).

Esta distribuição permite observar uma relação coerente com a hipótese, indicando que os indivíduos com maior nível de escolaridade parecem ter uma perceção mais crítica sobre a atuação das empresas no que diz respeito à proteção de dados pessoais, possivelmente devido a um maior conhecimento ou sensibilização para os riscos associados à privacidade digital.

Gráfico 4

Distribuição percentual da confiança nas empresas quanto à proteção de dados pessoais segundo o nível de escolaridade



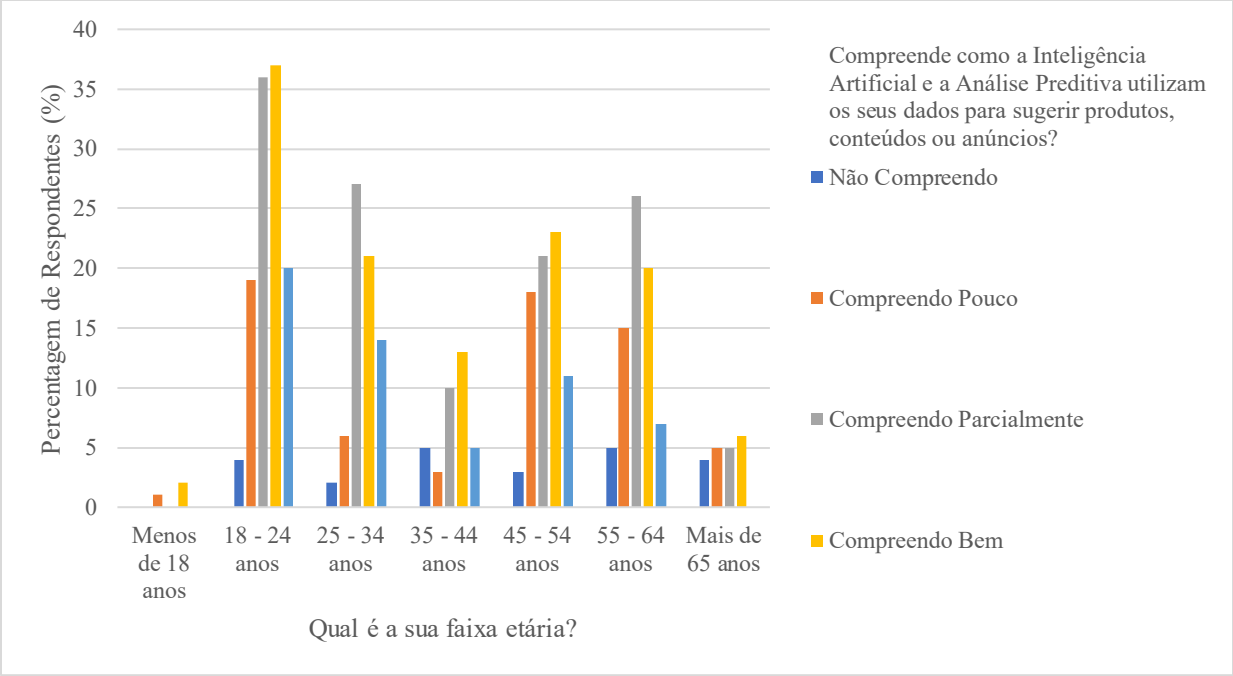
Nota: dados da pesquisa do autor (2025)

A análise da compreensão sobre como a Inteligência Artificial e a Análise Preditiva utilizam os dados pessoais para sugerir produtos, conteúdos ou anúncios, em função da faixa etária, revela padrões diferenciados de perceção. Os indivíduos mais jovens, especialmente no grupo etário dos 18 aos 24 anos, apresentam uma elevada proporção de respostas que indicam compreensão parcial ou boa, sendo estas as categorias mais frequentes nesta faixa, o que poderá estar relacionado com uma maior familiaridade com tecnologias digitais e algoritmos de recomendação. No entanto, observa-se também um número relevante de jovens que afirmam compreender totalmente o processo, o que contrasta com faixas etárias mais elevadas. Entre os indivíduos dos 25 aos 34 anos e dos 45 aos 54 anos, a compreensão parcial e boa mantém-se predominante, embora com uma ligeira redução nas respostas de compreensão total. Já nos grupos mais velhos, sobretudo acima dos 55 anos, a percentagem de respostas de não compreensão ou compreensão reduzida aumenta, sugerindo possíveis barreiras no acesso ou no conhecimento aprofundado sobre o funcionamento destas tecnologias, como indica o Gráfico 5.

Esta distribuição aponta para uma tendência em que a compreensão mais aprofundada sobre o papel da IA e da análise preditiva na personalização de conteúdos se concentra nos grupos etários mais jovens, enquanto os mais velhos revelam níveis mais baixos de familiaridade ou clareza sobre o tema.

Gráfico 5

Distribuição percentual da compreensão sobre a utilização de dados pela Inteligência Artificial e Análise Preditiva para sugerir produtos, conteúdos ou anúncios, por faixa etária



Nota: dados da pesquisa do autor (2025)

Capítulo 4 – Resultados

Para a análise dos dados recolhidos neste estudo, optou-se pela utilização de testes estatísticos não paramétricos, dada a natureza das variáveis (predominantemente ordinais e categóricas) e a ausência de normalidade em parte das distribuições, conforme avaliado previamente. Os métodos não paramétricos apresentam a vantagem de não exigirem pressupostos rigorosos sobre a forma da distribuição dos dados, o que oferece resultados robustos mesmo em amostras de menor dimensão ou assimétricas (Schober & Vetter, 2020).

O teste de *Kruskal-Wallis* foi aplicado para comparar diferenças entre três ou mais grupos independentes, quando a variável dependente era ordinal ou quando as variáveis contínuas não cumpriam os pressupostos de normalidade. Este teste baseia-se na ordenação dos valores observados e compara a distribuição entre os grupos (Schober & Vetter, 2020). Quando o teste apresentou significância estatística, procedeu-se à realização de comparações múltiplas com correção de *Bonferroni*. A correção de *Bonferroni* ajusta o nível de significância e divide o valor de α pelo número de comparações efetuadas, garantindo que a probabilidade global de rejeitar

incorretamente a hipótese nula se mantenha controlada. Apesar de ser um método conservador, é amplamente reconhecido pela sua eficácia no controlo de falsos positivos (García-Pérez, 2023).

Para a avaliação de relações entre variáveis ordinais, recorreu-se ao coeficiente de correlação de *Spearman*, uma medida não paramétrica que avalia a intensidade e direção de associações constantes, com valores compreendidos entre - 1 e 1. Este coeficiente permite identificar tendências relacionais consistentes, mesmo quando a associação não é linear (Yang & Lee, 2025).

O teste U de *Mann-Whitney* foi utilizado para comparar dois grupos independentes em variáveis ordinais ou contínuas sem distribuição normal. Assim como o *Kruskal-Wallis*, este teste baseia-se nos ranks das observações e é uma alternativa não paramétrica ao teste t de amostras independentes (Emerson, 2023).

O teste do Qui-Quadrado (x^2) foi aplicado para examinar associações entre variáveis categóricas, o que avalia a discrepância entre frequências observadas e esperadas sob a hipótese de independência. Em situações em que as frequências esperadas eram reduzidas, utilizou-se o método de Monte Carlo, que recorre a simulações repetidas para estimar o valor p de forma mais fiável (Reshid, 2023).

Após a identificação de associações significativas no teste x^2, foi calculado o V de *Cramer* para medir a força da relação, que varia entre 0 (sem associação) e 1 (associação perfeita) (Akoglu 2023). Adicionalmente, analisaram-se os resíduos ajustados para identificar quais as combinações de categorias contribuíram mais para a associação observada, valores absolutos superiores a mais ou menos 1,96 indicaram diferenças estatisticamente significativas (Okwonu, Ahad, Aoanapudor & Arunave, 2023).

4.1 Análise de Hipóteses

Hipótese 1

Para testar a Hipótese 1, a): Consumidores mais jovens percebem melhor os riscos de privacidade online do que os mais velhos foi utilizado o teste *Kruskal-Wallis*. Como mostra a tabela 8, este teste indicou que não existem diferenças estatisticamente significativas no nível de conhecimento sobre riscos de privacidade online entre as diferentes faixas etárias, H (6) = 9,461, p = 0,149. Isto quer dizer que a análise não encontrou evidências de que a idade influencia o nível de conhecimento sobre riscos de privacidade online. Ou seja, na amostra estudada, jovens e pessoas

mais velhas apresentam níveis semelhantes de perceção destes riscos. Assim, não se rejeitou a hipótese nula. Foram analisadas as comparações múltiplas entre os grupos etários através do método de *Bonferroni*, contudo, dado que o teste global de *Kruskal-Wallis* não indicou diferenças estatisticamente significativas, estas análises não foram aprofundadas.

Tabela 8

Resultado do teste de *Kruskal-Wallis* sobre conhecimento de riscos de privacidade online por faixa etária

	Estatística de tese (H)	p-valor	Resultados
Hipotese 1 a)	9,641	p = 0,419	Não se rejeita a hipótese nula

Nota: N = 394; nível de significância considerado $\alpha = 0,05$.

Para testar a hipótese de que consumidores com maior nível de escolaridade percebem melhor os riscos de privacidade online (hipótese 1b), recorreu-se ao teste de *Kruskal-Wallis*, adequado para variáveis ordinais e não paramétricas. Os resultados revelaram diferenças estatisticamente significativas entre os grupos de escolaridade quanto ao conhecimento sobre riscos de privacidade online, H (5) = 18,936, p = ,002, como mostra a tabela 9. De forma a identificar entre quais grupos essas diferenças ocorrem, foram realizadas comparações múltiplas *post-hoc* com correção de *Bonferroni*. Como se pode observar na tabela 10, os resultados indicaram que os participantes com ensino básico apresentaram perceções significativamente mais baixas sobre riscos de privacidade online quando comparados com os participantes com ensino secundário (z = -3,37, p = ,011), mestrado (z = -3,12, p = ,027) e doutoramento (z = -2,96, p = ,046).

Estes dados sugerem uma relação positiva entre o nível de escolaridade e a perceção dos riscos de privacidade online, sustentando a hipótese de que níveis mais elevados de educação estão associados a maior literacia digital e, consequentemente, a uma maior sensibilidade face a questões de privacidade e proteção de dados pessoais.

Tabela 9

Resultado do teste de *Kruskal-Wallis* sobre conhecimento de riscos de privacidade online por nível de escolaridade

	Estatística de tese (H)	p-valor	Resultados

Hipotese 1 b)	18,936	p = 0,002	Rejeita-se a hipótese nula

Nota: N = 394; nível de significância considerado α = 0,05.

As análises *post-hoc* com correção de *Bonferroni*, demonstradas na tabela 10, revelam que os participantes com ensino básico apresentaram níveis significativamente diferentes de conhecimento sobre riscos de privacidade online quando comparados com aqueles com mestrado (p = 0,027) e doutoramento (p = 0,046). Não se verificaram diferenças significativas entre os restantes grupos. Logo, os resultados indicam que a escolaridade está associada a diferenças claras no conhecimento sobre riscos de privacidade. Participantes com ensino básico revelaram menos conhecimento comparativamente a quem possui mestrado ou doutoramento. Isto sugere que níveis mais altos de formação académica podem contribuir para uma maior consciência sobre questões de privacidade.

Tabela 10

Comparações múltiplas entre grupos de escolaridade quanto à perceção dos riscos de privacidade online (teste de *Dunn* com correção de *Bonferroni*)

Comparação	Estatística z	p (ajustada)
Ensino básico - Mestrado	-3,12	0,027
Ensino básico - Ensino secundário	-3,37	0,011
Ensino básico - Doutoramento	-2,96	0,046

Nota: Teste de *Kruskal-Wallis* seguido de comparações múltiplas (*post-hoc*) com correção de *Bonferroni*. Apenas pares com diferenças estatisticamente significativas (p < ,05) estão incluídos.

Hipótese 2

Para testar a Hipótese 2, a): Indivíduos mais velhos tendem a confiar menos nas empresas, foi usado o coeficiente de correlação de *Spearman*. Este teste revelou uma associação negativa e estatisticamente significativa entre a faixa etária e a confiança nas empresas para proteger devidamente os dados pessoais (r = - 0,115, p = 0,023), conforme detalhado na tabela 11.

Foi observada uma tendência ligeira para que a confiança nas empresas diminua com a idade. Embora o efeito seja fraco, sugere que participantes mais velhos podem ser mais céticos em relação à capacidade de as empresas protegerem dados pessoais.

Tabela 11

Correlação de *Spearman* entre faixa etária e confiança nas empresas

	Coeficiente de Spearman (r)	p-valor	Resultados
Hipótese 2 a)	- 0,115	p = 0,023	Correlação negativa fraca e significativa

Nota: A correlação é significativa ao nível de 0,05 (2 extremidades).

Para testar a Hipótese 2, b): Indivíduos com maior nível de escolaridade tendem a confiar menos nas empresas, foi usado o coeficiente de correlação de *Spearman*. Este teste confirmou que não existe uma associação estatisticamente significativa entre o nível de escolaridade e a confiança nas empresas para proteger devidamente os dados pessoais (r = - 0,036, p = 0,473), de acordo com os dados representados na tabela 12.

O nível de escolaridade não mostrou impacto significativo na confiança nas empresas. Noutras palavras, independentemente da formação académica, os níveis de confiança mantiveram-se semelhantes.

Tabela 12

Correlação de *Spearman* entre o nível de escolaridade e a confiança nas empresas

	Coeficiente de Spearman (r)	p-valor	Resultados
Hipótese 2 b)	- 0,036	p = 0,473	Correlação negativa muito fraca e não significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; não se verificou significância estatística ao nível de 0,05 (2 extremidades)

Hipótese 3

Para testar a Hipótese 3, que propunha a existência de uma associação negativa entre a preocupação com privacidade e a frequência de compras online, aplicou-se o coeficiente de correlação de *Spearman*. Os resultados da tabela 13, indicaram que não existe qualquer associação estatisticamente significativa entre a frequência com que os participantes realizam compras online e o impacto do receio de uso indevido dos dados pessoais na desistência de compras (r = 0,040; p = 0,434; IC95% [-0,062; 0,141]).

Contrariamente ao esperado, a análise não revelou evidências de que consumidores mais preocupados com a privacidade desistam com maior frequência de realizar compras online. Em termos práticos, a frequência de compras online mostrou-se independente do nível de preocupação com a privacidade, o que sugere, que nesta amostra, o receio quanto ao uso indevido dos dados pessoais não influencia o comportamento de compra. Assim, a hipótese nula não foi rejeitada, logo não confirma a relação negativa esperada.

Tabela 13

Correlação de *Spearman* entre a frequência de compras online e receio que levou à desistência de compra

	Coeficiente de Spearman (r)	**p-valor**	**Resultados**
Hipótese 3	0,040	p = 0,434	Correlação positiva extremamente fraca e não significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; não se verificou significância estatística ao nível de 0,05 (2 extremidades)

Hipótese 4

Para testar a Hipótese 4: As frequências de compra online são diferentes se o consumidor sofreu ou não violações, foi utilizado o teste *Mann-Whitney*. O teste U não revelou diferenças estatisticamente significativas na frequência de compras online entre participantes que já sofreram uma violação de privacidade online e aqueles que nunca passaram por tal experiência (U = 16011,500; p = 0,062). Apesar dos postos médios indicarem uma tendência para maior frequência de compras no grupo que sofreu violação (215,29 vs. 191,77), a diferença não atingiu significância estatística (vide tabela 14).

Embora os participantes que já sofreram uma violação de privacidade tendam a comprar online ligeiramente mais vezes do que os que não tiveram essa experiência, a diferença não foi estatisticamente significativa. Isto sugere que ter passado por uma violação não altera de forma relevante a frequência de compras online.

Tabela 14

Teste U de Mann-Whitney para a frequência de compras online em função de ter sofrido violação de privacidade

	Estatística U	p-valor	Resultados
Hipótese 4	U = 16011,50	p = 0,062	Diferença não significativa entre os grupos

Nota: Postos médios: Não sofreu violação = 191,77; Sofreu violação = 215,29. Nível de significância adotado $\alpha = 0,05$.

Hipótese 5

Para testar a Hipótese 5: Existe associação entre o nível de conhecimento dos consumidores com Inteligência Artificial e Análise Preditiva e a sua compreensão sobre como estas tecnologias utilizam os seus dados, usou-se o coeficiente de correlação de *Spearman*. Como se observa na tabela 15, o coeficiente de correlação de *Spearman* afirma que existe uma associação positiva moderada e estatisticamente significativa entre o nível de familiaridade com conceitos de Inteligência Artificial e Análise Preditiva e a compreensão sobre como estas tecnologias utilizam os dados para sugerir produtos, conteúdos ou anúncios ($r = 0,611$; $p < 0,001$; IC [0,543; 0,671]). Ou seja, participantes que demonstram maior familiaridade com conceitos de Inteligência Artificial e Análise Preditiva tendem a compreender melhor como estas tecnologias utilizam os dados para personalizar ofertas. A relação é moderada e clara, indicando que o conhecimento técnico influencia a compreensão prática.

Tabela 15

Correlação de *Spearman* entre familiaridade com IA/AP e compreensão do uso dos dados

	Coeficiente de Spearman (r)	p-valor	Resultados
Hipótese 5	r = 0,611	p < 0,001	Correlação positiva moderada e significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; intervalo de confiança de [0,543; 0,671].

Hipótese 6

Para testar a Hipótese 6: Existe uma associação positiva entre o grau de confiança dos consumidores nas empresas e a frequência de compras online, aplicou-se o coeficiente de correlação de *Spearman*. Os resultados demonstrados na tabela 16, revelaram que não existe

associação estatisticamente significativa entre as variáveis (r = - 0,009; p = 0,856; IC [- 0,111; 0,093]).

Contrariamente ao que era esperado, os dados indicaram uma correlação negativa extremamente fraca e não significativa, o que sugere que o nível de confiança nas empresas não influencia a frequência de compras online. Por outras palavras, confiar mais ou menos nas empresas para proteger devidamente os dados pessoais, não revelou ser um fator determinante para a regularidade das compras online nesta amostra. Assim, a hipótese nula não foi rejeitada, e a relação positiva não foi confirmada.

Tabela 16

Correlação de *Spearman* entre confiança nas empresas e frequência de compras online

	Coeficiente de Spearman (r)	**p-valor**	**Resultados**
Hipótese 6	r = - 0,009	p = 0,856	Correlação negativa extremamente fraca e não significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; intervalo de confiança de 95% [-0,111; 0,093].

Hipótese 7

Para testar a Hipótese 7: Consumidores que realizam compras online com maior frequência estão mais dispostos a partilhar dados pessoais sensíveis, procedeu-se à sua operacionalização em cinco análises distintas, correspondentes a diferentes tipos de dados pessoais: nome e e-mail, número de telemóvel, endereço, número de cartão de crédito e localização em tempo real. Desta forma, tornou-se possível compreender de forma mais detalhada em que medida a disposição para partilhar cada tipo de dado sensível se relaciona com a frequência de compras online.

Para a análise do nome e e-mail, o teste do Qui-quadrado indicou que existem diferenças estatisticamente significativas na predisposição para fornecer nome e e-mail consoante o nível de confiança nas empresas para proteger devidamente os dados pessoais, x^2 (3) = 8,439, p = 0,038. O valor de V de *Cramer* foi de 0,146, indicando que a força da associação é fraca. Apesar da significância estatística, verificou-se que a predisposição para fornecer nome e e-mail é elevada em todos os níveis de confiança, variando entre 79,5% e 92,6%. Os resíduos ajustados revelaram que a maior discrepância positiva ocorreu no grupo que "Discorda" e fornece o nome e e-mail

(resíduo ajustado = 2,2), enquanto a maior discrepância negativa se verificou no grupo que "Discorda" e não fornece (resíduo ajustado = -2,2). Verificou-se uma relação fraca, mas estatisticamente significativa, entre a confiança nas empresas e a disposição para fornecer nome e e-mail. Apesar disso, a predisposição para partilhar estes dados foi alta em todos os níveis de confiança, o que indica que este tipo de informação é visto como pouco sensível pela maioria (vide tabelas seguintes).

Tabela 17

Associação entre confiança nas empresas e fornecimento de nome e e-mail

Confia nas empresas	Não fornece	Fornece	Total	% em confiança	Resíduo ajustado
Discordo Totalmente	8	31	39	20,5%/79,5%	1,3/-1,3
Discordo	8	100	108	7,4%/92,6%	-2,2/2.2
Nem discordo, nem concordo	29	132	161	18,0%/82,0%	2,1/-2,1
Concordo/Concordo totalmente	9	77	86	10,5%/89,5%	-1,0/1,0
Total	54	340	394	13,7%/86,3%	

Nota: Os valores apresentados correspondem às frequências observadas, percentagens dentro de cada nível de confiança e resíduos ajustados.

Tabela 18

Resultados do teste do Qui-quadrado para associação entre confiança nas empresas e fornecimento de nome e e-mail

Teste	Valor	p (bilateral)	V de Cramer
Qui-Quadrado de Pearson	8,439	0,038	0,146
Razão de verossimilhança	8,755	0,033	
Teste Fisher-Freeman-Halton	8,585	0,033	

Na análise referente à partilha do número de telemóvel, foi realizada uma tabulação cruzada entre a variável confiança nas empresas para proteger os dados pessoais e a variável disposição para partilhar o número de telemóvel. Os resultados representados na tabela 20, mostram uma associação estatisticamente significativa, confirmada pelo teste do Qui-quadrado de *Pearson* (x^2 (4) = 15,101; p = 0,004). A associação linear também se mostrou significativa (p < 0,001), o que sugere a existência de uma tendência clara entre as variáveis. Adicionalmente, o valor da medida de associação V de *Cramer* (V = 0,196; p = 0,004) indica uma relação de intensidade fraca a moderada, mas estatisticamente relevante, entre a confiança nas empresas e a disposição em fornecer o número de telemóvel.

Observou-se que os consumidores que apresentam níveis mais elevados de confiança nas empresas revelaram maior disponibilidade para partilhar o número de telemóvel, ao passo que aqueles que discordam ou discordam totalmente tenderam a rejeitar essa partilha. Estes resultados apoiam parcialmente a hipótese formulada, evidenciando que a confiança desempenha um papel fundamental na decisão de disponibilizar este tipo de dado pessoal, como mostra a tabela 19.

Tabela 19

Associação entre confiança nas empresas e fornecimento do número de telemóvel

Confia nas empresas	Não fornece	Fornece	Total	% em confiança	Resíduo ajustado
Discordo Totalmente	32	7	39	82,1%/17,9%	3,1/-3,1
Discordo	69	39	108	63,9%/36,1%	1,2/-1,2
Nem discordo, nem concordo	90	71	161	55,9%/44,1%	-1,0/1,0
Concordo	37	42	79	46,8%/53,2%	-2,4/2,4
Concordo totalmente	4	3	7	57,1%/42,9%	-0,1/0,1
Total	232	162	394	58,9%/41,1%	

Nota: Os valores apresentados correspondem às frequências observadas, percentagens dentro de cada nível de confiança e resíduos ajustados.

Tabela 20

Resultados do teste de Qui-quadrado para associação entre confiança nas empresas e fornecimento do número de telemóvel

Teste	Valor	p (bilateral)	V de Cramer
Qui-Quadrado de Pearson	15,101	0,004	0,196
Razão de verossimilhança	16,006	0,003	
Teste Fisher-Freeman-Halton	13,040	< 0,001	

Na análise referente à partilha do endereço de envio, foi realizada uma tabulação cruzada entre a variável confiança nas empresas para proteger os dados pessoais e a disposição para fornecer o endereço. Os resultados (vide tabela 22) revelaram uma associação estatisticamente significativa, confirmada pelo teste do Qui-quadrado de *Pearson* ($x^2(4) = 9{,}799$; p = 0,044), bem como pela razão de verossimilhança (p = 0,042). Adicionalmente, a associação linear por linear também se mostrou significativa ($x^2(1) = 8{,}863$; p = 0,003), o que sugere a existência de uma tendência clara entre as variáveis. O valor da medida de associação V de *Cramer* (V = 0,158; p = 0,041) indica uma relação de intensidade fraca, mas estatisticamente relevante, entre a confiança nas empresas e a disposição em fornecer o endereço de envio.

Verificou-se, na tabela 21, que os consumidores que apresentaram níveis mais elevados de confiança nas empresas mostraram maior disponibilidade para partilhar o seu endereço. Em contraste, indivíduos que revelaram baixo nível de confiança, nomeadamente os que discordaram ou discordaram totalmente, tenderam a recusar fornecer esta informação. Estes resultados dão suporte parcial à hipótese formulada, reforçando a ideia de que a confiança desempenha um papel importante na decisão de disponibilizar dados pessoais de natureza sensível, ainda que, neste caso, a força da associação seja relativamente fraca.

Tabela 21

Associação entre confiança nas empresas e fornecimento do endereço

Confia nas empresas	Não fornece	Fornece	Total	% em confiança	Resíduo ajustado
Discordo Totalmente	29	10	39	74,4%/25,6%	1,9/-1,9
Discordo	69	39	108	63,9%/36,1%	1,0/-1,0
Nem discordo, nem concordo	96	65	161	59,6%/40,4%	-0,1/0,1
Concordo	40	39	79	50,6%/49,4%	-1,9/1,9
Concordo totalmente	2	5	7	28,6%/71,4%	-1,7/1,7
Total	236	158	394	59,9%/40,1%	

Nota: Os valores apresentados correspondem às frequências observadas, percentagens dentro de cada nível de confiança e resíduos ajustados.

Tabela 22

Resultados do teste do Qui-quadrado para associação entre confiança nas empresas e fornecimento do endereço

Teste	Valor	p (bilateral)	V de Cramer
Qui-Quadrado de Pearson	9,799	0,044	0,158
Razão de verossimilhança	9,910	0,042	
Teste Fisher-Freeman-Halton	8,863	0,003	

Na análise referente à variável partilha do número de cartão de crédito/débito, foi realizada uma tabulação cruzada com a variável confiança nas empresas para proteger adequadamente os dados pessoais. Os resultados indicados na tabela 24 não revelaram associação estatisticamente significativa entre as variáveis ($x^2(3) = 2,523$; p = 0,471), sugerindo que o nível de confiança nas empresas não exerce influência relevante na decisão de fornecer, ou não, esta informação sensível. A medida de associação V de *Cramer* confirmou esta ausência de efeito, apresentando um valor baixo (V = 0,080; p = 0,471), indicativo de uma relação fraca e não significativa. Em termos práticos, observou-se que a maioria dos consumidores, independentemente do grau de confiança

declarado, optou por não disponibilizar o número de cartão, com percentagens que variaram entre 89,5% e 97,4%, como indica a tabela 23.

Deste modo, ao contrário do observado noutras variáveis (como número de telemóvel ou endereço), o fornecimento do cartão de crédito/débito não apresentou variações expressivas em função da confiança nas empresas. Estes resultados indicam que este tipo de dado é percecionado como altamente sensível, o que leva a uma retenção generalizada por parte dos consumidores, ainda que confiem nas entidades envolvidas.

Tabela 23

Associação entre confiança nas empresas e fornecimento do número de cartão de crédito/débito

Confia nas empresas	Não fornece	Fornece	Total	% em confiança	Resíduo ajustado
Discordo Totalmente	38	1	39	97,4%/2,6%	1,4/-1,4
Discordo	100	8	108	92,6%/7,4%	0,4/-0,4
Nem discordo, nem concordo	146	15	161	90,7%/9,3%	-0,6/0,6
Concordo/Concordo Totalmente	77	9	79	89,5%/10,5%	-0,8/0,8
Total	361	33	394	91,6%/8,4%	

Nota: Os valores apresentados correspondem às frequências observadas, percentagens dentro de cada nível de confiança e resíduos ajustados.

Tabela 24

Resultados do teste do Qui-quadrado para associação entre confiança nas empresas e fornecimento do número de cartão de crédito/débito

Teste	Valor	p (bilateral)	V de Cramer
Qui-Quadrado de Pearson	2,532	0,471	0,080

Razão de verossimilhança	3,079	0,380
Teste Fisher-Freeman-Halton	2,178	0,140

Na análise da variável referente à partilha da localização em tempo real, os resultados da tabulação cruzada, constatados na tabela 25, revelaram que a maioria dos inquiridos, independentemente do nível de confiança nas empresas, recusa fornecer este tipo de dado sensível, com percentagens de recusa a variar entre 85,7% e 95,7%. Já na tabela 26, o teste de Qui-quadrado de *Pearson* não evidenciou associação estatisticamente significativa entre a confiança nas empresas e a disposição para fornecer a localização em tempo real, $x^2(4) = 4{,}099$, $p = 0{,}393$. Da mesma forma, a associação linear por linear também não foi significativa ($p = 0{,}863$). As medidas de associação (V de *Cramer* = 0,102; p = 0,393) confirmam a inexistência de uma relação relevante entre as variáveis, indicando que a decisão de partilhar a localização em tempo real não depende significativamente do nível de confiança nas empresas.

De forma prática, estes resultados sugerem que a partilha de informação relativa à localização em tempo real é percebida pelos consumidores como altamente intrusiva e sensível, sendo rejeitada de forma transversal, independentemente do grau de confiança nas organizações.

Tabela 25

Associação entre confiança nas empresas e fornecimento da localização em tempo real

Confia nas empresas	**Não fornece**	**Fornece**	**Total**	**% em confiança**	**Resíduo ajustado**
Discordo Totalmente	36	3	39	92,3%/7,7%	-0,1/0,1
Discordo	98	10	108	90,7%/9,3%	-0,9/0,9
Nem discordo, nem concordo	154	7	161	95,7%/4,3%	1,9/-1,9
Concordo	71	8	79	89,9%/10,1%	-1,1/1,1
Concordo Totalmente	6	1	7	85,7%/14,3%	-0,7/0,7
Total	365	29	394	92,6%/7,4%	

Nota: Os valores apresentados correspondem às frequências observadas, percentagens dentro de cada nível de confiança e resíduos ajustados.

Tabela 26

Resultados dos testes de associação entre confiança nas empresas e fornecimento da localização em tempo real

Teste	Valor	p (bilateral)	V de Cramer
Qui-Quadrado de Pearson	4,099	0,393	0,102
Razão de verossimilhança	4,218	0,377	
Teste Fisher-Freeman-Halton	5,124	0,244	

Hipótese 8

Para testar a Hipótese 8: Consumidores que leem as políticas de privacidade com maior frequência apresentam maior conhecimento sobre riscos de privacidade online, foi usado o coeficiente de correlação de *Spearman*, como é demonstrado na tabela 27. O teste revelou uma associação positiva fraca e estatisticamente significativa entre a leitura das políticas de privacidade antes de aceitar os termos de um serviço online e o nível de conhecimento sobre riscos de privacidade online ($r = 0,269$; $p < 0,001$; IC [0,172; 0,361]).

Existe uma relação fraca, mas significativa, entre ler políticas de privacidade e ter maior conhecimento sobre riscos online. Isto sugere que, embora o efeito não seja muito forte, a leitura frequente das políticas pode contribuir para aumentar a consciência sobre privacidade.

Tabela 27

Correlação de *Spearman* entre leitura das políticas de privacidade e conhecimento sobre riscos de privacidade online

	Coeficiente de Spearman (r)	P-valor	Resultados
Hipótese 8	r = 0,269	p < 0,001	Correlação positiva fraca e significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; intervalo de confiança de [0,172; 0,361].

Hipótese 9

Para testar a Hipótese 9: Consumidores de menor faixa etária apresentam maior compreensão sobre como a Inteligência Artificial e a Análise Preditiva usam os seus dados, para isto foi usado, também, o coeficiente de correlação de *Spearman*. O coeficiente de correlação de *Spearman* revelou uma associação negativa fraca e estatisticamente significativa entre a compreensão sobre como a Inteligência Artificial e a Análise Preditiva utilizam os dados e a faixa etária dos participantes (r = - 0,144; p = 0,004; IC [- 0,242; - 0,043]). Os resultados mostram que participantes mais jovens compreendem melhor como a Inteligência Artificial e a Análise Preditiva utilizam dados pessoais. A associação é fraca, mas significativa, o que indica que a idade pode influenciar a literacia digital neste contexto (vide tabela seguinte).

Tabela 28

Correlação de *Spearman* entre compreensão sobre o uso de dados por IA/AP e faixa etária

	Coeficiente de Spearman (r)	**P-valor**	**Resultados**
Hipótese 9	r = - 0,144	p = 0,004	Correlação negativa fraca e significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; intervalo de confiança de 95% [–0,242; –0,043].

Hipótese 10

Para testar a Hipótese 10: Consumidores com maior familiaridade sobre Inteligência Artificial e Análise Preditiva, leem as políticas de privacidade com maior frequência, foi utilizado o coeficiente de correlação de *Spearman*. O teste indicou uma associação positiva fraca e estatisticamente significativa entre a leitura das políticas de privacidade antes de aceitar os termos de um serviço online e o nível de familiaridade com conceitos de Inteligência Artificial e Análise Preditiva (r = 0,219; p < 0,001; IC [0,120; 0,314]), como é demonstrado na tabela 29. Ou seja, participantes com maior familiaridade com IA e Análise Preditiva tendem a ler políticas de privacidade com maior frequência antes de aceitar termos de serviço. Embora a relação seja fraca,

é estatisticamente relevante, o que sugere que o conhecimento tecnológico está ligado a maior atenção a práticas de privacidade.

Tabela 29

Correlação de *Spearman* entre leitura de políticas de privacidade e familiaridade com IA/AP

	Coeficiente de Spearman (r)	**P-valor**	**Resultados**
Hipótese 10	r = 0,219	p < 0,001	Correlação positiva fraca e significativa

Nota: A correlação foi calculada pelo coeficiente de *Spearman*; intervalo de confiança de 95% [0,120; 0,314].

Capítulo 5 – Discussão dos Resultados

A hipótese 1 a) desta investigação procurou compreender se os consumidores mais jovens têm uma perceção mais elevada dos riscos associados à privacidade online, quando comparados com os consumidores de faixas etárias mais avançadas. No entanto, os resultados obtidos não revelaram diferenças estatisticamente significativas entre os grupos etários. Deste modo, a hipótese foi rejeitada, ou seja, no contexto da amostra estudada, jovens e adultos de faixas etárias mais elevadas demonstram níveis semelhantes de perceção relativamente aos riscos de privacidade online, o que significa que a H1 a) não foi confirmada. Esta ausência de diferenças entre faixas etárias pode ser interpretada à luz das mudanças sociais e tecnológicas dos últimos anos, nomeadamente da crescente democratização da literacia digital. A perceção dos riscos online parece estar mais associada a variáveis como o grau de escolaridade, a frequência de utilização da internet e experiências pessoais com situações de violação de privacidade, do que à idade cronológica dos indivíduos (Park, 2011). Neste sentido, os dados obtidos desafiam a ideia preconcebida de que os utilizadores mais jovens estão, por definição, mais preparados para lidar com questões de privacidade online. A perceção de risco resulta de uma multiplicidade de fatores, que inclui atitudes, experiências prévias e contexto social, e não pode ser compreendida apenas com base na variável idade.

A segunda hipótese (1b) procurava compreender se os consumidores com níveis mais elevados de escolaridade revelam uma perceção mais consciente dos riscos associados à privacidade online. Os resultados vieram confirmar esta suposição, o que mostra que os indivíduos com menor nível de escolaridade tendem a demonstrar uma sensibilidade reduzida face às ameaças ligadas à proteção de dados pessoais no ambiente digital, ou seja a H1 b) foi confirmada. Esta conclusão está alinhada com aquilo que a literatura científica tem vindo a indicar, existe uma relação entre o grau de escolaridade e a literacia digital. Pessoas com uma formação académica mais avançada, não só apresentam maior familiaridade com o uso das tecnologias, como também possuem uma capacidade acrescida para avaliar de forma crítica as consequências da partilha de informação online (Park, 2011). Além disso, a consciência dos riscos digitais parece ser influenciada pelo nível de literacia em proteção de dados. Utilizadores com menor escolaridade frequentemente não reconhecem toda a complexidade das ameaças à sua privacidade, tornando-se assim mais suscetíveis a práticas abusivas de recolha de dados. Esta limitação pode não decorrer apenas de um défice técnico, mas também da ausência de competências reflexivas que lhes permitam antecipar as consequências futuras das suas escolhas e comportamentos online Barth e Jong (2017). Neste contexto, os dados reforçam a relevância de se considerar a escolaridade como um fator determinante na forma como os utilizadores percecionam e lidam com os riscos de privacidade digital.

A hipótese 2 a) procurava compreender se os indivíduos mais velhos tendem a revelar níveis mais baixos de confiança nas empresas no que respeita à proteção dos seus dados pessoais. Os resultados obtidos confirmam esta expectativa, embora a associação encontrada seja fraca. Ainda assim, os dados revelam uma tendência estatisticamente significativa: à medida que a idade aumenta, a confiança nas empresas tende a diminuir. Os utilizadores mais velhos são frequentemente mais cautelosos no ambiente online, ou seja, a H2 a) foi confirmada. Esta postura pode estar relacionada com uma menor familiaridade com as práticas tecnológicas atuais ou com uma exposição acumulada a notícias sobre falhas de segurança e utilização indevida de dados por parte das empresas. Tal sensibilidade pode traduzir-se numa atitude mais crítica em relação às organizações, sobretudo no que diz respeito à forma como estas gerem a informação pessoal dos utilizadores (Beldad, Jong & Steehouder, 2010). Importa reconhecer que, apesar de estatisticamente significativa, a relação identificada é de baixa intensidade. Isto indica que, embora exista uma tendência geral, outros fatores poderão também desempenhar um papel relevante, como o nível de

literacia digital, o grau de contacto com as tecnologias ou mesmo o tipo de empresa envolvida. Não obstante, os resultados sugerem que as empresas devem prestar particular atenção à forma como constroem relações de confiança com públicos mais velhos.

A hipótese 2 b) procurava compreender se indivíduos com níveis de escolaridade mais elevados tendem a demonstrar menor confiança nas empresas quanto à proteção dos seus dados pessoais. No entanto, os resultados obtidos não confirmaram esta hipótese. Não foi identificada qualquer associação estatisticamente significativa entre o grau de instrução e a confiança depositada nas organizações, o que sugere que, na amostra analisada, o nível de escolaridade não teve impacto relevante nas perceções de confiança. A confiança nas entidades responsáveis pelos dados parece depender mais da perceção de transparência, segurança regulatória e conformidade, como sugerem. Elementos como eficácia percebida das políticas, clareza no uso dos dados, confiança no cumprimento do GDPR e responsabilização institucional são determinantes da experiência e satisfação dos indivíduos com o quadro legal, (Mutimukwe, Viberg, Oberg & Pargman, 2022). Deste modo, é plausível considerar que, no que diz respeito à proteção de dados, a confiança seja construída mais a partir da perceção de responsabilidade e transparência por parte das empresas do que da formação académica do consumidor.

A terceira hipótese teve como objetivo compreender se existe uma relação entre a preocupação com a privacidade dos dados pessoais e a frequência com que os consumidores realizam compras online. No entanto, os resultados não evidenciaram qualquer associação estatisticamente significativa entre estas variáveis, o que significa que a H3 não foi confirmada. Muitos utilizadores manifestam uma preocupação com a privacidade, mas isso nem sempre se traduz em mudanças comportamentais concretas, como evitar compras ou abandonar transações. Ou seja, apesar de o receio existir, outros fatores, como conveniência, preço ou urgência da compra, acabam por se sobrepor às preocupações com a proteção de dados (Barth & Jong, 2017). Estes resultados sugerem que o comportamento de compra online pode não estar tão ligado à perceção de risco como se poderia supor. Tal não invalida a existência de preocupação com a privacidade, mas indica que esta pode não ser um fator determinante na decisão de concluir ou abandonar uma compra. Para as empresas, isto reforça a importância de adotar práticas éticas e transparentes na gestão de dados, mesmo quando estas não parecem afetar, de forma direta e imediata, os hábitos de consumo.

A quarta hipótese procurava perceber se a experiência prévia de uma violação de privacidade influencia a frequência com que os consumidores realizam compras online. Intuitivamente, poderia esperar-se que indivíduos que já foram alvo de uma violação tivessem maior relutância em continuar a comprar pela internet. Contudo, os resultados obtidos não confirmam a hipótese 4. Com o tempo, muitos consumidores tornam-se menos reativos a ameaças de privacidade. Em vez de evitarem determinados comportamentos, ajustam as suas expectativas ou transferem a responsabilidade para as plataformas e empresas. Neste caso, quem já sofreu uma violação pode não necessariamente evitar compras, mas tornar-se mais vigilante ou seletivo em relação aos sites e marcas com que interage (Acquisti, Brandimarte & Loewensdtein, 2015). Assim, os dados obtidos não invalidam a importância da privacidade na decisão de compra online, mas indicam que o seu impacto comportamental pode ser mais complexo do que uma simples relação de causa e efeito. A experiência de ter sido vítima de uma violação de dados não parece, por si só, suficiente para modificar a frequência de compras. O comportamento do consumidor online continua a ser influenciado por um conjunto multifatorial de motivações, resistências e perceções de risco que importa continuar a explorar.

A quinta hipótese teve como objetivo compreender se existiu relação entre o nível de familiaridade com conceitos de Inteligência Artificial e Análise Preditiva, e a compreensão sobre a forma como estas tecnologias utilizam os dados pessoais dos consumidores. Os resultados sugerem que há uma associação positiva, moderada e estatisticamente significativa entre as duas dimensões, ou seja, pessoas mais familiarizadas com os fundamentos destas tecnologias estão, à partida, mais conscientes dos processos automatizados que moldam a sua experiência digital. Isto significa que a H5 foi confirmada. Não se trata apenas de saber que os dados estão a ser usados, mas de perceber de que forma, com que finalidade e através de que mecanismos. (Hassan, Abdelraouf & El-Shihy, 2025) demonstraram que o grau de compreensão sobre personalização algorítmica varia bastante entre grupos sociais e que esse conhecimento tende a estar ligado a uma perceção mais crítica sobre os efeitos que os algoritmos têm no comportamento e nas escolhas individuais. No fundo, estes dados reforçam a importância de investir em iniciativas de literacia digital que não se limitem ao uso técnico das ferramentas, mas que ajudem os cidadãos a perceber como funcionam os sistemas que moldam, cada vez mais, as suas interações online. A compreensão é, afinal, o primeiro passo para a participação ativa e consciente num ecossistema digital em constante transformação.

A sexta hipótese investigava se existia uma relação entre o grau de confiança dos consumidores nas empresas e a frequência de compras online. No entanto, a análise estatística não apontou qualquer associação significativa entre estas variáveis, o que indica que confiar ou não nas empresas não determina necessariamente quantas vezes se compra online, logo a H6 não foi confirmada. Apesar de a confiança digital poder ajudar a reduzir o receio associado às compras na internet e a aumentar a satisfação com a experiência, isso não significa, por si só, que leve os consumidores a comprar com maior frequência. A confiança tende a contribuir para uma experiência mais segura e positiva em momentos pontuais, mas nem sempre se traduz num comportamento de compra repetido (Hipólito, Dias & Pereira, 2025). Isto aponta para a possibilidade de a frequência de compras online depender de outros fatores, como a conveniência, o preço, as necessidades imediatas ou até o atendimento ao cliente. Portanto, mesmo não tendo uma correlação estatisticamente distinta, este padrão fortalece que a confiança é um importante condutor da satisfação e da redução do risco percebido, mas não como determinante da frequência de compra.

A sétima hipótese procurava averiguar se os consumidores que compram online com maior frequência estão mais dispostos a partilhar dados pessoais sensíveis. Para testar esta hipótese, foram analisadas cinco categorias distintas de dados: nome e e-mail, número de telemóvel, endereço de envio, número de cartão de crédito e localização em tempo real. No entanto, os resultados mostraram que a disposição para partilhar varia bastante consoante o tipo de dado, logo a H7 foi parcialmente confirmada.

No que diz respeito ao nome e e-mail, os dados mostraram uma associação estatisticamente significativa com a confiança nas empresas. Curiosamente, verificou-se uma elevada predisposição para partilhar este tipo de informação, mesmo entre os consumidores menos confiantes. Este padrão sugere que nome e e-mail são percecionados como dados pouco sensíveis, muitas vezes vistos como "naturais" no registo em plataformas digitais. Tal como referido por Belanger e Crossler (2011), a partilha destes dados tornou-se praticamente automática, fruto da sua normalização nas plataformas digitais. Sobre a partilha do número de telemóvel, os resultados apresentaram uma associação mais clara e significativa. Os consumidores com maior confiança nas empresas demonstraram maior abertura para partilhar este dado, em contrapartida os mais desconfiados revelaram resistência. Esta tendência confirma a perceção do número de telemóvel

como um dado mais intrusivo, sobretudo por estar diretamente ligado ao contacto pessoal ou à autenticação de identidade destacam que quando os dados podem ser usados para contacto pessoal ou validação, os utilizadores tornam-se mais seletivos, sendo a confiança um elemento essencial para quebrar essa hesitação (Zaeem & Barber, 2021).

Quanto ao endereço de envio, os resultados apontaram para uma associação estatisticamente significativa, ainda que fraca, com a confiança nas empresas. A grande parte dos consumidores que indicaram maior confiança mostraram-se mais disponíveis a partilhar o endereço, algo que pode ser justificado pelo próprio contexto das compras online, onde esse dado é muitas vezes essencial. O endereço físico é um dos dados cuja partilha tanto depende da confiança como da perceção de necessidade, (Belen-Saglam, Nurse & Hodges, 2022).

No caso do número de cartão de crédito/débito, os resultados foram claros: a grande maioria dos participantes recusou fornecer este dado, independentemente do seu nível de confiança nas empresas. Não se registaram associações estatisticamente significativas, o que evidencia que a confiança, neste caso, não é suficiente para superar a perceção de risco. Como defendido por Kokolakis (2017), os dados bancários continuam a ser considerados os mais sensíveis, devido às potenciais consequências financeiras diretas, sendo por isso alvo de uma proteção muito mais cautelosa.

No que concerne à localização em tempo real não se verificou qualquer associação significativa entre a confiança e a predisposição para partilhar esta informação. Esta recusa geral parece estar associada à perceção de vigilância ou invasão, mesmo em contextos em que a empresa seja considerada de confiança. A localização é um dos elementos mais sensíveis aos olhos dos consumidores, por estar associada à sua mobilidade, rotina e esfera pessoal, o que leva à sua rejeição, sobretudo em contextos onde o benefício da partilha não é evidente, (Ying, Huang, Qian & Song, 2023).

Em síntese, os resultados sugerem que a confiança nas empresas pode, de facto, influenciar a disposição para partilhar certos dados, sobretudo os mais sensíveis. Porém, quando está em causa informação percecionada como altamente sensível, como o número de cartão ou a localização em tempo real, a preocupação dos consumidores prevalece. Estes padrões reforçam a ideia de que os utilizadores gerem a sua privacidade de forma seletiva, ajustando o grau de partilha ao tipo de dado e ao risco percebido que lhe está associado.

A oitava hipótese propunha que os consumidores que leem, com mais frequência, as políticas de privacidade tendem a apresentar maior conhecimento sobre os riscos associados à privacidade online. Os dados vieram comprovar essa relação, ou seja, a H8 foi confirmada. Este padrão de associação encontra respaldo na literatura. Os consumidores com maior literacia em segurança digital tendem a prestar mais atenção às políticas de privacidade, sendo este comportamento especialmente evidente entre os que demonstram maior preocupação com a sua privacidade e possuem alguma formação na área (Ibdah, Lachatr, Raparthi & Bacha, 2021). Por outro lado, Pan, Ruan, Chang, Lyu e Li (2024) observaram que a atenção dedicada a estas políticas depende também do contexto de utilização, ou seja, quanto maior for a necessidade de usufruir de uma aplicação ou serviço, menos atenção é dada à leitura desses documentos, sobretudo quando os utilizadores se sentem vulneráveis ou pressionados a prosseguir rapidamente. Apesar destes dados, a leitura das políticas de privacidade continua a ser um hábito pouco comum. Muitos utilizadores optam por aceitá-las sem ler, frequentemente por não conseguirem compreender a linguagem técnica em que estão escritas. Em suma, os resultados reforçam a ideia de que incentivar este tipo de leitura pode contribuir para aumentar a perceção dos riscos de privacidade, ainda que de forma gradual.

A nona hipótese partia da ideia de que os consumidores de menor faixa etária apresentam maior compreensão sobre como a Inteligência Artificial e a Análise Preditiva usam os seus dados. Os resultados confirmaram isso, pois indicaram que à medida que a idade aumenta, a compreensão destes mecanismos tende a diminuir ligeiramente, o que faz com que a H9 foi confirmada. As gerações mais novas cresceram num ambiente digital rodeado em tecnologia, como redes sociais, algoritmos de recomendação e *chatbots*, o que cria uma familiaridade com o contexto digital. Com isto, os mais novos não só usam essas ferramentas, mas compreendem como elas funcionam mesmo que de forma intuitiva. Ernst (2025) identificou que adolescentes demonstram uma consciência superior sobre lógica algorítmica e personalização online quando comparados com grupos etários mais elevados. A exposição contínua à cultura digital, comum nos mais jovens, alimenta uma compreensão mais reflexiva sobre como algoritmos moldam os nossos fluxos de informação. É importante frisar que não estamos a falar de diferenças marcantes entre idades, mas sim de tendências. Existem adultos mais velhos com elevada literacia digital e igualmente capazes de compreender os processos de IA e AP. Todavia, em média, a familiaridade contínua com tecnologia confere aos jovens uma vantagem clara.

A décima hipótese procurava perceber se existe uma relação entre a familiaridade com Inteligência Artificial e Análise Preditiva, e a frequência com que os consumidores leem políticas de privacidade. Os resultados revelaram uma correlação positiva moderada, ainda que não forte, mas estatisticamente significativa. Isto indica que quem compreende melhor o funcionamento destes sistemas tecnológicos tende a envolver-se mais na leitura de detalhes que protegem os seus dados pessoais, logo a H10 foi confirmada. Bajnaid & Aljasir (2025) revelam que os utilizadores com mais literacia sobre privacidade digital adotam com mais frequência comportamentos de proteção, como ajustar as definições de privacidade ou controlar quem acede aos seus dados. Ou seja, o resultado está alinhado com uma lógica: quanto mais entendemos do sistema digital, mais inclinados estamos a ler as letras pequenas. É uma prática menos habitual, mas que está claramente reforçada por uma base de conhecimento e isso, em última análise, reforça a autonomia e o poder crítico do consumidor digital.

Capítulo 6 - Conclusão

O presente estudo teve como objetivo analisar as preocupações de privacidade dos consumidores online relativamente à utilização de Inteligência Artificial (IA) e da análise preditiva pelas empresas, no sentido de influenciar o comportamento de compra, do consumidor. Este objetivo partiu da pressuposição de que, no atual contexto digital, as organizações recorrem crescentemente a estas tecnologias para recolher e interpretar dados pessoais, o que levanta questões éticas e de confiança no relacionamento com os consumidores. Acresce referir que esta investigação também foi motivada por uma curiosidade pessoal em compreender de que forma as empresas conseguem, através do uso de dados e de ferramentas tecnológicas, influenciar os consumidores a realizarem compras.

O enquadramento teórico demonstrou que a adoção crescente de IA e de análise preditiva no comércio eletrónico levanta questões éticas e de confiança. Se, por um lado, estas ferramentas permitem às empresas antecipar necessidades, otimizar ofertas e personalizar a experiência do cliente, por outro, colocam em causa a proteção da privacidade e a transparência das práticas de recolha e utilização de dados.

Do ponto de vista metodológico, foi adotada uma abordagem quantitativa, suportada pela aplicação de um questionário estruturado a 394 participantes, cujos dados foram tratados

estatisticamente com recurso ao *software IBM SPSS Statistics*. Este desenho metodológico permitiu testar hipóteses concretas e analisar relações estatisticamente significativas entre variáveis demográficas, comportamentais e cognitivas, o que garante robustez na análise dos resultados.

Entre os principais resultados, destaca-se que o nível de escolaridade está positivamente associado à perceção dos riscos de privacidade online, o que pode sugerir que a literacia académica contribui para uma maior consciência sobre a proteção de dados. Por outro lado, a idade não revelou impacto significativo no nível de perceção dos riscos, embora se tenha observado uma ligeira tendência para menor confiança nas empresas por parte de indivíduos mais velhos. Outro resultado relevante indica que a frequência de compras online não está diretamente relacionada com a preocupação com a privacidade, o que sugere que receios sobre tratamento de dados não se traduzem, necessariamente, em menor consumo digital. Adicionalmente, verificou-se que a confiança nas empresas não influencia significativamente a frequência de compras, ao reforçar a ideia de que a perceção de risco não condiciona de forma determinante o comportamento de compra.

No que diz respeito à disposição para partilhar dados pessoais sensíveis, os resultados mostraram diferenças relevantes, dependendo do tipo de informação em causa. Dados como o nome e email foram disponibilizados pela maioria dos inquiridos, independentemente do nível de confiança nas empresas, o que indica que estes são percecionados como dados menos sensíveis. No caso do número de telemóvel e endereço verificou-se uma associação significativa entre a confiança nas empresas e a predisposição para partilha. Por outro lado, quando estavam em causa o número do cartão de crédito ou a localização em tempo real, a tendência foi de recusa generalizada, independentemente do grau de confiança nas organizações. Em termos de literacia digital, a familiaridade com conceitos de IA e análise preditiva mostrou estar associada a uma maior compreensão sobre a forma como os dados são utilizados para personalizar ofertas, assim como a uma maior propensão para a leitura de políticas de privacidade. Observou-se, ainda, que participantes mais jovens tendem a compreender melhor estas tecnologias, o que revela a existência de diferenças geracionais no modo como os consumidores interpretam o uso dos seus dados.

De um modo geral, a investigação permitiu concluir que, embora os consumidores demonstrem preocupações com a privacidade, estas não se traduzem, de forma direta, em comportamentos de

rejeição ou diminuição de compras online. Contudo, a literacia digital e o conhecimento sobre as tecnologias emergem como fatores centrais na formação de perceções, o que pode desempenhar um papel relevante na confiança e no grau de atenção exercido pelos consumidores.

Assim, este estudo contribui para a literatura ao mostrar a complexidade da relação entre preocupações com a privacidade, confiança organizacional e comportamento de consumo, num contexto marcado pela crescente utilização de IA no comércio eletrónico. Do ponto de vista prático, os resultados realçam a necessidade de maior transparência e de estratégias de comunicação mais claras por parte das empresas, no sentido de fortalecer a confiança dos consumidores e promover práticas de utilização de dados eticamente responsáveis.

6.1 Relevância para a área de Gestão

Do ponto de vista da Gestão, esta investigação oferece contributos importantes para a compreensão das dinâmicas que orientam o comportamento do consumidor em ambientes digitais. Atualmente, o comércio eletrónico vive de confiança, sem ela, dificilmente os consumidores se sentem confortáveis em partilhar dados ou em manter relações duradouras com as marcas. Os gestores enfrentam, assim, um grande desafio, que passa por tirar partido da inovação tecnológica, como a Inteligência Artificial e a análise preditiva, sem perder de vista os princípios éticos ligados à privacidade e ao respeito pelo consumidor. Os resultados obtidos neste estudo mostram que, embora a análise preditiva use ferramentas poderosas para influenciar decisões de compra, a perceção de privacidade por parte dos consumidores pode tornar-se um elemento diferenciador e importante na relação com a marca. Assim, as empresas não devem encarar a privacidade apenas como uma exigência legal, mas como uma dimensão estratégica da sua gestão. Investir em transparência organizacional e em comunicação clara sobre o uso de dados, pode ser tão ou mais importante do que apostar apenas em tecnologias sofisticadas.

Para além disso, a privacidade pode ser vista como uma vantagem competitiva sustentável. Empresas que conseguem transmitir confiança e demonstrar respeito pelos direitos dos consumidores têm maior probabilidade de fidelizar clientes e construir relações de longo prazo. A confiança torna-se, assim, um recurso subjetivo, mas com elevado valor estratégico, capaz de originar diferenciação num mercado onde a concorrência é intensa e as opções de consumo são abundantes.

Em síntese, esta dissertação reforça a ideia de que a gestão moderna não pode limitar-se a explorar as ofertas da tecnologia. Deve, antes, integrar princípios éticos e práticas de gestão de dados que coloquem o consumidor no centro das decisões estratégicas. Ao fazê-lo, as organizações não apenas minimizam riscos de credibilidade e legais, como também criam valor partilhado, ao fortalecer a confiança digital como base da sua competitividade e sustentabilidade a longo prazo.

6.2 Limitações do estudo

Embora este estudo tenha trazido contributos relevantes, não esteve isento de limitações que merecem ser reconhecidas. A primeira está relacionada com a dimensão e a representatividade da amostra. Apesar de terem sido recolhidas 394 respostas válidas, esse número não representa totalmente a população portuguesa. Embora seja uma amostra significativa, é possível que não reflita todas as realidades, perfis e experiências existentes no país. Outra limitação baseia-se no facto de os dados recolhidos dependerem das respostas dadas pelos próprios participantes nos questionários. Sendo que são respostas baseadas em opiniões individuais, podem estar sujeitas a enviesamentos, como a tendência para responder de forma socialmente desejável ou até a dificuldade em interpretar algumas questões.

A terceira limitação baseia-se na seleção da literatura científica. Numa era marcada por um excesso de informação, em que novos estudos e artigos são constantemente publicados sobre Inteligência Artificial, privacidade e comportamento do consumidor, tornou-se um desafio escolher quais as fontes mais relevantes e atuais para integrar no enquadramento teórico. Este processo obrigou a uma triagem criteriosa. Soma-se ainda a própria complexidade do tema em estudo, a privacidade digital e o uso da IA são áreas em constante transformação, sujeitas a rápidas mudanças tecnológicas, sociais e regulatórias. Esta realidade faz com que qualquer investigação nesta área tenha o risco de se tornar parcialmente desatualizada num curto espaço de tempo, o que limita o alcance temporal das conclusões apresentadas.

Por fim, estas limitações, ainda que tenham representado desafios ao longo da investigação, não retiram valor ao trabalho desenvolvido. Pelo contrário, ajudam a enquadrar de forma realista os resultados alcançados e abrem caminho para que futuros estudos possam superar estas restrições, ao explorar o tema com maior profundidade e abrangência.

6.3 Recomendações para Estudos Futuros

Com base nos resultados obtidos, é possível destacar várias recomendações para futuras investigações. Em primeiro lugar, será pertinente aplicar metodologias mistas, ao combinar abordagens quantitativas e qualitativas, poderá enriquecer a compreensão do fenómeno ao captar também perceções mais subjetivas dos consumidores. A análise de casos empresariais concretos poderá igualmente trazer contributos importantes, ao avaliar, de que forma, práticas de transparência e comunicação impactam diretamente a confiança do consumidor.

Para além disso, investigações futuras poderiam analisar o papel das emoções nas decisões de compra online, ao verificar como fatores emocionais interagem com a confiança e com as preocupações de privacidade. Também as redes sociais representam um campo fértil de estudo, uma vez que juntam, de forma particular, a exposição pública e a utilização de dados pessoais, o que pode influenciar a confiança digital dos consumidores.

Por fim, futuras investigações poderiam dedicar-se a avaliar o impacto da regulação existente sobre a confiança dos consumidores e as estratégias empresariais. A implementação de leis como o RGPD na Europa, bem como a criação de novas legislações específicas para a IA, poderão desempenhar um papel determinante na forma como os consumidores percebem a utilização dos seus dados pessoais e na forma como as organizações estruturam as suas práticas de gestão.

Capítulo 7 – Referências Bibliográficas

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Antosova, I., Psurny, M., & Stavkova, J. (2023). Changes in Consumer Purchasing Decisions: Traditional and Emerging Factors in the Dynamic Marketing Landscape Over 15 years. *Marketing and Management of Innovations, 14*(3), 85-96. https://doi.org/10.21272/mmi.2023.3-08

Asniar, A., & Surendro, K. (2019). Predictive analytics for predicting customer behaviour. *2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT)*, 230-233. https://doi.org/10.1109/ICAIIT.2019.8834571

Akoglu, H. (2018). User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine, 18*(3), 91-93. https://doi.org/10.1016/j.tjem.2018.08.001

Bajnaid, W., & Aljasir, S. (2025). Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region. *Journalism and Media*, *6*(1), 8. https://doi.org/10.3390/journalmedia6010008

Barth, S., & Jong, M. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Belanger, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041. https://doi.org/10.2307/41409971

Belen-Saglam, S, Nurse, J., & Hodges, D. (2022). An investigation into the sensitivity of personal information and implications for disclosure: A UK perspective. *Frontiers in Computer Science, 4,* 908245. https://doi.org/10.3389/fcomp.2022.908245

Beldad, A., Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869. https://doi.org/10.1016/j.chb.2010.03.013

Belk, R. W., Belanche, D., & Flavián, C. (2023). Key concepts in artificial intelligence and technologies 4.0 in services. *Service Business, 17*(1), 1-9. https://doi.org/10.1007/s11628-023-00528-w

Bishop, C. (2006). *Pattern recognition and machine learning*. Springer.

Buczak, A. L., & Guven, E. (2021). Artificial intelligence (AI) in cybersecurity: A review. *Computer Science Review, 40*, 100318. https://doi.org/10.1016/j.cosrev.2020.100318

Bracanovic, T. (2019). Predictive analytics, personalized marketing and privacy. *Revue Roumaine de Philosophie, 63*(2), 263–275.

Campbell, M., Hoane Jr., A. J., & Hsu, F. (2002). Deep Blue. *Artificial Intelligence*, *134* (1-2), 57-83. https://doi.org/10.1016/S0004-3702(01)00129-1

Carta dos Direitos Fundamentais da União Europeia. (2000). Jornal Oficial da União Europeia, C 326, 26/10/2012, p. 391-407. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT

Carter, D. (2018). How real is the impact of artificial intelligence? The business information survey 2018. *Business Information Review*, *35(3),* 99-115. https://doi.org/10.1177/0266382118790150

Cheng, Y., Mei, S., Zhong,W., & Gao, X. (2021). Managing consumer privacy risk: The effects of privacy breach insurance. *Eletronic Commerce Research*, *23,* 807-841. https://doi.org/10.1007/s10660-021-09492-x

Chintalapati, S., & Pandey, S. K. (2022). Artificial intelligence in marketing: A systematic literature review. *International Journal of Market Research, 64*(1), 38-68. https://doi.org/10.1177/14707853211018428

Constituição da República Portuguesa. (1976). *Diário da República*, n.º 86/1976, Série I de 10 de abril de 1976. Recuperado de https://dre.pt/dre/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775

Convenção Europeia dos Direitos Humanos. (1950). Conselho da Europa. https://www.echr.coe.int/documents/convention_por.pdf

Dias, T., Gonçalves, R., Costa, R., Pereira, L., & Dias, A. (2023). The impact of artificial intelligence on consumer behaviour and changes in business activity due to pandemic effects. *Human Technology, 19* (1), 121-148. https://doi.org/10.14254/1795-6889.2023.19-1.8

Dick, S. (2019). Artificial Intelligence. *Harvard Data Science Review, 1*(1), 2-8 https://doi.org/10.1162/99608F92.92FE150C

Emerson, R. W. (2023). Mann-Whitney U test and t-test. *Journal of Visual Impairment & Blindness*, *117*(1), 57-61. https://doi.org/10.1177/0145482X221150592

Evstratov, A. E., & Guchenkov, I. Y. (2020). The limitations of artificial intelligence (legal problems). *Russian Journal of Criminology, 4*(2), 13-19. https://doi.org/10.24147/2542-1514.2020.4(2).13-19

Ernst, J. (2025). Undertanding algorithmic recommendations: A qualitative study on children's algorithm literacy in Switzerland. *Information, Communication & Society,* 1-17. https://doi.org/10.1080/1369118X.2024.2382224

Fassiaux, S. (2023). Preserving consumer autonomy through European Union regulation of artificial intelligence: A long-term approach. *European Journal of Risk Regulation, 14*(4), 710-730. https://doi.org/10.1017/err.2023.58

F. Olan, J. Suklan, E. O. Arakpogun and A. Robson. (2024). Advancing Consumer Behavior: The Role of Artificial Intelligence Technologies and Knowledge Sharing. *IEEE Transactions on Engineering Management*, *71*, 13227-13239. https://doi.org/10.1109/TEM.2021.3083536

García-Pérez, M. A. (2023). Use and misuse of corrections for multiple testing. *Methods in Psychology, 8*, 100120. https://doi.org/10.1016/j.metip.2023.100120

GDPR Info. (n.d.*). General Data Protection Regulation (GDPR) - Official legal text*. https://gdpr-info.eu/

Gu, S., Slusarczyc, B., Hajizada, S., Kovalyona, I., Sakhbieva, A. (2021). A Impact of the COVID-19 Pandemic on Online Consumer Purshasing Behavior. *Journal of Theoretical and Applied Eletronic Commerce Research, 16*, 2263-2281. https://doi.org/10.3390/jtaer16060125

Hajjaji, Y., Boulila, W., Farah, I., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review, 39,* 100318. https://doi.org/10.1016/j.cosrev.2020.100318

Han, J., Pei, J., & Tong, H. (2022). Data Mining: *Chapter 1 - Introduction* (4.ª ed.). Elsevier. https://doi.org/10.1016/B978-0-12-811760-6.00011-4

Hassan, N., Abdelraouf, M. & El-Shihy, D. (2025). The moderating role of personalized recommendations in the trust–satisfaction–loyalty relationship: an empirical study of AI-driven e-commerce. *Future Business Journal, 11,* 66. https://doi.org/10.1186/s43093-025-00476-z

Hipólito, F., Dias, Á., & Pereira, L. (2025). Influence of Consumer Trust, Return Policy, and Risk Perception on Satisfaction with the Online Shopping Experience. *Systems*, *13*(3), 158. https://doi.org/10.3390/systems13030158

Ibdah, D., Lachtar, N., Raparthi, S., & Bacha, A. (2021). "Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Towards Privacy Policies. *IEEE*, *9*, 166465-166487. https://doi.org/10.1109/ACCESS.2021.3130086

Information Commissioner's Office. (2019). *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources

Jones, M. (2025, February 5). *A neural networks deep dive: An introduction to neural networks and their programming*. IBM Developer. https://developer.ibm.com/articles/cc-cognitive-neural-networks-deep-dive/

Kazim, E., & Koshiyama, A. S. (2021). A high-level overview of AI ethics. *Patterns 2*(9), 1-12. https://doi.org/10.1016/j.patter.2021.100314

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Kumar, V., & Garg, D. (2018). Predictive analytics: A review of trends and techniques. *International Journal of Computer Applications, 182*(1), 31-37. http://dx.doi.org/10.5120/ijca2018917434

Lee, C., Cheang, P. Y. S., & Moslehpour, M. (2022). Predictive analytics in business analytics: Decision tree. *Advances in Decision Sciences, 26*(1), 1-30. http://dx.doi.org/10.47654/v26y2022i1p1-30

Lobanova, I. A., & Shapovalova, N. A. (2020). Artificial intelligence as a factor in the digital transformation of marketing. *Economics Profession Business, 4*(2), 13-19. https://doi.org/10.24147/2542-1514.2020.4(2).13-19

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute.

Mercante, T. (2023). *Análise preditiva: Aplicada para a solução de problemas reais.* Editora Sencac São Paulo. https://www.google.pt/books/edition/An%C3%A1lise_preditiva/DquzEAAAQBAJ?hl=pt-PT&gbpv=1&dq=importancia+da+estatistica+na+analise+preditiva&pg=PT7&printsec=frontcover

McCulloch, W.S., Pitts, W. (1943) A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, 5, 115-133 https://doi.org/10.1007/BF02478259

Morris, M., & Wesson, P. (2022). Sampling hard-to-reach populations: Advances in methods and applications. *Current Epidemiology Reports, 9*(2), 38-47. https://doi.org/10.1007/s40471-022-00287-8

Mühlhoff, R. (2021). Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology, 23*(4), 675–690. https://doi.org/10.1007/s10676-021-09606-x

Mutimukwe, C., Viberg, O., Oberg, L., Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development and validation. *British Journal of Educational Technology, 53*(6), 2115-2132. https://doi.org/10.1111/bjet.13234

Naz, H., & Kashif, M. (2023). Artificial intelligence and predictive marketing: an ethical framework from managers' perspective. *Spanish Journal of Marketing – ESIC*, *29* (1), 22-45. https://doi.org/10.1108/SJME-06-2023-0154

Niebel, C. (2021). The impact of the general data protection regulation on innovation and the global political economy. *Computer Law and Security Review*, 40. https://doi.org/10.1016/j.clsr.2020.105523

Okwonu, F. Z., Ahad, N. A., Apanapudor, J. S., & Arunaye, F. I. (2023). Chi-square and adjusted standardised residual analysis. *ASM Science Journal*, *16*, 1-15. https://doi.org/10.32802/asmscj.2023.985

Ozturk, O. (2024). The impact of AI on international trade: Opportunities and challenges. *Economies, 12*(11), 298. https://doi.org/10.3390/economies12110298

Pan, Y., Ruan, Y., Chang, M., Lyu,D., & Li, Y. (2024). Read or skip privacy polices when installing apps on wearable devices: the roles of perceived necessity and threat clues. *Humanities & Social Sciences Communcations, 11*(1), 210. https://doi.org/10.1057/s41599-024-02989-4

Park, Y. (2011). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. https://doi.org/10.1177/0093650211418338

Predictive Success Corporation. (2019, May 6). *A brief history of predictive analytics: How we've come to be able to predict the future*. *Medium*. https://medium.com/@predictivesuccess/a-brief-history-of-predictive-analytics-f05a9e55145f

Reshid, T. M. (2023). Monte Carlo simulation and derivation of chi-square statistics. *American Journal of Theoretical and Applied Statistics, 12*(3), 51-65. https://doi.org/10.11648/j.ajtas.20231203.13

Robbins, S. (2020). AI and the path to envelopment: knowledge as a first step towards the responsible regulation and use of AI-powered machines. *AI & Society. 35,* 391-399. https://link.springer.com/article/10.1007/s00146-019-00891-1

Samuel, A. (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development*, *3*(3), 210-229, https://doi.org/10.1147/rd.33.0210

Schober, P., & Vetter, T. R. (2020). Nonparametric statistical methods in medical research. *Anesthesia & Analgesia, 131*(6), 1862-1863. https://doi.org/10.1213/ANE.0000000000005101

Schwecke, T. J. (2021). *Applications of predictive analytics: Evolution, integration in modern society, and ethical concerns*. University of Wisconsin–Milwaukee. https://uwm.edu/actuarial-science/wp-content/uploads/sites/549/2021/06/annotated-Predictive_Analytics_Paper-7.pdf?utm_source=chatgpt.com

Shaik, M. (2023). Impact of artificial intelligence on marketing. *East Asian Journal of Multidisciplinary Research, 2*(3), 993-1004. https://doi.org/10.55927/eajmr.v2i3.3112

Shrestha, Y. R., Krishna, V., & Von Krogh, G. (2021). Augmenting organizational decision-making with deep learning algorithms: Principles, promises, and challenges. *Journal of Business Research, 123*, 588-603. https://doi.org/10.1016/j.jbusres.2020.09.068

Slater, P., & Hasson, F. (2025). Quantitative Data Quality Assurance, Analysis and Presentation. *Journal of Psychiatric and Mental Health Nursing,* 32, 723-727. https://doi.org/10.1111/jpm.13143

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167-196. https://doi.org/10.2307/249477

Supply Chain Magazine. (2024, janeiro 25). *8 tendências de inteligência artificial para acompanhar em 2024*. Supply Chain Magazine. https://www.supplychainmagazine.pt/2024/01/25/8-tendencias-de-inteligencia-artificial-para-acompanhar-em-2024/

Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems, 91*, 101469. https://doi.org/10.1016/j.is.2019.101469

Turing, A (1950). I - Computing Machinery and Intelligence. *Mind, 59*(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433

União Europeia. (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de*

Dados). *Jornal Oficial da União Europeia, L119*, 1-88. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Veale, M., & Zuiderveen Borgesius, F. J. (2021). The impact of the General Data Protection Regulation on innovation and the global political economy. *Computer Law & Security Review, 40*, 105523. https://doi.org/10.1016/j.clsr.2020.105523

Verma, S. (2019). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Vikalpa*, *44*(2), 97-98. https://doi.org/10.1177/0256090919853933

Verma, S., Sharma, R., Deb, S., & Maitra, D. (2021). Artificial intelligence in marketing: Systematic review and future research direction. *International Journal of Information Management Data Insights, 1*(1), 100002. https://doi.org/10.1016/j.jjimei.2020.100002

Wolniak, R., & Grebski, W. (2023). Functioning of predictive analytics in business. *Scientific Papers of Silesian University of Technology. Organization and Management Series, 175,* 603-616. http://dx.doi.org/10.29119/1641-3466.2023.175.40

Yang, H., Lee, H. (2025). Common statistical methods used in medical research. *Kosin Medical Journal*, *40*(1), 1-8. https://doi.org/10.7180/kmj.24.160

Ying, S., Huang, Y., Qian,L & Song, J. (2023). Privacy paradox for location tracking in mobile social networking apps: The perspectives of behavioral reasoning and regulatory focus. *Journal of Consumer Behaviou, 190,* 122412. https://doi.org/10.1016/j.techfore.2023.122412

Zaeem, R. N., & Barber, K. S. (2021). *Human and privacy rights* (UTCID Report #21-09). The University of Texas at Austin, Center for Identity.

Zasuwa, J. (2023). Artificial intelligence in marketing: Literature review and future research directions. *Scientific Papers of the Częstochowa University of Technology Management, 175*, 524-530. http://dx.doi.org/10.29119/1641-3466.2023.175.40

Apêndice

Apêndice 1

Questionário online "Preocupações de Privacidade com o uso da Inteligência Artificial e da Análise Preditiva no Comportamento de Compra do Consumidor On-line"

Preocupações de Privacidade com o uso da Inteligência Artificial e da Análise Preditiva no Comportamento de Compra do Consumidor On-line

Caro/a participante,

O meu nome é Carolina Ventura e estou, atualmente, a desenvolver a minha dissertação de mestrado, no âmbito do Mestrado em Gestão, na Universidade Europeia.

O presente estudo tem como objetivo analisar as preocupações de privacidade dos consumidores online, em relação à conduta das empresas, quando utilizam Inteligência Artificial e Análise Preditiva, para influenciar o comportamento de compra.

Para uma melhor compreensão sobre o tema desta investigação, peço que leia as seguintes definições:
Inteligência Artificial (IA) - "Aptidão de um sistema para interpretar com precisão dados provenientes do exterior, aprender a partir deles e aplicar esses conhecimentos de forma adaptativa e flexível, para atingir metas e executar tarefas específicas." (Hermann, 2022, p.45)

Análise Predititva - "A análise preditiva é a prática de analisar grandes quantidades de dados, ao usar ferramentas de IA , com
o objetivo de prever eventos futuros, incluindo o comportamento e preferências humanas futuras." (Bracanovic, 2019, p.264)

É neste contexto que venho solicitar a sua participação, mediante o preenchimento deste questionário.

O preenchimento deste inquérito é voluntário e levará aproximadamente 5 minutos. As suas respostas serão tratadas de forma **confidencial,** sendo exclusivamente para **fins académicos**.

Desde já, agradeço pela sua participação.

Se tiver alguma dúvida ou questão, não hesite em contactar-me através de carolina.ventura01@hotmail.com.

Secção 1: Conhecimento e Comportamento Relacionados à Privacidade Online

1. Como avalia o seu conhecimento sobre riscos de privacidade online? *

- ◯ Muito Baixo
- ◯ Baixo
- ◯ Médio
- ◯ Alto
- ◯ Muito Alto

2. Costuma ler as políticas de privacidade antes de aceitar os termos de um serviço online? *

- ◯ Nunca
- ◯ Raramente
- ◯ Por vezes
- ◯ Sempre

3. Considera que os seus dados pessoais podem ser comprometidos em virtude de usos indevidos na internet? *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem discordo, nem concordo
- ◯ Concordo
- ◯ Concordo totalmente

Secção 2: Confiança nas Empresas e Partilha de Dados Pessoais

4. Já evitou fornecer informações pessoais num site online por falta de confiança? *

- ◯ Sim
- ◯ Não

5. Se respondeu "Sim", quais foram os principais motivos (pode selecionar mais do que uma opção)

- ☐ Reputação da empresa desconhecida ou negativa
- ☐ Experiências negativas anteriores
- ☐ Excesso de informação solicitada
- ☐ Falta de opções de consentimento
- ☐ Medo de exposição dos dados pessoais
- ☐ Outra:

6. Confia nas empresas para protegerem devidamente os seus dados pessoais? *

- ◯ Discordo Totalmente
- ◯ Discordo
- ◯ Nem discordo, nem concordo
- ◯ Concordo
- ◯ Concordo Totalmente

Secção 3: Impacto das Preocupações e Experiências na Compra Online

7. O receio de que os seus dados pessoais possam ser usados indevidamente já fez com que desistisse de uma compra online? *

- ◯ Discordo Totalmente
- ◯ Discordo
- ◯ Nem discordo, nem concordo
- ◯ Concordo
- ◯ Concordo Totalmente

8. Alguma vez já sofreu de uma violação de privacidade online, como roubo de dados, conta *hackeada* ou uso indevido de informações pessoais? *

- ◯ Sim
- ◯ Não

9. Se respondeu "Sim", após essa experiência a sua intenção de compra em plataformas digitais:

- ◯ Diminui significativamente
- ◯ Diminui ligeiramente
- ◯ Permaneceu inalterada
- ◯ Aumentou ligeiramente
- ◯ Aumentou significativamente

Secção 4: Conhecimento sobre IA e Análise Preditiva

10. Qual é o seu nível de familiaridade com os conceitos de Inteligência Artificial e Análise Preditiva? *

- ◯ Muito Baixo
- ◯ Baixo
- ◯ Moderado
- ◯ Alto
- ◯ Muito Alto

11. Compreende como a Inteligência Artificial e a Análise Preditiva utilizam os seus dados para sugerir produtos, conteúdos ou anúncios? *

- ◯ Não Compreendo
- ◯ Compreendo Pouco
- ◯ Compreendo parcialmente
- ◯ Compreendo Bem
- ◯ Compreendo Totalmente

12. Quais destes tipos de dados, acredita que as empresas recolhem para prever e personalizar as suas preferências? (pode selecionar mais do que uma opção) *

- ☐ Histórico de pesquisas
- ☐ Localização Geográfica
- ☐ Tempo gasto em determinados conteúdos
- ☐ Compras anteriores
- ☐ Interações nas redes sociais
- ☐ Nenhuma destas opções
- ☐ Outra: _____

Secção 5: Reputação e Confiança na Partilha de Dados

13. A reputação de uma empresa influencia: a sua confiança na mesma, na sua decisão de comprar online e de fornecer os seus dados pessoais? *

- ◯ Discordo Totalmente
- ◯ Discordo
- ◯ Nem discordo, nem concordo
- ◯ Concordo
- ◯ Concordo Totalmente

14. Em relação aos seus dados pessoais, qual das seguintes opções estaria mais disposto a compartilhar com uma empresa online, se esta tiver uma boa reputação? (pode selecionar mais do que uma opção) *

- ☐ Nome e e-mail
- ☐ Número de telemóvel
- ☐ Endereço de envio
- ☐ Número de cartão de crédito/débito
- ☐ Localização em tempo real
- ☐ Nenhum dos anteriores
- ☐ Outra: _____

15. Género *

- ◯ Masculino
- ◯ Feminino
- ◯ Prefiro não dizer
- ◯ Outra: _____

16. Qual é a sua faixa etária? *

- ◯ Menos de 18 anos
- ◯ 18 - 24 anos
- ◯ 25 - 34 anos
- ◯ 35 - 44 anos
- ◯ 45 - 54 anos
- ◯ 55 - 64 anos
- ◯ Mais de 65 anos

17. Qual é o seu nível de escolaridade? *

- ◯ Ensino básico
- ◯ Ensino Secundário
- ◯ Licenciatura
- ◯ Pós-Graduação
- ◯ Mestrado
- ◯ Doutoramento

18. Com que frequência realiza compras online? *

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Frequentemente
- ◯ Sempre