INSTITUTO POLITÉCNICO DE LISBOA

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

INTELIGÊNCIA ARTIFICIAL NUMA SEGURADORA: ESTUDO DE CASO SOBRE OS DESAFIOS ÉTICOS, OPERACIONAIS E DE SEGURANÇA

BEATRIZ SIMÃO NEVES

Lisboa, janeiro 2026

INSTITUTO POLITÉCNICO DE LISBOA

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

INTELIGÊNCIA ARTIFICIAL NUMA SEGURADORA: ESTUDO DE CASO SOBRE OS DESAFIOS ÉTICOS, OPERACIONAIS E DE SEGURANÇA

BEATRIZ SIMÃO NEVES

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão e Empreendedorismo, realizada sob a orientação científica da Professora Doutora Tânia Jesus.

Constituição do Júri:

Presidente do Júri: Especialista Carlos Nunes

Arguente: Doutor Pedro Pinheiro

Orientador: Doutora Tânia Jesus

Agradecimentos

A realização desta dissertação foi um desafio em vários aspetos, além de todo o esforço depositado para que a sua concretização fosse possível. Pude contar com o apoio de várias pessoas, presentes na minha vida, que me fizeram acreditar de que somos capazes de tudo o que queremos, e que nada é impossível, a não ser que assim o decidamos.

Começando pela minha orientadora da dissertação, a Professora Doutora Tânia Jesus, que me apoiou no necessário, acompanhou durante este tempo e que acreditou nas minhas capacidades.

À minha família, que acreditou em mim desde o início, que me apoiou nesta decisão de embarcar no desafio que foi realizar o mestrado, que me deu a mão nos momentos difíceis e que disse "tu consegues", o meu mais profundo agradecimento.

Aos meus amigos, que igualmente me apoiaram nesta jornada, especialmente a uma amiga que partilhou comigo este caminho. Obrigada pelo apoio, pelo companheirismo, paciência e força para que me ajudassem a concretizar esta meta.

A todos, família, amigos, professores e instituição do ISCAL, o meu agradecimento.

Resumo

A dissertação realizada pretende analisar o impacto da implementação da Inteligência Artificial numa seguradora com atuação em Portugal, com um especial foco nos desafios éticos, operacionais e de segurança que ela implica, aquando da sua aplicação no setor em causa.

Depois do estabelecimento de tecnologias no dia a dia de cada indivíduo, a inteligência artificial surge para revolucionar a forma como percecionamos o mundo tecnológico, tanto a nível de lazer como a nível laboral. No setor segurador abriu portas para a possibilidade de automatização de processos, produtos desenvolvidos à medida do cliente, a maior facilidade em detetar fraudes e ainda a otimização na análise de risco e de dados. Estas possibilidades representam também desafios e inquietações quanto à transparência e enviesamento de dados sensíveis, proteção de dados e a fiabilidade nestes tipos de sistemas, ainda pouco avaliados.

Para este estudo, foram selecionados três colaboradores da seguradora em estudo, que representam os desafios estudados ao longo da investigação, sendo eles das áreas de Risco, *Compliance* e *Contact Center*. Esta escolha permite identificar o estágio de implementação de inteligência artificial em que a seguradora se encontra, mas também identificar os diferentes papéis de cada área e as suas perceções relativamente aos riscos e benefícios. O *Contact Center* é a área com uma aplicação mais direta, enquanto as áreas de *Compliance* e Risco desempenham um papel mais prudente, definindo o tipo de controlo ético e regulatório a aplicar.

Os resultados apresentados demonstram que, dependendo do papel de cada colaborador, a perceção relativamente à inteligência artificial muda e é dada uma grande ênfase à importância da criação de uma governação bem sustentada, promovendo a inovação tecnológica.

Palavras-chave: Inteligência Artificial, ética, segurança, operacional, seguro

Abstract

This study aims to analyze the impact of the implementation of Artificial Intelligence in an insurance company operating in Portugal, with a special focus on the ethical, operational, and security challenges it poses when applied in this sector.

After the establishment of technologies in the daily lives of everyone, artificial intelligence has emerged to revolutionize the way we perceive the technological world, both in terms of leisure and work. In the insurance sector, it has opened the door to the possibility of process automation, customer-tailored products, easier fraud detection, and optimization of risk and data analysis. These possibilities also represent challenges and concerns regarding the transparency and bias of sensitive data, data protection, and the reliability of these types of systems, which have yet to be fully evaluated.

For this study, three employees from the insurance company under study were selected, representing the challenges studied throughout the investigation, from the areas of Risk, *Compliance*, and *Contact Center*. This choice allows us to identify the stage of artificial intelligence implementation at which the insurance company finds itself but also identifies the different roles of each area and their perceptions regarding risks and benefits. The *Contact Center* is the area with the most direct application, while the *Compliance* and Risk areas play a more prudent role, defining the type of ethical and regulatory control to be applied.

The results presented show that, depending on the role of each employee, the perception of artificial intelligence changes, and great emphasis is placed on the importance of creating well-supported governance, promoting technological innovation.

Keywords: Artificial Intelligence, ethics, security, operational, insurance

Índice

Índice de Tabelas

Índice de abreviaturas

IA – Inteligência Artificial

NLP - Processamento Linguagem Natural

RGPD - Regulamento Geral sobre a Proteção de Dados

ML - *Machine Learning*

LGPD – Lei Geral de Proteção de Dados

AI Act- Artificial Inteligence Act

IoT – Internet das Coisas

SWOT - *Strengths, Weaknesses, Opportunities, Threats*

APS – Associação Portuguesa de Seguradoras

ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões

CNPD - Comissão Nacional de Proteção de Dados

IVR – Resposta Interativa por Voz

1. Introdução

A Inteligência Artificial (IA) está a revelar ser uma tecnologia transformativa quanto ao funcionamento das organizações. Oferece soluções alternativas e eficientes para a análise e tratamento de dados, transformação de processos, anteriormente manuais, para automatizados.

Uma vez que o setor segurador, o setor escolhido para o estudo, é altamente regulamentado, composto por estruturas bem hierarquizadas e depende fortemente de dados estatísticos, a implementação de IA apresenta ser um desafio, com uma evolução mais faseada, uma vez que apresenta potenciais impactos a nível operacional, estratégico e ético.

A implementação de IA nas seguradoras tem demonstrado possibilidades de otimização de tarefas atualmente rotineiras, como é o caso do atendimento ao cliente por meio de *chatbots*, ou ainda a triagem de emails recorrendo a processamento de linguagem natural (NLP). Esta tecnologia permite ainda a capacidade para deteção de fraudes, a análise preditiva de risco e personalização dos produtos, à medida do cliente. O desenvolvimento da tecnologia para a criação destas inovações fortaleceu a forma como se perceciona a IA, passando a abordá-la como uma ferramenta estratégica, com a capacidade de melhorar a eficiência, reduzir custos a longo prazo e responder com maior celeridade às necessidades e pedidos dos clientes.

Além dos benefícios apresentados, a IA levanta questões importantes relacionadas com a transparência algorítmica, enviesamento nos dados, a possível substituição de funções humanas por um "robot", o alinhamento das tecnologias com o Regulamento Geral sobre a Proteção de Dados (RGPD) e a perceção dos riscos digitais exigem um cuidado acrescido e uma gestão cautelosa. Ter assente a complexidade destes desafios leva a que seja relevante investigar a forma como a IA está a ser integrada nas seguradoras. Além disso, entender como os profissionais desta área percecionam a entrada deste tipo de tecnologia no seu dia a dia demonstrará a sua abertura para novas tecnologias, ou por outro lado, o nível de resistência à mesma.

Assim, o objetivo principal desta investigação passou por analisar os impactos da introdução da Inteligência Artificial na seguradora escolhida, dando como foco principal os desafios éticos, operacionais e de segurança que a empresa enfrenta. Como método de estudo, recorreu-se a uma abordagem qualitativa, por meio da realização de entrevistas semiestruturadas a três colaboradores, das áreas de Risco, *Compliance* e *Contact Center*. A escolha destas três áreas permitiu dar enfoque aos principais objetivos da investigação, sendo estas operacionais, estratégicas e regulatórias, e avaliar como a IA está a ser percecionada e regulada pela organização.

A investigação realizada foi conduzida com método exploratório, com a finalidade de entender a utilidade da IA no setor segurador, e refletir sobre a forma de implementação, determinando quais as ferramentas de governação tecnológica e se estas garantem a conformidade ética e legal.

Com a elaboração deste estudo, pretende-se contribuir para o debate académico que está atualmente a ocorrer em torno deste tema ainda considerado recente, fornecer outras sugestões de temas a investigar, e ainda com o objetivo de apoiar a adoção destas tecnologias de uma forma consciente, segura e eficiente.

1.1. Importância do tema

O tema escolhido "Inteligência Artificial numa seguradora: estudo de caso sobre os desafios éticos, operacionais e de segurança" foi escolhido pela pertinência no panorama atual que está a atravessar, no contexto de transformação digital que o setor dos serviços financeiros, e neste caso, o setor segurador. O rápido desenvolvimento tecnológico, que nos últimos tempos foi impulsionado principalmente por algoritmos de *machine learning*, *Big Data* e automação inteligente, tem vindo a resultar numa alteração quanto aos modelos tradicionais de operação, gestão e relacionamento com cliente.

Uma vez que o setor segurador foi historicamente construído com alicerces de confiança, previsibilidade, regulamentação rigorosa. a introdução da IA não se limita apenas a uma questão de eficiência ou de modernização, mas sim a uma reestruturação no modo como se avaliam riscos, na tomada de decisão de sinistros e na forma como se gerem as informações sensíveis dos clientes. Com base no descrito, surgiram as questões suficientes para criar um debate quanto às implicações éticas, à sustentabilidade operacional das inovações tecnológicas, e também muito importante, a segurança dos dados processados por sistemas inteligentes.

O tema escolhido ganha relevância pela grande discussão que continua a existir à volta do tema IA, além de que foi relevante entender qual a visão dos colaboradores relativamente a este tema, que neste caso se centrou no setor segurador. Assim, dando voz às áreas de Risco, *Compliance*, e *Contact Center* permitiu alcançar a complexidade do processo de transformação bem como a contribuição para uma construção com base em boas práticas relativamente à adoção responsável de IA.

A investigação desenvolvida permitiu um aprofundamento do tema no âmbito académico, e disponibilizou algumas das perceções úteis para estudos futuros que abordem a inovação equilibrada, a conformidade legal e a sustentabilidade organizacional.

1.2. Objetivos da investigação

O estudo teve como objetivo principal entender a forma e o estágio de como a IA está a ser implementada numa seguradora em Portugal, e quais os impactos apresentados pela transformação tecnológica, ao nível ético, operacional e de segurança. Tal como mencionado anteriormente, a digitalização no setor segurador apresenta ser cada vez mais um fator determinante quanto à sua competitividade, e assim torna-se importante avaliar tanto os benefícios operacionais da utilização da IA como os riscos e desafios associados à mesma, se está em concordância com os regulamentos e se centra na confiança com os clientes.

A investigação desenvolvida focou-se principalmente na perceção de três colaboradores das seguradora escolhida, sendo eles das áreas de Risco, *Compliance*, e *Contact Center*, e esta escolha teve como principal objetivo captar as diferentes visões sobre o tema da IA entre cada área, e entender se o seu entendimento era distinto ou se se conciliava em algum ponto. Esta escolha baseou-se no seu papel a nível organizacional e na forma como percecionam a inovação tecnológica. A área de Risco desempenha um papel analítico e de suporte à decisão. O *Compliance* tem a responsabilidade de garantir a conformidade ética e legal do processos, enquanto a área do *Contact Center* apresenta uma dimensão operacional com uma maior e mais direta relação com o cliente.

Através da experiências e perspetivas dos profissionais, o pretendido na investigação desenvolvida foi, por um lado, identificar os processos em que a IA já se encontra presente, e por outro, reconhecer os obstáculos associados à sua aplicação e as expectativas associadas à evolução futura desta tecnologia. Assim, o estudo desenvolvido aponta contribuir para o desenvolvimento de um conhecimento mais detalhado sobre a transformação digital que está a decorrer na seguradora em estudo, incentivando uma reflexão crítica sobre a implementação equilibrada entre inovação, segurança, ética e sustentabilidade.

1.3. Metodologia e estrutura da investigação

A investigação desenvolvida seguiu uma abordagem qualitativa, com natureza exploratória, e a principal técnica de recolha de dados foi a realização de entrevistas semiestruturadas. A metodologia escolhida permitiu uma compreensão mais aprofundada das experiências, perspetivas e interpretações dos colaboradores da seguradora selecionada, sobre a implementação da IA nessa organização. O objetivo estudo é avaliar as implicações éticas, operacionais e de segurança.

As entrevistas foram realizadas a três colaboradores, que exercem diferentes funções em áreas distintas, sendo estas Risco, *Compliance* e *Contact Center*, o que permitiu uma recolha diversificada e complementar. A escolha foi intencional, e teve por base a experiência de cada um

e o nível de envolvimento, seja ele direto ou indireto, em processos relacionados com a implementação de IA na seguradora. Para as entrevistas foi elaborado previamente um guião, conforme os guiões de entrevista apresentados nos anexos 2, 3 e 4, com perguntas abertas que por um lado orientaram a conversa, mas que por outro permitiram uma maior flexibilidade para o aprofundamento de aspetos que fossem considerados relevantes. Após as entrevistas, os dados recolhidos foram analisados por temática, de forma a identificar padrões, divergências e convergências nas respostas obtidas.

A dissertação desenvolvida organizou-se em seis capítulos. A primeira tratou-se da Introdução, parte em que se contextualizou o problema, os principais objetivos da investigação, a importância do tema e as questões que orientaram a investigação.

A segunda foi a Revisão da Literatura, que abordou a evolução histórica dos seguros, o desenvolvimento da IA, os principais tipos de IA, as suas formas de aplicação no setor segurador, e também os desafios éticos operacionais e de segurança associados. A parte seguinte remeteu para a metodologia adotada, realizando uma análise do setor, bem como uma breve caraterização da empresa, o tipo de abordagem metodológica, as técnicas de recolha e análise de dados, e por fim as limitações do estudo.

Na quarta parte analisaram-se e interpretaram-se os resultados obtidos nas entrevistas, dividindo-as por temas e depois por comparação entre áreas. A quinta parte foi dedicada à apresentação dos resultados, comparando-os com a literatura anteriormente reunida e analisada. A última parte do estudo expôs as conclusões, identificando as maiores contribuições verificadas na investigação, quais as limitações detetadas e propostas para possíveis investigações futuras.

A estrutura definida teve como objetivo garantir que a abordagem fosse clara, coerente e fundamentada com o objetivo do estudo, e permitiu uma compreensão abrangente relativamente à complexidade que a integração de IA no setor segurador envolve.

2. Revisão de Literatura

2.1. Introdução ao Seguro

Antes de se mencionar e definir a palavra "seguro", é necessário entender qual a sua origem. Porque é que existe? De onde vem a necessidade?

São desempenhadas diariamente atividades pelos humanos que envolvem risco a vários níveis e de diferentes formas. Estas atividades podem ser do foro profissional, pessoal. Tanto pode acontecer a nível físico, um risco a que estamos expostos diariamente por meio de um acidente, doença, etc , como pelo "risco" que envolve a compra de uma casa, automóvel, ou outro objeto de grande valor (Guedes-Vieira, 2012).

O risco é algo inevitável, no entanto, o instinto humano é procurar o contrário, ou seja, eliminar o risco. Esta procura é realizada por meio de o localizar, perceber de que forma pode ser minimizado ou controlado. De certa forma, "assegurado" (Guedes-Vieira, 2012).

Dessa forma é possível concluir que "o risco está tão intimamente ligado à atividade [humana] como a morte à vida" (Jacob, 1979).

O termo encontrado para se definir a necessidade de reduzir o risco é o seguro. De realçar que o seguro não diminui em momento algum os riscos associados à vida humana ou por exemplo de uma empresa. O seguro "nasceu" para diminuir as consequências de eventos do quotidiano, por meio de uma compensação (Guedes-Vieira, 2012). Ferguson (2009) defende que "o impulso financeiro mais básico é poupar para o futuro porque o futuro é imprevisível". Para que se concretize a compensação a alguém perante uma situação de risco dito concretizado, é necessário existir algo por escrito que garanta o que está coberto em caso de sinistro.

Os primeiros indícios da origem dos seguros, na altura considerados acordos mútuos, datam os anos 4700 a.C., e mais tarde no século XVIII a.C. Nestas épocas estes acordos funcionavam como uma "assistência mútua" (Guedes-Vieira, 2012), e apresentavam-se por forma de solidariedade e de compensação, no caso de mercadorias não chegarem ao seu destino por motivo de algum acidente ou imprevisto. Já na Grécia antiga, era pago um subsídio aos familiares daqueles que fossem para a guerra e falecessem durante a mesma (Guedes-Vieira, 2012).

Nestas épocas mencionadas, os acordos funcionavam de forma direta, sem a intervenção de terceiros, e é na Idade Média que este panorama se altera. No âmbito do comércio marítimo, é criado um "empréstimo", que consiste na transferência do risco a um terceiro, que assume o risco da mercadoria se perder, mediante uma remuneração, mais tarde conhecida como "prémio" (Guedes-Vieira, 2012).

O seguro contra incêndios surgiu depois de 1666 em Londres, aquando de um grande incêndio, que destruiu centenas de edifícios e que tirou a vida também a centenas de pessoas (Guedes-Vieira, 2012).

Inicialmente, em Portugal, não existiam contratos de seguro por escrito, pelo que estes eram celebrados de forma verbal na sua grande maioria. Denominam-se por contratos de seguro os documentos por escrito, com uma componente jurídica e todas as coberturas e exclusões, para que possa saber qual o risco que é assumido pela terceira parte. Uma vez que não existiam muitos contratos por escrito, e não se sabia o que estava coberto, criou-se o cargo de "escrivão de seguros", que atualmente conhecemos como Autoridade Portuguesa de Regulação e de supervisão de Seguros, ou ASF (Autoridade de Supervisão de Seguros e Fundos de Pensões) conforme Guedes-Vieira (2012).

Os restantes seguros, como por exemplo o automóvel, surgem nos anos seguintes, ao longo do tempo contribuindo para que os séculos XVII e XVIII fossem marcados pelo impulsionamento do crescimento do setor segurador (Masci, 2011).

2.1.1. Seguro de Vida

O seguro de vida surge mais tarde, no final do século XVII (Guedes-Vieira, 2012). A primeira apólice foi emitida em 1536, também em Londres, para um comerciante que pagou um prémio que o assegurava que, caso falecesse no espaço de um ano, a sua família receberia uma indemnização (Masci, 2011). Nesta época não existiam tabelas atuariais que apresentavam do nível de risco perante determinada situação, e que por sua vez implicariam pagar um prémio maior ou menor, o que levou à falência de muitas empresas (Bernstein, 1998).

Por conseguinte, os anos seguintes foram dedicados ao desenvolvimento do seguro de vida, com avanços no estudo da probabilidade e da estatística. John Graunt fundou a ciência da demografia ao analisar registos de nascimentos e falecimentos em Londres, que lhe permitiu estabelecer padrões de mortalidade, bem como a esperança média de vida, que são atualmente as bases para os seguros de vida (Graunt, 1975). Edmund Halley foi o autor da primeira tabela de mortalidade baseada em dados estatísticos publicada (Halley, 1693). Esta tabela permitiu calcular a expectativa de vida com mais precisão. Mais tarde, Abraham de Moivre desenvolveu o conceito de distribuição normal e aprofundou os cálculos de risco em seguros de vida (Stigler, 1986).

Estes foram algumas das figuras que permitiram o surgimento de seguradoras de vida mais organizadas, e com uma maior facilidade em definir prémios que contribuíram para que a partir do século XVIII, o seguro de vida começasse a expandir-se para outros países, tornando-se um setor mais estruturado.

2.1.2. Expansão nos séculos XVIII e XIX

Durante e após a revolução industrial, o seguro de vida foi-se tornando mais acessível (Masci, 2011). Por sua vez, o aumento da longevidade e melhorias na medicina reduziram os riscos associados aos seguros de vida, tornando-os mais rentáveis para as seguradoras (Cain & Hopkins, 1993). Fatores como o desenvolvimento das tabelas atuariais e da matemática dos seguros permitiram que a atribuição de prémios aos clientes fosse mais exata. Com a Revolução Industrial surgiram mudanças nos padrões de emprego e segurança, aumentando dessa forma a procura por seguros de vida de proteção contra a perda da renda (Pearson, 2004).

Assim, o seguro de vida tornou-se um elemento essencial no planeamento financeiro das famílias, assegurando uma melhor estabilidade económica dos dependentes em caso de falecimento do tomador do seguro (Rubinstein, 1993). Facilitou o crescimento do mercado de capitais, pois criou um incentivo à poupança, proporcionando uma rede de segurança às empresas. Por sua vez, as poupanças "alimentam a economia, uma vez que são investidas através da intermediação financeira, contribuindo assim para a concretização das iniciativas dos empresários" (Masci, 2011).

2.2. Evolução da Inteligência Artificial

A IA pode ser definida de diferentes formas, dependendo da perspetiva adotada. As abordagens clássicas da IA podem ser organizadas ao longo de duas dimensões: algumas focam-se nos processos de pensamento e raciocínio, enquanto outras consideram o comportamento da máquina. Além disso, algumas abordagens medem o sucesso da IA em comparação com a cognição humana, enquanto outras a avaliam com base em um desempenho ideal de racionalidade (Russell & Norvig, 2009).

Em 2021, Russell e Norvig defenderam a Inteligência Artificial como sendo a capacidade de sistemas computacionais de realizar tarefas que tradicionalmente exigem inteligência humana, como o conhecimento, o raciocínio, a resolução de problemas, a perceção e o processamento de linguagem natural (Russell & Norvig, 2021). De acordo com Nilsson (1998), a IA é um campo da ciência da computação dedicado ao estudo de agentes inteligentes, ou seja, sistemas que percebem seu ambiente e tomam decisões para maximizar as suas chances de sucesso em atingir objetivos predefinidos.

O conceito de IA remonta à década de 1940, quando pioneiros como Alan Turing discutiram a possibilidade de máquinas que poderiam "pensar". Turing introduziu o famoso Teste de Turing em 1950, uma experiência para avaliar se uma máquina pode exibir comportamento indistinguível do humano (Turing, 1950). Este marco teórico pavimentou o caminho para a pesquisa formal no campo. Este passa por quatro etapas:

A primeira etapa é “Agir como um humano: O Teste de Turing”. Alan Turing propôs, em 1950 (Turing, 1950), um teste para definir IA baseado na interação entre humanos e máquinas. Um computador é considerado inteligente se um avaliador humano não conseguir distingui-lo de outro ser humano com base nas respostas em formato de texto. Para passar no teste, um sistema deve ter habilidades em quatro campos. São eles o processamento de linguagem natural, a representação de conhecimento, o raciocínio automatizado e o conhecimento de máquina.

Uma versão expandida, o "Teste de Turing Total", adiciona desafios percetivos e motores, exigindo também visão computacional e robótica. No entanto, poucos pesquisadores esperam diretamente passar no teste, pois acreditam que é mais produtivo focar nos princípios fundamentais da IA do que simplesmente imitar o comportamento humano (Turing, 1950; Russell & Norvig, 2009).

A segunda etapa passa por “Pensar como um humano: A abordagem da modelagem cognitiva”. Esta abordagem de “pensar como um humano” procura modelar o pensamento humano para reproduzi-lo em máquinas. Para isso, são utilizados métodos como introspeção, experimentação psicológica e neuroimagem. Um programa de IA que apresenta padrões de raciocínio semelhantes aos humanos pode ser considerado um modelo válido da cognição humana.

A ciência cognitiva é um campo interdisciplinar que une a IA à psicologia experimental. Um exemplo clássico é o "*General Problem Solver*" (GPS), criado por Newell e Simon (1961), que visava imitar o raciocínio humano na resolução de problemas. Atualmente, há uma distinção mais clara entre estudar o funcionamento do pensamento humano e desenvolver sistemas de IA eficientes, o que permitiu avanços em ambas as áreas (Newell & Simon, 1961; Wilson & Keil, 1999).

Na terceira etapa, Alan Turing analisa “Pensar racionalmente: As "leis do pensamento"”. Esta abordagem baseia-se na lógica formal, originada na filosofia aristotélica. Aristóteles propôs regras de raciocínio que resultam em conclusões corretas a partir de premissas verdadeiras. No século XIX, os lógicos desenvolveram notações formais para representar relações entre objetos e fatos do mundo. Em 1965, surgiram programas capazes de resolver qualquer problema expressável em lógica formal (Russell & Norvig, 2009).

Apesar do potencial teórico, essa abordagem enfrenta dois desafios principais: traduzir o conhecimento informal em lógica formal e lidar com a complexidade computacional, pois mesmo problemas simples podem exigir um poder computacional inatingível. Assim, embora a lógica continue a ser uma ferramenta importante, esta não é suficiente para resolver todos os desafios da IA (Russell & Norvig, 2009).

Por fim, “Agir racionalmente: A abordagem do agente racional”. Um agente é qualquer sistema que realiza ações, e um agente racional é aquele que procura o melhor resultado possível com

base no conhecimento próprio e nas circunstâncias. Diferente da abordagem baseada em lógica, que foca no raciocínio correto, a abordagem do agente racional enfatiza a tomada de decisão eficiente, mesmo em cenários de incerteza (Russell & Norvig, 2009).

Os agentes racionais precisam de diversas habilidades, como representação do conhecimento, raciocínio e conhecimento de máquinas. Esta abordagem é mais geral que a das "leis do pensamento", pois engloba diferentes estratégias de ação além do raciocínio lógico. Além disso, a racionalidade pode ser matematicamente definida, o que torna este modelo mais adequado ao desenvolvimento científico da IA (Russell & Norvig, 2009).

Entretanto, atingir a racionalidade perfeita é inviável em ambientes complexos devido às limitações computacionais. Portanto, grande parte da pesquisa em IA tem como objetivo desenvolver sistemas com "racionalidade limitada", ou seja, capazes de agir de forma adequada mesmo sem recursos computacionais infinitos (Russell & Norvig, 2009).

Noutro contexto, em 1956, o termo IA foi mencionado durante a conferência de Dartmouth, organizada por John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon. Este evento é frequentemente considerado o nascimento oficial da IA como disciplina académica (McCarthy et al., 1956). Nas décadas seguintes, o campo passou por avanços e períodos de estagnação, conhecidos como "invernos da IA", devido às limitações tecnológicas e ao excesso de expectativas (Crevier, 1993).

Nos últimos anos, o progresso em áreas como conhecimento profundo (deep learning) e redes neurais artificiais revolucionou o campo, levando a aplicações práticas de IA em reconhecimento de fala, visão computacional, robótica e diagnósticos médicos (Goodfellow, Bengio & Courville, 2016). Estas tecnologias são alavancadas por avanços na capacidade computacional e no acesso a grandes volumes de dados, tornando a IA uma ferramenta crucial em diversos setores.

2.2.1. Porquê definir Inteligência Artificial?

Tem sido demonstrado por vários autores a dificuldade definir IA. Para uns, não é considerado um problema essa falta de definição, pois uma parte de conceitos científicos amadurece ao longo dos anos. No entanto, Wang (2019) defende que esta dificuldade pode acarretar problemas na organização de pesquisas bem como no debate público sobre o tema.

Desta forma, é difícil prever capacidades futuras da IA e estabelecer critérios claros para a regulamentação da IA, afetando a formulação de estratégias e políticas públicas.

Wang (2019) defende que “Um programa é tradicionalmente projetado para fazer algo de uma maneira correta e predeterminada, enquanto a mente é construída para fazer o seu melhor com os recursos que possui.” Assim, embora seja possível discutir qual é a solução ou resposta correta,

isto não deve ser usado como critério de design para um sistema semelhante à mente (Wang, 2019).

Em 1995, Wang (1995) defende inteligência como sendo "a capacidade de um sistema de processamento de informações de se adaptar ao seu ambiente enquanto opera com conhecimento e recursos insuficientes".

2.2.2. Tipos de Inteligência Artificial

A IA geral (chatgpt 4.0, rôbots que tentam combinar visão computacional, entre outros) visa realizar diversas tarefas semelhantes às que os humanos fazem, enquanto a IA restrita é projetada para executar apenas atividades específicas. São alguns exemplos de IA restrita os assistentes virtuais com a Alexa e a Siri, sistemas de reconhecimento de imagem e fala (face ID e sistema de transcrição automática), *chatbots* de atendimento ao cliente, entre outros. Atualmente, todas as aplicações de IA fazem parte da segunda categoria. Para alcançar uma IA geral, ainda é preciso superar desafios como o desenvolvimento de senso comum, autoconsciência e a capacidade de estabelecer os seus próprios objetivos.

Outras formas de referir ou segmentar a IA passam por defini-la como fraca ou forte.

Por um lado, a IA fraca, também conhecida como IA restrita, refere-se a sistemas projetados para executar tarefas específicas, facilitando ou substituindo o trabalho humano em processos administrativos, operacionais ou analíticos. Estes sistemas são amplamente utilizados na atualidade, englobando assistentes virtuais, algoritmos de recomendação e sistemas de reconhecimento de imagem e voz (Schwab, 2016). A IA fraca não possui consciência, compreensão genuína ou capacidade de tomar decisões de forma autónoma fora dos parâmetros programados (Russell & Norvig, 2009).

Por outro lado, a IA forte visa replicar integralmente as capacidades cognitivas humanas, abrangendo perceções, crenças e outros estados mentais complexos (High-Level Expert Group on AI, 2018). A IA forte teria a capacidade de aprender de forma autónoma, tomar decisões independentes e adaptar-se a novos contextos sem necessidade de reprogramação. Entretanto, ainda não existe um sistema que atenda plenamente a esses requisitos, uma vez que as condições necessárias para que um computador possa ser descrito como verdadeiramente inteligente permanecem controversas (Walch, 2019).

2.2.3. Aspetos Tecnológicos e Desafios

Tanto a IA fraca como a forte são construídas a partir de algoritmos avançados, diferenciando-se pelos seus objetivos e finalidades (Joshi, 2019). Apesar dos avanços na área, a IA forte ainda

enfrenta desafios significativos, como a ausência de um critério claro para definir o sucesso e limitações técnicas que impedem o desenvolvimento de sistemas autónomos. Segundo o Stanford University Department of Philosophy (2018), uma das principais dificuldades está em determinar até que ponto um computador pode ser considerado capaz de pensar por si próprio, sem qualquer assistência humana. A evolução deste tipo de tecnologia deve ser acompanhada com atenção, tanto por pesquisadores quanto por formuladores de políticas, a fim de garantir que o seu desenvolvimento ocorra de forma ética e alinhada com os interesses humanos.

Embora a IA fraca já esteja amplamente integrada à sociedade e às atividades económicas, a IA forte permanece como um objetivo distante, ainda sujeito a discussões filosóficas e desafios tecnológicos. A evolução deste tipo de tecnologia deve ser acompanhada com atenção, tanto por pesquisadores quanto por formuladores de políticas, a fim de garantir que o seu desenvolvimento ocorra de forma ética e alinhada com os interesses humanos.

Muitos sistemas de IA dependem de grandes volumes de dados para funcionar bem. No entanto, se os dados utilizados forem tendenciosos ou não representarem corretamente toda a diversidade da sociedade, isto torna-os expostos a distorções se os dados forem incompletos, desequilibrados ou historicamente enviesados. Nestes casos, a IA pode tomar decisões injustas e favorecer certos grupos (Mehrabi et al., 2021).

Algumas técnicas de aprendizagem de máquinas produzem resultados eficazes, mas sem fornecer explicações claras sobre como chegaram a essas conclusões (Burrell, 2016). Este tipo de IA é referido como de *black box* (ou caixa-preta). Já a explicabilidade visa criar sistemas que possam justificar as decisões de maneira compreensível para os humanos (Doshi-Velez & Kim, 2017).

A IA atual funciona a partir de objetivos pré-definidos por humanos. Ou seja, recebe uma meta e utiliza métodos próprios para atingi-la. Apesar disso, alguns tipos de IA conseguem escolher caminhos diferentes para alcançar seu objetivo, aumentando a autonomia dentro dos limites estabelecidos na sua programação (Russell & Norvig, 2021).

Esta realidade coloca em evidência a importância de se garantir que os sistemas de IA operem dentro de limites éticos e legais previamente estabelecidos, reforçando a necessidade de um acompanhamento atento por parte de investigadores, reguladores e organizações (Floridi & Cowls, 2019).

2.2.4. Processamento de Linguagem natural (NLP) – O que é?

O Processamento de Linguagem Natural (NLP - *Natural Language Processing*) é uma forma de inteligência artificial que permite que os computadores compreendam, interpretem e processem a linguagem humana de uma forma automatizada. Combina técnicas de linguagem computacional

para analisar maiores volumes de textos e fala, possibilitando extrações de informações, tradução automática, reconhecimento de fala (Blohm et al., 2019).

É utilizado no setor segurador no âmbito do atendimento ao cliente, com o fim de automatizar atendimentos via *chatbots*, para analisar contratos, detetar fraudes e melhorar a experiência do cliente (pois permite uma maior rapidez na resposta). Apesar de todos os benefícios que o NLP pode trazer, há ainda que ter em conta os desafios que apresenta, quanto à privacidade dos dados de conformidade com o RGPD, de forma a garantir a aplicação segura deste tipo de tecnologia (Blohm et al., 2019).

Uma vez que o NLP é uma área de IA que possibilita a interação entre humanos e máquinas, esta combina técnicas de linguística computacional, e passa por várias etapas e componente fundamentais para que seja possível analisar textos e falas de forma eficiente. (Blohm et al., 2019).

O primeiro passo do NLP envolve a recolha de dados, por meio de documentos, emails, transcrições de chamadas, etc. No setor dos seguros, esta recolha pode envolver contratos de apólices, reclamações de sinistros e interações com clientes, pelos variados meios (Zarifis, Kawalek & Azadegan, 2021).

O segundo passo passa pelo pré processamento dos dados. Este deve estar na forma mais básica, ou seja, o texto passa por um processo de normalização e estruturação. O texto é dividido em palavras ou frases menores, a palavras em si são reduzidas à sua forma básica (Zarifis, Kawalek & Azadegan, 2021).

2.3. Implementação de IA na seguradora

A utilização de IA nos diversos setores de atividade tem vindo a aumentar significativamente nos últimos anos. As seguradoras não são exceção.

A forma como os utilizadores interagem com os assistentes de saúde, tem vindo a alterar-se (Zuo, 2025). Com a introdução de IA no serviço ao cliente, os clientes podem receber um apoio e informações em tempo real e de uma forma mais personalizada. Esta evolução permite uma continuidade na competitividade entre empresas dentro do setor. Permitiu a automação de processos que no passado eram manuais, a melhoria da experiência do cliente e a otimização da gestão de riscos (Koetter et al., 2019; Zuo, 2025).

No caso das seguradoras, estas obtêm uma redução nos custos operacionais, aumentam a eficiência na deteção de fraudes, tornam o atendimento ao cliente numa experiência mais personalizada e ágil, e melhor o processamento de sinistros e a análise de risco. Olhando de uma perspetiva mais conservadora e vendo além dos inúmeros benefícios, é importante ter em conta

os riscos associados, e o cumprimento de questões regulatórias e preocupações quanto à proteção de dados (Zuo, 2025).

Como já referido anteriormente, existem várias formas de tirar proveitos da IA na atividade seguradora, como por exemplo por meio de *Chatbots* e assistentes virtuais. Estes assistentes são regularmente utilizados no atendimento ao cliente. Utilizam o Processamento de Linguagem Natural (NLP), que permite entender e responder às questões dos clientes de uma forma rápida e ágil (Koetter et al., 2019).

2.3.1. Formas de implementação de IA nas seguradoras

Os *chatbots* são uma forma de IA já muito conhecida a ser implementada em empresas, neste caso no setor dos seguros. Pode ser aplicado para fornecer informações sobre apólices, pagamentos de prémios, registo de sinistros, alterações de dados, novas contratações. Os seus principais benefícios incluem a disponibilidade de 24h no atendimento e a rapidez no atendimento. No entanto, enfrenta também desafios no que toca a pedidos mais específicos dos clientes, e a necessidade de manter as bases de dados sempre atualizadas (Koetter et al., 2019).

Através da automação de processos (RPA – *Robotic Process Automation*), é uma forma de aplicação de IA fundamental para o setor de seguros. Permite a realização automática de tarefas repetitivas, com o objetivo de reduzir a intervenção humana e melhorar a eficiência operacional (Zuo, 2025).

Como exemplos de casos em que a automação pode ser implementada, destaca-se o processamento automático de sinistros, verificação de documentos enviados pelos clientes ou análise de contratos e apólices, para a identificação de possíveis erros (Zuo, 2025).

Desta forma, a automação de processos origina uma significativa redução de erros humanos e aumento da agilidade na tomada de decisões. Esta implementação carece de monitorização e ajustes constantes (Zuo, 2025).

A deteção de fraude é um dos principais desafios enfrentados pelas seguradoras, e com um sistema de IA que esteja equipado com modelos de *Machine learning*, ou seja, que se concentra no desenvolvimento de algoritmos que permitem aos sistemas computacionais aprenderem sem a necessidade de serem programados (Mehta & Devarakonda, 2018). Esta ferramenta analisa grandes volumes de informação e pode identificar padrões suspeitos e prevenir fraudes numa fase mais inicial, antes do processamento de pagamentos.

Esta tecnologia traz consigo benefícios como a redução de perdas financeiras que tenham indícios fraudulentos e a melhoria de e na eficiência da investigação de sinistros. A implementação desta tecnologia depende do fornecimento de grandes volumes de dados, para que possa treinar os

modelos de deteção e que torne possível minimizar falsos positivos, que podem afetar sinistros e clientes legítimos (Zuo, 2025).

Outro potencial uso de IA nas seguradoras é a análise de risco realizada por um sistema para esse fim. Através da análise a dados de cada cliente, como o historial médico podem ajudar a fornecer recomendações de um seguro personalizado e feito à medida do cliente. Isto garante que o cliente pague um seguro que satisfaça as suas necessidades especificas, de forma a garantir a sua satisfação e retenção (Zuo, 2025).

2.3.2. Tendências da IA no setor segurador

A literatura mais recente demonstrou que a utilização de IA no setor segurador se encontra numa fase de maior consolidação, pois deixou de se limitar a projetos experimentais e passou a integrar de uma forma mais transversal em áreas como a subscrição de seguros, o processamento de sinistros, a deteção de fraudes, o apoio ao cliente e a gestão de risco. Uma revisão sistemática a autores como Bhattacharya et al., (2025) permitiu concluir que a esta tecnologia passou a adquirir um papel estrutural nas seguradoras, sobretudo nos ramos automóvel, de saúde de habitação, devido à sua capacidade de aumentar a eficiência operacional, a melhoria da avaliação de risco e apoio à inovação em processos e produtos.

Outros debates demonstraram também, por outro lado, que o a atenção já não está apenas na automação tradicional, mas no potencial da IA generativa e IA *agentic*, ou seja, sistemas com uma maior capacidade de raciocínio, a produção de conteúdo, apoio à decisão e interação avançada com clientes e colaboradores. Segundo a McKinsey & Company (2025), estas tecnologias podem transformar a atividade seguradora como conhecemos atualmente. Ainda, o seu valor depende menos da simples adoção tecnológica e mais da capacidade das empresas para redefinir processos, integrar equipas e rever o modelo operacional como um todo.

Com a evolução tecnológica, é aumentada a necessidade de governação, supervisão e controlo. Foram identificados alguns desafios, como a qualidade de governação dos dados, a conformidade regulatória, as implicações éticas das decisões automatizadas e a necessidade de modelos explicáveis. Estes aspetos sugerem que o avanço da IA nas seguradoras não deve ser analisado apenas numa lógica de eficiência, mas também ser igualmente enquadrado por princípios de transparência, responsabilização e confiança institucional (Bhattacharya et al., 2025).

Ao nível regulatório europeu, esta preocupação é igualmente visível. Em 2025, a EIOPA publicou sobre a governação e gestão de risco na utilização de sistemas de IA em seguros, e esclareceu que as seguradoras devessem adotar uma abordagem baseada no risco e na proporcionalidade, dando uma especial atenção à governação dos dados, manutenção de registos, *fairness*, cibersegurança, explicabilidade e supervisão humana. Este mesmo rumo demonstra que a adoção da IA no setor

tende a apresentar uma evolução num quadro em que inovação e conformidade são tratadas como dimensões interdependentes e não como objetivos opostos (EIOPA, 2025).

Desta forma, a produção científica e institucional estudada sugeriu que a IA no setor segurador se encontra a evoluir de uma forma lógica de experimentação com o objetivo de uma integração estratégica. Esta evolução visa reforçar a ideia de que o sucesso da IA nas seguradoras dependerá não apenas da afinação dos algoritmos utilizados, mas também da capacidade organizacional que garanta uma governação robusta, um alinhamento regulatório responsável e a utilização responsável da tecnologia.

2.4. A relação entre a IA e as seguradoras: ética, operacional e segurança

Tem vindo a haver cada vez mais consenso em relação ao potencial da IA, que traz consigo o potencial de transformar a economia e a sociedade, por meio de permitir o "computador" realize inúmeras tarefas que inicialmente se acreditava que dependiam totalmente da mão e inteligência humana (Eling et al., 2021)

O aumento da popularidade da IA "resultam da combinação de dois desenvolvimentos que permitem a sua utilização produtiva" (Eling et al., 2021). Um deles é que a IA está cada vez mais maturada, graças ao desenvolvimento nos algoritmos de *Machine learning*,e em Deep Learning (Abrardi et al. 2019). O segundo é a informação disponível de grande volume de dados, também conhecido por *Big Data* que, "combinando com o rápido aumento da capacidade de computação dos sistemas modernos de tecnologias da informação, acelera o desenvolvimento e aumenta a precisão das aplicações de inteligência artificial" (Eling et al., 2021).

2.4.1. Questões Éticas na Implementação da IA em Seguros

Com o rápido desenvolvimento tecnológico no setor de saúde, muitos acreditam que a IA irá revolucionar este setor (Gerke, Minssen & Cohen, 2020). Com a sua rápida evolução vêm vários desafios e considerações a ter em conta para que a IA esteja alinhada em termos éticos e legais.

Como já referido anteriormente, *Machine learning* (*ML*) segundo Mehta & Devarakonda (2018) trata-se de "sistemas computacionais que aprendem a partir de dados sem serem explicitamente programados". É uma forma de estatística aplicada, que foi descrita pela primeira vez na década de 1950.

Os autores Mehta & Devarakonda (2018) dividem *ML* em dois termos diferentes: supervisionada e não supervisionada.

A primeira trata-se de algoritmos que são treinados com conjunto de dados já rotulados. Neste caso de *ML* supervisionada, a relação entre entrada e saída de dados já é conhecida, facilitando uma previsão dos algoritmos (Mehta & Devarakonda, 2018).

Já *ML* não supervisionada são algoritmos que encontram padrões e estruturas nos dados, mas sem rótulos pré-definidos (Mehta & Devarakonda, 2018).

Existe ainda a *Machine learning* tradicional e profunda. Mehta & Devarakonda (2018) definem *ML* tradicional como funcionalidades que são identificadas por humanos, e a "máquina" depende da extração manual de modelos estatísticos e algorítmicos matematicamente interpretáveis. *ML* profunda, também conhecida como *Deep ML* ou *deep learning*, necessita de uma grande quantidade de dados para extrair caraterísticas suas e realizar previsões. Para processar esta grande quantidade de dados, é necessário um processador com maior capacidade.

Pode existir uma discriminação algorítmica ao utilizar IA nas seguradoras. Caso os dados utilizados estejam enviesados, por meio de modelos de IA mal treinados, estes podem levar a previsto, baseando-se em padrões históricos de risco, mas sem considerar fatores individuais que poderiam minimizar a sua generalização (Zarifis et al., 2021).

Na perspetiva do consumidor, a perceção com que o cliente fica ao saber que a empresa utiliza, se se encontrar perante a ideia de que a IA é injusta ou que tende a discriminar certos grupos, pode originar a uma menor predisposição para utilizar planos que empreguem tais tecnologias. Neste sentido, poderá existir uma sensação de injustiça algorítmica (Zarifis et al., 2021).

A crescente incorporação de IA nas seguradoras também levanta preocupações éticas e jurídicas relevantes quanto à privacidade dos dados e ao seu uso. Quanto maior o volume de dados, maior será o risco associado ao seu tratamento (Gerke et al., 2020). Como exemplo deste risco, os autores referem o caso do Royal Free NHS Foundation Trust, em 2017, no qual dados de 1,6 milhão de pacientes foram partilhados com o *Google DeepMind*, uma empresa de IA focada no desenvolvimento de sistemas de *Machine learning*, que, por meio de recolha de dados, cria algoritmos. Esta partilha aconteceu sem um consentimento adequado, o que gerou críticas e sanções regulatórias no Reino Unido. O incidente ilustrou o risco que o entusiasmo com a inovação sem a legislação adequada pode marginalizar os direitos à privacidade (Gerke et al., 2020).

Os sistemas baseados em *Machine learning*, principalmente quando recorrem ao uso de "*black box*es", ou traduzindo, "caixa preta", podem ser de difícil compreensão. Logo, desafia os modelos tradicionais de consentimento.

O termo "*Black box*" é utilizado maioritariamente para descrever sistemas de IA em que os processos internos (desses sistemas) de tomada de decisão são de difícil interpretação. Bearman e Ajjawi (2023) referem que a IA deve ser compreendida, não apenas pela sua estrutura técnica,

mas também pela relação entre humanos e "computadores" em cada contexto específico de uso. Um sistema de IA atua como "*black box*" quando, no decorrer de uma interação contextualizada, um sistema fornece um julgamento sobre esse contexto, oferecendo um curso de ação ideal, mas em que não é explícita a origem deste julgamento. Uma vez que existe esta falta de rastreamento, os autores Bearman e Ajjawi (2023) propõem que, em vez de evitar este uso, que se deve aprender a atuar com competência em cenários de opacidade, incerteza e ambiguidade, que são caraterísticas comuns aquando da utilização de sistemas de IA. Assim, o que se pretende não é explicar a IA, mas desenvolver a capacidade crítica de trabalhar com sistemas cujos mecanismos internos não são plenamente compreensíveis, mas com impactos reais e tangíveis (Bearman & Ajjawi, 2023).

Neste sentido, o uso de dados pessoais sensíveis levanta questões sobre privacidade e consentimento. Regulamentações como LGPD e RGPD impõem limites sobre os quais os dados podem e devem ser recolhidos e utilizados, exigindo uma maior transparência por parte das seguradoras (Gerke et al., 2020).

A Regulamentação Geral de Proteção de Dados da União Europeia (RGPD) oferece um alcance mais abrangente. O artigo 1º (2) do RGPD indica que o regulamento tem como objetivo defender o direito à proteção de dados pessoais. Esta regulamentação inclui o direito de não se submeter a decisões automatizadas (ver Anexo 1), segundo o Regulamento (UE) 2016/679 (2016, Artigo 22.º, n.º 1):

> "Decisões individuais automatizadas, incluindo definição de perfis
>
> 1.O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar."

Entre outros, este inclui ainda o dever de fornecer informações sobre a lógica envolvida na tomada de decisão que sejam automatizadas, conforme os artigos 13º-15º, bem como obrigações especificas para o processamento de dados pessoais, de acordo com o artigo 9º (Gerke et al., 2020).

A utilização de IA numa organização, nomeadamente nas seguradoras, desafia os modelos tradicionais de consentimento informado, uma vez que os sistemas baseados em *machine learning*, em particular os *black box*es, pode ser de difícil compreensão, tanto para profissionais como para o próprio cliente. Estes aspetos podem colocar em questão até que ponto é necessário explicar aos clientes como a IA funciona, e mesmo se estes podem recusar o seu uso (Gerke et al., 2020).

Neste sentido, a transparência e explicabilidade das empresas com os seus clientes é cada vez mais um ponto a ter em consideração.

A transparência refere-se à capacidade de tornar claro ao consumidor qual o papel que a IA desempenha em processos decisivos, como por exemplo a precificação ou a aceitação para determinados planos de saúde (Zarifis et al., 2020). Os autores Zarifis, Kawalek e Azadegan (2020) referem que realizaram testes que mostraram que o facto de as empresas tornarem explícita a presença de IA no processo de compra, influenciou negativamente a confiança no consumidor. Este fenómeno pode estar ligado à perceção de que a IA é menos previsível, menos controlável e menos "humana", fatores estes que afetam a relação de confiança.

A transparência, embora essencial do ponto de vista ético e regulamentar, pode paralelamente gerar resistência se não for acompanhada por estratégias que promovam compreensão e segurança (Zarifis et al., 2020).

2.4.2. Impactos Operacionais da IA no Setor de Seguros

A adoção de IA em seguradoras tem permitido um impulso em termos financeiros, permitindo a redução de custos operacionais e o aumento da eficiência na análise de riscos e fraudes. No entanto, estes avanços apresentam também desafios económicos e financeiros (Eling et al., 2021).

A automatização de tarefas e processos que no passado seriam realizados manualmente, como por exemplo o processamento de sinistros, atendimento ao cliente e ainda análise de documentos permitiram uma redução de custos administrativos, redução de pessoal não especializado (Aslam et al., 2022). O aumento da eficiência, da qualidade e da precisão permitem às empresas uma maior janela para aumentar rendimentos (Eling et al., 2021).

Além da modernização dos processos internos, a IA permitiu transformar profundamente os modelos de precificação de produtos, e abriu portas para o estabelecimento de modelos de negócio inovadores (Eling et al., 2021).

Tradicionalmente, a precificação de seguros era baseada em avaliações estáticas de riscos, elaboradas no momento da assinatura contrato. Contudo, o uso de IA combinado com tecnologias *Big Data* e dispositivos de Internet das Coisas (Iot) possibilitou a implementação de precificação dinâmica. Eling, Nuessle e Staubli (2021) afirmam que os algoritmos de *machine learning* conseguem processar grandes volumes de dados em tempos real permitindo uma análise contínua do comportamento dos clientes e a atualização frequente de prémios, de acordo com o risco calculado.

A Iot pode ser definida como um "conjunto de dispositivos inteligentes que interagem de forma colaborativa para cumprir um objetivo comum" (Sicari et al. 2015).

Outro modelo de precificação de produtos passa pela criação de seguros baseados em comportamento, em que a seguradora acompanha em tempo real variáveis comportamentais do cliente. Este modelo acompanha hábitos, padrões de atividade física ou estilos de vida, adaptando dessa forma o contrato de seguro ao cliente em particular, de forma personalizada (Eling et al., 2021).

Desta forma, a IA permite a precificação personalizada com base em dados de comportamento, métricas e estilos de vida dos segurados. No entanto, esta modernização pode resultar em seguros mais acessíveis e adaptados às necessidades de clientes com menor risco, excluindo consumidores de alto risco do mercado, criando desafios regulatórios e éticos (Eling et al., 2021).

A implementação de IA nas seguradoras pode facilitar a deteção de fraudes, no então, em caso de pouco controlo nos processos já automatizados, pode causar o inverso, resultando uma maior vulnerabilidade e exposição a fraudes (Eling et al., 2021). Falhas tecnológicas ou ataques cibernéticos são outros riscos de baixa frequência, mas de alta gravidade que as seguradoras podem enfrentar. Eventos deste tipo podem gerar grandes perdas financeiras num curto espaço de tempo (Eling et al., 2021). Asslam et al. (2022) referem que as perdas financeiras associadas a fraudes são geralmente associadas a grandes quantias, prejudicando a lucratividade das seguradoras e levando por sua vez ao aumento dos prémios a clientes que não cometam fraudes.

Este impacto destabiliza a estrutura de preços e prejudica a confiança dos clientes e prejudica a confiança dos consumidores, neste caso no sistema dos seguros. Assim, a deteção precoce de fraudes, proporcionada pela IA, pode não só reduzir perdas financeiras de maior valor, mas também contribui para manter prémios mais acessíveis em preservar a sustentabilidade do setor (Asslam et al., 2022).

A dependência crescente de tecnologias complexas é um aspeto relevante a ter em conta. As seguradoras ficam mais expostas a riscos operacionais, como falhas de sistema, bugs nos algoritmos ou problemas de interoperabilidade entre sistemas. Para combater esta dependência é imperativo desenvolver estratégias robustas de resiliência cibernética e continuidade de negócios, bem como a constante atualização e monitorização das soluções tecnológicas adotadas (Eling et al., 2021).

2.4.3. Segurança da IA no Setor de Seguros

A segurança é um fator crítico na implementação de IA nas seguradoras, e a proteção contra fraudes, ataques cibernéticos e fiabilidade dos algoritmos.

A proteção de dados sensíveis é uma prioridade no setor dos seguros, dada a natureza confidencial das informações de clientes. O uso de IA e de sistemas *blockchain*, quando bem implementados, pode fortalecer significativamente a segurança dessas informações. Conforme indica o autor

Zamharir (2025), a segurança pode ser vista como a garantia de que os dados pessoais dos clientes estão protegidos contra fraudes e violações. Esta é uma definição essencial para garantir a confiança do cliente.

A integração de b*lockchain* nestes processos proporciona uma camada adicional de segurança, garantindo a estabilidade dos dados e a transparência das transações, o que ajuda a mitigar riscos de acessos não autorizados e de manipulação de dados. Crosby et al. (2016) defendem que a natureza descentralizada do *blockchain* oferece uma proteção robusta contra falhas e ataques cibernéticos. Esta é, portanto, uma aplicação essencial no setor dos seguros, em que a privacidade e a integridade dos dados são fundamentais.

É, no entanto, importante ter em conta que a implementação deste tipo de tecnologias não é imune de desafios. A conformidade com regulamentações de privacidade de dados, como o RGPD, e as questões relacionadas à escalabilidade dos sistemas de *blockchain* são obstáculos significativos (Zamharir, 2025). Estas questões relevantes exigem que as seguradoras desenvolvam soluções para equilibrar a proteção de dados com a necessidade de processar grandes volumes de informações de forma eficiente.

Os ataques cibernéticos e a manipulação de algoritmos são ameaças que afetam diretamente a integridade dos sistemas de IA bem como a segurança dos dados no setor de seguros. Estes tipos de ataques podem ocorrer de várias formas, incluindo a manipulação de dados de entrada para gerar resultados enviesados ou enganosos em modelos preditivos. A manipulação de algoritmos pode ser realizada por hackers para alterar as decisões de crédito, classificação de risco ou outras avaliações automatizadas (Papernot et al., 2016).

O uso do *blockchain* pode mitigar esses riscos, uma vez que garante a transparência nas transações dos registos. Este aspeto é particularmente importante no contexto dos seguros, pois a manipulação de dados pode resultar em fraudes significativas. O autor Zamharir (2025) menciona que o *blockchain* é eficaz para prevenir ataques cibernéticos devido à infraestrutura descentralizada que o carateriza, e que torna mais difícil aos hackers a alteração de dados sem a sua deteção.

Os modelos de IA necessitam de ser constantemente auditados e ajustados para evitar enviesamentos e garantir que continuem eficazes nas análises de riscos. Em caso de falhas nestes modelos podem comprometer a precificação de seguros e gerar perdas financeiras significativas (Eling et al, 2021).

Papernot et al. (2016) argumentam que a segurança de modelos de *Machine learning* deve incluir não apenas a proteção contra manipulação de dados, mas também a verificação e validação contínua dos modelos para garantir que eles funcionem corretamente em diferentes cenários e não sejam suscetíveis a fraudes.

Desse modo, conclui-se que a segurança da aplicação da IA no setor dos seguros envolve vários aspetos, passando pela proteção de dados sensíveis e pela segurança dos modelos preditivos. A integração de tecnologias como o *blockchain* oferece soluções promissoras, devido ao reforço de segurança das informações fornecidas pelos clientes. No entanto, enfrenta ainda vários desafios quanto à conformidade com regulamentações de privacidade e à resistência a ataques cibernéticos e manipulação de algoritmos (Zamharir, 2025). Já a segurança nos modelos preditivos necessita de ser aprimorada para garantir que decisões automatizadas não sejam manipuladas (Papernot et al, 2016).

2.4.4. Enquadramento Regulatório da Inteligência Artificial na União Europeia- AI Act

A evolução da adoção dos sistemas de IA nos diversos setores económicos, em particular no setor segurador, levou a União Europeia a criar a necessidade de desenvolver um enquadramento regulatório específico, tendo como objetivo garantir que estes tipos de tecnologias sejam utilizados de forma segura, ética e conforme os direitos fundamentais. Neste contexto, destacou-se a *Artificial Intelligence Act (AI Act)*, que foi proposto pelo Parlamento Europeu, e que integra a primeira tentativa de regulamentação abrangente da IA a nível global (European Parliament & Council, 2024).

O *AI Act* trata-se de uma abordagem que está centrada no risco, e que classifica os sistemas de IA em diferentes categorias, com base no seu impacto potencial sobre os indivíduos e a sociedade. Desta forma, são definidos quatro níveis principais: (i) risco inaceitável; (ii) risco elevado; (iii) risco limitado; (iv) risco mínimo. Os sistemas categorizados como risco inaceitável são proibidos, devido à probabilidade alta de colocarem em causa direitos fundamentais. Já os sistemas de alto risco, nos quais são incluídas as aplicações utilizadas em áreas como seguros, saúde ou recrutamento, estão sujeitos a requisitos rigorosos de conformidade (European Parliament & Council, 2024).

Nos sistemas de alto risco, o regulamento impõe certas obrigações específicas, como por exemplo no que diz respeito à qualidade de governação dos dados, à transparência dos algoritmos, à supervisão humana e à robustez técnica dos sistemas. Estas exigência têm como objetivo garantir que as decisões automatizadas são fiáveis, explicáveis e não discriminatórias (Floridi & Cowls, 2019).

No caso dos sistemas de risco limitado, estes estão sujeitos principalmente a obrigações de transparência, logo os utilizadores deverão ser informados de que estão a interagir com este tipo de tecnologia. É o caso dos *chatbots* ou de conteúdos gerados automaticamente. Já os sistemas de

risco mínimo, não estão sujeitos a requisitos específicos, por estes apresentarem um impacto reduzido, incluindo aplicações como spam e videojogos (European Parliament & Council, 2024).

O *AI Act* articula-se com o RGPD, reforçando os direitos já estabelecidos, como é o caso dos indivíduos não serem sujeitos a decisões exclusivamente automatizadas cum um impacto significativo nas suas vidas (European Parliament & Council, 2024). Esta ligação reforça a importância de garantir a proteção dos dados pessoas num contexto em que os sistemas de IA dependem fortemente do processamento de grandes volumes de informação.

No setor segurador, a adoção deste enquadramento regulatório assume uma especial relevância, sendo que muitas das soluções baseadas em IA, como é o caso da análise de risco, a deteção de fraude ou a precificação de apólices, podem ser consideradas como sistemas de alto risco. As seguradoras serão assim obrigadas a adotar práticas robustas de governação, que asseguram não apenas a eficiência dos sistemas, mas também a conformidade legal e ética (Eling et al., 2021).

Neste sentido, conclui-se que a *AI Act* representa um marco importante na regulação da IA, com vista em promover uma abordagem equilibrada entre inovação tecnológica e proteção dos direitos fundamentais, sendo particularmente relevante em setor altamente regulados, como é o caso dos seguros.

2.5. Objetivos de investigação

O presente estudo tem como objetivo compreender os impactos da implementação IA no contexto organizacional de uma seguradora que opera em Portugal, dando especial atenção aos desafios éticos, operacionais, e de segurança. Tendo em consideração a diversidade funcional das áreas envolvidas para o estudo- Risco, *Compliance* e *Contact Center*- definiu-se um conjunto de objetivos de investigação, com o intuito de orientar o percurso metodológico e a análise dos dados.

O primeiro objetivo visa compreender como a IA tem sido implementada na seguradora no geral, procurando identificar os processos em que esta tecnologia foi implementada e de que forma influência as tarefas do dia a dia dos colaboradores. O segundo objetivo passa por explorar os benefícios percebidos pelos profissionais no uso da IA, tanto na vertente de eficiência operacional, como no apoio à decisão, na melhoria do atendimento ao cliente e qualidade dos serviços prestados.

Já o terceiro objetivo está direcionado para os desafios associados à utilização da IA, dando uma particular ênfase às preocupações éticas, tais como a transparência, o enviesamento dos dados ou a substituição das funções humanas, às preocupações financeiras, quanto ao investimento, retorno e sustentabilidade, e por fim às questões de segurança, incluindo a proteção de dados e riscos cibernéticos.

Por último, o quarto objetivo pretende analisar a forma como a perceção dos colaboradores envolvidos no estudo é influenciada pela área funcional a que pertencem. Por outras palavras, avalia se a visão sobre os benefícios e riscos da IA varia consoante o papel desempenhado na organização.

Estas questões não só enquadram a recolha e a análise de dados, mas também refletem a natureza exploratória do estudo, possibilitando uma leitura aprofundada e contextualizada das experiências individuais dos participantes face à transformação digital que a IA representa no setor segurador.

2.6. Súmula da Revisão de Literatura e análise SWOT

2.6.1. Súmula da Revisão de Literatura

A crescente integração da IA nas diversas áreas de negócio tem vindo a transformar o setor segurador. Nesta área, a IA é uma ferramenta estratégica que permite às seguradoras automatizar processos, personalizar serviços otimizar a análise de risco de apólices e prevenir fraudes. Esta aplicação levanta questões éticas, jurídicas e de segurança que devem ser cuidadosamente analisadas (Eling et al., 2021; Gerke, Minssen & Cohen, 2020).

O conceito de seguro nasceu pela necessidade humana de mitigar os efeitos dos riscos, que por sua vez são inevitáveis. O primeiro registo de algo semelhante a seguros surgiu nas civilizações antigas, como os acordos de assistência mútua, em 4700 a.C, até à idade média com os contratos marítimos. Nestas épocas, o "seguro" evoluiu como um mecanismo de compensação e segurança por perdas de mercadoria (Guedes-Vieira, 2012). O seguro de vida surge no final do século XVII, e é desenvolvido com base em avanços na estatística e na demografia (Graunt, 1975; Halley, 1693; Stigler, 1986).

A IA, definida como a capacidade de sistemas computacionais realizarem tarefas tradicionalmente humanas, foi desenvolvida pelos trabalhos realizados por Alan Turing (1950), e foi mais tarde consolidada como uma disciplina científica na conferência de Dartmouth (McCarthy et al., 1956). Russell e Norving (2009; 2021) classificam as abordagens de Turing em quatro vertentes: agir como humano, pensar como humano, pensar racionalmente e agir racionalmente. Atualmente, estes termos evoluíram para IA restrita (ou fraca) e IA geral (ou forte), que são aplicadas a tarefas mais especificas e a tarefas que ainda estão em desenvolvimento e visam replicar a cognição humana, nomeadamente pela capacidade de elaborar um raciocínio, planeamento, resolução de problemas, compreensão da linguagem natural e ainda a adaptação a contextos complexos sem intervenção humana (High-Level Expert Group on AI, 2018; Walch, 2019).

A aplicação de IA no setor segurador tem-se verificado um promotor em diversas áreas. Exemplos dessas aplicações são os *Chatbots* e os assistentes virtuais. Estes são baseados em processamento

de Linguagem Natural (NLP), que melhoram o atendimento ao cliente (Blohm et al., 2019). Outra aplicação desta tecnologia trata-se de *Robotic Process Automation* (RPA), que aumenta a eficiência de processos e reduz erros humanos (Zuo, 2025). A deteção de fraudes e a análise preditiva de riscos são áreas fortemente beneficiadas por algoritmos de *Machine learning* (Mehta & Devarakonda, 2018; Koetter et al., 2019). A IA permite também oferecer uma melhor personalização de apólices, contratadas à medida de cada necessidade específica de cada cliente (Zuo, 2025).

Os desafios éticos da IA em seguros estão relacionados com o enviesamento algorítmico, a opacidade dos sistemas de *black box* e a proteção dos dados pessoais (Bearman & Ajjawi, 2023). Algoritmos erradamente treinados com dados enviesados podem perpetuar discriminações e afetar negativamente grupos vulneráveis. (Zarifis et al., 2021). Já o Regulamento Geral sobre a Proteção de Dados (RGPD) impõe regras claras quanto ao tratamento automatizado de dados e garante aos cidadãos o direito a não serem submetidos a decisões exclusivamente automatizadas (Regulamento (UE) 2016/679).

Numa perspetiva económico financeira, a IA pode proporcionar ganhos financeiros através da redução dos custos operacionais e do aumento da eficiência na análise de sinistro e de riscos (Eling et al., 2021; Aslam et al., 2022). A precificação dinâmica de apólices, suportada por *Big Data* e dispositivos IoT também permitem ajustar os prémios em tempo real de acordo com o comportamento e necessidades dos segurados (Sicari et al., 2015; Eling, Nuessle & Staubli, 2021). É importante ter conta os riscos associados, como as falhas tecnológicas, ciberataques ou manipulação de algoritmos, que poderão influenciar comprometer a sustentabilidade do setor (Papernot et al., 2016).

A segurança da implementação da IA é imprescindível. A proteção dos dados pessoais, o combate a ciberataques e a fiabilidade dos algoritmos preditivos são aspetos fundamentais a ter em conta. Relativamente ao uso de *blockchain*, este pode reforçar a segurança e a integridade dos dados, oferecendo uma maior transparência e resistência a manipulações (Crosby et al., 2016; Zamharir, 2025). Em simultâneo, é necessário garantir a conformidade com a legislação em vigor e implementar auditorias regulares aos sistemas de IA para garantir a sua fiabilidade e equidade (Papernot et al., 2016; Eling et al., 2021).

2.6.2. Análise SWOT- síntese de benefícios e desafios à implementação de IA nas seguradoras

Por forma a melhor analisar os benefícios e desafios relacionados com a implementação da IA no setor, realizar uma análise SWOT (*Strengths, Weaknesses, Opportunities, Threats*) pode facilitar esta visão.

Este tipo de análise permite visualizar de uma forma estruturada, clara e estratégica os fatores internos e externos ao setor que influenciam a implementação de IA. Visa facilitar a compreensão crítica quanto aos pontos fortes e fracos da IA enquanto tecnologia tanto aplicada como avaliada pelas áreas de gestão de risco, de *Compliance* e de atendimento ao cliente, e olhando também para quais as suas oportunidades e ameaças relativas à sua implementação.

De uma forma esquematizada e como resumo do indicado acima foi desenvolvida a seguinte tabela, construída com base em evidências científicas e contributos apresentados pelos autores estudas ao longo da revisão da literatura, aos níveis operacionais e de segurança, éticos e tecnológicos da IA no contexto segurador.

TABELA 1 ANÁLISE SWOT

Categoria	Elementos	Fontes
Forças (*Strengths*)	- Automatização de tarefas repetitivas e de baixo valor - Melhoria no atendimento ao cliente por meio de *chatbots* - Deteção de fraudes com algoritmos de *machine learning* - Eficiência na análise de risco e sinistros - Personalização de apólices (*Taylor made*)	Eling et al. (2021); Zuo (2025); Koetter et al. (2019); Mehta & Devarakonda (2018)
Fraquezas (*Weaknesses*)	- Falta de transparência nos algoritmos (caixa-preta) - Potencial enviesamento nos dados e risco de discriminação - Falta de confiança e resistência à mudança por parte de colaboradores e clientes - Dependência tecnológica de fornecedores externos - Implementação ainda limitada em algumas áreas	Bearman & Ajjawi (2023); Zarifis et al. (2021); Papernot et al. (2016)
Oportunidades (*Opportunities*)	- Precificação dinâmica com base em dispositivos IoT - Redução de custos operacionais e aumento da escalabilidade - Reforço da segurança e transparência com *blockchain* - Melhoria da experiência do cliente e competitividade no setor - Integração com outras tecnologias emergentes (RPA, NLP)	Sicari et al. (2015); Crosby et al. (2016); Zamharir (2025); Eling, Nuessle e Staubli (2021)
Ameaças (*Threats*)	- Ciberataques e vulnerabilidades tecnológicas - Manipulação ou falhas nos algoritmos preditivos - Reação negativa de clientes a decisões automatizadas - Incertezas regulatórias e necessidade de conformidade com RGPD - Dificuldade em manter auditoria e explicabilidade da IA	Papernot et al. (2016); Regulamento (UE) 2016/679; Floridi & Cowls (2019)

Fonte: Elaboração própria

Esta análise revela a potencialidade da IA no setor segurador, em particular quando se menciona a personalização dos produtos disponíveis e à melhoria da eficiência operacional, traduzindo-se numa vantagem competitiva significativa (Eling et al., 2021; Zuo, 2025). Quanto às fragilidades existentes, estas merecem especial atenção. É necessário ter em conta a transparências dos algoritmos, o enviesamento dos dados e a resistência dos colaboradores relativamente à mudança tecnológica (Bearman & Ajjawi, 2023).

Eling, Nuessle e Staubli (2021) revelam que algumas das oportunidades passam pela integração de IoT, Zamharir (2025) refere que o uso de *blockchain* pode ter a finalidade de reforço da segurança, e é ainda referida a possibilidade de cumprir com as exigências dos consumidores mais digitais.

Já as ameaças incluem os riscos de cibersegurança, a avaliação regulamentar constante, por ser incerta, e a necessidade de agir em conformidade com o RGPD (Papernot et al., 2016; Regulamento UE 2016/679).

A análise realizada demonstrou que, através de uma implementação gradual, com princípios éticos e uma regulamentação bem estruturada relativamente à inteligência artificial, é possível existir uma inovação tecnológica equilibrada, protegendo o consumidor e mantendo uma sustentabilidade organizacional.

3. Metodologia

3.1. Introdução à Metodologia

Os objetivos da presente investigação passam por compreender os desafios éticos, operaconais e de segurança associados à implementação de IA no setor segurador. De forma a alcançar este propósito, optou-se por escolher uma abordagem qualitativa de natureza exploratória, pois esta é considerada a mais adequada para aceder às perceções, experiência e interpretações dos profissionais que lidam com esta tecnologia em contexto organizacional.

Dada a natureza emergente do fenómeno em estudo sendo ele o impacto da IA nos processos internos de uma seguradora, exigem uma metodologia que permita captar os significados atribuídos pelos colaboradores à transformação tecnológica em curso. A abordagem qualitativa permite, desta forma, obter uma compreensão profunda e contextualizada, indo além da quantificação dos fenómenos, e valorizando a dimensão subjetiva e interpretativa (Creswell, 2014; Denzin & Lincoln, 2018).

Neste seguimento, a estratégia escolhida para este estudo baseia-se na realização de entrevistas a colaboradores de uma seguradora, de diferentes áreas, mas complementares escolhidas para este estudo, as áreas de Risco, *Compliance* e *Contact Center*. Estas áreas, apesar de distintas, foram escolhidas pela sua envolvência em projetos relacionados com inovações tecnológicas, com a IA a desempenhar um papel crescente na análise preditiva de risco, na monitorização da qualidade dos serviços e na automatização do atendimento ao cliente.

As entrevistas realizadas têm como objetivo recolher dados e informações que permitam explorar (i) o nível de implementação da IA na organização, (ii) os benefícios percebidos e as limitações sentidas e (iii) os principais desafios enfrentados nos domínios ético, financeiro e da segurança dos dados.

Estes principais objetivos foram atingidos por meio da resposta às seguintes questões: (i) Como a IA está a ser implementada na seguradora e de que forma esta influencia o trabalho diário dos colaboradores?; (ii) Quais os benefícios percebidos pelos profissionais no uso da IA, a nível operacional e estratégico?; (iii) Quais os principais desafios e preocupações éticas, financeiras e de segurança associados à utilização da IA?; (iv) De que forma a perceção dos colaboradores sobre a IA varia consoante a sua área funcional?

A escolha da realização de entrevistas como forma de recolha de dados justifica-se pela flexibilidade que oferece ao investigador, pois permite manter uma linha orientadora a todos os entrevistados, e por outro lado oferece ao participante a oportunidade de explorar temas emergentes durante a conversa.

A metodologia desta investigação será aprofundada nos pontos seguintes, detalhando os procedimentos de amostragem, recolha e análise de dados e considerações éticas.

A produção de conhecimento científico exige rigor, sistematização e clareza, de forma a facilitar qual o caminho a seguir e quais os objetivos que se querem alcançar. Deste modo, a metodologia assume um papel importante, uma vez que serve como reflexão crítica sobre os métodos utilizados na presente investigação.

A palavra método surge da palavra grega "méthodos", e é formada por duas palavras: "metá", que significa "no meio de", e "odós", que significa "caminho". Unindo estas duas palavras, Método significa "ao longo do caminho", por outras palavras, é uma "forma de proceder ao longo de um caminho" (FERRARI, 1982)

O termo metodologia, dividido em método (já definido acima) e "logia", "logos" no latim, que significa discurso ou estudo, ou seja, um estudo de métodos.

De forma a complementar esta definição, Gil (2008) descreve a metodologia como um ramo do conhecimento que se ocupa da análise crítica e sistemática dos processos utilizados na construção do conhecimento científico. Já Charmaz (2014) considera que a metodologia envolve tanto a lógica de investigação como pressupostos ontológicos e epistemológicos à escolha de métodos e técnicas.

3.2. Análise do Setor Segurador

O setor segurador em Portugal tem revelado uma evolução marcada pela recuperação pós pandémica, mas, além disso, os últimos anos foram marcado pela modernização tecnológica e pela resiliência operacional. O relatório anual Associação Portuguesa de Seguradores (APS, 2025) e o relatório da Associação de Supervisão de Seguros e Fundos de Pensões (ASF, 2025) identificam as variações relevantes quanto aos prémios emitidos, na distribuição entre os ramos de Vida e Não Vida e também nos Resultados Líquidos obtidos pelas seguradoras.

Como forma de análise sucinta, a tabela abaixo agrupa os principais indicadores:

TABELA 2 PRINCIPAIS INDICADORES DO SETOR SEGURADOR

Ano	Prémios Totais (M€)	Vida (M€)	Não Vida (M€)	Resultado Líquido (M€)
2020	10 090	—	—	450
2021	13 509	—	—	646
2022	12 301	6 021	6 035	903
2023	12 178	5 159	6 665	692
2024	14 318	6 960	7 358	519

Fonte: adaptado de APS(2025) e ASF (2025)

No início do período em análise, em 2020, os prémios totais emitidos fora de 10 090 milhões de euros, e o Resultado líquido foi de 450 milhões de euros. Em contraste, em 2021 e nos seguintes anos verificou-se uma recuperação gradual nos prémios. Em 2021 subiu para os 13 509 milhões de euro representando um acréscimo de 33, 9%, e um Resultado Líquido de 646 milhões (ASF, 2025).

Entre 2021 e 2023 houve uma estabilização nos valores, apenas verificando um ligeiro decréscimo entre 2021 e 2022. Após este período, em 2024 verificou-se um aumento acentuado para 14 318 milhões de euros. Este crescimento aconteceu pelo reforço do ramo Vida, que aumentou 1 800 milhões euros relativamente ao ano anterior.

O ramo Não Vida apresentou um crescimento constante desde 2020, refletido pelo crescimento da procura por seguros de saúde e automóvel (APS, 2025). Em 2024 verificou-se o valor em prémios pagos mais alto, atingindo os 7 358 milhões de euros.

Quanto aos Resultados Líquidos, o valor mais alto registado aconteceu em 2022, com 903 milhões de euros. Após este ano, em 2023 e 2024 os valores desceram, atingido os 519 milhões de euros. Esta diminuição atribuiu-se ao aumento dos custos com sinistros, à instabilidade dos mercados e novos investimentos em transformação digital (APS, 2025).

Com os dados apresentados, conclui-se que que setor demonstrou uma capacidade de adaptação num contexto inconstante, em que é reforçado o papel estratégico da inovação, da eficiência operacional e da gestão de risco, sendo estes os pilares da sustentabilidade futura do setor.

3.3. Tipo de estudo e abordagem metodológica

Para a realização desta dissertação, o modelo escolhido foi o estudo qualitativo. Neste contexto, a metodologia ganha especial relevância para o tema escolhido, uma vez que se trata de um campo em que a flexibilidade, a profundidade e a compreensão subjetiva são privilegiadas. O autor Patton (2015) defende que a metodologia qualitativa visa interpretar os significados atribuídos pelos indivíduos às suas experiências, sendo particularmente adequada para estudos de comportamento organizacional. Neste caso particular a técnica utilizada será a realização de entrevistas.

Assim, a escolha metodológica está profundamente relacionada com a natureza do problema de pesquisa, que neste caso será o nível ético na implementação de IA nas seguradoras. Kvale e Brinkmann (2009) evidenciam que, em estudos qualitativos, a coerência entre os objetivos da investigação, o enquadramento teórico e os métodos utilizados são essenciais para garantir a validade e a credibilidade dos resultados.

Este trabalho seguiu uma abordagem qualitativa, tendo por base uma perspetiva exploratória e interpretativa, que visou compreender em profundidade as perceções e experiências dos colaboradores relativamente à utilização da Inteligência Artificial na atividade seguradora nesta empresa em específico, bem como entender quais as perspetivas a nível ético, financeiro e de segurança.

A escolha da abordagem qualitativa justificou-se pelo interesse em aceder às perceções subjetivas e experiências dos participantes em ambiente laboral, o que não seria possível através de métodos quantitativos padronizados (Patton, 2015; Kvale & Brinkmann, 2009).

Para estas entrevistas, optou-se por seguir um modelo semiestruturado, pois o objetivo é permitir uma maior flexibilidade na recolha de dados, não deixando de seguir uma estrutura orientadora, mas aberta à exploração temas relevantes emergentes durante a conversa (Seidman, 2006).

Para a realização das entrevistas, foram escolhidas as áreas de Risco, *Compliance* e de *Contact Center*. Esta seleção é intencional pois é baseada na experiência e na envolvência destes indivíduos em sistemas de IA, pelo seu envolvimento nos projetos da empresa. Esta escolha teve o objetivo de garantir que os entrevistados pudessem contribuir de uma forma útil com o seu conhecimento relevante e contextualizado sobre os temas em análise.

A realização entrevista procurou captar a diversidade de experiências e perceções sobre a adoção de Inteligência Artificial, consoante as diferentes áreas de atuação de cada entrevistado. Dessa forma, foi possível ter uma visão transversal da organização. Os nomes dos participantes nas entrevistas foram mantidos em anónimo, e os dados foram codificados para garantir a confidencialidade.

3.4. Técnica de recolha de dados

As entrevistam realizadas respeitaram os princípios éticos da investigação científica, e asseguraram o anonimato, a voluntariedade e consentimento dos participantes. Anteriormente à realização das entrevistas, foi lido a cada entrevistado um termo de consentimento, com descrição do tema em estudo e os direitos dos participantes. De salientar que os resultados obtidos nas entrevistas são exclusivamente para uso académico, e tratados com confidencialidade.

As entrevistas foram realizadas em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD), no que diz respeito à recolha tratamento e conservação dos dados pessoais sensíveis.

Uma vez que se pretendia a possibilidade de explorar, de forma aprofundada e flexível, as perceções, experiências e opiniões dos participantes relativamente à utilização da IA no seu contexto de trabalho, a técnica escolhida para a recolha de dados foi a entrevista semiestruturada. Esta técnica foi aplicada em colaboradores de diferentes áreas da seguradora, sendo estas Risco, *Compliance* e *Contact Center*.

As características que definem as entrevistas semiestruturadas passam pela sua estrutura baseada em temas e questões de resposta aberta, que permitem ao entrevistado um espaço para desenvolver livremente as suas respostas e introduzam novos tópicos que sejam considerados relevantes para o tema em questão. Esta abordagem é particularmente útil quando se pretende compreender fenómenos complexos, como o impacto da IA em práticas organizacionais, que podem variar significativamente entre departamentos e indivíduos.

Como instrumento de recolha de dados, o guião da entrevista foi previamente elaborado, desenvolvido a partir dos objetivos do estudo e com questões sobre o nível de implementação da IA, quais os benefícios e limitações percebidas que resultaram dessa aplicação, os desafios éticos e preocupações com a segurança e privacidade do uso de dados, e quais os impactos operacionais e expectativas futuras. Esta recolha permitiu ser possível o máximo de informações relevantes para o estudo.

As entrevistas foram realizadas individualmente, tiveram uma duração 20 a 30 minutos, e foram conduzidas por videoconferência. Estas entrevistas foram gravadas mediante consentimento

informado prévio, para posterior transcrição e análise. A gravação teve como objetivo manter a fiabilidade e integridade dos dados recolhidos, tornando possível uma análise mais rigorosa e detalhada.

Além da recolha de dados relevantes em termos descritivos, a técnica escolhida para este estudo permitiu captar nuances e outras dimensões que seriam difíceis de captar por meio de questionários ou outros métodos mais estruturados. Logo, esta flexibilidade é essencial para a natureza exploratória da investigação realizada, pois permitiu aos participantes uma contribuição com reflexões espontâneas, exemplos concretos e experiências pessoais relacionadas com a sua realidade profissional.

3.5. Análise dos dados

Após detalhar a técnica de recolha de dados, quanto à análise de dados, as entrevistas foram gravadas e transcritas de forma integral, e analisadas com base na análise temática sugerida por Braun e Clarke (2006), que se trata de um método que consiste em identificar padrões recorrentes nas respostas dos entrevistados, permitindo construir uma narrativa interpretativa coerente com os objetivos da investigação. Foi realizada uma familiarização dos dados, ou seja, leitura das transcrições, um agrupamento de respostas por temas, uma revisão dos temas, pela verificação da coerência e consistência temática, definição e nomeação dos temas, e por fim uma redação do relatório analítico. As questões encontram-se divididas por temas, o que facilitou a sua análise.

Uma vez que o objetivo é respeitar a natureza exploratória do estudo, após a transcrição integral das entrevistas, foi feita uma leitura detalhada das respostas dadas, com o intuito de captar o conteúdo das falas, quais a preocupações, e os significados atribuídos à presença de IA nos processos organizacionais.

Após a leitura das entrevistas, a abordagem para a sua análise foi descritiva e interpretativa, e orientada pela comparação das perceções e experiências individuais dos entrevistados, e tendo em conta o contexto específico de cada área funcional. O objetivo de entrevistar diferentes áreas não é apenas identificar elementos comuns nas suas respostas, mas é também compreender como a função desempenhada influencia a visão de cada colaborador relativamente aos impactos da IA na organização.

Para a interpretação dos dados recolhidos seguiu-se uma lógica de contraste entre os entrevistados, tendo em consideração a particularidade de cada área de atuação.

Relativamente à área de risco, esperou-se explorar a forma com a IA influencia a tomada de decisão analítica, a responsabilidade analítica e a avaliação preditiva sobre os resultados. A área de *Compliance* focou-se na perceção do controlo e supervisão de processos e regulamentação

trazida pela IA. Ao entrevistar a área do *Contact Center*, o objetivo centrou-se em compreender os resultados da IA na interação direta com o cliente, na mudança no tipo de resposta ao cliente, que seria automatizado, e potencialidade na substituição de tarefas humanas desempenhadas atualmente.

Quanto às entrevistas realizadas, para a sua análise, foi inicialmente realizada a transcrição das entrevistas, e posteriormente foi efetuada a leitura das mesmas, a fim de verificar padrões ou diferenças entre as várias áreas, podendo estes padrões estar assim alinhados com o que foi defendido pelos diversos autores mencionados na investigação.

Este tipo de abordagem permitiu uma compreensão contextualizada e detalhada sobre os impactos da IA na seguradora estudada, tendo em conta as diferentes experiências entre as funções de cada trabalhador. Para realizar a interpretação final dos dados analisados, esta foi construída de forma refletiva, comparando e interligando os dados empíricos com os objetivos do estudo, bem como com a literatura estudada.

4. Apresentação e análise dos resultados

4.1. Caracterização dos Participantes

No decorrer do estudo, o método de estudo passou pela realização de entrevistas semiestruturadas a três colaboradores de uma seguradora. O objetivo era obter uma compreensão mais aprofundada e multidimensional relativamente à forma como a IA está a ser incorporada na organização em causa. As áreas escolhidas para este estudo foram as de risco, *Contact Center* e *Compliance*, por estas tornarem possível captar diferentes perspetivas sobre os benefícios, desafios e implicações da IA, tendo em conta as especificidades funcionais de cada área.

O entrevistado da área de risco é colaborador da empresa há dois anos e é o responsável pela gestão de risco tecnológico, avaliação de ativos e gestão de prestadores. Tem ainda como responsabilidades a sua contribuição nas áreas de negócio e de cibersegurança, conferindo-lhe uma visão ampla sobre os riscos emergentes que estejam associados à adoção de novas tecnologias. A além das suas responsabilidades, tem o papel de avaliar e mitigar riscos através da identificação de controlos e medidas corretivas. Estas vertentes permitem que seja uma mais valia para refletir sobre as implicações técnicas e operacionais da IA

O colaborador do responsável pelo *Contact Center* conta com 8 anos de experiência na organização, e assume a liderança das equipas responsáveis pelo atendimento ao cliente. A sua principal função passa pela manutenção da eficácia dos canais de comunicação, na estabilização dos tempos de espera e na melhoria da experiência do cliente. Esta área é principalmente exposta e sensível à introdução de ferramentas de IA, uma vez que estas impactam diretamente a interação com os clientes e a qualidade percebida do serviço prestado.

Relativamente ao colaborador da área de *Compliance*, este desempenha funções na empresa há mais de 10 anos, e acumula as responsabilidades de Encarregado de Proteção de Dados (DPO). O seu papel no dia a dia é garantir a conformidade legal da organização, monitorizando a aplicação de regulamentos como o RGPD. Atua como ponto de contacto com a Comissão Nacional de Proteção de Dados (CNDP) para questões relacionadas com a proteção de dados. Interage com titulares de dados e apoia na formação às áreas sobre temas de proteção de dados. A sua perspetiva é essencial no estudo para auxiliar na compreensão dos limites legais e éticos da aplicação de IA no contexto segurador.

4.2. Análise Temática das Entrevistas

A análise qualitativa das entrevistas permitiu a identificação de cinco principais temas que refletem algumas das preocupações e oportunidades associadas à implementação de IA: (1)

Implementação da IA, (2) Benefícios Operacionais, (3) Preocupações Éticas, (4) Segurança da Informação e (5) Perspetivas Futuras.

4.2.1. Implementação da IA:

Consoante a área, o nível de perceção de implementação de IA varia um pouco. De uma perspetiva geral, esta encontra-se ainda numa fase muito inicial.

O departamento de Risco ainda não dispões de soluções de IA ativamente implementadas. No entanto, participa já nesta discussão, reconhecendo o seu potencial para a automatização e apoio à decisão de processos complexos, avaliando o nível de risco de cada projeto. Foi destacado por este entrevistado que a adoção deverá ser precedida por provas de conceito, e forma a garantir a fiabilidade e segurança desta tecnologia.

Apesar da sua fase embrionária, a área do *Contact Center* é a que apresenta um nível de aplicação prática mais avançado. Trata-se de um sistema de IVR (Resposta Interativa por Voz) baseado em IA. Esta solução permitirá um atendimento telefónico automatizado e mais rápido. Numa fase inicial irá fazer o encaminhamento de clientes para a linha correta mais rápido, e no futuro o bot permitirá ao cliente um autosserviço, ou seja, as solicitações que o cliente fizer em linha, serão resolvidas diretamente pelo bot, sem a necessidade de este passar a chamada para um operador humano. A colaboradora menciona ainda um outro projeto, abrangente a todas as equipas da organização, que se trata de triagem e gestão de emails, facilitando o seu tratamento.

A área de *Compliance*, embora não esteja diretamente envolvida no desenvolvimento operacional, desempenha um papel de supervisão, colabora na definição de uma política interna para governação da IA, e participa na avaliação de impacto dos projetos em curso.

4.2.2. Benefícios Operacionais

Os entrevistados no estudo destacaram melhorias associadas à aplicação da IA. Entre elas foi referida a automatização de tarefas que atualmente são repetitivas e administrativas, como por exemplo a triagem de emails ou encaminhamento de chamadas. A sua aplicação surge como uma forma eficaz de aumentar a produtividade, reduzir erros humanos e permitir aos colaboradores que passem a desempenha tarefas de valor acrescentado.

No *Contact Center*, a IA é observada como um facilitador de eficiência. Permite uma resposta mais rápida e personalizada ao cliente, contribuindo para a satisfação e fidelização. O colaborador da área de risco salienta a possibilidade de utilizara a IA como um acelerador de análise documental e a identificação de riscos, permitindo a redução significativa do tempo de resposta.

Pela perspetiva do *Compliance*, este considera que a IA tem o potencial de apoiar a celeridade de processos, desde que sejam salvaguardadas as questões legais e éticas.

4.2.3. Preocupações Éticas

As implicações éticas da utilização da IA foram referidas pelos três entrevistados, expondo diferentes perspetivas. O colaborador do risco mencionou a desconfiança atual relativamente à IA e comparou-a com a que existia inicialmente quando foi implementado o uso da cloud, e destaca que a aceitação desta tecnologia dependerá do grau de confiança que se conseguir estabelecer. A principal preocupação desta área prende-se com a possibilidade de existirem "alucinações" por parte da IA. Por alucinações entende-se que são respostas incorretas geradas por sistemas, quando não lhe são fornecidas as explicações claras para as suas decisões. Na visão do colaborador do *Contact Center* a preocupação passa pela transparência para o cliente, que deve ser informado sempre que estiver a interagir com este tipo de sistemas. Na perspetiva do *Compliance*, é realçado o risco para a discriminação algorítmica, para o enviesamento dos dados e decisões opacas, reforçando a importância da necessidade da explicabilidade dos sistemas e da responsabilização dos envolvidos.

4.2.4. Segurança da Informação

Entre as prioridades mencionadas, a proteção dos dados pessoais e a gestão segura das tecnologias emergentes foi comum entre as diferentes áreas. Para mitigar estes riscos, a área de risco mencionou que se encontra a elaborar uma política interna para a regulação da utilização da IA, tendo em conta os requisitos técnicos mínimos para o uso seguro destas ferramentas.

Em concordância com a área de risco, a área de *Compliance* referiu que está a ser implementado um modelo de cláusulas contratuais especificas, que exigem medidas técnicas e organizativas robustas por parte dos fornecedores de soluções de IA. O cuidado com o desenvolvimento destas medidas revela um alinhamento com o RGPD, nomeadamente a proteção desde o início do processo até à interpretação dos dados processados.

A área de *Contact Center* implementou uma solução baseada em IA, para efeitos de proteção dos dados dos clientes com terceiros, que se trata de uma solução baseada em cloud privada. Além dessa medida, foram criados mecanismos de controlo de acesso rigorosos para os prestadores de serviços externos. Estas medidas são cruciais para a mitigação de partilha de dados pessoais de clientes.

4.2.5. Perspetivas Futuras:

Os entrevistados reconheceram o papel cada vez mais relevante da IA no futuro da organização. A área de risco prevê uma adoção generalizada, uma vez que a pressão dos mercados nacionais e internacionais assim o impulsionam. O *Contact Center* considera a implementação da IA uma mudança inevitável, de forma a manter garantida a competitividade do mercado. Contudo, destaca a importância de formar os colaboradores para a realização de mais analíticas, ou seja, não tanto para a tarefa.

O *Compliance* alerta para a importância de formação contínua e acompanhamento ético e legal dos processos, de forma a garantir a sustentabilidade e responsabilidade da adoção da IA. A literacia digital e o desenvolvimento de uma cultura de ética tecnológica são prioridades, e são pilares essenciais para o sucesso da transformação digital.

4.3. Comparação entre as diferentes áreas

Além de revelar diferentes etapas de maturidade na adoção de IA, a análise comparativa entre as áreas de risco, *Contact Center* e *Compliance* apresentam prioridades distintas e perspetivas moldadas pelo papel específico que cada departamento desempenho na organização.

A área do *Contact Center* é a que se destaca como a mais avançada e a mais recetiva à adoção de tecnologias como a IA. Pelo colaborador desta área foram identificados dois projetos em curso. Um deles é o IVR inteligente, e outro um sistema de triagem e encaminhamento de emails para as diferentes áreas. Ambas as soluções têm como objetivo melhorar a eficiência no atendimento ao cliente, reduzir o tempo de resposta e aliviar as equipas operacionais de tarefas repetitivas e e de menor valor. Este destacou também os benefícios imediatos de aumento da produtividade e a melhoria da experiência do cliente, mas também revela que estas implementações estão a apresentar alguma resistência por parte dos colaboradores, com o receio de perda de funções e dúvidas quanto à fiabilidade das respostas automatizadas. Esta resistência tem origem no carácter transformacional da IA, que interfere diretamente com a forma como cada colaborador olha para a sua tarefa, e a comunicação entre o cliente e a organização.

Por outro lado, o departamento de risco apresenta uma visão mais conservadora e ponderada quanto à IA. Não tem projetos ativos diretamente na sua área, mas está envolvida nos já mencionados, demonstrando a consciência relativamente ao potencial da sua adoção, e auxiliando na avaliação de riscos, particularmente através da análise de grandes volumes de dados e da automatização de processos analíticos. A ponderação desta área decorre da necessidade de assegurar que os resultados apresentados pelas ferramentas de IA são fiáveis e sem erros ou alucinações, de forma a evitar que decisões erradas neste domínio possam ter consequências estratégicas para a organização. A desconfiança inicial, verificada já aquando da implementação

da *cloud*, é um reflexo da cultura de mitigação de risco e da valorização da segurança e previsibilidade sobreposta à rapidez na inovação.

A área de *Compliance*, por sua vez, atua como a defensora ética e legal da organização ao longo do processo de transformação digital. Este departamento não desenvolve diretamente ferramentas de IA, mas assume um papel essencial na definição de políticas, cláusulas contratuais, requisitos técnicos que garantam a conformidade legal e a proteção de dados pessoais. É destacado o envolvimento ativo na elaboração de um modelo de governação da IA, a avaliação de impacto em proteção de dados, e também a exigência de garantias contratuais aos fornecedores de soluções tecnológicas. O foco desta área centra-se em assegurar que a inovação tecnológica não influencia negativamente os direitos dos clientes e os seus dados nem viola os princípios do RGPD. Além disso, o *Compliance* destaca com missão institucional a promoção da literacia digital e uma cultura de responsabilidade ética entre os colaboradores, sendo essencial o acompanhamento crítico do desenvolvimento tecnológico.

Neste sentido, a comparação entre as três áreas evidencia uma interligação de abordagens. O *Contact Center* estimula a inovação por meio da eficiência e da experiência do cliente. A área de risco reforça a necessidade de fiabilidade, segurança e controlo sobre os resultados formados pela IA. Por outro lado, o *Compliance* opera como uma âncora normativa e ética, assegurando que a transformação digital decorre dentro dos parâmetros legais e morais do setor. É importante ter em consideração que as diferentes perspetivas e visões relativas a este tema é essencial para uma adoção equilibrada e sustentável da IA, em que a inovação tecnológica é desenvolvida com vigilância ética e regulamentar

4.4. Respostas às Questões de Investigação

Para responder às questões de investigação introduzidas, recolheu-se informação das áreas de Risco, *Compliance* e *Contact Center* de uma seguradora em Portugal. As entrevistas realizadas permitiram responder às questões colocadas no ponto 2.5. de forma estruturada. A sua análise permitiu compreender a forma como a IA está a ser implementada e de que forma é vista, quais os potenciais impactos esperados, assim como os principais desafios enfrentados.

Questão 1: Como a IA está a ser implementada na seguradora e de que forma esta influencia o trabalho diário dos colaboradores?

O nível de implementação de inteligência artificial na empresa encontra-se em fase inicial, uma vez que a área de *Contact Center* se encontra com um projeto em curso para implementação (ver Anexo 3). Trata-se de um IVR inteligente (*Interative Voice Response*) com IA para atendimento automatizado aos clientes. Outro projeto também em desenvolvimento trata-se de uma aplicação baseada em IA que permite realizar de uma forma mais rápida e eficaz a triagem de emails pelas

diferentes equipas. Estas duas iniciativas permitirão uma clara transformação digital dos processos operacionais atualmente existentes.

As restantes áreas não verificam soluções baseadas nas tarefas realizadas no dia a dia. No entanto, na área de risco, o entrevistado reconhece o potencial deste tipo de tecnologia no apoio a processos de avaliação de risco de ativos, análise de indicadores e gestão de incidentes de segurança (ver Anexo 2). Por este trabalhador, a IA é visualizada como um facilitador do trabalho do dia a dia, tendo a capacidade de melhorar a tomada de decisão e reduzir o esforço manual relacionado com a recolha e tratamento de dados. Esta área envolve-se maioritariamente em projetos relacionados com IA para auxiliar na perceção do nível de risco e no cumprimento das leis quanto à sua implementação.

Quanto à área de *Compliance*, a abordagem passa maioritariamente pelo ponto de vista regulamentar e ético (ver Anexo 4). O participante destaca a importância da criação tanto de um modelo de governação da IA como de uma política interna que defina regras claras para o seu uso. Assim, apesar de não estar diretamente envolvida em projetos de IA para as suas atividades operacionais, auxilia de uma forma estratégica no seu controlo e enquadramento normativo.

Questão 2: Quais os benefícios percebidos pelos profissionais no uso da IA, a nível operacional e estratégico?

De uma forma geral, os entrevistados reconhecem que a utilização da IA proporciona benefícios à organização. Numa perspetiva operacional, os benefícios passam pela automatização de tarefas repetitivas, pela redução dos tempos de espera, melhoria da experiência do cliente e também pelo aumento da eficiência interna.

O entrevistado do *Contact Center* realça a rentabilização do tempo dos colaboradores, permitindo libertá-los de tarefas administrativas para outras que permitam focar-se em funções de maior valor acrescentado para a empresa e para a própria evolução profissional do colaborador. Por este a IA é vista como uma ferramenta para reduzir o erro humano, aumento da produtividade e melhoria dos níveis de satisfação dos clientes.

Pela perspetiva da área de Risco, a IA tem o potencial para no futuro desempenhar um papel crucial no apoio à decisão estratégica, pela análise de grandes volumes de dados e pela capacidade de criar relatórios automatizados que auxiliem a avaliação e mitigação de riscos.

O *Compliance* entende que o principal benefício está relacionado com a possibilidade de melhorar a monitorização de processos, permitindo a facilitação quanto à rastreabilidade e conformidade legal, desde que sejam garantidas as condições de segurança e de privacidade de dados.

Questão 3: Quais os principais desafios e preocupações éticas, financeiras e de segurança associados à utilização da IA?

Nas três entrevistas realizadas é possível verificar-se que existem preocupações transversais nos três principais domínios, sendo eles éticos, operacionais e de segurança da informação.

No âmbito ético, a transparência algorítmica é mencionada, bem como a necessidade de garantir que s utilizadores sabem que estão a interagir com sistemas automatizados, e ainda o risco de decisões enviesadas ou não explicáveis.

O *Compliance* reforça a importância de existir um escrutínio ético permanente, e alerta para os riscos de discriminação, desinformação e perda de controlo sobre os processos em curso (ver Anexo 4). Estas preocupações alinham-se com os riscos descritos na literatura acerca da "caixa preta algorítmica" (Burrell, 2016).

Numa perspetiva financeira, todos os entrevistados reconhecem a necessidade de grandes investimentos para a implementação de IA, particularmente no que toca à infraestrutura tecnológica e formação dos trabalhadores. Por outro lado, verificam que existe um potencial retorno positivo, através da melhoria da eficiência e da redução dos custos operacionais. Para isto, pode pensar-se num equilíbrio entre investimento e retorno, sendo um fator chave para a sustentabilidade das iniciativas de IA.

Em termos de segurança, a proteção dos dados pessoais, o cumprimento do RGPD e a prevenção de ciberataques são preocupações que devem ser levadas em conta. Como exemplos de medidas adotadas pela organização para a mitigação dos riscos são o uso de clouds privadas, criação de políticas internas de regulação de IA e a exigência de clausulas contratuais com fornecedores. As aplicações destas práticas na organização demonstram que existe uma atenção crescente à governação tecnológica, uma vez que o setor dos seguros é fortemente regulado.

Questão 4: De que forma a perceção dos colaboradores sobre a IA varia consoante a sua área funcional?

Após realizadas as três entrevistas, verificou-se que a perceção relativamente à IA difere consoante a área e o papel que cada funcionário desempenha na empresa. A área de *Contact Center*, que tem responsabilidades que são mais operacionais e orientadas para o cliente, olha para a IA como um aliado à melhoria do desempenho, aumento da produtividade e agilidade nas respostas às exigências do mercado.

Em contraste, a área de Risco tem uma função mais analítica e estratégica, logo, adota uma abordagem mais cautelosa, que se foca na necessidade de garantir a fiabilidade e robustez da

tecnologia, antes de ser posta em prática. Esta abordagem acontece pelo facto de existir receio de que decisões erradas possam causar impactos severos, a nível reputacional e financeiro.

O *Compliance*, enquanto área normativa, destaca os riscos legais, os limites éticos e a necessidade de garantir que o uso de IA respeita os direitos dos titulares de dados. O seu papel foca-se na criação de políticas internas, avaliação de impacto em proteção de dados e sensibilização dos colaboradores para os riscos associados ao uso indevido da IA.

As diferenças entre as áreas demonstram que a IA é percecionada de forma diferente, e que a sua aceitação, utilização e regulação dependem fortemente das funções e responsabilidades de cada área. Existindo esta diversidade de perspetiva permite criar uma visão mais equilibrada e critica da transformação digital no setor segurador.

5. Discussão dos resultados face à literatura e contributos do estudo

5.1. Discussão dos resultados face à literatura

Os resultados recolhidos neste estudo comprovam diversos aspetos discutidos ao longo da revisão da literatura sobre a implementação da Inteligência Artificial na empresa do setor segurador. Entre eles quais as suas dimensões a nível tecnológico, ético, financeiro e da segurança da informação.

Os desafios técnicos e organizacionais apontados pelos autores Russell e Norvig (2021) e Goodfellow et al. (2016) está alinhada com a diversidade de níveis de maturidade na implementação da IA entre os diferentes departamentos abordados. Estes destacam a complexidade pertencente à integração de algoritmos de aprendizagem automática em ambientes controlados. O entendimento de que a IA ainda está em fase inicial, conforme relata o entrevistado da área de risco, alinha-se com a forma como Crevier (1993) e McCarthy et al. (1956) descrevem como os ciclos de avanço e estagnação nas fases históricas da IA.

Quanto aos benefícios operacionais, os dados certificam os estudos de Koetter et al. (2019) e Zuo (2025), que evidenciam ganhos de eficiência, redução de custos operacionais e melhoria da experiência do cliente, por meio da automação de certos processos. No caso da área do *Contact Center*, a implementação de um IVR inteligente confirma o potencial transformador da IA em tarefas de atendimento ao cliente, que é uma tendência já verificada noutras organizações.

Na vertente ética, existem grandes preocupações relacionadas com a opacidade dos algoritmos, o risco de resultados enviesados e ausência de explicabilidade, questões estas que se encontram descritas pelos autores Doshi-Velez e Kim (2017), Burrell (2016), Mehrabi et al. (2021) e Floridi e Cowls (2019), que defendem também a importância de garantir transparência, justiça algorítmica e responsabilização do uso da IA. As entrevistas realizadas revelam que as preocupações são particularmente relevantes e mencionadas nas áreas de risco e *Compliance*, uma vez que são as que garantem que o funcionamento deste tipo de tecnologias esteja de acordo com a legislação. Estes refletem uma consciência ética crescente nas organizações que têm como objetivo implementar este tipo de tecnologias de forma regulada, segura e justa.

No que diz respeito à segurança da informação, os envolvidos nas entrevistas revelaram algumas medidas implementadas, tais como a utilização de cloud privada, cláusulas com fornecedores e o desenvolvimento de políticas internas para regulamentar o uso da IA. Estes aspetos estão de acordo com o exposto no Regulamento Geral de Proteção de Dados (RGPD) e com o exposto por Zamharir (2025) e Gerke et al. (2020), em que é referida a importância de garantir a segurança dos dados sensíveis, sobretudo quando processados em sistemas automatizados baseados em tecnologias como NLP e *machine learning*.

A literacia digital e a formação contínua surgem ao longo da revisão da literatura, mencionadas através das rápidas mudanças e evoluções que acontecem no mercado, e demonstram a necessidade continua de capacitação, preparação e sensibilização ética dos colaboradores. Os entrevistados referem igualmente esta necessidade. Há que oferecer aos colaboradores as ferramentas e formação necessárias para que possam estar preparados para acompanhar estas rápidas mudanças.

As entrevistas realizadas confirmam o papel estratégico da IA quanto à transformação do setor segurador, tal como indicado por Eling et al. (2021) e Mehta e Devarakonda (2018), que realçam os impactos económicos, a capacidade preditiva dos sistemas e os desafios na deteção de fraudes. O equilíbrio entre inovação e regulamentação que é apontado pelos entrevistados espelha também o argumento de Floridi e Cowls (2019) que descrevem a importância de uma IA que seja eficaz, ética inclusiva e segura.

Os resultados desta investigação, além de validar a literatura existente, também ilustra, de forma empírica, como a IA está a ser experienciada em diferentes setores da seguradora, confirmando que a sua implementação exige uma abordagem holística que equilibre benefícios operacionais com exigências éticas e regulamentares.

5.2. Contributos do estudo

Quanto aos contributos que este trabalho trouxe, em primeiro lugar este contribuiu para aproximar a literatura teórica da realidade organizacional da empresa em estudo. Demonstrando de uma forma empírica a forma como a IA pode estar a ser percecionada e integrada em diferentes áreas funcionais da seguradora. Este estudo permitiu verificar de uma forma mais concreta e individual como os benefícios, os desafios e as resistências à sua implementação variam consoante a o contexto profissional dos colaboradores.

Em segundo lugar, o estudo ofereceu um contributo analítico relevante ao evidenciar que a adoção desta tecnologia não ocorre de uma forma linear dentro da organização, sendo influenciada pelo grau de proximidade operacional nas atividades do dia a dia com tecnologia, devido às exigências regulatórias de cada área e pela natureza das responsabilidades desempenhadas.

Numa terceira perspetiva, este trabalho reforçou a importância da existência de uma abordagem integrada e organizada da IA no setor segurador, expondo que a sua implementação bem sucedida, além da eficiência técnica dos sistemas, depende também de fatores como a governação, a formação de colaboradores, a proteção dos dados dos clientes, a supervisão ética e a confiança entre cliente e organização.

Em último lugar, o estudo contribuiu igualmente do ponto de vista objetivo, identificando aspetos que poderão apoiar decisões futuras de gestão, no que diz respeito à capacitação interna, na

definição de políticas de utilização responsável da IA, mas também no equilíbrio entre a inovação tecnológica e a conformidade legal. O trabalho realizado permitiu desta forma acrescentar valor no debate académico sobre a IA e seguros, mas também levou a uma reflexão organizacional sobre as possibilidades de transformação digital no setor.

6. Conclusão

6.1. Principais conclusões

O estudo realizado teve como objetivo compreender de que modo a Inteligência Artificial impacta o setor segurador dando um principal foco aos desafios éticos, operacionais e de segurança na empresa em questão. Para complementar o estudo, foram realizadas três entrevistas semiestruturadas a três colaboradores, que pertencem às áreas de Risco, *Compliance* e *Contact Center* de uma seguradora. Assim, foi possível recolher diferentes pontos de vista e identificar perceções complementares sobre a adoção de IA.

Após análise à primeira questão, quanto à fase em que se encontra e à forma como a IA está a ser implementada na organização, os resultados obtidos pelos entrevistados revelaram que a IA ainda se encontra numa fase inicial, ainda que em diferentes fases consoante a área funcional. O *Contact Center* revela ser a área com maior avanço quanto à aplicação se solução automatizadas, nomeadamente os sistemas de IVR com base em IA. Esta área revelou ainda outro projeto, transversais às restantes áreas da companhia, que se trata de realizar uma triagem automática de emails. Estes dois projetos demonstram melhoria operacionais significativas. Em contraste, e pela necessidade de assim o ser, as áreas de Risco e *Compliance* apresentam uma postura mais reservada, pois refletem sobre as implicações da IA quanto ao nível da fiabilidade dos resultados, das exigências regulamentares e proteção dos pessoais, como por exemplo o RGPD.

Relativamente à questão dos benefícios, o estudo revelou também que as áreas apresentam diferentes perspetivas quanto à aplicação da IA, dependendo da função desempenhada pelo trabalhador. Por uns, é reconhecida a utilidade para a automação de processos que no presente são desempenhados de forma manual, a melhoria da eficiência, para que seja possível a dedicação a tarefas de valor acrescentado. Outros valorizam em primeiro lugar a garantia de uma implementação ética, e em segurança e alinhada com o RGPD. Assim, tendo em conta as diferentes perspetivas, refletidas por apenas três trabalhadores relativamente à gestão da mudança tecnológica, é possível verificar a complexidade da transformação digital.

A terceira questão, referente aos desafios e às preocupações éticas, operacionais e de segurança, foi demonstrado nas entrevistas que estes aspetos estão presentes em todas as respostas. Existem preocupações partilhadas pelos entrevistados que estão relacionadas com a transparência algorítmica, com a discriminação e perda de controlo, mas também é tido em consideração o grande investimento necessário e os riscos de cibersegurança. Para enfrentar os desafios, os entrevistados apresentaram algumas medidas adotadas, entre elas o uso de *clouds* privadas e a criação de políticas internas, que juntas apresentam uma tentativa de mitigação dos riscos, de uma forma estruturada.

Por fim, a última questão aborda a perceção da IA entre cada colaborador entrevistado, consoante a sua área funcional. A área operacional, o *Contact Center*, percecionam a IA como uma oportunidade de melhoria de processos e de produtividade. Em contraste, as áreas de Risco e de *Compliance* adotam uma postura mais crítica e regulamentar, e evidenciaram a necessidade de equilibrar inovação com ética, segurança e conformidade.

Assim, é possível concluir que a IA representa uma ferramenta estratégica o potencial para a transformação dos modelos operacionais, neste caso, das seguradoras. Além disso, na visão de cada participante, é importante ter conta que para existir sucesso na sua implementação, é necessário que as organizações garantam mecanismos de governança eficazes, proporcionar formações continuas aos colaboradores e assegurar que a inovação tecnológica acontece de forma responsável, ética e regulada.

6.2. Limitações do estudo

O estudo realizado permitiu uma compreensão aprofundada quanto à realidade da implementação de inteligência artificial na seguradora em questão. No entanto, o estudo revelou algumas limitações.

Apesar das três entrevistas realizadas terem sido escolhidas de forma estratégica e para que demonstrasse o papel de áreas muitos distintas, apresentando resultados que descrevem bem a situação atual da empresa estudada, a amostra pode ser considerada reduzida. Com uma amostra maior, por exemplo entrevistando um elemento da área de tecnologia, poderia alargar a visão quanto ao potencial da tecnologia.

Quanto à natureza do estudo, o método de recolha de dados escolhido, de carácter qualitativo e exploratório, por meio da realização de entrevistas semiestruturadas, permitiu uma visão menos restrita e com possibilidade de maior contextualização do tema. Por outro lado, a falta de dados quantitativos pode levar à carência de aferição de relações casuais entre variáveis, bem como de resultados mais exatos.

Conforme descrito nas três entrevistas, a organização escolhida para o estudo ainda se encontra numa fase inicial de adoção de IA. O que por um lado pode demonstrar a realidade empresarial atual quanto à utilização destas tecnologias, revela por outro uma limitação na análise de impactos concretos a médio e longo prazo.

Uma vez que o estudo foi realizado apenas com base em perspetivas internas, não abrangendo para outras organizações, dentro ou fora do ramo segurador, restringiu a compreensão global do setor, ou o estado de avanço da tecnologia face a outras organizações, entendendo melhor quais os desafios apresentados e oportunidades que possam estar associadas à IA.

6.3. Sugestões para investigações futuras

Considerando as limitações do estudo descritas anteriormente, existem algumas sugestões para investigações futuras, que permitirão aprofundar e complementar a investigação e resultados obtidos.

Tal como descrito acima, relativamente à amostra escolhida, poder-se-á abranger o estudo tanto a um número mais alargado de colaboradores, como utilizar outras companhias de seguros, de forma a poder existir uma maior comparação dentro do setor. Poderá mesmo comparar-se com outros setores, menos regulados, na tentativa de investigar se o estágio de implementação já se encontra em fases mais avançadas.

Além de comparar com outras seguradoras e/ou setores, avaliar qual a perspetiva entendida pelos *stakeholders*, por exemplo clientes, quanto à automatização de processos alterações no tipo de atendimento e atenção ao cliente, para avaliar as questões transparência e confiança nas decisões baseadas em IA.

Com os estudos que vão surgindo ao longo do tempo sobre a IA, a sua implementação, benefícios e perceções, seria interessante analisar de uma forma mais consistente quais os efeitos da IA nos processos organizacionais, na cultura do mundo corporativo e nos resultados operacionais da empresa.

Outra vertente interessante a estudar, além da ética, de segurança e tecnológica, seria averiguar quais os impactos a nível ambiental, se os benefícios ultrapassam a poluição que causa e que medidas devem ser tomada para garantir um uso sustentável da tecnologia.

Em último lugar, aplicaria uma metodologia mista, de forma a combinar a profundidade e abrangência do estudo qualitativo com o detalhe da análise quantitativa. Este tipo de estudo permite a possibilidade de compreender o fenómeno da IA nas organizações em Portugal, contribuindo para a construção de boas práticas de implementação e regulação no futuro.

Referências bibliográficas

Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022*). Insurance Fraud Detection: Evidence from Artificial Intelligence and Machine learning.* Research in International Business and Finance, 62, 101744.

Associação Portuguesa de Seguradores. (2025). *Seguros em Portugal: Panorama 2024* (Ed. julho 2025). APS. https://www.apseguradores.pt/

Autoridade de Supervisão de Seguros e Fundos de Pensões. (2025). *O mercado segurador: Relatório estatístico 2024*. Lisboa: ASF. https://www.asf.com.pt/

Bearman, M., & Ajjawi, R. (2023). *Can AI be ethical? A critical exploration of generative AI in qualitative research*. Qualitative Research in Health, 3(1), 1–9. https://doi.org/10.1016/j.qrh.2023.100193

Bernstein, P. L. (1998). *Against the Gods: The Remarkable Story of Risk*. New York. John Wiley and Sons.

Bhattacharya, S., Castignani, G., Masello, L., & Sheehan, B. (2025). AI revolution in insurance: Bridging research and reality. Frontiers in Artificial Intelligence, 8, 1568266. https://doi.org/10.3389/frai.2025.1568266

Blohm, M., Dukino, C., Kintz, M., Kochanowski, M., & Koetter, F. (2019). *Towards a Privacy Compliant Cloud Architecture for Natural Language Processing Platforms*. Fraunhofer IAO, University of Stuttgart.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in *machine learning* algorithms. *Big Data & Society*, *3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Cain, P. J. & Hopkins, A. G. 1993. *British Imperialism: Innovation and Expansion, 1688–1914*. London: Longman.

Charmaz, K. (2014). *Constructing Grounded Theory* (2nd ed.). Sage Publications.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Crevier, D. (1993). AI: The Tumultuous History of the Search for Artificial Intelligence. Basic Books.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *Blockchain* technology: Beyond bitcoin. *Applied Innovation Review*, 2, 6-10.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable *machine learning*. *arXiv preprint* arXiv:1702.08608. https://arxiv.org/abs/1702.08608

Eling, M., Nuessle, D., & Staubli, J. (2021). *The Impact of Artificial Intelligence Along the Insurance Value Chain and on the Insurability of Risks*. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(2), 205-241.

European Insurance and Occupational Pensions Authority. (2025). Opinion on artificial intelligence governance and risk management. EIOPA.

European Parliament & Council. (2024). Regulation (EU) 2024/... laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union.

Ferguson, N. (2009). *The ascent of money: A financial history of the world*. Penguin Books.

FERRARI, T. A. (1982). *Metodologia da pesquisa científica.* São Paulo: McGraw-Hill.

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, *1*(1). https://doi.org/10.1162/99608f92.8cd550d1

Gerke, S., Minssen, T., & Cohen, G. (2020). *Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare*. Artificial Intelligence in Healthcare, Chapter 12.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social* (6ª ed.). São Paulo: Atlas.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

Graunt, J. (1975). *Natural and Political Observations Mentioned in a Following Index, and Made Upon the Bills of Mortality*. Gregg International.

Guedes-Vieira, Manuel (2012) *Introdução aos Seguros,* Vida Económica, Porto

Halley, E. (1693). *An Estimate of the Degrees of the Mortality of Mankind*. Philosophical Transactions of the Royal Society. https://doi.org/10.1098/rstl.1693.0007

High-Level Expert Group on AI. (2018). "A Definition of AI: Main Capabilities and Scientific Disciplines." European Commission.

Jacob, Nicolas, Les Assurances, 2ª edição, Dalloz, Paris, 1979, pág.5

Joshi, N. (2019, 20 de dezembro). *7 types of artificial intelligence*. Forbes. https://www.forbes.com/sites/nirajjoshi/2019/12/20/7-types-of-artificial-intelligence/

Koetter, F., Blohm, M., Drawehn, J., Kochanowski, M., Goetzer, J., Graziotin, D., & Wagner, S. (2019). *Conversational Agents for Insurance Companies – From Theory to Practice*. Fraunhofer Institute for Industrial Engineering & University of Stuttgart.

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing* (2nd ed.). Sage Publications.

Masci, P. (2011). Journal of the Washington Institute of China Studies, Spring 2011, Vol. 5, No. 3, p25-68

Masci, P. (2011). *The History of Insurance: Risk, Uncertainty and Entrepreneurship*. University of Rome

McCarthy, J., Minsky, M., Rochester, N., & Shannon, C. (1956). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.

McKinsey & Company. (2025, 15 de julho). The future of AI in the insurance industry. McKinsey & Company.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in *machine learning*. *ACM Computing Surveys*, *54*(6), 1–35. https://doi.org/10.1145/3457607

Mehta, N., & Devarakonda, M. V. (2018). *Machine learning, natural language programming, and electronic health records: The next step in the artificial intelligence journey?* Journal of Allergy and Clinical Immunology, 141(6), 2019-2021. DOI: 10.1016/j.jaci.2018.02.025.

Newell, A., & Simon, H. A. (1961). General Problem Solver.

Nilsson, N. J. (1998). Artificial Intelligence: A New Synthesis. Morgan Kaufmann.

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., & Li, B. (2016). The limitations of deep learning in adversarial settings. 2016 *IEEE European Symposium on Security and Privacy* (EuroS&P), 372-387.

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (4th ed.). Sage Publications.

Pearson, R. (2004). *Insuring the Industrial Revolution: Fire Insurance in Great Britain, 1700-1850* (Modern Economic and Social History) Ashgate Publishing

Rubinstein, W. D. (1993). Capitalism, Culture and Decline in Britain, 1750–1990. London: Routledge.

Russell, S. J., & Norvig, P. (2009). *Artificial intelligence: A modern approach* (3rd ed.). Pearson.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Schwab, K. (2016). "The Fourth Industrial Revolution." Crown Business.

Seidman, I. (2006). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (3rd ed.). Teachers College Press.

Sicari, S., A. Rizzardi, L.A. Grieco, and A. Coen-Porisini (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76: 146–164. https://doi.org/10.1016/j.comne t.2014.11.008

Stanford University Department of Philosophy. (2018). "Artificial Intelligence." In Stanford Encyclopedia of Philosophy. Metaphysics Research Lab - Center for the Study of Language and Information Stanford University.

Stanford University. (2018). *The One Hundred Year Study on Artificial Intelligence (AI100): 2018 report*. Stanford University. https://ai100.stanford.edu/2018-report

Stigler, S. M. (1986). *The History of Statistics: The Measurement of Uncertainty before 1900*. Harvard University Press.

Turing, A. M. (1950). *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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, L 119, 1-88. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679

Walch, K. (2019). "Rethinking Weak vs. Strong AI." Forbes.

Wang, P. (1995). *Non-Axiomatic Reasoning System: Exploring the essence of intelligence* (Doctoral dissertation, Temple University).

Wang, P. (2019). *On defining artificial intelligence*. Journal of Artificial General Intelligence, 10(2), 1–37. https://doi.org/10.2478/jagi-2019-0002

Wilson, R. A., & Keil, F. C. (1999). The MIT Encyclopedia of the Cognitive Sciences. MIT Press.

Zamharir, M. A. (2025). *The Impact of Blockchain Technology on Customer Loyalty in the Insurance Industry:* The Mediating Roles of Transparency, Security, and Efficiency. Preprints.org.

Zarifis, A., Kawalek, P., & Azadegan, A. (2021). *Evaluating If Trust and Personal Information Privacy Concerns Are Barriers to Using Health Insurance That Explicitly Utilizes AI*. Journal of Internet Commerce, 20(1), 66-83.

Zuo, J. (2025). *AI Usage Case Study in Healthcare and Health Insurance Sector*. Everbright Actuarial Consulting Limited.

Anexos

Anexo 1 - Legislação do setor segurador (Lei n.º 147/2015, de 9 de setembro)

"Lei n.º 147/2015, de 9 de setembro

Aprova o regime jurídico de acesso e exercício da atividade seguradora e resseguradora, bem como o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à Autoridade de Supervisão de Seguros e Fundos de Pensões, transpondo a Diretiva 2009/138/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, procede à quinta alteração ao Decreto-Lei n.º 12/2006, de 20 de janeiro, à primeira alteração ao regime jurídico do contrato de seguro, aprovado pelo Decreto-Lei n.º 72/2008, de 16 de abril, à segunda alteração ao Decreto-Lei n.º 40/2014, de 18 de março, e revoga o Decreto de 21 de outubro de 1907 e o Decreto-Lei n.º 90/2003, de 30 de abril."

Esta lei define as regras para operar no setor segurador e transpõe a Diretiva Solvência II (2009/138/CE), que estabelece exigências de solvência e gestão de riscos, estabelece a supervisão da Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) e exige transparência e avaliação de risco, elementos críticos na implementação de IA.

O Código das Sociedades Comerciais (Decreto-Lei n.º 262/86, de 2 de setembro) estabelece as normas gerais de funcionamento das empresas em Portugal, incluindo as seguradoras.

Governação Corporativa

Artigo 64º- Deveres dos administradores (gestão prudente e diligente, essencial no uso da IA).

1 - Os gerentes ou administradores da sociedade devem observar:

a) Deveres de cuidado, revelando a disponibilidade, a competência técnica e o conhecimento da actividade da sociedade adequados às suas funções e empregando nesse âmbito a diligência de um gestor criterioso e ordenado; e

b) Deveres de lealdade, no interesse da sociedade, atendendo aos interesses de longo prazo dos sócios e ponderando os interesses dos outros sujeitos relevantes para a sustentabilidade da sociedade, tais como os seus trabalhadores, clientes e credores.

2 - Os titulares de órgãos sociais com funções de fiscalização devem observar deveres de cuidado, empregando para o efeito elevados padrões de diligência profissional e deveres de lealdade, no interesse da sociedade."

RGPD

“Artigo 1.º

Objeto

A presente lei assegura a execução, na ordem jurídica interna, do 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, doravante designado abreviadamente por Regulamento Geral de Proteção de Dados (RGPD).” IA na análise de risco e na definição de prémios de seguro pode levantar questões de tratamento de dados sensíveis.

(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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados))

Artigo 22º- RGPD

Artigo 22.º

“Decisões individuais automatizadas, incluindo definição de perfis

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

2. O n.º 1 não se aplica se a decisão:

a)For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;

b)For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou

c)For baseada no consentimento explícito do titular dos dados.

3. Nos casos a que se referem o n.º 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

4. As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular."

Este artigo garante o direito à explicabilidade de decisões automatizadas e a supervisão humana.

https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1986-34443975-67044099

Anexo 2 - Entrevista 1- colaborador do departamento de risco

Introdução à entrevista

Entrevistadora:

Olá e muito obrigada pela tua disponibilidade para participar nesta entrevista. Este estudo faz parte de uma investigação académica no âmbito de uma dissertação de mestrado e tem como objetivo compreender como a inteligência artificial está a ser implementada no setor segurador, com especial foco nos benefícios e nos desafios éticos, operacionais e de segurança que essa tecnologia pode representar para os profissionais e para as organizações.

Pretende-se através desta entrevista, escolher a opinião e experiência profissional, tendo em conta o teu contato direto com processos ou ferramentas que possam estar a ser transformadas ou influenciadas por soluções de inteligência artificial.

A tua perspetiva é particularmente relevante por atuar numa área específica, neste caso, o risco, e será fundamental para compreender como estas tecnologias estão a ser integradas de formas distintas dentro da mesma organização.

A entrevista terá a duração aproximada de 20 a 30 minutos e os dados recolhidos serão utilizados exclusivamente para fins académicos, sendo garantido o anonimato e a confidencialidade de todas as respostas. Com a tua autorização a entrevista será gravada apenas para facilitar a transcrição e posterior análise. Se em algum momento desejares interromper ou retirar a tua participação, podes fazê-lo livremente sem qualquer consequência.

Posso então confirmar que compreende este propósito do estudo e que consentes participar nesta entrevista?

Entrevistado:

Sim confirmo.

Contextualização profissional:

Entrevistadora:

Podes descrever qual a tua função atual que desempenhas e há quanto tempo trabalhas na empresa?

Entrevistado:

Estou na empresa há quase 2 anos. Estou na equipa de gestão de risco e faço a gestão de risco ligada às componentes tecnologia.

Desempenho o papel de identificação de riscos, acompanhamento dos riscos e também tem algumas funções na gestão de prestadores, na parte também de continuidade de negócio e tudo o que envolva um bocadinho de cibersegurança.

Entrevistadora:

Quais são as tuas principais responsabilidades do dia a dia?

Entrevistado:

Ora o principal é fazer avaliações de risco a nível dos ativos, que poderão ser aplicações ou infraestrutura ao mesmo prestador e dessas avaliações, fazer a identificação de quais é que poderão ser os riscos que estão associados a esses ativos, e ao mesmo tempo, em conjunto com as áreas, principalmente a tecnologia, fazer o levantamento dos controlos que poderão mitigar os riscos ou então identificar os planos de ação que poderão passar por exemplo por aceitar o risco, transferir o risco, e então com esse levantamento nós depois fazemos a mensuração e fazendo a identificação da probabilidade de acontecer o risco x o nível de impacto que esse risco poderia ter ao acontecer - aí são medidos vários níveis de impacto- e vamos chegar a um nível de risco residual, quando aplicamos os controlos e a percentagem de mitigação desses controlos. Desta forma, temos uma visão de como é que os ativos estão em termos de risco.

Essa informação, depois é passada em vários fóruns e relatórios e permite também à administração e ao órgão de direção tomar determinadas medidas que facilitem a mitigação dos riscos e a redução do risco da companhia.

Entrevistadora:

E como é que descreverias a cultura organizacional da empresa, especialmente no que diz respeito à adoção de novas tecnologias?

Entrevistado:

Nós, atendendo à estrutura da empresa, temos uma abordagem muito virada para novas tecnologias de experimentação de novas tecnologias. Temos alguns projetos agora que estão a começar em que já envolvem aqui uma série de tecnologias que estão mais na moda, mas o

objetivo da empresa é sempre ir começar com uma experimentação – normalmente por provas de conceito-, perceber qual é que será o impacto que essas novas tecnologias teriam no nosso dia a dia e na melhoria da qualidade dos nossos produtos para os clientes, e atendendo ao resultado dessas provas de conceito, avançar com essas tecnologias em sistemas de produção que permitam esta tal melhoria do serviço.

Portanto, eu vejo em termos de apetite a novas tecnologias muito grande por parte da nossa empresa, também devido ao tamanho que ela tem a necessidade de se diferenciar num mercado que está muito regulamentado e que não permite muitas alterações que sejam fora do padrão.

Experiência com tecnologia

Entrevistadora:

Quais são as soluções de inteligência artificial que foram implementadas na empresa até ao momento.

Entrevistado:

Realmente, nós não temos nenhuma, pelo menos de conhecimento nosso. Aquilo que se está a pensar, ainda olhando aqui um bocadinho também para aquilo que é o mercado segurador, e como é que esta nova tecnologia de inteligência artificial vem ajudar, há uma série de vertentes que já começam a ser implementadas ao nível das seguradoras que vem facilitar aqui muitas vezes a operação, e ao mesmo tempo também o contato com o cliente e a resposta ao cliente, que muitas vezes pelos processos burocráticos demora muito tempo.

Por outro lado, também há, não só no mercado segurador, mas mais transversal, na facilidade de chegar a informação quando há dúvidas, quando não há certezas sobre determinados temas, o utilizar a inteligência artificial para nos ajudar também vai conseguir tomadas de decisão mais estruturadas que hoje em dia, sem inteligência artificial, demoraria muito mais tempo de investigação.

Entrevistadora:

Como é que tu achas que pode vir a ser esse processo de implementação deste tipo de tecnologias? Consideras que houve ou haverá resistência ou mais um entusiasmo por parte dos colaboradores?

Entrevistado:

Eu acho que vai haver um mix.

Atualmente, as empresas têm, em termos de colaboradores, vários estilos, digamos assim, e várias caraterísticas de pessoas, que umas são mais abertas a novas tecnologias, outras são menos abertas a novas tecnologias.

Estamos a falar do mercado segurador. Nós temos aqui um mercado já muito antigo, o mercado segurador é um mercado muito antigo e então dentro das próprias seguradoras há um espectro ao nível etário muito alargado. Enquanto se estivéssemos a falar aqui de uma startup em que normalmente o espectro de idades de é muito curto, são empresas que são muito ligadas aos jovens e a um dinamismo diferente, em termos das seguradoras, tem muita regulamentação, já são mais antigas, têm um espectro muito alargado que incluem jovens, têm muito mais facilidade de integração com estas novas tecnologias e outras pessoas que são um bocadinho mais de processos mais rotineiros e que as deixa mais confortável são muitas vezes mais adversas estas novas tecnologias.

No entanto, eu acho que aquilo que vemos na globalidade é que cada vez há mais uma, uma identificação da inteligência artificial como um facilitador e como algo que vem ajudar e isso vê-se em todos estes espectros etários.

Portanto, eu acho que em termos da empresa não é uma questão de se vai ser aceite ou não se vai ser aceite e de como é que poderemos implementar ou não podemos implementar. Acho que é um bocadinho mais por aí.

Implementação de inteligência Artificial

Conhecimento sobre Inteligência Artificial

Entrevistadora:

Tens conhecimento de iniciativas ou projetos que envolvam inteligência artificial na empresa e se puderes detalhar alguns deles?

Entrevistado:

Era como eu estava a dizer em termos da empresa, nós não temos ainda nada implementado.

O que eu posso dar também uma ideia em termos daquilo que eu conheço em termos de mercado segurador, há aqui umas vertentes que a inteligência artificial tem vindo a trazer um elevado valor.

Um deles tem a ver, por exemplo, nas chamadas automáticas em que atualmente - ou até agora - estas chamadas eram respondidas por humanos ou por um e IVR muito limitado, em que o

utilizador teria de escolher, carregando nas teclas (opções), no seu telefone para conseguir ir avançando num guia que depois permitisse dar a resposta. Nota-se que a nível do mercado segurador e mesmo de outras de outras áreas que esta vertente de incluir IA como uma simulação humana, vem melhorar este relacionamento com o cliente e o cliente ao mesmo tempo muitas vezes nem se percebe que está a falar com IA e consegue receber a resposta às suas necessidades muito mais depressa, e, ao mesmo tempo, com custo mais baixo, porque normalmente o custo que estes sistemas têm é muito mais baixo do que termos uma equipa humana a fazer o trabalho. Esta será uma das vertentes.

Outra das vertentes é que ela também já tinha aqui falado, tem a ver com facilidade de chegarmos à informação, por exemplo, na componente de regulamentação normalmente as regulamentações são muito densas, estendem-se por várias vários documentos, e termos uma IA que nos consiga pesquisar rapidamente em todos os documentos que existem, determinados conceitos que nós precisamos para elaborar o trabalho que está a ser feito, permite-nos também numa área, por exemplo, de *Compliance*, ajudar aqui na resposta mais rápida às necessidades de confirmação que estamos a cumprir ou não estamos a cumprir.

Em termos de gestão de risco, também há aqui algumas componentes, se bem que levanta aqui de alguns temas, devido também às questões mais negativas que são associadas à IA, como alucinações, como más interpretações, mas em termos de gestão de risco também poderá vir aqui a ajudar bastante, porque o que hoje em dia é feito de forma manual também na avaliação de determinados casos, poderemos ter aqui em termos de avaliação de risco de diferentes casos, por exemplo, recebemos um novo contrato, ou uma nova proposta para um determinada para uma unidade de risco, determinada pessoa, avaliar o que está envolvido ou as características da pessoa que sejam relevantes para o risco e a IA fazer esse trabalho todo que hoje em dia é feito manualmente, mas rapidamente a fazer ali uma avaliação e dar-nos ali os indicadores que nós necessitamos para depois dar a resposta final pode ser ali uma componente que nos vem trazer essa essa informação.

A partir daí também a indo daqui um bocadinho mais longe. Se calhar um futuro não tão próximo, mas que também está a aproximar-se, tem a ver aqui com um bocadinho também com a componente mais de saúde em que poderemos num futuro próximo começar a ter chamadas automáticas, bem que entre um bocadinho aqui na questão ética e moral, mas termos em vez de termos um médico à frente da pessoa, termos uma máquina, uma inteligência artificial que interpreta os dados de um cliente ou de um paciente, e consegue dar ali uma resposta, por exemplo, de que medicamento é que ele poderá utilizar para o problema que ele está a dar. Eu acho que estas vertentes são as que eu vejo assim mais para breve e que estão já a começar a ser implementadas. No entanto, isto traz aqui algumas questões éticas e de segurança, que depois têm de ser previstas.

Aplicações práticas:

Entrevistadora:

Relativamente às aplicações práticas, em que áreas é que esses processos na seguradora irão ser aplicados e como é que isso impacta o teu trabalho, ou se consideras que isso impacta o teu trabalho?

Entrevistado:

Sim, eu já dei aqui alguns [exemplos], mas eu acho que, por exemplo, a nível da gestão de risco é um dos casos claros, mesmo a minha gestão de risco atual em termos de tecnologia pode vir a ser muito facilitada com a interpretação dos indicadores, que é aquilo que nós fazemos hoje em dia, perceber quais é que são os riscos que podem advir de determinados ativos.

Existir uma inteligência artificial consiga combinar toda esta informação e dar uma decisão ou identificar os riscos todos vai facilitar muito aqui a esta esta gestão. A nível de *Compliance*, como também já tinha dito também se calhar é outra área que vai ter aqui um boost muito grande a nível de informação, e acho que também ao nível de outras áreas, como por exemplo, se formos aqui um bocadinho mais para a componente mais de contabilidade, que são aquelas e aquelas componentes mais de validação da informação de transações, a IA vai conseguir simular as ações humanas e permitir que tudo aquilo que se faz hoje em dia de lançamentos, de validações antes de fazer estes lançamentos destas transações, que cria estas validações que atualmente são manuais e passar passarem a ter.

Portanto, isto dando aqui alguns exemplos porque acho que, numa globalidade todas as áreas vão ser afetadas. Quando entramos por exemplo para a área de segurança de informação, também é outra que já hoje em dia tem muitas componentes de IA que nos permitem, por exemplo, identificar rapidamente o que é que são incidentes que são reais e os que não são reais, logo, distinguir aí essas 2 vertentes. Ao mesmo tempo, também identificar que possíveis respostas, ou mesmo aplicar diretamente a resposta a um incidente que esteja a acontecer, por exemplo, cibernético e tudo isso, com a IA e com a sua evolução, nós vamos conseguir aqui também reduzir um bocadinho aqui o esforço humano nestas componentes.

Obviamente que há a discussão de que haverá sempre aqui um componente humano, mas isso é algo discutível.

Benefícios observados

Eficiência operacional:

Entrevistadora:

Quais as melhorias ou benefícios que podes verificar com a implementação da inteligência artificial nos processos da empresa?

Entrevistado:

Sim, aqui uma há uma componente, por exemplo, a nível documental. Hoje em dia, a componente documental é sempre um esforço muito grande para as empresas, porque as equipas estão muito focadas no dia a dia, no fazer, no entregar, e tudo o que são estas componentes mais suporte, como é [o caso da] documentação fica sempre um bocadinho de lado porque o foco é outro.

A IA, e dando o exemplo com o que estamos aqui a ter de uma transcrição de uma entrevista, por exemplo, vem-nos ajudar depois a facilitar este processo de documentação e acho que isso também transversalmente na empresa, vai-nos ajudar a ter um grau de informação muito melhor e mais estruturado. Acho que esse será um dos grandes também facilitadores do da IA. Fora isso, é um bocadinho aqueles que eu já tinha dito. Tem a ver mesmo com a redução do trabalho manual para trabalho automatizado e de garantia que o que está a ser feito está a ser feito corretamente.

Atendimento ao cliente:

Entrevistadora:

E tu consideras que haverá a mudanças na forma como os clientes serão atendidos devido ao uso da inteligência artificial? Podes exemplificar?

Entrevistado:

Claramente. Como também já tinhas dado aqui a ideia, um dos projetos que está a avançar mais depressa em termos de mercado, tem a ver com esta ligação com o cliente, com a resposta da inteligência artificial às perguntas do cliente e, portanto, acho que sim, acho que estas ligações com o cliente cada vez mais - e isto tem a ver também um bocadinho com as novas tecnologias com a facilidade também dos jovens em adotar estas novas tecnologias muito cedo -, temos uma vivência mais tecnológica, sem aquela necessidade tanto de contato direto. Eu acho que vai ser completamente transformada a forma como hoje tratamos os clientes e como os clientes vão ver as próprias empresas de seguros.

Desafios e considerações éticas

Preocupações éticas:

Entrevistadora:

E agora falando aqui numa parte mais das considerações e preocupações éticas.

Existem preocupações que estejam relacionadas com utilização de inteligência artificial da empresa, como, por exemplo, a privacidade dos dados ou decisões automatizadas, certo?

Entrevistado:

O que está a acontecer nas empresas é um bocadinho o que aconteceu há alguns anos, quando foi adotada as clouds públicas, ou seja, nós, quando foi adotado as clouds públicas, as empresas olhavam com desconfiança para a cloud pública, porque não sabiam onde é que estavam. Era algo que não controlavam a 100%, portanto, colocar os seus dados em algo que não se controla e cria aqui um risco muito grande.

Aquilo que foi acontecendo foi que, à medida que foram sendo dadas garantias por parte das dos principais players de cloud, as empresas começaram a ganhar a confiança que era necessária para colocar os seus dados nestas clouds porque também perceberam a vantagem que teriam em colocá-los lá, ao mesmo tempo que era dada a garantia que esses dados estavam seguros. Eu acho que com a IA está a acontecer o mesmo.

Nós percebemos que existem 3/4 grandes players em termos de inteligência artificial, que vem muito dos que já existem no mercado em termos tecnológicos. No entanto, ainda não chegámos ao grau de confiança de que a inteligência artificial é realmente controlada por estes por estes players e que eles nos conseguem dar a garantia que não existem, por exemplo, alucinações e respostas, por exemplo, a clientes diretamente da IA que possam se criar aqui impactos em termos reputacionais em termos de negócio, que é algo do qual a empresa vive e que podem causar aqui muitos problemas para a empresa. Enquanto não for criada esta confiança e mecanismos que consigam controlar a própria inteligência artificial, vamos andar sempre aqui um bocadinho na gestão do próprio risco, porque por um lado nós temos aqui facilitação e vamos ter aqui um impacto positivo em termos financeiros, em termos de experiência para o cliente. Por outro lado, vamos ter que assumir este risco que poderemos ter aqui problemas ao utilizar a inteligência artificial. Portanto, o que se observa em termos das empresas é um bocadinho esta balança entre o usar e não usar consoante a confiança que podem ter ou não podem ter, é um bocadinho isto.

Segurança da informação:

Entrevistadora:

Como é que a empresa lida com a segurança dos dados processados por sistemas de inteligência artificial? Existem protocolos específicos para o efeito?

Entrevistado:

Atualmente estamos a iniciar essa discussão. O que nós estamos a começar a fazer é a definir uma política de utilização de inteligência artificial, ou seja, definir o que é que é possível ou não é possível fazer , quais é que são os nossos limites em termos de aceitação destas plataformas, quais são as características que nós aceitamos e depois a partir daí, implementar para tudo o que vier [de] projetos, estas medidas para que se possa utilizar a inteligência artificial, ou seja, estamos a começar na parte governativa para depois entramos para a parte tecnológica. Ao mesmo tempo, está-se também a começar a identificar quais é que serão, em termos tecnológicos, as componentes que serão obrigatórias, que cada IA tenha para que possamos trabalhar com ela. É um bocadinho nestas 2 vertentes que estamos a trabalhar neste momento.

Perspetivas futuras

Expectativas da evolução:

Entrevistadora:

Quais é que são as expectativas em relação ao futuro da inteligência artificial na seguradora? Acreditas que haverá uma expansão no uso deste tipo de tecnologia?

Entrevistado:

Sim, eu acho que sim, claramente pelo valor que traz, acho que cada vez mais vai ser uma adoção generalizada por parte das empresas. Isto porque, apesar de nós estarmos na Europa, onde o ambiente é muito regulamentado, nós competimos com a China, competimos com os Estados Unidos, onde as regras são um bocadinho menos apertadas. Portanto, nós vamos ter que ter aqui uma aproximação a esta tecnologia muito mais ao nível da aceitação do que propriamente da criação de entraves à mesma.

Preparação e capacitação:

Entrevistadora:

Tens conhecimento se a empresa oferece formações ou certificações para que os funcionários se adaptem às novas tecnologias?

Entrevistado:

Sim, a empresa tem uma política de formação e de incentivo ao conhecimento muito forte e isso é muito positivo. Cada vez mais as pessoas estão informadas sobre este tipo de situações. Vão a fóruns, vão a palestras, congressos para perceberem o que é que podem fazer ou não podem fazer.

Encerramento

Entrevistadora:

Existe algum aspeto que tu aches relevante que ainda não tínhamos abordado?

Entrevistado:

Eu acho que passámos pelos pontos principais. Há sempre a questão ética que se levanta, pois nós não sabemos realmente o que é que se está a passar dentro da inteligência artificial. Mas na prática nós vamos ter que a adotar.

Obviamente que em termos globais há um movimento de tentar humanizar a inteligência artificial, ou seja, não ser um robô em si, mas ser um robô que tem diretrizes como um humano pensaria, para tentar criar estas barreiras éticas e que a IA comece a criar estas interpretações mais éticas e acho que poderá ser aqui um grande desafio e está a ser um grande desafio que que o seja. No entanto, eu acho que cada vez mais a IA vai evoluindo e vai ganhando também com a aprendizagem estas necessidades e estas vertentes ou virtudes que o mantém e que hoje em dia a IA ainda não tem.

Entrevistadora:

Gostarias de acrescentar alguma coisa sobre a implementação da inteligência artificial na organização e de que forma é que pode impactar a ética da mesma?

Entrevistado:

Temos que adotar, mas temos que ter cuidado a adotar. Acho que deixava esta frase.

Entrevistadora:

Muito obrigada pela tua participação.

Anexo 3 - Entrevista 2- Colaborador departamento *Contact Center*

Introdução à entrevista

Entrevistadora:

Olá e muito obrigada pela tua disponibilidade para participar nesta entrevista. Este estudo faz parte de uma investigação académica no âmbito de uma dissertação de mestrado e tem como objetivo compreender como a inteligência artificial está a ser implementada no setor segurador, com especial foco nos benefícios e nos desafios éticos, operacionais e de segurança que essa tecnologia pode representar para os profissionais e para as organizações?

Pretende-se através desta entrevista, escolher a opinião e experiência profissional, tendo em conta o teu contato direto com processos ou ferramentas que possam estar a ser transformadas ou influenciadas por soluções de inteligência artificial.

A tua perspetiva é particularmente relevante por atuar numa área específica, neste caso, o *Contact Center*, e será fundamental para compreender como estas tecnologias estão a ser integradas de formas distintas dentro da mesma organização.

A entrevista terá a duração aproximada de 20 a 30 minutos e os dados recolhidos serão utilizados exclusivamente para fins académicos, sendo garantido o anonimato e a confidencialidade de todas as respostas. Com a tua autorização a entrevista será gravada apenas para facilitar a transcrição e posterior análise. Se em algum momento desejares interromper ou retirar a tua participação, podes fazê-lo livremente sem qualquer consequência.

Posso então confirmar que compreendes este propósito do estudo e que consentes participar nesta entrevista?

Entrevistado:

Sim

Contextualização profissional:

Entrevistadora:

Podes descrever qual a tua função atual que desempenhas e há quanto tempo trabalhas na empresa?

Entrevistado:

Estou há 8 anos na empresa e sou responsável pelos *Contact Center*s.

Entrevistadora:

Quais são as tuas principais responsabilidades do dia a dia?

Entrevistado:

Manter funcional toda a comunicação com o cliente via call center a estabilizar o tempo de espera e [melhorar] a experiência do cliente.

Entrevistadora:

E como é que descreverias a cultura organizacional da empresa, especialmente no que diz respeito à adoção de novas tecnologias?

Entrevistado:

Estamos num processo de transformação digital, apesar de haver muita dificuldade em conseguir coordenar esforços com as áreas de tecnologia, dado não sermos ainda uma empresa totalmente independente tecnologicamente.

Experiência com tecnologia:

Entrevistadora:

Quais são as soluções de inteligência artificial que foram implementadas na empresa até ao momento?

Entrevistado:

Até ao momento estamos a trabalhar com *bots* em sessões mais simplificadas, portanto, em caixas muito estanques, em processos mais simples como identificação de e-mails, registo de pedidos, coisas muito mais funcionais. Ainda não estamos na verdadeira transformação digital da coisa, ou seja, ainda não temos a IA no seu todo a fazer uma tarefa até ao fim, substituindo uma pessoa.

Entrevistadora:

Como é que tu achas que pode vir a ser esse processo de implementação deste tipo de tecnologias? Consideras que houve ou haverá resistência ou mais um entusiasmo por parte dos colaboradores?

Entrevistado:

Verifico alguma desconfiança. Não tanto desconfiança no sentido de correr mal, acho que é mais desconfiança da qualidade do trabalho que se possa vir a desempenhar, e também na possibilidade de extinção de futuro, de postos de trabalho. Sinto que é mais isto.

Implementação de Inteligência artificial

Conhecimento sobre inteligência artificial:

Entrevistadora:

Tens conhecimento de iniciativas ou projetos que envolvam inteligência artificial na empresa e se puderes detalhar alguns deles?

Entrevistado:

Sim. Temos 2 projetos que eu conheço bastante bem. O primeiro é IA no atendimento, portanto, estamos a converter o atendimento telefónico que existe hoje em modelo de IVR.

O IVR é uma plataforma de chamadas que são automaticamente distribuídas, não é também com IA mas sim como um programa de base.

Com IA vamos ter um robot a falar com a pessoa [cliente], e que vai encaminhar a pessoa para um sítio correto da chamada sem haver qualquer ação humana. Neste projeto, este é o primeiro processo que que estamos a desenvolver para IA no seu todo. Depois vamos ter um auto serviço que é o cliente ser identificado no IVR e ter opções como receber condições, saber data do débito do valor do prémio. Também temos outro projeto com inteligência artificial que se vai tratar das caixas de e-mails em que vai haver um *Bot* que vai distribuir o correio ou os e-mails recebidos para as áreas corretas, Sem necessitar também de intervenção.

Aplicações práticas:

Entrevistadora:

Tendo em conta estes dois projetos que tens conhecimento, relativamente às aplicações práticas, em que áreas é que esses processos na seguradora irão ser aplicados e como é que isso impacta o teu trabalho, ou se consideras que isso impacta o teu trabalho?

Entrevistado:

Em termos de impacto IVR vamos ter uma diminuição das chamadas fora de âmbito e, portanto, vamos. melhorar a experiência do cliente, melhorar os tempos de espera, logo, menos custos para a seguradora. Na gestão das caixas de email, vamos ter menos volume de trabalho para as pessoas, diretamente, os e mails serão atribuídos às equipas que que devem tratar, portanto, as equipas das operações vão ser beneficiadas, ficando com mais tempo livre para se dedicarem a outras tarefas.

Benefícios observados

Eficiência operacional:

Entrevistadora:

Quais as melhorias ou benefícios que podes verificar com a implementação da inteligência artificial nos processos da empresa?

Entrevistado:

Sim. Acima de tudo, estamos a tentar rentabilizar o tempo das pessoas, ou seja, quando há processos muito manuais, primeiro podem levar ao erro, e em segundo pelo desgaste da própria pessoa a fazer tarefas muito rotineiras que não acrescentam valor. Penso que este tipo de tarefas passando para máquinas ou robots, liberta as pessoas a fazerem coisas mais produtivas e se calhar ao final do dia lhes traz mais um sentimento, não te pertença, mas sim um dever cumprido.

Atendimento ao cliente:

Entrevistadora:

E tu consideras que haverá a mudanças na forma como os clientes serão atendidos devido ao uso da inteligência artificial? Podes exemplificar?

Entrevistado:

Ainda não estamos a verificar na nossa operação, apesar de estar a acompanhar outras operações que já estão a fazer.

Existe alguma resistência em falar com robots. Verifica-se porque se perde um bocadinho a parte humana, mas melhora a sua qualidade de serviço ao longo do tempo, ou seja, o cliente que seja atendido por um robot, com uma boa experiência, e em que tenha sido resolvido o tema que o levou a contactar, liberta tempo de espera para os outros clientes que precisem de falar com operadores. Portanto, pela minha visão, acho que é um ponto positivo para o atendimento e para a experiência de cliente.

Desafios e considerações éticas

Preocupações éticas:

Entrevistadora:

E agora falando aqui numa parte mais das considerações e preocupações éticas.

Existem preocupações que estejam relacionadas com utilização de inteligência artificial da empresa, como, por exemplo, a privacidade dos dados ou decisões automatizadas, certo?

Entrevistado:

Sim. Transversalmente na área em que trabalhamos e em outras também. No início deste ano foi comunicado já uma nova publicação que se deve aplicar nestes casos. Portanto, a pessoa tem que saber que está a falar com um robot, todos os dados têm que ser gravados em clouds privadas, não podem ser partilhadas entre bases [de dados] porque estes robôs assentam em tecnologia Microsoft, tecnologia da Google, e o que acontece é que tem que ser áreas estanques que não podem ser partilhadas com outras empresas. Quando se está a montar este tipo de projetos e outros, este tipo de situações devem sempre ser acautelados: que não há partilha de dados, garantir sempre a confidencialidade, o tratamento dos dados, por aí.

Segurança da informação:

Entrevistadora:

Como é que a empresa lida com a segurança dos dados processados por sistemas de inteligência artificial? Existem protocolos específicos para o efeito?

Entrevistado:

Sim, existem protocolos específicos de segurança. Neste projeto em concreto, o que fizemos foi uma cloud particular, portanto, não temos uma cloud partilhada com a empresa que nos está a prestar o serviço, e é tudo instalado nesta cloud que é a nossa. Portanto, não há partilha [de dados]. Estes users foram criados em máquinas que não são acessos, da empresa [prestadora de serviços], aos quais nós podemos limitar o acesso, quanto e como quisermos.

Perspetivas futuras

Expectativas de evolução:

Entrevistadora:

Quais é que são as expectativas em relação ao futuro da inteligência artificial na seguradora? Acreditas que haverá uma expansão no uso deste tipo de tecnologia?

Entrevistado:

Sim. Acredito que é o futuro, portanto, será sempre o futuro das empresas. Para as empresas que não avançarem, a transformação digital vai ter um caminho penoso. Já várias empresas estão a adotar a transformação e a transformação digital e a restringir cada vez mais a pessoa humana para a tarefa rotineira porque neste caso, estamos a libertar pessoas para que possam olhar e para fazer melhoria dos outros serviços. Não significa que tenha que haver extinção dos postos de trabalho, não é isso que eu que eu estou a referir, mas podemos converter as pessoas a olhar, não para a tarefa, mas para o negócio ou para o todo como áreas de melhoria.

Preparação e capacitação:

Entrevistadora:

Tens conhecimento se a empresa oferece formações ou certificações para que os funcionários se adaptem às novas tecnologias?

Entrevistado:

A empresa oferece não significa que as pessoas queiram participar.

Encerramento

Entrevistadora:

Existe algum aspeto que tu aches relevante que ainda não tínhamos abordado?

Entrevistado:

Não acho que aprofundámos bastante cada ponto.

Um dos aspetos importantes é a velocidade com que estas transformações ocorrem. Eu acho que é importante, pois não se falava de IA nas empresas. Falava-se num mercado comum, o termo "inteligência artificial" surgia pontualmente, mas à velocidade que estamos a desenvolver conceitos e a aplicá-los, penso que vai ser. verdadeiramente transformador em 5 anos.

Entrevistadora:

Gostarias de acrescentar alguma coisa sobre a implementação da inteligência artificial na organização e de que forma é que pode impactar a ética da mesma?

Entrevistado:

A IA é um dos pilares do futuro, ou seja, todos vamos estar em algum momento ligado a uma IA, seja no telefone, seja nas televisões, seja no nosso dia a dia a trabalhar. Vamos ter ferramentas de IA por todo o lado.

A ética tem de estar sempre a par. Não nos podemos nunca esquecer que são máquinas e que têm mutações, como tudo. Cabe ao ser humano criar essas barreiras para que não haja erros e problemas de no futuro de acessos, de partilha de dados que devam acontecer ou até mesmo outro tipo de situações, como aconteceu recentemente um engenheiro que. queria acabar com uma Ia e ele ameaçou que despedia o engenheiro, algo deste género.

Há que há que ter limites no limite da utilização, passando a redundância, e com isto tem que se criar éticas, legislações e formas de patrono.

Entrevistadora:

Muito obrigada pela tua participação.

Entrevistado:

Obrigada eu.

Anexo 4 - Entrevista 3- Colaborador departamento *Compliance*

Introdução à Entrevista

Olá e muito obrigada pela tua disponibilidade para participar nesta entrevista. Este estudo faz parte de uma investigação académica no âmbito de uma dissertação de mestrado e tem como objetivo compreender como a inteligência artificial está a ser implementada no setor segurador, com especial foco nos benefícios e nos desafios éticos, operacionais e de segurança que essa tecnologia pode representar para os profissionais e para as organizações.

Pretende-se através desta entrevista, escolher a opinião e experiência profissional, tendo em conta o teu contato direto com processos ou ferramentas que possam estar a ser transformadas ou influenciadas por soluções de inteligência artificial.

A tua perspetiva é particularmente relevante por atuar numa área específica, neste caso, o *Compliance*, e será fundamental para compreender como estas tecnologias estão a ser integradas de formas distintas dentro da mesma organização.

A entrevista terá a duração aproximada de 20 a 30 minutos e os dados recolhidos serão utilizados exclusivamente para fins académicos, sendo garantido o anonimato e a confidencialidade de todas as respostas. Com a tua autorização a entrevista será gravada apenas para facilitar a transcrição e posterior análise. Se em algum momento desejares interromper ou retirar a tua participação, podes fazê-lo livremente sem qualquer consequência.

Posso então confirmar que compreende este propósito do estudo e que consentes participar nesta entrevista?

Entrevistado:

Sim confirmo.

Contextualização Profissional:

Entrevistadora:

Pode descrever qual a função atual que desempenha, e há quanto tempo trabalha na empresa?

Entrevistado:

Exerço as funções de Responsável de *Compliance* e acumulo com as de Encarregada de Proteção de Dados (EPD), que são também conhecidas como DPO (Data Protection Officer). As [funções]

de *Compliance* há cerca de 10 anos e as de DPO foi em 2018, na altura em que entrou em vigor o RGPD.

Entrevistadora:

Quais são as suas principais responsabilidades no dia a dia?

Entrevistado:

Como responsável de *Compliance*, tenho de garantir/verificar ou monitorizar que a entidade atua em conformidade com todas as leis, regulamentos e políticas internas aplicáveis à atividade.

Como EPD ou DPO, tenho de prestar aconselhamento e garantir o cumprimento das regras de proteção de dados, tanto para o responsável pelo tratamento quanto para o subcontratante. Adicionalmente existem deveres de cooperação com a CNPD (Comissão Nacional de Proteção de Dados), pois atuo como ponto de contacto para questões relacionadas com a proteção de dados. Também interajo com os titulares de dados e apoio na formação às áreas sobre temas de proteção de dados.

Entrevistadora:

Como descreverias a cultura organizacional da empresa, especialmente no que diz respeito à adoção de novas tecnologias?

Entrevistado:

Diria que a cultura organizacional da empresa é muito centrada na experiência do cliente e isso tem inevitavelmente impacto em matéria de adoção de novas tecnologias. Tudo deve girar à volta do elemento central, que é proteger as pessoas e os seus bens, proporcionando-lhes a melhor experiência possível, sobretudo em situações que podem ser extremamente difíceis, como a ocorrência de sinistros. As soluções tecnológicas acabam por ir beber inevitavelmente aos valores pelos quais a entidade se pauta, sendo a componente de proximidade fundamental nesta equação.

Experiência com Tecnologia:

Entrevistadora:

Que soluções de IA foram implementadas na empresa até ao momento?

Entrevistado:

Sei que existem várias soluções a serem analisadas por diferentes áreas, mas apenas estive diretamente envolvida na avaliação de impacto (no âmbito da proteção de dados) relativamente a uma delas. Esta iniciativa está relacionada com um processo de IVR.

Entrevistadora:

Como foi o processo de implementação dessas tecnologias? Houve resistência ou entusiasmo por parte dos colaboradores?

Entrevistado:

Quando falamos de inteligência artificial, há inevitavelmente um fascínio e entusiasmo pelas enormes potencialidades que as mesmas podem representar. De um modo geral, são acolhidas com enorme entusiasmo pela maioria dos colaboradores. Contudo, as áreas de defesa (2as linhas) das entidades acabam por ter um papel mais difícil que consiste em identificar os riscos que estes processos novos podem conter. Não se trata de oposição nem resistência. Não pretendemos remar contra a inovação. Somos pró-inovação. Contudo, há que identificar riscos e tentar, na medida do possível, mitigá-los ou eliminá-los.

Implementação de Inteligência Artificial

Conhecimento sobre IA:

Entrevistadora:

Tem conhecimento de iniciativas ou projetos que envolvam inteligência artificial na empresa? Pode detalhar?

Entrevistado:

Já falei sobre o tema mais acima.

Aplicações Práticas:

Entrevistadora:

Em que áreas ou processos da seguradora a IA tem sido aplicada? Como é que isso impacta o seu trabalho?

Entrevistado:

A empresa encontra-se atualmente a desenhar um modelo de governo e uma política para um uso responsável destas tecnologias. Estou diretamente envolvida no processo de desenho, pois impactará necessariamente no meu trabalho. Qualquer tratamento de dados pessoais que envolva tecnologia de IA irá inevitavelmente requerer uma avaliação de impacto na proteção dos dados.

Benefícios Observados

Eficiência Operacional:

Entrevistadora:

Que melhorias ou benefícios verificou com a implementação da IA nos processos da empresa?

Entrevistado:

Creio que ainda é prematuro esse tipo de medição, mas no modelo já implementado diria que os benefícios são sobretudo em termos de celeridade dos processos associados sem necessidade de input humano.

Atendimento ao Cliente:

Entrevistadora:

Houve mudanças na forma como os clientes são atendidos devido ao uso de IA? Podes exemplificar?

Entrevistado:

Não sou a melhor pessoa para descrever a componente operativa desta utilização.

Desafios e Considerações Éticas

Preocupações Éticas:

Entrevistadora:

Existem preocupações éticas relacionadas com o uso de IA na empresa, como privacidade de dados ou decisões automatizadas?

Entrevistado:

Claro que sim. É uma das nossas grandes preocupações. Estamos empenhados em criar condições para que a IA seja implementada de forma responsável, ética e segura, respeitando a proteção de dados pessoais.

Segurança da Informação:

Entrevistadora:

Como é que a empresa lida com a segurança dos dados processados por sistemas de IA? Há protocolos específicos?

Entrevistado:

Como referi anteriormente, estamos atualmente a desenhar uma política de IA. Contudo, posso mencionar que serão exigidos aos prestadores de serviços de IA inúmeras garantias de segurança (medidas técnicas e organizativas) que forneçam a robustez adequada aos processos. À semelhança do que aconteceu com o RGPD, também iremos adaptar clausulados contratuais para garantir deveres e obrigações dos prestadores nestas matérias, bem como para imputar e/ou definir responsabilidades.

Perspetivas Futuras

Expectativas de Evolução:

Entrevistadora:

Quais são as tuas expectativas em relação ao futuro da IA na seguradora? Acredita que haverá expansão no uso deste tipo de tecnologia?

Entrevistado:

Não tenho dúvidas que adotaremos muitas soluções com IA a futuro. No passado, quando se falava em IA, as áreas de defesa (risco e *Compliance*) ficavam assustadas. Posso assegurar que temos de passar do medo para o controlo. Há que controlar a operação. Se os riscos forem devidamente identificados e mitigados, diria que todos temos a ganhar. Não podemos parar a

inovação nem a transformação. Temos de ser parte dela. A regulamentação, infelizmente, nem sempre anda à mesma velocidade que a tecnologia, mas a ideia é tentar acompanhar o mais possível.

Preparação e Capacitação:

Entrevistadora:

A empresa oferece formações ou certificações para que os funcionários se adaptem às novas tecnologias baseadas em IA?

Entrevistado:

Esta empresa é uma das melhores para se trabalhar, precisamente porque investe imenso em formação. Não conheço outra entidade tão generosa em dotar os seus colaboradores de ferramentas (formações, certificações, participações em conferências, etc…). Aprender é fundamental. Atualmente estamos a fornecer um curso de três módulos a todos os colaboradores sobre IA. A literacia neste campo é essencial.

Encerramento

Entrevistadora:

Há algum aspeto que ache relevante que ainda não tenhamos abordado?

Entrevistado:

Deixe-me perguntar ao ChatGPT (risos).

Entrevistadora:

Gostaria de acrescentar algo sobre a implementação de IA na organização e de que forma pode impactar a ética da mesma?

Entrevistado:

Apenas posso prometer que é um tema que acompanharei bem de perto nos próximos tempos: com entusiasmo e sem medo! O que é importante é controlar este processo. Uma das formas de o

controlar é precisamente dotá-lo de ética. A validação de projetos deste calibre tem inevitavelmente de passar por um escrutínio ético.

É primordial que se garanta transparência, responsabilidade e capacidade para explicar modelos. Em simultâneo, devem-se evitar riscos e danos como a discriminação, o viés (bias em inglês) e a desinformação, sob pena de não se atuar com justiça ou equitativamente.

A nossa preocupação é, sobretudo, com os nossos clientes. A confiança que depositam em nós é um ativo fundamental. A ética tem, por isso, um papel fundamental na construção ou manutenção desta confiança.

Entrevistadora:

Muito obrigada pela tua participação