INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Mecanismos de mitigação de fraudes: Implementação na última milha no *E-commerce*

Francisca Araújo de Sousa

Mestrado em Gestão

Orientador:
Mestre Abel José de Cruz Camelo, Professor Auxiliar Convidado
ISCTE-Instituto Universitário de Lisboa

Maio, 2025

BUSINESS
SCHOOL

Departamento de Marketing, Operações e Gestão Geral

Mecanismos de mitigação de fraudes: Implementação na última milha no *E-commerce*

Francisca Araújo de Sousa

Mestrado em Gestão

Orientador:
Mestre Abel José de Cruz Camelo, Professor Auxiliar Convidado
ISCTE-Instituto Universitário de Lisboa

Maio, 2025

Agradecimentos

Chegar até aqui foi uma conquista que, em todo o meu percurso, se demonstrou desafiadora e repleta de superação e de pessoas incríveis que, de diferentes formas, tornaram este caminho mais leve e possível. Este trabalho é fruto não só de muita dedicação e vontade, mas também de muito apoio, paciência e incentivo daqueles que estiveram ao meu lado.

Ao meu orientador, Professor Abel Camelo, a minha mais sincera gratidão. O seu conhecimento, disponibilidade e paciência foram essenciais para que esta investigação ganhasse forma.

À minha família, o meu maior alicerce, agradeço por todas as oportunidades que me proporcionaram que me permitiram chegar até aqui, agradeço não so pelo apoio incondicional, mas por acreditarem em todas as minhas capacidades, mesmo quando estas, por vezes, eram invisíveis aos meus olhos.

Aos meus amigos que viveram esta fase perto de mim, que sentiram os diversos estágios de emoções e que sempre me apoiaram, obrigado.

Agradeço profundamente a todos os entrevistados e intermediários cujo envolvimento possibilitou a realização desta pesquisa, obrigado pela sua disponibilidade e simpatia em todo o processo.

Por fim, a todos que, de alguma forma fizeram parte desta trajetória, meu sincero obrigado.

Resumo

O *e-commerce* tem vindo a registar um crescimento exponencial nos últimos anos, assumindo-se como um canal estratégico para a sustentabilidade e expansão das empresas no mercado. Contudo, este crescimento é acompanhado por novos desafios, nomeadamente ao nível da logística de última milha, fase que se demonstra particularmente crítica e vulnerável a fraudes, não só pela necessidade crescente de garantir entregas e devoluções ágeis, como também pelo aumento do número de intervenientes logísticos devido à distância entre o produto e o cliente.

Assim, através da realização de entrevistas a profissionais das áreas da logística, *e-commerce* e fraudes, foi possível obter dados relevantes e reais que permitiram contribuir para o objetivo da investigação, e perceber de que modo as empresas com canal *e-commerce* B2C em Portugal podem combater as fraudes na última milha, apurando as fraudes mais frequentes e os mecanismos de mitigação existentes e em prática.

Os resultados demonstram que, atualmente, apesar das fraudes na última milha não serem percecionadas como um problema significativo, os retalhistas reconhecem a necessidade de monitorização e avaliação contínua das mesmas. Deste modo, é constatável que o grau de adoção de mecanismos antifraude é moderado, sendo ainda limitada a implementação de mecanismos tecnológicos mais avançados.

As conclusões sugerem que, existem diversos mecanismos disponíveis para diferentes realidades empresariais, sendo a sua implementação realizada de acordo com a maturidade digital e operacional, riscos percecionados, tipos de fraudes enfrentadas e recursos disponíveis, necessitando de uma integração gradual de mecanismos tecnológicos à medida que a empresa evolui, visando um equilíbrio eficaz entre mecanismos tecnológicos e processuais.

Palavras-chave: *E-commerce*, Última milha, Fraude Logística, Mecanismos de Mitigação de Fraudes

Classificação JEL: M10 – General Business Administration, L81 – Retail and Wholesale Trade: *E-commerce*

Abstract

E-commerce has experienced exponential growth in recent years, establishing itself as a strategic channel for the sustainability and expansion of companies in the market. However, this growth is accompanied by new challenges, particularly in terms of last-mile logistics, a phase that is particularly critical and vulnerable to fraud, not only because of the growing need to ensure fast deliveries and returns, but also because of the increase in the number of logistics players due to the distance between the product and the customer.

Thus, through interviews with professionals in the areas of logistics, e-commerce, and fraud, it was possible to obtain relevant and real data that contributed to the research objective and to understand how companies with B2C e-commerce channels in Portugal can combat fraud in the last mile, identifying the most frequent types of fraud and the existing and practical mitigation mechanisms.

The results show that, although last-mile fraud is not currently perceived as a significant problem, retailers recognize the need for continuous monitoring and evaluation. It is clear, therefore, that the adoption rate of anti-fraud mechanisms is moderate, and the implementation of more advanced technological mechanisms is still limited.

The conclusions suggest that there are several mechanisms available for different business realities, and their implementation is carried out according to digital and operational maturity, perceived risks, types of fraud faced, and available resources, requiring a gradual integration of technological mechanisms as the company evolves, aiming for an effective balance between technological and procedural mechanisms.

Keywords: E-commerce, Last Mile, Logistics Fraud, Fraud Mitigation Mechanisms

JEL classification: M10 – General Business Administration, L81 – Retail and Wholesale Trade: E-commerce

Índice

Agradecimentos i

Resumo iii

Abstract v

Glossário de Abreviaturas, Siglas e Acrónimos xi

1. Introdução 1

1.1. Contexto e relevância do tema 1

1.2. Problema e foco de investigação 2

1.3. Objetivos 3

1.4. Questões de investigação 4

1.5. Metodologia da investigação 4

1.6. Estrutura da dissertação 6

2. Revisão da Literatura 9

2.1. *E-commerce* 9

2.1.1. Relevância e crescimento do *e-commerce* 10

2.2. Logística no *e-commerce* 11

2.3. Última milha no *e-commerce* 12

2.4. Fraudes na última milha no *e-commerce* 14

2.5. Mecanismos de combate à fraude na última milha 19

2.6. Síntese da revisão da literatura 27

3. Metodologia 31

3.1. Seleção da amostra 32

3.2. Técnica de análise de conteúdos 32

3.2.1. Codificação 33

3.2.2. Categorização 33

3.2.3. Identificação de temas amplos 34

4. Análise e Discussão de Resultados 35
4.1. Amostra 35
4.2. Resultados 36
4.2.1. Desafios potenciadores de fraudes na última milha no *e-commerce* português 36
4.2.2. Fraudes na última milha no *e-commerce* português 37
4.2.3. Mecanismos de controlo e mitigação de fraudes na última milha no *e-commerce* português 42
4.2.4. Grau de adoção dos mecanismos antifraudes nas empresas portuguesas 57
4.2.5. Recomendação de mecanismos por perfil de empresa e recursos disponíveis 60
5. Conclusão 65
5.1. Considerações finais 65
5.2. Contribuições 69
5.3. Limitações da investigação 69
5.4. Sugestões para investigações futuras 70
Referências Bibliográficas 73
Anexos 83
Anexo A – Tabela de estruturação do guião de entrevistas 83
Anexo B - Citações dos profissionais sobre as fraudes na última milha identificadas 84
Anexo C – Mecanismos de mitigação de fraudes na última milha: Fraudes mitigadas e modo de atuação 85
Anexo D – Restrições sumarizadas dos mecanismos antifraudes identificados 86
Anexo E - Justificação dos mecanismos não recomendados para certos perfis de empresas e recursos 87

Índice de Figuras, Gráficos e Tabelas

Figuras

Figura 1.1 - Passos gerais da estruturação da tese.....5
Figura 1.2 - Abordagem funil dos conceitos definidos na Revisão de Literatura.....5

Gráficos

Gráfico 4.1 - Distribuição dos entrevistados por área de atuação e anos de experiência.....36

Tabelas

Tabela 2.1 - Fraudes na última milha identificadas na revisão da literatura 29
Tabela 2.2 - Mecanismos antifraude identificados na revisão da literatura 30
Tabela 4.1 - Tipos de fraudes mencionados.....38
Tabela 4.2 - Mecanismos de mitigação de fraudes na última milha mencionados 43
Tabela 4.3 - Grau de adoção dos mecanismos antifraudes existentes.....58
Tabela 4.4 - Perfis de empresas face à maturidade digital e operacional.....61
Tabela 4.5 - Mecanismos antifraudes recomendados por perfil de empresa e recursos financeiros.....62

Glossário de Abreviaturas, Siglas e Acrónimos

B2C – Business-to-Consumer

DL – Deep Learning

FMCG – *Fast Moving Consumer Goods*

GPS – *Global Positioning System*

IA – Inteligência Artificial

IoT – Internet of Things

MD – Maturidade Digital

ML – Machine Learning

MO – Maturidade Operacional

OECD – Organization for Economic Co-operation and Development

RFID – *Radio Frequency Identification* (Identificação por Radiofrequência)

3PL – *Third Part Logistics*

1. Introdução

O primeiro capítulo desta investigação é elaborado de modo a introduzir o tema em estudo e a estrutura a ser seguida para a investigação em curso, contextualizando a sua relevância no panorama académico e empresarial atual. É posteriormente exposto o problema de investigação, os objetivos e as questões de investigação orientadoras do estudo. Apresenta, igualmente, de forma sucinta, a metodologia de investigação adotada, e, por fim, apresenta uma visão geral da estrutura da dissertação, com a descrição sucinta dos conteúdos abordados em cada capítulo.

1.1. Contexto e relevância do tema

No mercado frenético e digital em que nos encontramos, de alta procura e oferta, as empresas necessitam de investir no *e-commerce* [1], isto é, fazer uso da internet para vender o seus produtos e serviços de forma a manterem-se competitivas e atualizadas às expectativas dos consumidores.

De facto, o *e-commerce* tem vindo a assumir um papel cada vez mais significativo nos modelos de negócio devido ao seu crescimento exponencial verificado nos últimos anos (Dima *et al.*, 2023). Contudo, o crescimento do *e-commerce* traz consigo alguns problemas (Forbes *et al.*, 2005), como o aumento dos desafios enfrentados no processo de última milha (Alverhed *et al.*, 2024).

A última milha caracteriza-se por ser a etapa da logística que ocorre desde o centro de transporte até ao cliente final (Lu *et al.*, 2023), e numa perspetiva de logística inversa, representa a recolha e o transporte do produto devolvido pelo cliente de volta ao centro de distribuição, loja ou ponto de recebimento (DahNAY, 2024). Esta etapa tem sofrido um aumento da sua relevância devido ao crescimento do *e-commerce* (Lu *et al.*, 2023), a separação do espaço físico e do cliente, as múltiplas formas de entregas, o número crescente de devoluções e o distanciamento geográfico dos consumidores surgem como fatores catalisadores para o aumento da complexidade dos processos logísticos de última milha. De facto, logística da última milha é vista como uma das etapas mais desafiantes e críticas (Bauer *et al.*, 2020) e apresenta-se como a atividade mais ineficiente e onerosa de todo processo logístico (Pourrahmani & Jaller, 2021). É nesta etapa onde são estabelecidas as interações diretas com

[1] Devido à ampla adoção internacional e ao alinhamento com a terminologia da literatura académica, ao longo da presente investigação será feito uso do termo inglês para designar comércio eletrónico.

os consumidores, e se abrem mais portas para a ocorrência de fraudes, tanto no processo de entrega quanto no processo inverso, de devolução, e por isso, no contexto de fraudes, o conceito de última milha é usado de forma ampliada para incluir tanto a entrega quanto as devoluções, uma vez que ambas ocorrem na mesma etapa crítica da cadeia e apresentam riscos semelhantes. A ocorrência de fraudes nas devoluções dos produtos é considerada um dos maiores problemas dos grandes retalhistas, dada a sua contribuição na diminuição dos lucros da empresa, contabilizando um decréscimo de 10 a 20% dos lucros (King, 2004 como citado em Shih *et al.*, 2021).

Assim, face ao crescimento do *e-commerce* e à vulnerabilidade a fraudes na logística de última milha, o estudo de mecanismos de combate às fraudes na última milha, surge como um tema de extrema relevância para investigação. Entende-se por mecanismos os controlos, tecnologias, políticas, procedimentos, estratégias e práticas que permitem prevenir, detetar e mitigar as fraudes na última milha. Deste modo, ao recorrer a dados empíricos obtidos através de entrevistas a profissionais do setor, este estudo contribui para reduzir a lacuna entre o conhecimento teórico e a realidade prática das organizações, oferecendo uma perspetiva atualizada, contextualizada e validada por experiências reais. Neste sentido, alarga a compreensão académica sobre os riscos logísticos emergentes e as estratégias de resposta que as empresas adotam, ou deixam de adotar, em função da sua maturidade digital e operacional e recursos, abrindo assim espaço para explorar recomendações de melhorias. Deste modo, a utilidade desta investigação estende-se à formação académica de gestores, profissionais de logística e investigadores, ao fornecer um quadro analítico que articula teoria, prática e inovação no combate às fraudes. Numa vertente empresarial, esta investigação permite identificar boas práticas e oferecer orientações valiosas que podem ser adotadas pelas empresas, sendo sobretudo relevante para empresas menos conscientes dos riscos ou das soluções disponíveis. Assim, o estudo possibilitará às empresas proteger a sua saúde financeira e garantir a confiança do consumidor, garantindo a competitividade das operações de *e-commerce* e, em simultâneo, melhorar algumas vulnerabilidades da última etapa do processo logístico.

1.2. Problema e foco de investigação

Com o desenvolvimento das plataformas digitais e o crescimento exponencial do *e-commerce* surgem mudanças nas estruturas tradicionais das empresas (Lee, 2012). Estas mudanças vêm acompanhadas por oportunidades e desafios que carecem de alguma análise.

O desenvolvimento do *e-commerce* desencadeou um aumento significativo nas entregas diretas aos clientes, acabando por fortalecer a importância do papel da logística da última milha tornando-a cada vez mais complexa, dinâmica (Viu-Roig & Alvarez-Palau, 2020) e mais vulnerável. Por conseguinte, as trocas diretas ocorridas no *e-commerce* permitem, por vezes, eliminar alguns intermediários, como operadores de caixa e lojistas, tanto numa fase de compra como numa fase devolução, em contrapartida de um aumento dos intervenientes logísticos. Deste modo, o aumento de intervenientes logísticos e a eliminação do contacto físico direto abrem portas à ocorrência de fraudes na última milha (Westland, 2022), que impactam negativamente as empresas, devido à existência de mais pontos de risco (transporte, *hub*, ponto de recolha), à falta de verificação física dos produtos no momento de compra e devolução, e à dependência de dados digitais, que podem ser mais facilmente manipulados, pirateados ou falsificados.

Deste modo, o elevado número de fraudes na última milha ocorrentes no seio das empresas que utilizam o canal de *e-commerce* apresenta-se como um problema crítico, de gestão que carece de análise e reflexão, sendo, consequentemente, o problema foco a ser endereçado na presente investigação.

Por conseguinte, de forma a endereçar o problema identificado é estabelecido o foco da investigação que, numa perspetiva macro, remete à perceção de como as empresas portuguesas, que implementam no seu modelo de negócio o canal *e-commerce*, podem mitigar as fraudes na última milha.

1.3. Objetivos

Atendendo ao problema do setor apresentado e ao foco da investigação, definem-se os seguintes objetivos específicos:

- **(OE1)** Identificar os desafios enfrentados na última etapa do processo logístico potenciadores de fraudes;
- **(OE2)** Identificar os principais tipos de fraude na última milha;
- **(OE3)** Identificar e avaliar os mecanismos disponíveis para o combate à fraude;
- **(OE4)** Identificar quais os principais desafios na implementação dos mecanismos de combate a fraude;

- **(OE5)** Compreender o grau de adoção de mecanismos de combate à fraude por parte de empresas que utilizam o canal de *e-commerce*.

1.4. Questões de investigação

De modo a concretizar os objetivos descritos no subponto anterior, são formuladas as seguintes questões de investigação:

Questão 1: Quais são os desafios enfrentados na última milha no *e-commerce* potenciadores de fraudes?

Questão 2: Quais são as principais fraudes na última etapa do processo logístico no *e-commerce*?

Questão 3: Como podem as principais fraudes na última milha ser mitigadas e quais os mecanismos de combate e os seus desafios de implementação, num contexto de *e-commerce*?

Questão 4: Qual é o grau de adoção dos mecanismos antifraudes identificados num contexto real de empresas que utilizam o canal de *e-commerce*?

1.5. Metodologia da investigação

A presente tese segue o formato de dissertação que assenta num design de pesquisa qualitativo experimental, por meio da realização de entrevistas semiestruturadas. Posto isto, de forma a realizar a investigação, procede-se à definição de um design de investigação de modo a estabelecer os passos gerais da estruturação da mesma. O design de investigação caracteriza-se por um planeamento lógico e estruturado, elaborado de modo a orientar um estudo de forma eficiente e organizada. Este design define os objetivos do estudo, a metodologia e as técnicas a serem empregues para alcançar os objetivos definidos (Khanday & Khanam, 2019).

Posto isto, para a concretização da tese são seguidos os seguintes passos estruturados:



Figura 1.1 - Etapas da Investigação

Fonte: Elaboração própria

Assim, na elaboração preliminar é descrita a relevância do tema em investigação, bem como os objetivos e questões de investigação e, o problema adjacente ao estudo.

Numa segunda instância, procede-se à realização da revisão de literatura. Deste modo, atendendo à problemática e aos objetivos estabelecidos, apresenta-se na Figura 1.2 os principais conceitos abordados nesta etapa.



Figura 1.2 - Abordagem funil dos conceitos definidos na Revisão de Literatura

Fonte: Elaboração própria

Para a concretização da revisão de literatura, procede-se à realização de uma fase de pesquisa e seleção onde são recolhidos artigos e fontes de informação necessárias para a

conceptualização dos conceitos referidos. Após a seleção procede-se ao entendimento do conteúdo recolhido e por fim ao desenvolvimento da revisão de literatura sustentada pelos autores e fontes selecionadas na fase de seleção.

Na terceira fase, na recolha de dados, pretende-se verificar quais são os mecanismos implementados em empresas reais, de modo a verificar se as empresas usufruem dos mecanismos ao seu dispor para combater as fraudes, usufruindo, deste modo, de uma abordagem qualitativa através da implementação de entrevistas semiestruturadas com profissionais com experiência profissional em empresas que utilizam o canal de *e-commerce*.

Na fase de análise e discussão dos resultados, realiza-se uma análise de conteúdo para analisar aprofundadamente os dados obtidos, seguida do cruzamento dos dados recolhidos na fase de entrevistas com os mecanismos identificados na literatura, auferindo desta forma o enquadramento entre a teoria proposta por investigações académicas e a prática efetivada no mercado real, permitindo uma reflexão crítica sobre as dinâmicas observadas no mercado real, contribuindo assim para uma compreensão mais aprofundada do tema. Por fim, após a análise dos dados obtidos estruturam-se recomendações para as empresas combaterem o problema das fraudes na última milha.

Por último, na fase das considerações finais, retiram-se as conclusões principais da investigação respondendo a cada questão de investigação formulada e identificam-se as limitações do estudo permitindo assim sugerir recomendações para investigações futuras.

1.6. Estrutura da dissertação

A estrutura da dissertação reparte-se em cinco capítulos sendo estes a Introdução, a Revisão de Literatura, a Metodologia, a Análise e Discussão de Resultados e, por fim, a Conclusão. Assim, a investigação reparte-se da seguinte forma:

Capítulo 1 – Introdução: Este capítulo é referente à etapa da elaboração preliminar mencionada no subponto anterior. Neste capítulo é abordado o tema em investigação e a relevância do estudo, bem como o problema adjacente, os objetivos da investigação e as questões de investigação.

Capítulo 2 – Revisão de Literatura: Neste capítulo é realizada uma conceptualização dos conceitos mais importantes para o entendimento do tema em estudo, recorrendo a uma

abordagem teórica assente em artigos científicos e websites de empresas e organizações. Desta forma, em primeira instância, são introduzidos conceitos de *e-commerce* bem como dados sobre o seu crescimento e a sua relevância no seio das empresas. Posteriormente, introduz-se o conceito de logística, a sua importância no setor do *e-commerce* e os desafios enfrentados no processo logístico da empresa, de modo a introduzir em seguida o conceito de última milha, bem como os desafios enfrentados no canal de *e-commerce* nesta etapa logística. Numa terceira instância é conceptualizado o conceito de fraudes e os possíveis impactos das mesmas, identificando de seguida as principais fraudes na última milha existentes no canal de *e-commerce* e os mecanismos existentes para mitigá-las. Por fim, é realizada uma síntese de toda a revisão de literatura de forma a reunir, num único ponto, as informações mais relevantes para o entendimento do tema em estudo.

Capítulo 3 – Metodologia: Neste capítulo apresenta-se a abordagem metodológica a seguir para a realização da investigação, sendo esta, uma abordagem qualitativa por meio de entrevistas semiestruturadas analisadas através de uma análise de conteúdo.

Capítulo 4 – Análise e Discussão de Resultados: Este capítulo centra-se na exploração aprofundada das informações recolhidas nas entrevistas. São, portanto, analisados e discutidos os desafios de última milha, enfrentados pelos retalhistas no mercado português, que tornam o processo logístico vulnerável a fraudes; os diferentes tipos de fraudes identificadas pelos entrevistados, bem como os mecanismos de prevenção, detenção e/ou de combate aplicados nas organizações com as quais os participantes detêm conhecimento ou contacto direto. Neste capítulo são vistas ainda, de uma forma integrada com a análise, as barreiras enfrentadas pelas empresas na implementação de práticas de mitigação das fraudes na última milha e o grau de adoção dos mecanismos disponíveis por parte das empresas. Por fim, são realizadas recomendações de mecanismos para empresas de *e-commerce* com base nos resultados obtidos, procurando contribuir para a melhoria das práticas de combate às fraudes na última milha ocorrentes no *e-commerce* B2C português.

Capítulo 5 – Conclusão: O último capítulo apresenta as principais conclusões do estudo, resultantes da análise dos dados à luz dos objetivos e questões de investigação. Este capítulo inclui ainda a reflexão sobre as limitações da investigação e termina com sugestões para estudos futuros, de forma a incentivar a continuação da exploração académica nesta área.

2. Revisão da Literatura

No presente capítulo apresentam-se conceitos teóricos fundamentais para o exercício da investigação. Em primeira instância abordam-se conceitos relacionados ao *e-commerce* de forma a compreender a base do tipo de negócio em estudo. De seguida, introduz-se o conceito de logística de modo a introduzir a etapa logística em foco na investigação, a última milha no *e-commerce*. Ainda neste capítulo abordam-se as principais fraudes na última milha, identificadas em investigações académicas e em empresas logísticas, e os mecanismos de mitigação que podem ser utilizados pelas empresas no combate a este tipo fraudes. Para isto, a revisão é sustentada na literatura existente e em informações de empresas relacionadas à área de logística e *e-commerce*.

2.1. *E-commerce*

Ao longo dos últimos anos o conceito de comércio eletrónico, também conhecido por *e-commerce*, tem sido alvo de diversas definições que mudam em consonância com a sua evolução e destaque no mercado. Desde meados dos anos 90 que o *e-commerce* tem sofrido rápidos desenvolvimentos, e por isso, devido ao seu crescimento exponencial, surgiu a necessidade de definições mais específicas e aceites internacionalmente de modo a monitorizar esta nova forma de comércio (Kunešová & Eger, 2017).

A Organization for Economic Co-operation and Development (OECD) (2013) e a Eurostat (2015) definem as transações de *e-commerce* de forma semelhante.

> A venda ou compra de bens ou serviços conduzida por redes de computadores por métodos especificamente projetados para o propósito de receber ou fazer pedidos; pagamento e entrega não são considerados. As transações podem ocorrer entre empresas, famílias, indivíduos, governos e outras organizações. A definição inclui pedidos feitos por meio de páginas web, extranet ou EDI e exclui pedidos por telefone, fax ou e-mail digitado manualmente (OECD, 2013, p.226).

Stallmann e Wegner (2014, p.6) empregam uma definição que caracteriza *e-commerce* como “a soma de todos os processos digitais de iniciação, negociação e/ou liquidação de transações comerciais entre entidades económicas que são realizadas através da internet. O foco está na compra e venda de bens e serviços".

Para efeitos da presente investigação, o conceito de *e-commerce* baseia-se na perspetiva de Lee (2012) que define *e-commerce* como o processo de compra, venda ou troca de produtos, serviços e informações fazendo uso das redes de telecomunicações.

O *e-commerce* pode ser classificado com base em diversas categorias (Kunešová & Eger, 2017), contudo, para o presente estudo, o foco recairá sobretudo no *e-commerce* Business-to-Consumer (B2C), ou seja, num modelo de negócios em que as transações ocorrem entre a empresa e os consumidores finais por meio da internet.

2.1.1. Relevância e crescimento do *e-commerce*

Segundo os autores Ngai & Wat (2002) e C.-C. Wang & Chen (2010) muitas empresas passaram a ver o *e-commerce* como uma prioridade no seu negócio. A possibilidade dada à empresa de melhorar a sua competitividade no mercado através da conexão com os seus parceiros comerciais e a popularidade do uso da internet como meio dos consumidores efetuarem compras e vendas de produtos ou serviços, foram fatores determinantes para o aumento da relevância da inclusão do *e-commerce* nos modelos de negócio (Ngai & Wat, 2002; Forbes *et al.*, 2005).

O número de utilizadores de internet tem vindo a crescer ao longo dos últimos anos de forma exponencial. Segundo Petrosyan (2024), em 2023 foram registados 5,4 mil milhões de utilizadores de internet em todo mundo, representando 67% da população mundial.

Na verdade, a internet e o desenvolvimento de dispositivos movéis proporcionaram um aumento do número de utilizadores que efetuam compras online, o que contribuiu para a oportunidade dos retalhistas aumentarem as vendas por meio eletrónico (Nguyen *et al.*, 2018). Segundo dados do Statista (2024), em Portugal, estima-se que a receita do mercado de *e-commerce* atinja cerca de 5,38 milhões de US dólares, com uma taxa de crescimento anual estimada em 8,95% até 2029, representado assim uma tendência crescente deste canal de negócios. De facto, a venda a partir de plataformas digitais tem se tornado cada vez mais popular devido à conveniência e acessibilidade oferecida por este serviço. Por vezes, os compradores não possuem tempo disponível para recorrer a lojas físicas, o que leva a um aumento do número de transações online que requerem entregas ao domicílio. Deste modo, os consumidores recorrem cada vez mais a formas de compras modernas e eficientes que sejam capazes de satisfazer as suas necessidades (Suska, 2022 como citado em Dima *et al.*, 2023).

Dado ao aumento verificado nos últimos anos na adesão à realização de compras online (Coppola, 2024), torna-se possível reforçar a premissa inicial da importância da adaptação dos modelos de negócios ao *e-commerce*, de modo a cobrirem as necessidades dos clientes e prosperarem no mercado. Para as empresas, o *e-commerce* traz também inúmeras vantagens como a possibilidade de expansão nos mercados, a redução de custos, maior eficiência e a possibilidade de interação 24 horas diárias sobre 7 dias por semana com todos os consumidores (Lazić *et al.*, 2024).

O autor Lazić *et al.* (2024), em semelhança a Nagai e Wat (2002) também defende a necessidade da priorização do *e-commerce*. Segundo o autor o mundo enfrenta atualmente a transição da Indústria 4.0 para a Indústria 5.0 e, por isso, as empresas necessitam fazer uso do *e-commerce* de modo a atender a requisitos do mercado do futuro que contemplam ambientes inteligentes, isto é, que permitam a interação entre o digital e o espaço real. Com isto, é possível afirmar que com o passar do tempo, a forma de comércio tradicional ocorrente em espaços físicos sem uso de plataformas digitais deixará de ser capaz de satisfazer os requisitos modernos e, por conseguinte, será cada vez mais necessário o uso de estruturas operacionais inovadoras (Cegarra-Navarro *et al.*, 2007; Silva *et al.*, 2022) como o *e-commerce*.

De uma forma sumária, é possível auferir que o desenvolvimento do *e-commerce* trouxe consigo uma mudança dos formatos de retalho, elevando cada vez mais a importância deste canal de venda. Deste modo, os grandes retalhistas viram a necessidade de aumentar os desenvolvimentos no *e-commerce* B2C (G. Wang *et al.*, 2023) de forma a fazer proveito dos seus benefícios. Por conseguinte, o desenvolvimento do serviço logístico surge como um fator de extrema relevância para o sucesso do desenvolvimento e da sustentabilidade do *e-commerce* (G. Wang *et al.*, 2023).

2.2. Logística no *e-commerce*

Como visto, o desenvolvimento do *e-commerce* assenta-se sobre a popularização da internet. As transações neste tipo de comércio ocorrem inicialmente através do aproveitamento da velocidade da internet, da segurança e da confiabilidade do suporte em rede, tornando possível uma interação ágil entre o fluxo de informação e o fluxo de capital (movimentações de dinheiro) com os consumidores. Numa fase posterior, ocorre o fluxo físico, onde os bens são entregues aos consumidores por meio de serviços logísticos e, após confirmarem o recebimento, os consumidores finalizam a transação (Wu *et al.* 2017 como citado em G. Wang *et al.*, 2023).

Contudo, para todo este processo ser assegurado é necessário um grande suporte logístico, sobretudo num modelo B2C onde a entrega eficiente de produtos físicos é fundamental para garantir a sobrevivência da empresa no mercado (G. Wang *et al.*, 2023).

Segundo G. Wang *et al.* (2023), embora o fluxo de capital e de informações ocorram de forma instantânea no ambiente digital, a entrega física dos produtos ao consumidor depende da logística. A logística é um processo que inclui o armazenamento, a gestão de stocks, o processamento de pedidos e a distribuição dos produtos, configurando assim operações vitais para uma conclusão bem-sucedida das transações. Num modelo B2C, o cliente acede ao site e faz um pedido, a organização comercial recebe este pedido e procede ao despacho das mercadorias para o cliente final conforme os termos acordados (Yu *et al.*, 2017; Adeniran *et al.*, 2022). Assim, de modo a garantir o sucesso deste processo, deve ser realizada uma logística eficiente que garanta a eficiência de todo o processo de entrega, desde a criação do pedido até à entrega do produto ao cliente (Hofmann & Rüsch, 2017). De uma forma inversa, o processo de logística inversa, garante que, em caso de devolução, haja um processo implementado que permita ao cliente devolver o seu produto ao retalhista (Gomes *et al.*, 2023).

Posto isto, a logística deve exercer uma função dinâmica e flexível, e ser capaz de se moldar às diversas restrições e demandas impostas no ambiente onde opera (Adeniran *et al.*, 2022). De certa forma, pode-se resumir logística pela agregação de três componentes, a de abastecimento, a de gestão de materiais e a componente de distribuição (Adeniran.*et al.*, 2022), sendo completada pela logística inversa que permite o retorno do produto seguindo um fluxo contrário, indo do cliente ao retalhista, e que termina com a extração do valor máximo desse produto por parte do retalhista, através da revenda, remanufatura ou reciclagem dos produtos devolvidos (Blackburn *et al.*, 2004; Hall *et al.*, 2013).

Posto isto, tal como afirma Y. Wang *et al.* (2020), com o aumento contínuo da popularidade das compras online, as empresas devem adotar práticas logísticas eficientes de modo a diminuir custos, a atender as necessidades e expectativas dos clientes digitais e deste modo garantir uma vantagem competitiva no mercado.

2.3. Última milha no *e-commerce*

O desenvolvimento do *e-commerce* e o paradigma crescente das compras online tornaram-se o novo normal. Contudo esta nova normalidade acarreta desafios drásticos na última milha (Viu-Roig & Alvarez-Palau, 2020).

Para a presente investigação é importante considerar tanto a epata de entrega de última milha como a logística inversa de última milha, sendo que, num contexto de análise de fraudes na última milha é relevante abordar o processo de entrega e de devolução, sendo assim ambos contidos no conceito de última milha.

A relevância da entrega de última milha tem vindo a desapegar-se ao longo dos anos da ideia de atividade de suporte, configurando atualmente uma componente essencial e crítica nas atividades das empresas (Bauer *et al.*, 2020). Este processo incentivou os retalhistas a investirem em diversas formas inovadoras de entregas, como compras feitas online com possibilidade de levantamento em loja física, entrega ao domicílio, em cacifos e pontos parceiros, entregas realizadas por veículos autónomos e, entregas gratuitas a partir de um determinado valor de compras (Lim *et al.*, 2017 como citado em Lim *et al.*, 2018).

Nos seus primórdios, o contexto de última milha era usado sobretudo pela indústria de telecomunicações (Lim *et al.*, 2018), contudo, com o tempo e o desenvolvimento do cenário empresarial e a globalização das cadeias de abastecimento, a última milha tornou-se um termo principalmente relacionados à logística e cadeia de abastecimento. Assim, apesar das múltiplas definições de entrega de última milha existentes, na presente investigação, é feito o uso da definição comumente aceite, sendo assim definida como "o último trecho de um serviço de entrega de encomendas business-to-consumer (B2C). Ocorre do ponto de penetração do pedido até o ponto de destino escolhido pelo destinatário final" (Lim *et al.*, 2018, p.310). O ponto de penetração do pedido refere-se ao local onde o stock é mantido e onde o pedido do cliente entra e ativa o processamento da encomenda do cliente (Lim *et al.*, 2018).

A entrega de última milha apresenta-se de facto como a atividade mais ineficiente e onerosa do processo logístico (Pourrahmani & Jaller, 2021). Segundo o relatório da Capgemini (2021), a logística da última milha representa cerca de 41% dos custos totais da cadeia de abastecimento, representado mais do dobro de qualquer outra categoria de despesas nesta cadeia. Esta ineficiência e os custos elevados devem-se, principalmente, a exigências complexas dos serviços que configuram desafios logísticos, devido à necessidade de entregas rápidas e precisas, uma vez que os prazos de entregas estão cada vez mais reduzidos devido à necessidade das empresas satisfazerem as necessidades dos consumidores em relação à rapidez e eficiência (Allen *et al.*, 2018), à pequena dimensão das encomendas, isto é, pedidos pequenos e individuais que tornam o custo por entrega mais alto em relação a entregas em massa e, por fim, devido à grande dispersão geográfica dos pontos de entrega, que tornam o percurso mais

longo e menos eficiente, aumentando não só os custos com transporte e tempo (Macioszek, 2018), como também as vulnerabilidades a fraudes. Deste modo, esta etapa aufere um grande encargo nos resultados financeiros das empresas.

Por sua vez, o processo oposto à entrega, isto é, o fluxo de produtos dos consumidores finais para as empresas, envolvendo o processo de recolha e processamento de devoluções de produtos, denomina-se por logística inversa (Shih *et al.*, 2021; Gomes *et al.*, 2023). Este fluxo é representado pelas trocas ou devoluções efetuadas pelos clientes após uma compra. Após a entrega de uma encomenda, cerca de 20 a 30% dos clientes tendem a efetuar a devolução dos produtos por variados motivos, por vezes por descontentamento, defeitos dos produtos, entrega dos produtos errados, produto danificado, descrições incompatíveis com a realidade do produto, arrependimento de compra ou por intenções fraudulentas ("5 Strategies for Retail Businesses to Reduce Last Mile Reverse Logistics Costs", 2022; Shih *et al.*, 2021; Ülkü & Gürler, 2018; Nguyen *et al.* 2018).

Assim, de forma a que as empresas se consigam manter competitivas, necessitam de garantir um processo de última milha eficiente, tanto nas entregas quanto devoluções. Para tal devem efetuar um processamento de pedidos rápido, realizar uma logística inversa contínua, reduzir os custos logísticos e atender às novas expectativas dos clientes por entregas rápidas, tudo isto num cenário de margens de lucro geralmente reduzidas devido ao excesso de concorrência (Hugos, 2015 como citado Gomes *et al.*, 2023; Gomes *et al.*, 2023; Richards, 2017; Silva *et al.*, 2022; Oláh *et al.*, 2018). Contudo, à medida que o *e-commerce* ganha peso e a integração dos canais online-offline se desenvolve, os comportamentos fraudulentos ocorrentes na última milha também se intensificam, o que configura um problema cada vez mais significativo para as empresas, contribuindo para perdas anuais de milhões de dólares (Stefanova & Stoyanova, 2023; Shih *et al.*, 2021).

2.4. Fraudes na última milha no *e-commerce*

Os riscos e desafios enfrentados na logística de última milha incluem variados fatores que podem comprometer a segurança e proteção dos produtos encomendados (Stefanova & Stoyanova, 2023).

O *e-commerce* permitiu estabelecer transições diretas com os consumidores, não necessitando geralmente de vendedores físicos ou operadores de caixa, diminuindo assim o nível de intermediários comuns do comércio tradicional. Contudo, esta diminuição, e a

consequente redução de processamentos monitorizados por humanos, em conjunto com o aumento de intervenientes logísticos necessários para fazer chegar a encomenda até ao cliente, ou do cliente ao retalhista (devoluções), configuram fatores que contribuem para o aumento de vulnerabilidades a fraudes (G. Wang *et al.*, 2023; Westland, 2022).

Segundo a Association of Certified Fraud Examiners (s.d.), fraude pode ser definida como qualquer atividade que se baseie no ato de enganar, uma pessoa singular ou uma organização, de forma a obter algum ganho.

Devido às altas pressões por parte dos consumidores por entregas rápidas, os retalhistas de *e-commerce* por vezes, tendem a ignorar alguns requisitos de segurança, tornando a cadeia de abastecimento mais vulnerável. Contudo, a existência de fraudes não está apenas relacionada a descuidos de segurança por parte dos retalhistas, existem evidências empíricas que comprovam que tanto os clientes quanto os funcionários e parceiros exercem conscientemente ações fraudulentas que prejudicam as empresas (Reynolds & Harris, 2005; Harris & Ogbonna, 2006).

As compras online proporcionaram uma distância entre consumidor e produto, impossibilitando o consumidor de tocar, sentir ou experimentar um produto, o que impulsiona o aumento constante da percentagem de devoluções no *e-commerce* (Salem & Alanadoly, 2024). De facto, esta distância influenciou os retalhistas a adotarem políticas de devoluções generosas de forma a atrair mais clientes, todavia, estas políticas conduzem a um acréscimo do número de produtos devolvidos, que por sua vez conduz a perdas de oportunidades de revenda dos produtos e a aumentos nos custos associados à gestão da logística inversa (Yan & Pei, 2019), contribuindo em simultâneo para a diminuição dos lucros do retalhista (Zhao *et al.*, 2020). Além disso, alguns consumidores acabam por fazer mau uso das políticas de devoluções estabelecidas pela empresa, envolvendo-se em práticas como devoluções oportunistas e devoluções fraudulentas (Liu & Du, 2023).

A devolução oportunista, trata-se de uma devolução feita por um cliente, que, embora tenha usado o produto, decide devolvê-lo para obter um reembolso em troca, aproveitando-se da existência de políticas de devoluções generosas (Sampaio, 2022). Este tipo de devoluções pode ser fraudulento se a devolução não for de acordo com os termos das políticas da empresa (Zhang *et al.*, 2023).

A devolução fraudulenta, é um tipo de fraude que ocorre no processo de última milha, caracterizada pelo ato do consumidor devolver um produto ao retalhista, ciente que tal devolução é contrária às normas e regulamentações legais ou às políticas da empresa aplicáveis,

incluindo por vezes a devolução de produtos funcionais, mas usados ou danificados pelo próprio cliente (Harris, 2008; Shih *et al.*, 2021).

Para além de fraudes de devolução existem fraudes de reembolso. A diferença entre estes dois tipos de fraude é que a primeira envolve a devolução da mercadoria de modo a reaver o dinheiro enquanto a segunda manipula o processo de reembolso sem existir necessariamente a devolução do produto (SEON, s.d.).

Uma forma de fraude nas devoluções é a fraude de devolução arbitrária de preços. Este tipo de fraude engloba alguns tipos de fraude como, a troca de mercadorias, onde os compradores encomendam um produto e ao efetuar a sua devolução substituem o produto comprado por um item falsificado, roubado ou por um semelhante, mas mais barato, e pedem reembolso total, ou então, devolvem uma versão mais antiga do produto ou um produto igual que já não funciona, utilizando a embalagem da mercadoria mais recente para efetuar a devolução (Zhang *et al.*, 2023; Shih *et al.*, 2021).

Por vezes, existem devoluções de produtos sem as peças de valor originais, a esta fraude dá-se o nome de *bricking*. Esta fraude também se encontra dentro da categoria de fraudes de devolução arbitrária de preços, sendo mais frequente em produtos de maior valor (Zhang *et al.*, 2023). O objetivo é utilizar ou revender as peças retiradas obtendo lucro e ainda pedir o reembolso à empresa onde comprou o item original através da devolução do produto.

Uma outra forma de devolução arbitrária de preços no *e-commerce* é a fraude de reembolso entre retalhistas, nesta fraude o consumidor compra um produto a um preço inferior e depois devolve-o sem recibo a outro retalhista que vende o produto a um preço superior, conseguindo desta forma ganhar pelo diferencial de preços (Zhang *et al.*, 2023).

De uma forma semelhante, a fraude de descontos, também permite ao infrator obter ganhos pelos diferenciais de preço ou ofertas promocionais, podendo ocorrer de três formas: (1) quando o consumidor compra o produto com desconto online, e pede o reembolso em loja física sem o recibo ou com o recibo falsificado; (2) quando o consumidor devolve itens incluídos em campanhas promocionais, como as de leve 2 pague 1 por exemplo, e tenta devolver o produto gratuito; (3) quando o consumir abusa do sistema de recompensas, realizando uma compra para obter pontos ou créditos de forma a usá-los na totalidade e depois devolver os produtos iniciais pelos quais pagou, ficando apenas com os adquiridos com os créditos (Zhang *et al.*, 2023).

Existe também a fraude de reembolso em múltiplos canais, onde, após receber o produto, o cliente solicita reembolsos pelos diversos canais da empresa, como telefone, loja online e loja física, explorando a falta de atualização entre os sistemas de atendimento e obtendo desta forma múltiplos reembolsos pelo mesmo item (Zhang *et al.*, 2023).

A fraude de *chargeback*, está também relacionada a pedidos de reembolso, contudo, ao contrário da anterior, o cliente após a receção da encomenda, entra em contacto direto com o banco associado ao pagamento para anular a transação por um motivo ilegítimo, como alegações falsas de produto não entregue ou de encomendas com defeitos. Existem vias de pagamento mais propícias a serem utilizadas para a tentativa deste tipo de fraude (como por exemplo o Paypal), pois geralmente tendem a favorecer o consumidor em detrimento do retalhista (Zhang *et al.*, 2023).

Por sua vez, o *wardrobing*, é um tipo fraude na última milha onde clientes adquirem um produto com o propósito de o usarem numa ocasião específica e, após o uso, devolvem-no para obterem o reembolso (Piron & Young, 2000; Zhang *et al.*, 2022).

Existe ainda a fraude de *jiffy bag*, onde o consumidor procede ao pedido de devolução e devolve uma caixa vazia, sem o produto que deveria ser devolvido, mas altera o comprovativo de envio de forma a mostrar que o peso do que enviou corresponde ao peso correto do produto original, ou coloca um material pesado para equivaler o peso do artigo. Deste modo o consumidor solicita o reembolso, fingindo que devolveu o produto real (Zhang *et al.*, 2023).

As devoluções fraudulentas impactam negativamente os lucros de uma empresa, podendo desencadear uma diminuição de 10 a 20% dos lucros, configurando deste modo uma preocupação crescente no seio dos retalhistas (King, 2004 como citado em Harris, 2008). De facto, as fraudes contribuem para desperdício de tempo, de recursos e de mão de obra necessária para processar todo o processo de devolução, aumentam as taxas administrativas relacionadas aos pedidos de reembolsos e aumentam os esforços de comunicação (Shih *et al.*, 2021). Para além disso, os retalhistas enfrentam um paradoxo, por um lado necessitam de políticas de devolução mais apertadas, por outro, sabem que isso pode prejudicar a reputação da marca e afetar as vendas negativamente (SEON, s.d.).

Por outro lado, existem fraudes que estão relacionadas à entrega das encomendas, como a fraude de produtos não recebidos. É uma fraude bastante popular onde os consumidores alegam falsamente que não receberam a sua encomenda na totalidade ou que receberam as encomendas, mas que faltam artigos ou peças ou ainda que chegaram peças danificadas, de forma a pedir o

reembolso e ficar com o produto ou obter uma substituição gratuita de modo a duplicar os itens encomendados (Zhang *et al.*, 2023; Sampaio, 2022; Purolator, 2023).

Adicionalmente, existem empresas que compensam os consumidores caso o tempo de encomenda seja superior ao previsto, e, portanto, há clientes fraudulentos que se aproveitam desta política para exercer comportamento fraudulentos alegando que o produto foi entregue com atraso, mesmo que tenha chegado dentro do prazo, com o intuito de pedir um desconto, reembolso parcial ou acumular créditos, praticando desta forma uma fraude por falsa reclamação de atraso de entrega (Zhang *et al.*, 2023)

Por sua vez, o roubo de encomendas, é também uma fraude ocorrente na última etapa do processo logístico e caracteriza-se por furtos realizados durante o embalamento de encomendas, no transporte, no ponto de recolha, no momento de entrega ou quando o produto é deixado sem vigilância à porta do cliente, não sendo esta última frequente em Portugal (Purolator, 2023). Apesar de roubo não configurar fraude em sentido estrito, no contexto logístico e empresarial muitas vezes o roubo é tratado dentro da categoria de fraudes operacionais, pois ambos resultam em perda e requerem controlos de prevenção e segurança similares, e como tal, na presente investigação o roubo de encomendas é tratado como uma fraude na última milha.

Por último, e podendo também estar relacionada com a fraude de roubo, a fraude de manipulação de endereço, ocorre quando o infrator altera a morada de entrega após a realização do pedido, mas antes do envio, de modo a levar a encomenda para um endereço falso ou incompleto, ou de um cúmplice ou ainda um ponto de entrega diferente ao inicialmente selecionado de modo a alegar que nunca recebeu a encomenda e reclamar uma compensação pelo infortúnio ou não pagar pelo serviço de entrega. Assim, a entrega pode não ficar devidamente registada e por isso a empresa não consegue comprovar quem realmente recebeu a encomenda, dificultando a recuperação dos bens desviados, pelo próprio cliente, de modo a pedir o reembolso pelo produto que alegadamente não recebeu, ou por outras pessoas com o intuito de deter a posse da mercadoria (ANANSI, s.d.).

É importante ressaltar que o custo real associado às fraudes vai além do custo de reembolso, inclui também despesas operacionais com investigações, medidas preventivas e gestão de clientes, contribuído assim todas estas atividades para uma redução significativa das margens de lucro dos retalhistas. Assim sendo, surge a necessidade de implementação de mecanismos de deteção de fraudes de modo a proteger interesses financeiros e a eficiência das operações e criar um ambiente de compras fiável (Gayam, 2020), reduzindo o impacto negativo das fraudes no seio das empresas.

2.5. Mecanismos de combate à fraude na última milha

Existem diversos mecanismos ao dispor das empresas, desde processuais, menos automatizados, a tecnológicos, que podem mitigar as fraudes na última milha.

Uma das formas mais tradicionais de reduzir o risco de fraude na última milha, é investir na formação dos funcionários com o intuito de os capacitar a identificar atividades suspeitas e a responder adequadamente perante uma situação possivelmente fraudulenta. Para além disso, a coordenação de horários de entrega para garantir a disponibilidade dos destinatários para receber encomendas e a requisição de uma assinatura do consumidor como comprovativo de recebimento da encomenda, podem surgir como estratégias que proporcionam a redução do número de roubos e do número alegações de não recebimento (Garg & Bindewari, 2024; Last Mile Logistics, 2023; Barabas, 2020), uma vez que há uma prova de entrega.

Contudo, à medida que as entregas sem contacto se tornam cada vez mais comuns devido às transações de *e-commerce*, que permitem entregas em pontos de recolha e cacifos, nem sempre é possível que o destinatário assine o comprovativo de entrega, e, portanto, as empresas podem adotar um mecanismo que consiste no comprovativo da prova de entrega através de fotografias do pacote com os respetivos documentos no local de entrega (Barabas, 2020) pedindo posteriormente, no momento de levantamento da encomenda por parte do cliente, a inserção de um código para levantamento, prevenindo desta forma a ocorrência de fraudes.

Para além disso, a implementação de câmaras nos locais de embalagem das encomendas pode também ajudar na mitigação de fraudes, visto que, caso um cliente tente alegar que não recebeu, ou recebeu o produto errado, ou que faltam alguns produtos, o retalhista pode aceder às câmaras e comprovar perante o cliente que os itens foram embalados e enviados conforme o acordado (Zhang *et al.*, 2023). Contudo não comprava se os produtos foram desviados no

transporte ou nos locais de recolha, assim esta solução deve ser aleada a comprovativos de entregas e tecnologias que permitam o rastreamento em tempo real das encomendas.

Segundo Garg e Bindewari (2024) a realização de auditorias de conformidade surge também um mecanismo útil à prevenção de fraudes na última milha, permitindo à empresa identificar fraudes já ocorridas e tentativas de fraude, corrigindo as vulnerabilidades de modo a aumentar a segurança logística.

É auferível que a fraude começa nos incentivos, por isso, a substituição da política de reembolsos em dinheiro por políticas de ofertas de vales ou cartões oferta, pode, de certa forma, reduzir as ações fraudulentas, uma vez que, em muitas das fraudes de devolução, os infratores desejam a obtenção de dinheiro por meio dos reembolsos, e assim, ao impedir a devolução monetária desincentiva-se consumidores fraudulentos a realizarem devoluções (SEON, s.d.).

Na mesma linha de raciocínio, as devoluções gratuitas representam incentivos à ocorrência de devoluções. Assim, as empresas podem implementar taxas de serviços de devolução, isto é, podem cobrar um montante aos consumidores, ou, deduzir do reembolso total o valor da devolução aplicável, de forma que os clientes procedam com o envio do produto que pretendem devolver. Este montante é imposto na tentativa de evitar o abuso da política devolução e amenizar os custos operacionais que a empresa incorre, como o de transporte ou de possíveis perdas derivadas da devolução, como a impossibilidade de revenda (Choi, 2013) permitindo em simultâneo dissuadir o cliente a realizar devoluções fraudulentas, pois será obrigado a pagar para realizar a transação.

A colocação de etiquetas nas partes internas dos produtos, é uma outra prática que, de certo modo, incentiva os consumidores a fazerem uso do produto e devolverem após a satisfação das suas necessidades. Deste modo, a colocação das etiquetas em locais visíveis, onde a não remoção da mesma dificulte o uso da peça, é uma estratégia desencorajadora a tentativas de fraude de *wardrobing*. Paralelamente, a mudança das políticas da empresa quanto à janela de tempo para efetuar devoluções, com vista à diminuição do tempo de trocas e devoluções, também pode desincentivar atividades fraudulentas (Zhang *et al.*, 2023).

Numa vertente mais tecnológica, a estratégia antifraude baseada na análise da pegada digital, permite identificar inconsistências e atividades suspeitas que podem indicar possíveis ações fraudulentas. Esta técnica examina todos os rastos digitais deixados pelos consumidores durante as interações online, como a ausência de redes sociais, endereços IP suspeitos, dados do dispositivo usado e comportamentos de navegação (SEON, s.d.). Assim, uma análise de

pesquisa inversa de e-mail ou uma verificação do número de telefone dos compradores durante o *checkout*, pode apresentar o risco inerente à realização de fraudes nas devoluções (Shih *et al.*, 2021). Contudo, as pegadas digitais não estão a salvo de falsificações por parte dos infratores. Deste modo, as pegadas podem ser protegidas contra falsificações através da programação de contratos inteligentes na blockchain Ethereum, permitindo em simultâneo a proteção de todos os envolvidos nas transações (Shih *et al.*, 2021).

Os contratos inteligentes na blockchain Ethereum são programas que executam acordos definidos entre as partes envolvidas de forma automática, sem a necessidade de envolver intermediários. Os contratos, registam as transações e mudanças de propriedade do produto na blockchain garantido que cada etapa do processo seja transparente e inalterável, o que permite às empresas rastrear de forma segura a propriedade e o histórico dos produtos, reduzindo a necessidade de verificações manuais, o que dificulta a ocorrência de fraudes, prevenindo a ocorrência de fraudes nas devoluções e trocas de produtos no *e-commerce* (Shih *et al.*, 2021). A automatização dos processos através dos contratos inteligentes permite simplificar o compartilhamento de informações e automatizar rejeições de pedidos de devolução potencialmente fraudulentas, reduzindo em simultâneo os custos operacionais que a empresa incorre neste processo (Shih *et al.*, 2021; Kshetri, 2018).

A utilização da tecnologia blockchain, é uma forma emergente no combate à fraude. De uma forma simplificada, a blockchain, é uma cadeia de blocos descentralizada que regista transações imutáveis numa rede de computadores segura e transparente formando uma cadeia de dados resistente a alterações e a fraudes (Olaoye & Potter, 2024). Com o uso da blockchain, as devoluções podem ser autenticadas de forma eficiente permitindo relacionar todas as transações a um cliente específico, criando um perfil de cliente.

Para além do perfil do cliente, a blockchain permite o registo de todas as transações envolta do produto, tanto numa fase de compra e entrega, quanto numa fase de devolução, através da atribuição e seguimento de números de séries únicos que são registados e armazenados numa base de dados segura. Com recurso a este mecanismo a origem de cada produto é conhecida, os produtos possuem registos e comprovativos, e não podem surgir do nada na cadeia de abastecimento, como acontece em caso de contrabando ou falsificações onde tentam devolver produtos sem documentação legítima ou sem rastreabilidade. Assim, em caso de devoluções fraudulentas, o sistema alerta o retalhista e permite-lhe verificar a legitimidade da devolução,

impedindo deste modo a ocorrência de fraudes (Tanwar *et al.*, 2020; Cekerevac *et al.*, 2024; Ülkü & Gürler, 2018).

Apesar do seu potencial, a blockchain enfrenta obstáculos como problemas em suportar um aumento substancial de dados, requer altos consumos de energia e enfrenta barreiras regulatórias. Portanto, estes obstáculos necessitam ser superados antes de uma adoção em larga escala deste mecanismo (Olaoye & Potter, 2024).

A Internet das Coisas, também conhecida como Internet of Things (IoT) é "um paradigma emergente que permite a comunicação entre dispositivos eletrônicos e sensores por meio da internet" (Kumar *et al.*, 2019, p.1), que potencializa uma enorme transformação na gestão das cadeias de abastecimento e nos processos de última milha. Com a IoT a aplicação de etiquetas de identificação por meio de radiofrequência (RFID), com ou sem sensores integrados; de códigos de barras e de dispositivos de *Global Positioning System* (GPS), tornou possível a identificação e rastreamento dos produtos em todas as etapas do processo logístico (Kshetri, 2018). De uma forma pormenorizada, os RFID permitem a identificação automática dos produtos fazendo uso de dois dispositivos principais, o leitor, que controla a comunicação, e as etiquetas, cada uma associada a um código eletrônico único para fins de identificação. O leitor emite sinais de rádio referência (RF) para interagir com as etiquetas, e estas respondem transmitindo o seu código de identificação (ID), permitindo uma leitura à distância e através de embalagens, realizando verificações em tempo real e em massa, o que reduz as oportunidades de adulteração. Algumas etiquetas podem incluir sensores integrados que permitem enviar, para além do código ID, dados recolhidos por esses sensores através de rádio frequências e tecnologias sem fio (Landaluce *et al.*, 2020) como dados de proximidade, de temperatura, de humidade ou de posição, por exemplo, tornando assim possível enviar informações sobre as circunstâncias em que os produtos se encontram (Sehrawat & Gill, 2019). Adicionalmente, os RFID também permitem rastrear os produtos, contudo, ao contrário do GPS, geralmente rastreiam de forma pontual, apenas em locais onde existem os leitores, a não ser que detenham sensores de localização integrados que permitam a localização contínua em tempo real dos produtos. Por sua vez, podem ser utilizados dispositivos GPS nas caixas ou veículos de transporte permitindo o *tracking* do conjunto de produtos contidos na caixa ou no veículo. Deste modo, as tecnologias GPS detêm também uma grande relevância pois permitem rastrear de forma precisa e em tempo real os produtos, permitindo obter coordenadas exatas e contínuas da localização dos produtos e identificar as horas associadas a cada movimentação (Prasanna & Hemalatha, 2012). Por fim, o código de barras, ainda que não seja a melhor tecnologia

disponível, quando comparada às técnicas de identificação mais recentes como os RFID (García *et al.*, 2006), são ferramentas de identificação padronizadas que possibilitam não só identificar o tipo de produto através dos códigos únicos atribuídos, como também permitem o rastreamento dos mesmos, sem a necessidade de uma introdução de dados manual, necessitando apenas de realizar a leitura individual dos códigos através de dispositivos apropriados necessitando de uma linha de visão direta, não permitindo contudo, rastrear uma unidade individual específica (Hanna & Pantanowitz, 2015), todavia não permitem a identificação de um item específico como os RFID e em caso de atualizações exigem a impressão de novas etiquetas.

Posto isto, estas tecnologias, permitem aprimorar o rastreamento e o registo de dados, permitindo um acompanhamento em tempo real, e se combinadas com a blockchain, podem deter uma camada de segurança e transparência particularmente valiosa (Kshetri, 2018). Desta forma, a gravação contínua dos dados obtidos pelas tecnologias IoT implementadas nos produtos permite criar um histórico completo sobre as informações dos produtos, tanto relativamente à sua localização, como à sua identificação e às suas características originais, permitindo assim ao retalhista mitigar fraudes na última milha. Estas informações ficam guardadas na blockchain ou, caso a empresa não utilize blockchain, numa outra base de dados utilizada pela empresa, como bases de dados centralizadas ou *clouds*, por exemplo.

Adicionalmente, a integração entre plataformas, isto é, a ligação e comunicação entre diferentes sistemas da empresa ou entre parceiros externos, surge também como um mecanismo com potencial na prevenção de fraudes, devido à partilha de dados em tempo real que confere a possibilidade cruzamento de informações permitindo assim a proteção do retalhista contra fraudes na última milha (Garg & Bindewari, 2024).

Para além dos mecanismos mencionados, as técnicas de Inteligência Artificial (IA), como a Machine Learning (ML) e Deep Learning (DL), fornecem também soluções inovadores eficazes na mitigação de fraudes na última milha. Estas tecnologias permitem, a automação dos processos de deteção, melhoram a precisão e ajudam na identificação de ameaças mesmo antes destas se materializarem, agindo assim de forma proativa. Deste modo, estas tecnologias contrastam-se dos sistemas baseados em regras estáticas, que exigem atualizações constantes e que se mostram incapazes de acompanhar a evolução das técnicas utilizadas pelos infratores (Gayam, 2020).

A qualidade e quantidade de dados utilizados para treinar os modelos de IA são determinantes para a sua eficácia. Dados como informações de transações, contendo o valor, o

endereço de cobrança e de envio; dados do consumidor, como a localização e o histórico de compras; e dados do dispositivo, como o endereço IP e o sistema operacional, são fundamentais para a eficácia dos modelos. Assim sendo, após a recolha e armazenamento destes dados, a engenharia de características surge como um processo crucial para o desempenho eficaz dos modelos de ML, permitindo a extração das informações mais relevantes dos dados recolhidos de modo a construir modelos mais eficazes para detetar padrões fraudulentos e realizar previsões (Gayam, 2020).

A aprendizagem contínua, associada à ML, permite analisar grandes quantidades de dados de transações tanto fraudulentas quanto legítimas, de modo a detetar padrões e comportamentos anômalos que indicam fraudes que seriam dificilmente detetáveis por humanos de forma preventiva (Gayam, 2020). A aprendizagem é realizada com base em todos os dados inseridos no sistema, permitindo assim uma adaptação continua para a melhoria da deteção de fraudes, tornando-se cada vez mais difícil a manipulação do sistema (SEON, s.d.), os modelos não detetam apenas padrões de fraudes já estabelecidos, mas também evoluem para lidar com novas ameaças. Aliado a estes mecanismos tecnológicos, o conhecimento especializado de equipas de analistas de fraudes e profissionais de segurança pode contribuir para a melhoria da eficácia dos modelos de IA, uma vez que permite alavancar o conhecimento especializado destes profissionais para determinar a legitimidade das transações suspeitas e, portanto, melhorar a precisão na identificação de transações fraudulentas ou legítimas (Gayam, 2020).

Esta tecnologia permite aplicar ferramentas preventivas através não só de análises de comportamento, que permitem a identificação de padrões de compras do consumidor, como também de análises de velocidade de transações que indicam as quantidades de produtos encomendadas, permitindo verificar a ocorrência de picos abruptos no volume de compras associados a uma conta. Estas análises permitem identificar desvios que possam sugerir a presença de atividades fraudulentas (Gayam, 2020).

Para além disso, através de serviços de verificação de endereços fornecidos por tecnologias de IA, torna-se possível verificar alterações frequentes ou inconsistências em endereços de entrega e locais geográficos suspeitos, fatores que podem surgir como indicadores de ações fraudulentas. A ML, pode validar e corrigir endereços de forma automática e em tempo real, reduzindo falhas nas entregas por erros de digitalização ou informações incorretas. Com recursos a algoritmos treinados para reconhecer padrões, a tecnologia compara os endereços fornecidos com endereços válidos contidos em bases de dados, identificando desta forma

possíveis erros, procedendo de seguida à correção dos mesmos. Com o passar do tempo e com a aprendizagem contínua e as correções realizadas com sucesso, estes modelos de IA, aprimoram as suas previsões e correções de endereços de forma automática (Gayam, 2020; RTS Labs, 2024).

A ML permite também às empresas prever o risco de perda de encomendas através de modelos de análise de dados que identificam entregas com alta probabilidade de extravio ou roubo, atribuído assim uma pontuação de risco às transações em tempo real. Deste modo, este mecanismo, permite não só reduzir os custos associados a reembolsos desnecessários como também otimizar processos através da análise das falhas, configurando assim uma estratégia proativa na mitigação de fraudes (Gayam, 2020; Leeuw *et al.*, 2023).

Uma outra forma de identificação de fraudes na devolução pode ser feita através da utilização de *blacklists* (listas negras), que são listas que contém endereços IP, nomes de domínio ou endereços de email indesejáveis e não confiáveis para efetuar transações (Gheorghiță *et al.*, 2023). Contudo, este processo pode ser bastante limitativo, caso não seja alinhado com as novas tecnologias, devido à necessidade da intervenção humana para realizar as atualizações e manutenções, o que torna o mecanismo demorado e sujeito a erros sobretudo quando exposto a ameaças em tempo real (Vinayakumar *et al.*, 2018). Assim, para melhorar a eficiência do uso deste mecanismo é importante integrar a ML, de modo a que os algoritmos consigam identificar padrões de comportamentos maliciosos e classificar novos endereços de internet potencialmente perigosos com rapidez e precisão, sendo capazes de analisar grandes volumes de dados em tempo real (Lison & Mavroeidis, 2017). Deste modo, será possível detetar possíveis infratores no momento em que o mesmo efetua a compra ou o pedido de devolução.

Complementarmente, pode ser criado um perfil do cliente onde os comportamentos dos consumidores são monitorizados permitindo identificar padrões que possam sugerir a ocorrência de devoluções fraudulentas. Este processo de deteção regista o ID do cliente (identidade do cliente) para cada devolução, registando informações como a frequência de devoluções, a quantidade e o valor das transações e, deste modo, torna-se possível desenvolver modelos de deteção de fraudes aplicados a cada cliente, permitindo identificar devoluções oportunistas ou fraudulentas e prevenindo perdas financeiras para os retalhistas (Ülkü & Gürler, 2018). O perfil de cliente pode ser realizado com uso de IA ou de forma manual, sendo que esta última se encontra mais suscetível a falhas, e posteriormente registado na blockchain, configurando uma camada extra de segurança, ou em base de dados tradicionais.

Relativamente à segurança, a IA, configura uma camada adicional na proteção do processo de última milha, permitindo a identificação de potenciais ameaças e anomalias em tempo real, incluído por exemplo atividades suspeitas junto dos transportes de mercadorias e violações de segurança nos processos de entrega, fazendo uso de sensores IoT ou câmaras equipadas com IA ou análises preditivas, minimizando desta forma a probabilidade de fraudes nesta etapa do processo logístico (RTS Labs, 2024). Para além disso, a IA pode contribuir para o aumento da segurança de alguns sistemas de entrega autônoma, exigindo, por exemplo, reconhecimento facial e outras ferramentas biométricas como comprovativo de prova entrega, garantindo que o produto é entregue apenas ao proprietário legal da encomenda (Xu *et al.*, 2022).

A DL, é uma subárea da ML que utiliza redes neurais profundas para processar grandes volumes de dados e identificar padrões complexos, que humanos ou algoritmos mais simples da ML não conseguem perceber. Nas redes neurais profundas existem redes neurais convulsionais que são projetadas para tarefas de análise de imagem e documentos, tornando-se assim bastante úteis na deteção de fraudes que envolvem informações visuais, como por exemplo a manipulação de imagens. Desta forma, a DL configura um sistema mais robusto e automatizado de proteção de fraudes no *e-commerce* (Gayam, 2020).

A utilização de drones, também pode ser reconhecida como um mecanismo de combate às fraudes na última milha. Segundo o Min (2015) os drones são pequenos veículos aéreos operados remotamente, sem piloto a bordo, guiado por GPS sem fio e podem conter câmaras e/ou sensores. Estes dispositivos podem captar constantemente e em tempo real imagens e localizações de forma precisa, devido ao GPS e à câmara integrada (Min, 2023). Apesar das implicações legais envolvidas relacionadas com a invasão de privacidade do cliente este método permite rastrear em tempo real as encomendas e verificar o estado de entrega do produto, sabendo exatamente onde e quando é que a entrega foi realizada, garantindo em simultâneo a entrega ao destinatário correto. Para além disso, a tecnologia de drones, ao ser equipada com sistemas de segurança como as câmaras e sensores, permite prevenir roubos e interceções durante o transporte (Min, 2023).

As empresas de *e-commerce*, podem também recorrer à contratação de um fornecedor externo para executar a logística da empresa, sendo estes designados por *Third Part Logistics* (3PL). Esta estratégia pode permitir aos retalhistas aproveitar os conhecimentos detidos pelo 3PL de forma a ultrapassar o grande desafio relativo às fraudes na última milha externalizando o tratamento das mesmas (Zhang *et al.*, 2023).

Assim, após a identificação dos mecanismos antifraudes identificados na literatura existente, é possível agrupar os mecanismos de IA, bem como as suas componentes de ML e DL, a técnica de análise de pegada digital e a utilização de *blacklists*, uma vez que todos estes mecanismos recolhem dados e processam-nos de modo a criar informação e estimar a probabilidade de fraude, sendo, portanto, usados como mecanismos preventivos. Deste modo, a este grupo de mecanismos é atribuída, para a presente investigação, a denominação de mecanismos de prevenção através de análise de dados.

2.6. Síntese da revisão da literatura

De uma forma sucinta, o *e-commerce* tem vindo a assumir um papel cada vez mais relevante no seio empresarial (Dima *et al.*, 2023), e por isso, devido ao seu crescimento registado nos últimos anos surgiu a necessidade de uma definição internacionalmente aceite, que apesar de conter algumas dissonâncias conforme os autores, detém na sua base um conceito semelhante. Organizações como a OECD e Eurostat e autores como Stallmann e Wegner (2014), Kalakota e Whinston (1997) e Lee (2012), apresentam diversas definições de *e-commerce* que convergem numa definição de *e-commerce* que, de uma forma geral, é definida pela utilização da internet para realizar compras, trocas ou vendas de produtos e serviços.

A mudança de paradigma na mente dos consumidores, o aumento verificado do número de utilizadores de internet e de compras realizadas online proporcionaram o aumento da importância da adaptação dos modelos de negócio para a integração e/ou desenvolvimento do canal de *e-commerce*. De facto, autores com Lazić *et al.* (2024), Nagai e Wat (2002) e G. Wang *et al.* (2023) defendem a importância da utilização do *e-commerce* para a subsistência das empresas no mercado atual e futuro. Contudo, o *e-commerce*, sobretudo o B2C, necessita de um grande suporte logístico de forma a garantir a entrega eficiente dos produtos encomendados (Hofmann & Rüsch, 2017; Y. Wang *et al.*, 2020; G. Wang *et al.*, 2023) e o sucesso do processamento de possíveis devoluções (logística inversa).

Assim a processo de última milha, que engloba a última etapa do processo logístico desde o ponto de penetração do pedido até ao local de entrega selecionado pelo consumidor (Lim *et al.*, 2018) e a logística inversa, isto é, a recolha e processamento dos produtos devolvidos, surge como uma componente cada vez mais relevante num contexto onde a utilização da internet e a popularização das compras online se intensificam (Shih *et al.*, 2021; Gomes *et al.*, 2023). Contudo, a última milha, ainda se configura numa etapa bastante ineficiente e onerosa, repleta

de vulnerabilidades que contribuem para a ocorrência de diversas fraudes na última milha que se refletem em perdas monetárias significativas para as empresas (Shih *et al.*, 2021), e com impactos financeiros, operacionais e reputacionais negativos.

O aumento das compras online contribui para um aumento do número de devolução devido à impossibilidade de tocar, de experimentar, ou de sentir os produtos (Salem & Alanadoly, 2024), contudo, nem todas as devoluções são de facto legítimas, por vezes os consumidores aproveitam-se de políticas brandas, característica da nova realidade de compras online, e de vulnerabilidades logísticas para cometer fraudes.

As devoluções podem ser classificadas como (1) oportunistas, se o cliente embora tenha usufruído do produto, decide devolvê-lo para obter um reembolso em troca, aproveitando-se deste modo das políticas de devoluções praticadas pelo estabelecimento (Sampaio, 2022), ou (2) fraudulentas se consumidor devolver um produto ao retalhista, ciente que tal devolução é contrária às normas e regulamentações legais ou às políticas da empresa aplicáveis (Harris, 2008; Shih *et al.*, 2021). Com isto, é possível auferir que devoluções oportunistas podem ser fraudulentas se o cliente estiver ciente que está a infringir as políticas de devolução estabelecidas (Zhang *et al.*, 2023).

Por sua vez, a necessidade por entregas rápidas e cómodas, e a dependência de múltiplos intervenientes logísticos para concretizar as entregas, configuram desafios que afetam os processos de verificação, aumentando assim a vulnerabilidade a fraudes na fase de entrega. Complementarmente, a distância física do vendedor e do cliente, característica das compras online, também se apresenta como um fator impulsionador à ocorrência de fraudes na fase de logística inversa, uma vez que esta distância, em caso de inexistência de controlos eficientes, facilita a concretização de devoluções fraudulentas.

Posto isto, diversos autores e empresas identificaram inúmeras fraudes ocorrentes no processo de última milha que se encontram expostas na Tabela 2.1.

Tabela 2.1 - Fraudes na última milha identificadas na revisão da literatura

Fonte: Elaboração Própria

	Anansi (s.d.)	Piron e Young (2000)	Purolator (2023)	Sampaio (2022)	Shih *et al.* (2021)	Zhang *et al.* (2023)
Fraude de troca de mercadorias					**x**	**x**
Bricking						**x**
Fraude de reembolso entre retalhistas						**x**
Fraude de descontos						**x**
Fraude de reembolso em múltiplos canais						**x**
Chargeback						**x**
Wardrobing		**x**				**x**
Jiffy bag						**x**
Fraude de produtos não recebidos			**x**	**x**		**x**
Fraude de reclamação de atraso na entrega						**x**
Roubo de encomendas			**x**			
Manipulação de endereços	**x**					

Assim, dada a ocorrência de fraudes no processo de última milha e o seu impacto negativo nas empresas, é crucial identificar e implementar mecanismos que permitam mitigá-las de modo melhorar a saúde financeira da empresa e criar um ambiente de confiança (Gayam, 2020). Nenhum mecanismo por si só é eficaz no combate ao problema das fraudes, e por isso os retalhistas devem procurar integrá-los, visando um equilíbrio entre mecanismos tecnológicos e processuais. Deste modo, a Tabela 2.2 representa os mecanismos identificados na revisão da literatura, com base em autores e empresas do meio logístico.

Tabela 2.2 - Mecanismos antifraude identificados na revisão da literatura

Fonte: Elaboração Própria

	Barabas (2020)	Choi (2013)	Garg e Bindewari (2024)	Gayam (2020)	Kshetri (2018)	Last Mile Logistics (2023)	Leeuw *et al.* (2023)	Lison e Mavroeidis (2017)	Min (2015)	Olaoye e Potter (2024)	RTS Labs (2024)	SEON (s.d.)	Shih (2021)	Tanwar *et al.* (2020)	Ülkü e Gürler (2018)	Zhang *et al.* (2023)
Treino dos funcionários			x			x										
Agendamento de entregas						x										
Comprovativo de prova de entrega	x															
Implementação de câmaras nos locais de embalamento de encomendas																x
Auditorias			x													
Políticas de devoluções antifraude		x										x				x
Etiquetagem em locais externos																x
Contratos inteligentes na blockchain Ethereum					x								x			
Tecnologia blockchain					x					x				x	x	
IoT (RFID, GPS, Código de Barras)					x											
Integração entre plataformas			x													
Mecanismos de prevenção através de análise de dados				x			x	x			x	x	x			
Entregas por drones									x							
3PL																x

3. Metodologia

O capítulo 3, tem como objetivo introduzir a metodologia a ser aplicada na investigação de modo a recolher e analisar os dados necessários para se responder às questões de investigação previamente definidas.

A abordagem de investigação caracteriza-se por um conjunto de planos e procedimentos de pesquisa que contemplam etapas de métodos de recolha, de análise e interpretação de dados. Assim, ao conduzir uma investigação, seleciona-se uma abordagem de pesquisa adequada ao tema em estudo (Grover, 2015), de modo a orientar o processo metodológico de forma coerente e fundamentada. Desta forma, para a investigação em curso, adota-se uma metodologia qualitativa experimental, na qual para a obtenção de dados primários se recorre à realização de entrevistas semiestruturadas a profissionais com experiência em empresas com canal de *e-commerce* B2C em Portugal. O objetivo consiste em identificar as fraudes na última milha ocorrentes no seio das empresas e os mecanismos utilizados por estas de modo a combatê-las. Numa fase posterior, analisam-se e discutem-se os dados referentes às práticas de combate a fraudes mencionadas nas entrevistas, comparando-as, em simultâneo, às práticas identificadas na literatura.

As entrevistas são amplamente utilizadas como metodologia de investigação em diversas áreas de conhecimento e utilizam, de uma forma geral, o diálogo para recolher informações relevantes para fins de pesquisa (Monday, 2020), permitindo que, de uma forma bilateral, ocorra uma troca de ideias e de informações (Pandey & Pandey, 2015). Existem três tipos de estruturas de entrevistas, as estruturadas, as semiestruturadas e as não estruturadas (Robson & McCartan, 2016). As entrevistas estruturadas seguem um formato semelhante de um questionário e proporcionam respostas mais superficiais, por sua vez, as semiestruturadas contemplam áreas de interesse previamente definidas e perguntas auxiliares para direcionar a conversa e, por último, as entrevistas não estruturadas têm um foco mais amplo, permitindo que o rumo da entrevista siga as direções sugeridas pelo entrevistado (Petty *et al.*, 2012).

Deste modo, e seguindo a ideologia defendida por Petty *et al.* (2012), define-se o guião de entrevistas com base em 5 pontos principais de estudo, os quais se desdobram em 10 perguntas auxiliares, como é possível verificar no Anexo A, permitindo desta forma abordar questões relativas ao processo de última milha das empresas, às fraudes na última milha registadas e aos mecanismos antifraudes utilizados ou em vias de implementação nas empresas portuguesas, bem como os desafios adjacentes na sua implementação.

3.1. Seleção da amostra

Para esta investigação utiliza-se a amostragem por conveniência, que consiste na escolha da amostra que demostre acessibilidade e disponibilidade para fornecer as informações necessárias para a investigação (Hesse-Biber & Leavy, 2011), tendo como foco profissionais com experiência em áreas de logística, *e-commerce* ou fraudes em empresas que detenham o canal de *e-commerce* B2C em Portugal. A amostra deve ser composta por profissionais com pelo menos 5 anos de experiência numa das áreas mencionadas (ou relacionadas) de modo a garantir um conhecimento aprofundado sobre as informações necessárias para a investigação.

Para tal, listam-se diversas empresas que utilizam o canal de *e-commerce,* bem como profissionais internos das áreas de interesse desta investigação, e profissionais externos a essas empresas, mas com experiências anteriores no ramo há menos de 5 anos. Posteriormente estabelece-se o contacto recorrendo a uma das duas formas, (1) contacto direto através das páginas de LinkedIn dos profissionais, (2) de uma forma mais indireta, contacto via e-mail com o departamento de recursos humanos das empresas, de modo a verificar a disponibilidade em fornecer informações e o posterior redireccionamento para os profissionais mais indicados a entrevistar.

Espera-se um período total de 2 meses para a realização da fase de identificação, contacto, agendamento e realização de entrevistas. Desta forma, de modo a agilizar e facilitar o contacto, as entrevistas realizam-se em formato online.

Posto isto, é necessário reforçar que a estruturação da amostra com profissionais capacitados e com elevados anos de experiência é fulcral para entender o funcionamento do mercado atual face ao combate as fraudes na última milha, permitindo desta forma averiguar a existência de lacunas no combate às mesmas.

3.2. Técnica de análise de conteúdos

A análise dos dados obtidos por meio das entrevistas realiza-se com base em técnicas de análise de conteúdo, técnica utilizada para ajudar "a reinterpretar as mensagens e a atingir uma compreensão dos seus significados num nível que vai além de uma leitura comum" (Moraes, 1999, p.2), permitindo deste modo, não só identificar os tipos de fraudes mais frequentes na empresa, como também os principais mecanismos adotados para mitigar as fraudes e os desafios de implementação adjacentes. Para além disso, esta análise permite averiguar as perceções dos entrevistados sobre a eficácia dos mecanismos antifraudes adotados e a necessidade de adoção de novos mecanismos.

Deste modo, aplica-se uma análise de conteúdo manifesta, analisando de forma direta e superficial as informações recolhidas nas respostas às entrevistas, em simultâneo de uma análise de conteúdo latente, permitindo interpretar significados profundos implícitos na transcrição das entrevistas (Kleinheksel *et al.*, 2020).

O processo de análise de conteúdo divide-se em três etapas tal como defendido por Kleinheksel *et al.* (2020). Numa primeira instância procede-se à codificação, isto é, através das transcrições das entrevistas identificam-se unidades de significados, como palavras ou expressões que representam algo relevante para o objetivo da pesquisa. Posteriormente, após a criação de vários códigos, os códigos relacionados agrupam-se em categorias permitindo estruturar os dados de forma lógica e coerente, sendo esta etapa denominada por categorização. Por fim, de uma forma integrada à discussão de resultados realiza-se a etapa da identificação de temas amplos, caracterizada por conectar as categorias de modo a identificar temas que permitem através da sua discussão explicar o objetivo da pesquisa.

3.2.1. Codificação

A codificação é a primeira etapa do processo de análise de conteúdo qualitativa, permitindo identificar, extrair e rotular unidades de significado a partir de dados brutos, que neste caso provem de entrevistas, transformando assim linguagem natural em dados organizados.

A codificação envolve a extração de unidades de significado através das frases, expressões ou palavras extraídas nas entrevistas que indiquem informações relevantes sobre (1) desafios de última milha; (2) fraudes na última milha; (3) mecanismos de mitigação utilizados; (4) eficiência percebida no combate à fraude; (5) desafios na implementação de mecanismos.

Após a extração de unidades de significados a cada unidade atribui-se um código descritivo (codificação), representando o seu significado central, agrupando as expressões semelhantes sob códigos comuns.

3.2.2. Categorização

Após a conclusão da etapa de codificação executa-se a segunda etapa da técnica de análise de conteúdo proposta por Kleinheksel *et al.* (2020), a categorização. Esta etapa consiste no agrupamento dos códigos identificados na etapa anterior em subconjuntos coerentes, denominados categorias, com base em semelhanças de conteúdo, contexto ou função. Assim,

definem-se categorias abrangentes, que organizam os dados de forma temática, garantindo que cada código se enquadra logicamente na sua categoria e que as categorias são mutuamente exclusivas e coletivamente exaustivas.

3.2.3. Identificação de temas amplos

Por fim, realiza-se a identificação e formação de temas amplos, o que representa a fase de análise de conteúdos em que as categorias, previamente definidas, são analisadas e integradas para identificar padrões e significados que permitam compreender de forma mais abrangente o fenómeno em estudo.

Segundo Kleinheksel *et al.* (2020), os temas amplos são sínteses analíticas que transcendem os dados descritivos e oferecem interpretações explicativas, isto é, passa a existir uma explicação do significado dos dados no contexto da investigação. Deste modo, esta etapa permite estruturar a discussão de forma coerente com os dados e com a literatura.

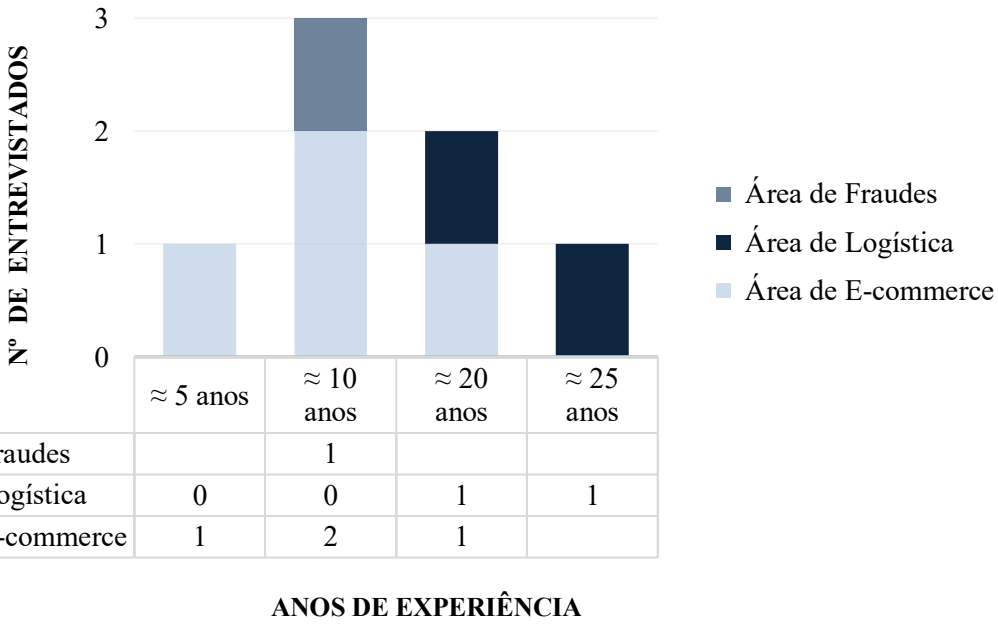
4. Análise e Discussão de Resultados

No presente capítulo realiza-se a interpretação e análise dos dados recolhidos nas entrevistas realizados no âmbito da investigação em curso, com o objetivo de identificar os principais mecanismos implementados para mitigar fraudes na última milha no *e-commerce*, a partir das informações recolhidas junto de diversos profissionais. Deste modo, analisam-se os mecanismos antifraudes, desafios e perceções relativamente ao fenómeno da fraude no mercado português, em simultâneo da exposição de possíveis explicações e limitações, ou seja, da discussão e reflexão dos resultados obtidos.

Posto isto, de forma a realizar a análise dos dados utiliza-se a técnica de análise de conteúdo descrita por Kleinheksel *et al.* (2020), sendo deste modo apresentada de forma conjunta a etapa da codificação, categorização e formação de temas amplos por forma a obter uma análise e discussão integrada e pormenorizada.

4.1. Amostra

Para fins da presente investigação foram realizadas entrevistas a 7 especialistas ligados ao comércio através do canal de *e-commerce* B2C em Portugal. De um total de 7 entrevistados, 2 profissionais já não se encontram vinculados a empresas deste tipo, mas possuem uma vasta experiência na área de logística e *e-commerce* B2C no seio português, e os restantes 5 ainda trabalham na área. Os profissionais entrevistados ocupam ou ocuparam, há menos de 5 anos, cargos de responsabilidade média/alta como gestores, líderes de equipa e diretores em áreas de atuação como o *e-commerce*, logística e gestão de operações relacionadas a fraudes em empresas internacionais ou multinacionais. Os participantes apresentam uma experiência profissional compreendida entre 5 e 25 anos, o que evidencia um nível de conhecimentos aprofundado sobre os setores mencionados. Posto isto, o Gráfico 4.1 evidencia de forma sucinta a caracterização da amostra, distribuindo os entrevistados por área de atuação e anos de experiência.



	≈ 5 anos	≈ 10 anos	≈ 20 anos	≈ 25 anos
Área de Fraudes		1		
Área de Logística	0	0	1	1
Área de E-commerce	1	2	1	

Gráfico 4.1 - Distribuição dos entrevistados por área de atuação e anos de experiência

Fonte: Elaboração Própria

Os profissionais entrevistados detêm conhecimentos sobre diversos setores do retalho nomeadamente o retalho especializado (eletrónico, decoração e utilidades para o lar), o retalho de moda, e por fim, o retalho alimentar e de bens de consumo diário, permitindo assim, averiguar as principais fraudes na última milha enfrentadas e os mecanismos de combate utilizados no seio empresarial.

4.2. Resultados

4.2.1. Desafios potenciadores de fraudes na última milha no *e-commerce* português

Com base nos dados adquiridos a estrutura de última milha revelou-se uma dimensão crítica e bastante onerosa, tanto numa fase de entrega como de devolução, tal como foi verificado na literatura.

A crescente popularização do *e-commerce* manifesta-se em altos desafios para as empresas. Segundo os profissionais entrevistados, a exigência dos consumidores por entregas rápidas; a

necessidade de políticas de devolução brandas, devido à impossibilidade de visualizar, tocar e experimentar o produto antes da compra; os desafios na rastreabilidade e comunicação; a dificuldade na gestão multicanal no processamento de devoluções; a alta rotatividade de colaboradores, que provoca a criação de equipas com colaboradores pouco qualificados; e a necessidade de existência de diversos métodos de entrega, de modo a corresponder à comodidade procurada pelo cliente digital, alavancam desafios de última milha que se configuram onerosos e suscetíveis a maiores vulnerabilidades, tal como a incidência de fraudes.

De acordo com os dados codificados, as práticas mais mencionadas relacionas às entregas incluem entregas realizadas na loja física e entregas ao domicílio realizadas por parceiros logísticos. Foram também mencionadas, embora com menos regularidade, as entregas em pontos de recolha parceiros e cacifos, de forma a alcançar as necessidades de minimizar custos e agilizar o processo de entrega através destes canais alternativos. O processamento das devoluções segue uma ótica semelhante, podendo ser processada uma devolução a partir da loja física e, embora com menos ocorrência, a partir do domicílio, pontos de recolha de parceiros ou cacifos. Assim sendo, de uma forma sucinta, as entregas e devoluções podem ocorrer a partir de diferentes meios, loja física, domicílio, ponto de recolha de um parceiro ou cacifos, informação que consta de forma semelhante na literatura existente.

Posto isto, foi denotada pelos entrevistados uma clara ligação entre o tipo de entrega/recolha e a ocorrência de fraudes, relatando que entregas onde existem menos intervenientes podem configurar menores riscos de fraudes, destacando-se, portanto, a entrega em loja física como o método mais seguro para as empresas. Contudo, é do conhecimento dos profissionais que as outras formas de entrega/recolha não podem ser descartadas, apesar da sua maior vulnerabilidade a fraudes, pois permitem satisfazer a necessidades dos clientes do mercado atual por entregas cômodas sem os mesmos necessitarem de fazer grandes deslocações para obter o produto. Deste modo, surge a necessidade de garantir a rastreabilidade em todas as fases da última milha e a implementação de mecanismos antifraudes de modo a mitigar a ocorrência de falhas e fraudes.

4.2.2. Fraudes na última milha no *e-commerce* português

De facto, as entrevistas revelaram uma diversidade significativa de práticas fraudulentas associadas ao processo de última milha, não só numa fase de entrega como de devolução. Foram identificadas a partir do processo de codificação, 12 tipos de fraudes que ocorrem no seio das

empresas, bem como o número de profissionais que as referiram (Nº de profissionais que mencionaram a fraude), como é possível observar na Tabela 4.1. (De uma forma mais pormenorizada, no Anexo B é possível constatar citações dos profissionais que descrevem as fraudes mencionadas, o que permitiu a atribuição dos códigos presentes na Tabela 4.1.)

Tabela 4.1 - Tipos de fraudes mencionados

Fonte: Elaboração Própria

Categoria	Código	Nº de Profissionais que Mencionaram a Fraude
Fraudes na última milha	Fraude de reembolso em múltiplos canais	1
	Jiffy Bag	3
	Fraude de produto não recebido	7
	Chargeback	2
	Bricking	2
	Roubo de encomendas	7
	Fraude por manipulação de endereços	2
	Wardrobing	2
	Fraude de descontos	2
	Fraude de reembolso entre retalhistas	2
	Fraude por falsificação do estado logístico de entrega	2
	Fraude exploratória por encomendas de teste	1
	Fraude de troca de mercadorias	1

Através da análise da Tabela 4.1 é possível verificar que as fraudes mais destacadas pelos entrevistados foram a fraude de produto não recebido e a fraude associada ao roubo de encomendas, ambas com 7 menções. Tal como retratado pelos participantes, a fraude de produto não recebido é uma fraude complexa na sua resolução pois pode estar associada a um engano doloso por parte dos clientes, de modo a manterem o produto e obterem o dinheiro em simultâneo, ou pode estar associado a despistes do produto realizados pelos transportadores, nos pontos de entrega parceiros ou por quem finalizou a encomenda. Em caso da alegação do cliente ser verdadeira, e o mesmo não receber de facto o produto, pode estar-se perante outra fraude, o roubo de encomendas, que pode ser efetuado por qualquer colaborador ou parceiro envolvido na transação ou mesmo pessoas externas à transação.

Outras fraudes, menos frequentes, mas igualmente relevantes devido à sua possibilidade de crescimento caso não sejam implementados os mecanismos corretos, incluem a fraude *jiffy bag,* com 3 menções, associada à devolução de caixas vazias ou com pedras, invés do produto

associado à devolução, seguida de fraudes com apenas 2 menções como o *wardrobing*, fraude caracterizada pela devolução de um produto após a sua utilização, com maior incidência no setor da moda e decoração e utilidades para o lar; o *chargeback*, relacionado a pedidos de reembolso diretamente ao banco associado ao pagamento de forma a obter o reembolso com alegações falsas relacionadas à encomenda; a fraude de *bricking*, descrita sobretudo perante a venda de produtos mais caros onde o cliente tenta efetuar a devolução de produtos sem as peças originais e associa o pedido de devolução a um pedido de reembolso; a fraude de manipulação de endereços, solicitando entregas para moradas não reais, na tentativa de não haver alguma cobrança ou desviarem as encomendas; a fraude de descontos onde por exemplo em campanhas leve 3 pague 2 clientes tentam posteriormente à compra devolver um dos artigos na tentativa de serem reembolsados na totalidade por esse artigo e permanecer com o artigo gratuito; e a fraude de troca entre retalhistas onde se verifica tentativas de devolução, sem o comprovativo de compra, de artigos iguais que não pertencem à empresa em causa, sendo esta fraude verificada sobretudo em empresas que vendem produtos que não são de marca própria, esta fraude é realizada na tentativa de comprarem um artigo mais barato num retalhista e posteriormente dirigirem-se a outro, que pratica um preço de venda superior, na tentativa de serem reembolsados e lucrarem pela diferença.

Por fim com apenas 1 menção, destacam-se as fraudes de reembolso em múltiplos canais, fazendo a exploração da fragilidade da empresa na integração omnicanal; fraude exploratória por encomendas de teste, na tentativa do infrator perceber o processamento de entregas da empresa de modo a posteriormente se aproveitar de forma fraudulenta das fragilidade detetadas e, por último, a fraude de troca de mercadorias, onde o cliente tenta devolver um artigo igual/semelhante, contudo, danificado ou obsoleto, ao comprado na tentativa de ficar com o novo e receber o reembolso pelo antigo.

A diversidade das fraudes encontradas revela que o problema não se limita a comportamentos oportunistas isolados, alastra-se a um fenómeno sistemático que evolui com as estratégias comercias e operacionais da empresa, aproveitando-se de vulnerabilidades estruturais, processuais e comportamentais que afetam transversalmente o setor do retalho. A partir das respostas foi possível observar que diferentes tipos de fraudes afetam com mais frequência diferentes tipos de retalho, por isso, apesar das múltiplas fraudes destacadas nem todas as empresas verificam o mesmo número de ocorrências e, nem sempre, o mesmo tipo de fraude. Assim sendo, a investigação permite verificar a existência de uma ligação entre o setor de atividade e o tipo de fraudes dominantes nas operações de última milha, permitindo desta

forma perceber que esta associação decorre não só pelas características dos produtos e serviços comercializados, mas também da complexidade operacional, das políticas de devolução praticadas, dos sistemas de controlo implementados e do comportamento dos consumidores típicos de cada setor.

A análise evidencia que setores com elevada complexidade logística e margens reduzidas, como o retalho alimentar e de bens de consumo diário (amplamente conhecido por FMCG - *Fast Moving Consumer Goods*) e o retalho de decoração e utilidade para o lar, enfrentam sobretudo fraudes operacionais e técnicas, isto é, fraudes que surgem de falhas nos processos logísticos, sistemas de controlo ou infraestrutura tecnológica, geralmente cometidas por funcionários ao manipularem processos internos, ou por agentes externos, como hackers que exploram as vulnerabilidades tecnológicas . Por sua vez, setores de maior valor por unidade e foco no consumidor, como o retalho de moda e o retalho eletrónico, são alvo de fraudes mais comportamentais, ou seja, fraudes que dependem da intenção deliberado do cliente ou colaborador, envolvendo a exploração consciente das vulnerabilidades e falhas do sistema, motivadas por impulsos pessoais, emoções ou pressões organizacionais, que resultam em manipulações, omissões ou práticas oportunistas e fraudulentas, como o caso de fraudes como *jiffy bag*; *bricking*; *wardrobing*; fraude de descontos; fraude de reembolsos entre retalhistas e fraude de troca de mercadorias no ato da devolução. É de realçar que apesar da suscetibilidade de cada tipo de retalho a cada tipo de fraudes, existem fraudes que são transversais a todos os tipos de retalho, como por exemplo o roubo de encomendas e a alegação de produtos não recebidos, como é constatável a partir da análise da Tabela 4.1.

Além disso, é possível verificar que a proliferação dos diferentes tipos de fraudes observados está fortemente relacionada com possíveis lacunas nos processos de rastreabilidade; no controlo de qualidade, tanto no processo de preparação e entrega como na devolução e na integração de sistemas. De forma adicional, a pressão por entregas rápidas aliadas a altos volumes de encomendas e a necessidade de terceirização do transporte logístico, são também por si fatores que aumentam a vulnerabilidade a fraudes. A pressão por entregas rápidas gera tentativas de aceleração dos processos e causa sobrecarga de recursos necessários para cumprir prazos curtos, o que pode levar à redução da atenção e do controlo rigoroso no processamento e entrega de encomendas, por sua vez a terceirização do transporte contribui para a perda de visibilidade operacional e controlo total sobre o produto, tendo este de ser dividido pelos intermediários envolvidos no processo de última milha, o que abre espaço para alegações de

não entrega, substituições de produtos ou mesmo manipulações do estado físico da encomenda quando não são aplicados mecanismos de combate eficientes.

A análise revela que as fraudes não são apenas múltiplas e distintas na sua execução, mas também heterogéneas quanto à sua origem, podendo ter origem externa ou interna à empresa. Face às respostas dos entrevistados é possível auferir que as prevalências das fraudes variam em consonância com o tipo de empresa e a sua antiguidade no mercado online, enquanto o impacto das mesmas varia com o número de ocorrências e/ou o valor dos produtos transacionados. De facto, foi observado que as tentativas de fraudes surgem com maior frequência em empresas com volumes elevados de operações, geralmente ligados a empresas com maior antiguidade no canal de *e-commerce*, contudo estas organizações detêm processos bem estruturados e mecanismos de controlo robustos, o que permite descrever a incidência das fraudes bem-sucedidas como residual. Em contrapartida, observou-se que empresas com menos tempo de experiência no canal de *e-commerce* não detêm tantos mecanismos de mitigação, mas também não registam ocorrências de fraudes na última milha significativas devido a fatores como o baixo volume de operações digitais e à elevada percentagem de entregas e devoluções realizadas em loja física. É de notar que a incidência de fraudes na última milha está também relacionada ao valor unitário dos produtos, sendo possível verificar que as empresas que detêm catálogos de menores valores, não registam tentativas significativas de fraudes, enquanto empresas com catálogos de valores superiores apresentam maior incidência de tentativas fraudulentas, contudo o número de fraudes bem-sucedidas é residual devido à eficiência dos mecanismos implementados.

Apesar de neste momento, para a maioria das empresas, as fraudes na última milha não se configurarem num grande desafio, há consciência por parte dos entrevistados que com o crescimento exponencial do uso do canal de *e-commerce* há uma grande tendência para o surgimento de novas formas de fraude e maior propensão ao crescimento do número de fraudes. Deste modo, pode ser verificada uma evolução paralela entre o crescimento do *e-commerce*, inovação logística e a criatividade fraudulenta. Desta forma, apesar de para cerca de 71% (5 dos 7 entrevistados) dos entrevistados o impacto das fraudes no seio das empresas não ser considerado elevado, o combate às fraudes na última milha é visto como uma das prioridades das empresas atuais, pois há uma consciencialização geral dos possíveis impactos negativos que as fraudes sistemáticas podem gerar a longo prazo, não só a níveis económicos e operacionais como também reputacional, uma vez que representam um problema ativo com possibilidade de crescimento paralela ao crescimento do *e-commerce.*

Posto isto, é possível verificar que os dados referentes às fraudes recolhidos através das entrevistas não só corroboram os principais conceitos teóricos abordados na revisão da literatura, como também contribuem com dados mais específicos e atualizados sobre a ocorrência prática e o nível de impacto atual das fraudes no seio empresarial português. Sendo deste modo possível comprovar a relevância desta investigação para a consciencialização do problema de fraudes na última milha e do tipo de fraudes que as empresas poderão estar expostas, permitindo deste modo um conhecimento prévio do problema permitindo a tomada de decisões de forma proativa.

4.2.3. Mecanismos de controlo e mitigação de fraudes na última milha no *e-commerce* português

Deste modo, com o crescimento do volume de operações no *e-commerce* e a complexidade crescente das cadeias logísticas, a prevenção de fraudes na entrega e devolução de encomendas tornou-se numa das prioridades para as empresas. De facto, a análise dos dados adquiridos nas entrevistas permite verificar que a abordagem de mitigação varia entre sistemas tecnológicos avançados, verificações manuais e políticas proativas ou reativas, dependendo da maturidade digital (nível de desenvolvimento e integração das tecnologias digitais numa organização), da maturidade operacional (nível de desenvolvimento, organização e eficiência dos processos internos e logísticos de uma organização), dos recursos disponíveis e da perceção de risco de cada empresa, evidenciando uma diversidade de mecanismos utilizados pelas organizações na tentativa de mitigar as fraudes na última milha. Estes mecanismos visam não só detetar fraudes, mas também desincentivar comportamentos oportunistas, proteger a integridade do processo logístico e assim preservar a saúde da empresa.

Através do processo de codificação foi possível identificar diversos tipos de mecanismos antifraudes na última milha do conhecimento dos entrevistados, como é observável na Tabela 4.2, variando entre mecanismos tecnológicos, que envolvem o uso de sistemas e maior automação, e processuais que abrangem mecanismos não automatizados que contemplam políticas, processos internos e práticas que exigem a intervenção humana. Para além disso, é também possível verificar quantos dos 7 entrevistados mencionaram o mecanismo, e quantos é que efetivamente reconhecem a implementação do mesmo nas empresas (Nº de empresas que implementam o mecanismo). De forma mais pormenorizada, é possível constatar no Anexo C os diversos mecanismos codificados bem como a sua atuação na mitigação de diferentes fraudes

e, no Anexo D, de forma sumarizada, as restrições de implementação ou utilização de cada mecanismo.

Tabela 4.2 - Mecanismos de mitigação de fraudes na última milha mencionados

Fonte: Elaboração Própria

Categoria	Código	Mecanismos Mencionados		Nº de Profissionais que Mencionaram o Mecanismo	Nº de Empresas que Implementam o Mecanismo
Mecanismos de mitigação na fraudes na última milha	Mecanismos de prevenção através de análise de dados	IA		7	4
		ML		7	4
		Blacklist e construção de perfis de risco		7	7
	IoT	RFID (com e sem sensores)		7	0
		Dispositivos GPS		2	2
		Código de barras		7	7
	Protocolo de segurança e contrato com parceiros de transporte	Portas de intrusão nos transportes		3	3
		Contratos com parceiros logisticos com objetivos estabelecidos		5	5
		Presença de pelo menos 2 funcionários no transporte		4	4
	Sistema de *reviews* de clientes			3	3
	Processo de controlo de qualidade no processamento de encomendas			6	6
	Comprovativo de prova de entrega/recolha	*Tracking* fotográfico na entrega e na recolha		2	0
		Sistema de autenticação de entrega	PIN, Assinatura	7	7
			Qr code, Autenticação biométrica	5	0
		Registo fotográfico pontual na entrega, na recolha e à chegada armazém		2	2
		Preenchimento de formulários de controlo de última milha		6	6
	Integração entre plataformas			7	7
	Agendamento de entregas e/ou recolhas associadas a devoluções			3	3
	Colocação de etiquetas térmicas			1	0
	Políticas de devoluções antifraude	Reembolsos em vales ou cartões de oferta		3	0
		Imposição de restrições sazonais nos prazos de devolução		2	0
		Exigência do comprovativo de compra para efetuar devolução		7	7
		Verificação do produto no momento de devolução		7	7
		Pagamento taxas de devolução		6	6
	Auditorias de conformidade para deteção de anomalias			7	7
	Capacitação de equipas antifraude	Equipas especializadas em análise de dados e fraudes		7	4
		Treino e sensibilização de funcionários		7	7
	Pagamento seguro e antecipado	Pagamento no ato da compra		6	6
		Limitação dos tipos de pagamento online		2	1
	Contratação de 3PL			1	0
	Blockchain			2	0
	Etiquetagem em locais externos			2	0
	Entrega por drones			2	0

É possível auferir que as tecnologias inteligentes e de rastreabilidade se destacam com alta frequência de menção. A adoção destas ferramentas revela uma forte aposta na automação e rastreamento como estratégias centrais de mitigação, contudo, a sua eficácia está condicionada à qualidade dos dados recolhidos, à capacidade de interpretação de forma contextualizada e a integração de plataformas.

A integração de tecnologias de IA juntamente com algoritmos de ML assume um papel central na antecipação e identificação de padrões anómalos, representando deste modo mecanismos de prevenção de fraudes através da análise de dados. Estes sistemas são capazes de processar grandes volumes de dados, detetando inconsistências em devoluções, perfis de clientes e comportamentos de compra que possam indiciar tentativas fraudulentas, permitido assim um acompanhamento em tempo real, o que possibilita a tomada de decisões preventivas. É possível a implementação de IA sem uso de ML, pois a utilização de IA permite automatizar decisões com base em cenários previstos, contudo necessita da definição de regras fixas e instruções manuais, enquanto o uso de algoritmos de ML permite que o sistema aprenda e se adapte a novos padrões de forma autônoma com base nos dados que vai obtendo. Estas soluções exigem investimentos significativos e uma integração com os sistemas existentes, o que pode representar um entrave para empresas com recursos limitados e com menor maturidade digital. De facto, apesar da alta frequência de menção, nem todas as empresas utilizam de facto IA e ML, devido ao seu alto custo de implementação e manutenção, à necessidade de deter conhecimento técnico e uma infraestrutura tecnológica avançada. Por vezes, o investimento necessário não compensa quando comparado com as perdas monetárias que ocorrem das fraudes, representado assim um custo-benefício negativo. Assim, apesar de todos os entrevistados terem mencionado estes mecanismos, apenas 4 demonstraram que estes métodos são de facto implementados nas empresas do seu conhecimento, tendo os restantes entrevistados mencionado a intenção de integração destes mecanismos no futuro, caso se verifique um aumento do risco de fraudes. É também possível relacionar a implementação destes mecanismos com a escala das operações e o grau de maturidade, empresas internacionais ou multinacionais, com elevada maturidade digital e mais vulneráveis a tentativas de fraudes tendem a utilizar este tipo de tecnologias, uma vez que geralmente apresentam um maior volume de receitas, permitindo ter recursos disponíveis para o investimento, e podem beneficiar dos conhecimentos de outras filiais espalhadas pelo mundo diminuindo assim os custos associados a tentativas de implementação.

Ainda relacionado a mecanismos de prevenção através da análise de dados, é possível destacar a utilização de *blacklists* e a criação de perfis de risco com o intuito de concentrar, numa lista, clientes com perfis anómalos que possam representar algum risco para a empresa, permitindo deste modo bloquear utilizadores que se demonstrem fraudulentos. A partir dos dados recolhidos é auferível que todas as empresas do conhecimento dos entrevistados apresentam um sistema de lista negra, isto é, *blacklists*, contudo em algumas empresas este

mecanismo é realizado recorrendo a tecnologias, sobretudo IA tornando o processo mais automatizado, enquanto noutras ainda se apresenta como um mecanismo realizado de forma manual, uma vez que não detêm tecnologias de IA.

Segundo os entrevistados mecanismos de prevenção através da análise de dados permitem mitigar fraudes como fraudes de reembolso em múltiplos canais; *chargeback*; fraude de produto não recebido; *bricking*; fraude de manipulação de endereços; fraude de descontos, mais propriamente a manipulação de sistemas de recompensas; tentativas de reembolso entre retalhistas; *wardrobing* e fraudes exploratórias por encomendas testes, devido à capacidade dos algoritmos de ML identificarem padrões anômalos nos pedidos de encomendas e devoluções, como por exemplo (1) clientes associados a pedidos recorrentes de reembolsos, (2) múltiplos pedidos semelhantes, que podem estar associados a burlas no sistema de segurança e (3) tentativas de exploração de promoções. Para além disso, este tipo de mecanismos permite a criação de perfis de risco que permitem o cruzamento de dados como o endereço a enviar, o método de pagamento utilizado e a frequência de devoluções associadas ao cliente, permitindo assim sinalizar possíveis fraudes antes de efetuar a entrega/ reembolsos e agir de forma proativa colocando posteriormente clientes fraudulentos na *blacklist* de modo a impedi-los de cometer novas tentativas de fraudes.

Deste modo, é possível concluir que os mecanismos de prevenção através da análise de dados mencionados nas entrevistas se demonstram coincidentes com os identificados na literatura, contudo a sua aplicação ainda é limitada devido a limitações operacionais ou relacionadas a custo, o que permite verificar que, mesmo sendo vistos na literatura como mecanismos eficazes na mitigação de fraudes na última milha, ainda não são utilizados de uma forma ampla no mercado, havendo ainda empresas (com menos maturidade digital, menos recursos financeiros e/ou menor volume de operações no canal online) que demostram agir de forma reativa e implementam mecanismos sobretudo processuais com intervenção manual, o que se confere numa abordagem, de certa forma, oposta à sugerida nos estudos académicos, uma vez que estes sugerem um equilíbrio entre intervenção humana e a utilização de tecnologias.

Por sua vez, mecanismos de mitigação relacionados a IoT, demonstram-se também pouco explorados no retalho português. Com base nas entrevistas é possível apurar que sistemas como as etiquetas RFID, com e sem sensores, e os GPS, ainda não são amplamente utilizados. De facto, todos os entrevistados mencionaram a utilização do tradicional código de barras, entrando

deste modo em conflito com o que foi apurado na literatura, uma vez que os estudos apontam este mecanismo como desatualizado e limitado em comparação com os anteriormente referidos.

Com base na literatura é possível verificar que etiquetas RFID com ou sem sensores integrados e uso de GPS são fundamentais para garantir a identificação (através da atribuição de um código único), efetuar uma leitura em massa dos itens (RFID) e o *tracking* do produto (GPS), confirmando a localização exata de cada item. Contudo, são mecanismos que exigem altos investimentos e, por isso, em empresas cujo o valor unitário por produto seja baixo e onde o risco de fraude é baixo não é vista uma justificação para a colocação de etiquetas RFID devido ao elevado custo de implementação, uma vez que, para além da necessidade de investimento numa infraestrutura de leitura (leitores e integração de sistemas), o custo da etiqueta RFID (mesmo as sem sensores integrados) é superior ao de um código de barras, e uma vez que os produtos de baixo valor apresentam margens reduzidas, torna-se difícil a absorção desse custo. De facto, pela análise das entrevistas, é possível constatar que mesmo que uma empresa detenha um catálogo amplo com preços diversificados pode não deter a necessidade de implementar etiquetas RFID pois a sua implementação deveria ser feita em todos os produtos e não apenas nos de maior valor, uma vez que isso representaria a necessidade de deter dois processos distintos dentro da mesma empresa, o que acarreta maiores riscos para a existência de lacunas nos processos logísticos. Deste modo, o custo-benefício da colocação de RFID deve ser analisado, tendo em conta o número de fraudes que a empresa está exposta e a ideia que para proteger apenas os itens de elevado valor, o investimento para a proteção destes tem de compensar a colocação destas etiquetas nos de baixo valor. Assim, visto que os entrevistados relatam a incidência de fraudes como residual, nenhum deles apresentou a tecnologia de RFID como mecanismo implementado nas empresas, sendo feito apenas uso de código de barras para identificar e rastrear os produtos sempre que há leitura do código de barras, ao longo do processo logístico. Como visto na literatura, a utilização de código de barras não permite a identificação individual de cada item abrindo assim possíveis hipóteses para vulnerabilidades a trocas ou roubos, deste modo, o investimento em tecnologias IoT mais avançadas, como os RFID, é mantido na mente dos profissionais como uma possível solução caso se denote um acréscimo no número de fraudes devido à alta contribuição destas tecnologias na mitigação de fraudes como a de produto não recebido*, jiffy bag*, roubo de encomendas, falsificação do estado logístico de entrega e fraude de troca de mercadorias.

Por sua vez, o sistema de GPS foi mencionado apenas por 2 entrevistados, sendo, no entanto, apenas utilizado nos camiões de transportes e não nas caixas de transporte,

configurando-se então como mecanismos aplicados pelos parceiros logísticos responsáveis pelo transporte, apresentando-se assim como mecanismos externos às empresas de retalho, mas que acabam por influenciar positivamente a empresa no combate à fraude na última milha pois permite-lhes aceder à localização contínua do pacote e receber alertas em caso de anomalias verificadas no transporte como paragens não autorizadas ou atrasos suspeitos. Deste modo, o uso de GPS surge como um mecanismo antifraude útil, tal como é retratado na literatura, contudo, é apenas eficaz se estiver integrado a um sistema de monitorização e alertas, com pessoas ou algoritmos a reagir a comportamentos suspeitos.

Deste modo, é possível auferir que uma boa relação com os parceiros logísticos permite reduzir a probabilidade de incendia de fraudes na última milha, sendo assim um dos motivos apontados pelos entrevistados pelos quais os retalhistas estabeleçam protocolos de segurança e contratos com objetivos definidos com os parceiros de transporte. Esta ligação permite às empresas beneficiar dos mecanismos utilizados pelas empresas transportadoras, como o GPS nos meios de transporte e as portas de intrusão; garantir a integração eficiente de sistemas de rastreabilidade e comunicação, de modo a que haja informação cruzada e coerente entre retalhista e transportadora e garantir um alinhamento de objetivos entre retalhista e transportadora, diminuindo as possíveis intensões fraudulentas dos funcionários encarregues do transporte. Assim torna-se possível assegurar uma maior segurança nas entregas e/ou nas devoluções, contribuindo desta forma para a diminuição de fraudes como a de roubo de encomendas, produtos não recebidos e manipulação do estado logístico de entrega. Numa lógica semelhante, foi também mencionada a prática de estarem sempre presentes pelo menos dois funcionários no ato de entrega/recolha de produtos (associada à devolução) em pontos que não sejam a loja física, deste modo os entrevistados acreditam que haja maior controlo sobre as encomendas e que haja um decréscimo nas tentativas fraudulentas como o roubo de encomendas e a manipulação do estado de entrega.

Assim, de modo a garantir uma boa seleção dos parceiros logísticos foi mencionada a possibilidade de implementação de sistemas de *reviews* onde os clientes possam avaliar o processo relacionado à entrega ou devolução das suas encomendas, permitindo assim aos retalhistas perceber a qualidade do serviço dos seus parceiros logísticos, de modo a selecionar apenas os parceiros que detenham o menor número de incidências associado. Deste modo, permite de certa forma perceber se a origem de possíveis fraudes provém do cliente ou do transportador, visto que, "se um parceiro tiver baixas incidências relacionadas a fraudes, e se o processo de qualidade no processamento das encomendas for preservado, então há maiores

possibilidades do ato fraudulento ocorrer por parte do cliente, contudo não é por si só um mecanismo decisivo e deve ser aliado a outros mecanismos que permitam detetar se o ato configura de facto uma fraude e se sim, apurar a origem da mesma de modo a atribuir responsabilidades"[2]. Todavia, o sistema de *reviews* não está apenas relacionado à escolha da melhor transportadora, também permite à empresa estabelecer um contacto contínuo permitindo um controlo no ponto de contacto com o cliente, pois a recolha e monitorização ativa de avaliações por parte dos clientes pode ajudar a sinalizar padrões de comportamento suspeito, como contas que sistematicamente alegam problemas com as entregas/devoluções, permitindo construir perfis de risco com utilização de IA ou mesmo de forma manual, dependendo do tipo de empresa, como foi analisado anteriormente.

Como mencionado de forma breve anteriormente, foi destacado pelos entrevistados a importância da existência de um processo de controlo de qualidade no processamento das encomendas, garantindo que os produtos enviados correspondem ao pedido e se encontram nas condições devidas, não deixando margens para reclamações indevidas. No entanto, esta medida exige procedimentos rigorosos e tempo adicional nas fases de embalagem e verificação, o que pode ser considerado inviável em operações com elevados volumes ou com modelos *fulfillment* terceirizados (modelo em que uma empresa delega a um parceiro externo o armazenamento, preparação e envio das encomendas aos clientes), pois acarreta mais custos e origina processos mais lentos. Contudo, apresenta-se como uma medida com alta frequência de menção e de implementação, visto que assegura que o conteúdo enviado é o correto e que está devidamente registado e embalado. Este mecanismo aliado com mecanismos de rastreabilidade e a seleção de transportadoras com baixas incidências reduz o espaço para alegações de não recebimento parcial/total, de forma a obter um reembolso, ou alegações de que o produto não chegou nas condições esperadas, na tentativa por parte do consumidor de devolver um produto igual/semelhante, mas danificado, ocorrendo numa fraude de troca de mercadorias.

Com alta taxa de menção e de implementação, destaca-se também a exigência de comprovativo de prova de entrega, isto é, a implementação de um sistema que exige ao cliente no ato de receção do produto a autenticação da receção do mesmo através de uma assinatura digital ou autenticação por PIN que é enviado por e-mail ou por mensagem para o telemóvel, de modo a comprovar que de facto recebeu a encomenda. Foi também mencionado por alguns entrevistados a possibilidade de utilização de QR code ou autenticação biométrica no ato de

[2] Citação de profissional 1

entrega, contudo, apesar da menção, estes dois métodos ainda não são utilizados no seio empresarial do conhecimento dos entrevistados. A utilização de um sistema eficiente que permita autenticar a entrega, permite mitigar não só o risco de fraudes como de produto não recebido ou manipulação do estado de entrega como também reduzir litígios que possam ocorrer entre cliente, retalhista ou parceiro. Todavia, foi mencionado que apesar das assinaturas digitais servirem, de momento, como autenticador suficiente para se concretizar a entrega, este mecanismo pode não ser tão eficiente quanto um PIN ou até mesmo um QR code, pois por vezes é difícil verificar se a assinatura é de facto a do proprietário da encomenda. De facto, 3 dos 7 entrevistados manifestaram acreditar que o futuro das entregas passa por autenticação por base ou de QR code, pois é único e é gerado no momento, diminuindo assim a possibilidade de transmissão o que permite aumentar a probabilidade da encomenda ser entregue ao proprietário legal, ou ainda, a autenticação biométrica quando se resolver assuntos associados à privacidade do consumidor, como o princípio da minimização de dados que estabelece que apenas devem ser recolhidos dados pessoais estritamente necessários para a finalidade pretendida. Deste modo, a autenticação biométrica pode ser aplicada apenas se detiver consentimento explícito, informado e livre do consumidor, o que pode representar entraves para a sua implementação.

Adicionalmente, foi também mencionada a utilização de provas fotográficas que configurem um registo visual contínuo, registando em fotos todos os pontos pelos quais a encomenda passa (*tracking* fotográfico), ou um registo visual pontual no momento de entrega, garantindo desta forma a integridade da mesma e impedindo fraudes como a falsificação do estado logístico de entrega ou de produto não recebido. Contudo, mais uma vez, este mecanismo pode levantar problemas, visto que os retalhistas não estão de momento autorizados a fotografar o cliente ou a propriedade do mesmo sem o seu consentimento, o que dificulta comprovar se de facto foi entregue ao cliente certo e na morada certa, por isso, este mecanismo não é visto como eficiente quando utilizado sozinho, necessitando sempre de estar a associado a um sistema de autenticação de entrega. Todavia, apesar de ter sido mencionado como um possível mecanismo antifraude, o *tracking* fotográfico ainda não é implementado por nenhuma das empresas do conhecimento dos entrevistados, contudo, é um mecanismo que aos olhos dos profissionais poderá ser implementado quando se verificar um aumento das fraudes e quando se ultrapassar as barreiras legais associadas, necessitando, contudo, da política da empresa, quanto ao reporte fotográfico, ser bem explícita para o cliente no momento da compra online. Do mesmo modo, foi também mencionada a utilização de um comprovativo fotográfico ou em formato de vídeo no momento de devolução iniciado pelo cliente no embalamento do produto até chegar ao

armazém de destino, na tentativa do produto devolvido ser suscetível a comparação com o estado original e desta forma deter provas visuais em caso de disputa com o consumidor, permitindo assim reduzir a incidência de fraudes como troca de mercadorias, *bricking*, e *jiffy bag*.

De uma forma geral, a prática de utilização de comprovativos de prova de entrega/devolução está positivamente relacionada à identificada na literatura, contendo, contudo, algumas inovações não descritas na literatura como a utilização de PIN ou QR code.

Aliado aos mecanismos de prova de entrega e de recolha foi também mencionado o preenchimento de formulários de controlo de última milha realizado por todos os colaboradores envolvidos desde a fase do processamento da encomenda até à entrega e, em possíveis devoluções, desde a recolha até à verificação do produto devolvido. Deste modo, é possível deter informações dos itens em cada ponto que passa, como por exemplo hora, local, peso, e permite registar os funcionários envolvidos em todas as transações, desincentivando deste modo tentativas de fraudes internas e da transportadora. Este mecanismo é geralmente integrado com a autenticação da receção ou da devolução do produto realizada pelo cliente. Assim sendo, torna-se possível mitigar fraudes como a de roubo de encomendas, *bricking, jiffy bag,* troca de mercadorias e produto não recebido, permitindo em simultâneo atribuir responsabilidades em caso de litígio. Para atingir a máxima eficácia, esta prática necessita de ser integrada em sistemas integrados de modo a ser possível aceder aos formulários de entregas no momento de devoluções, possibilitando assim a comparações de informações para detetar possíveis fraudes, podendo realizar a comparação de forma manual ou com utilização de IA permitindo criar alertas no momento de inserção de dados inconsistentes.

De facto, é de extrema importância as empresas deterem capacidades de integração entre plataformas internas e externas (entre a empresa e transportadoras por exemplo) aliadas a sistemas de informação interoperáveis, pois apenas desta forma é possível implementar uma monitorização ponta a ponta, isto é, um acompanhamento 360º do ciclo de vida da encomenda, procurando integrar todas as fases do processo logístico desde a preparação da encomenda até à sua entrega e possível devolução, exigindo assim uma grande capacidade de troca e armazenamento de informações. Desta forma, a integração entre plataformas permite criar um sistema que gera registos confiáveis, permitindo detetar fraudes ao cruzar informações de múltiplas fontes (como pagamentos, entregas, cliente) dificultando alegações como a de

produtos não recebido; a ocorrência de *bricking*, a falsificação do estado logístico de entrega, a ocorrência de roubo de encomendas e até mesmo a manipulação de endereços.

Por sua vez, a integração omnicanal surge como uma estratégia vantajosa tal como referido por todos os entrevistados, uma vez que permite alinhar o canal físico e digital numa única estrutura de controlo e atendimento, centralizando os dados entre os canais. Deste modo, ao reunir as informações num único sistema, torna-se possível detetar padrões suspeitos, como *chargeback*; deteção de mudanças frequentes de endereços associados ao mesmo cliente gerando em simultâneo alertas para a revisão manual antes da expedição da encomenda; fraude de descontos como o abuso de códigos promocionais, pois evita múltiplas utilizações, limitando o usos por cliente, produto ou período e, por fim, facilita a verificação cruzada para evitar reembolsos fraudulentas derivados de tentativas por parte do consumidor de realizar fraudes de reembolso entre retalhistas, ou tentativas de reembolso duplicado em diferentes canais ou, sté mesmo, fraudes de troca de mercadorias, uma vez que se torna possível verificar se o produto foi de facto comprado no retalhista, se o produto já tem um reembolso em curso ou terminado e se o produto está de facto associado ao perfil do cliente. Todavia, esta integração requer infraestruturas robustas, uma gestão de stock em tempo real e políticas uniformes entre canais, fatores que representam barreiras em empresas com menor maturidade. Ainda assim, revela-se como um dos principais mecanismos implementados pelas empresas com canal de *e-commerce* B2C, sendo visto como uma das prioridades de empresas multicanal.

Adicionalmente, foi também mencionada a importância do agendamento de entregas e/ou recolhas, associadas a devoluções, de modo a reforçar a validação no ato de entrega/recolha e, evitar deslocações desnecessárias permitindo deste modo reduzir os custos associados à última milha e minimizar o espaço aberto a tentativas de fraudes, o que denota uma clara orientação preventiva. Deste modo, o agendamento cria uma prova de que o cliente detinha conhecimento da entrega e se mostrou disponível para a mesma, reduzindo assim a margem para negar a sua receção. Para além disso, torna-se mais fácil garantir que a entrega é feita à pessoa certa e que o cliente está presente evitando que a encomenda fique vulnerável a roubos, contudo exige da empresa uma grande integração de informações atualizadas e em tempo real bem como processos logísticos robustos.

Uma outra prática emergente mencionada por um profissional é a colocação de etiquetas térmicas, em oposição da etiquetagem em locais externos mencionada na literatura que, segundo o entrevistado, pode danificar o produto mesmo antes da sua utilização. Todavia, as

etiquetas térmicas ainda se encontram em processo de desenvolvimento, não estando de momento disponíveis para utilização. Contudo, demonstram-se como um mecanismo inovador com competências para mitigar fraudes como o *wardrobing* que ocorrem sobretudo no setor da moda, uma vez que após um certo período em contacto com o calor e/ou humidade da pele a etiqueta muda de cor de forma irreversível, permitindo assim ao retalhista verificar se a peça já foi utilizada. Este mecanismo não consta na literatura existente visto que representa um mecanismo emergente no meio empresarial, ainda em fazes de teste.

Os dados demonstram que fraudes como o *wardrobing* também podem ser combatidas através de ajustes de políticas de devoluções, implementado assim políticas de devolução antifraudes. Neste âmbito, foi mencionado a substituição da política de reembolsos em dinheiro por políticas de ofertas de vales ou cartões oferta como um possível mecanismo antifraude, pois desincentiva compras com intenções de devoluções fraudulentas, contudo, não é um mecanismo atualmente implementado nas empresas do conhecimento dos entrevistados pois acaba por se configurar num mecanismo que pode diminuir a satisfação e intenções de compra de clientes que agem de boa-fé.

Adicionalmente, a mudança nas políticas de devolução como a imposição de restrições sazonais nos prazos de devolução de peças temáticas de forma a diminuir este prazo em épocas festivas como o Natal, Carnaval e *Halloween*, é vista como uma prática que pode proporcionar um decréscimo no número de devoluções fraudulentas, uma vez que esta restrição impossibilita a devolução de peças relacionadas aos temas festivos após o dia de comemoração. No entanto, não é um mecanismo atualmente utilizado em nenhuma empresa do conhecimento dos entrevistados, é apenas um mecanismo cuja implementação depende do crescimento de fraudes de *wardrobing* ou relacionadas, e que, como referido pelos entrevistados, obrigará os retalhistas a expressar a política de forma explícita e visível para todos os clientes. Todavia, de uma forma oposta à literatura, os entrevistados não veem a diminuição dos prazos de devolução de artigos, que não sejam relacionados a épocas festivas, como um método eficaz no combate às fraudes, pois acreditam que os infratores já realizam as compras com dolo fraudulento e não é pela diminuição deste prazo que deixarão de cometer as fraudes, simplesmente as realizarão mais cedo de forma a efetuar as devoluções dentro do limite legal. A análise, no entanto, demonstrou ser de extrema importância o estabelecimento de políticas claras de reembolso e contestação para proteger a empresa e o cliente de má-fé, sendo este o primeiro passo para efetuar qualquer mudança nas políticas de devolução.

Um mecanismo também ligado ao processo de devolução e que se demostrou uma prática aplicada de forma generalizada é a exigência do comprovativo de compra, a fatura, no momento de devolução. Desta forma, aos retalhistas podem mitigar fraudes relacionadas a reembolso entre retalhistas, roubo de encomendas, fraude de desconto, fraude de troca de mercadoria e fraude de reembolso em múltiplos canais, uma vez que é apresentado o comprovativo que permite identificar o artigo que o cliente pretende devolver e, de certa forma, aumentar a probabilidade da pessoa que efetua a devolução se tratar do proprietário legal. Para além disto, os dados recolhidos permitem identificar outro mecanismo relacionado às políticas de devolução, sendo este a verificação dos produtos no momento de devolução. Todos os entrevistados mencionaram este mecanismo como prática recorrente no seio empresarial pois permite à empresa confirmar, no ato de devolução, se o produto corresponde de facto ao que foi adquirido, analisando o estado, conteúdo e integridade do mesmo. Atualmente esta etapa de verificação é realizada pelos funcionários nas lojas físicas ou, em caso da devolução ser realizada fora da loja, nos armazéns após o transporte logístico, sendo o reembolso processado apenas depois da verificação, permitindo deste modo mitigar fraudes como *jiffy bag*, *bricking*, *wardrobing* e fraudes de troca de mercadorias no momento de devolução. Por último, relativamente ao processo de devolução, foi também mencionado a importância do pagamento de taxas de devolução à responsabilidade do consumidor quando as mesmas não são efetuadas em loja e não derivam de algum engano por parte do retalhista na preparação da encomenda. Deste modo, os profissionais acreditam que para além de ajudar a cobrir os custos de transporte acarretados pelas empresas, o pagamento de taxas de devolução pode desincentivar os infratores a efetuarem devoluções fraudulentas, uma vez que tem de pagar para devolver os produtos. Em contrapartida, reconhecem que pode ser um fator menos apreciado pelos clientes digitais, visto que mesmo que estejam a agir de boa-fé tem de pagar as taxas para poderem devolver o artigo. É possível verificar que a implementação no seio empresarial de políticas antifraude de devoluções, como a exigência do comprovativo de compra e o pagamento de taxas de devolução, vão de encontro ao que é proposto na literatura, apresentando-se como uma das práticas mais utilizadas pelas empresas portuguesas para prevenir e mitigar as fraudes na última milha.

Entre os mecanismos mais valorizados destacam-se também a execução regular de auditorias que permitem identificar padrões anómalos, abusos e falhas nos processos, através da análise sistemática de registos, transações e procedimentos de modo a verificar se estes estão a ser efetuados corretamente. Deste modo, num contexto de prevenção de fraudes, cruzam

dados de vendas, devoluções, inventários, entregas e comportamentos do cliente, à procura de incoerências ou padrões suspeitos. Desta forma, tal como defendido na literatura, configuram um papel dissuasor, uma vez que aumentam a transparência e a probabilidade de deteção de comportamentos fraudulentos, visto que, a perceção de controlo reduz a probabilidade de ocorrência de fraudes deliberadas, para além disso permite verificar vulnerabilidades, permitindo posteriormente definir medidas de combate às mesmas.

Por outro lado, destacam-se também com alta frequência de menção a capacitação de equipas antifraude, isto é, a necessidade, para algumas empresas, e a realidade já implementada noutras, da existência de equipas especializadas na análise de dados e deteção de fraudes que contribuem para a identificação de esquemas mais sofisticados e menos percetíveis, permitindo assim mitigar fraudes como, por exemplo, a fraude exploratória por encomendas de teste ou de manipulação de endereços. No entanto, este mecanismo implica um investimento significativo em recursos humanos qualificados e tempo de monitorização contínua, sendo geralmente viáveis apenas em organizações com maiores recursos e maturidade. Por sua vez empresas com menos recursos ou com baixas incidências fraudulentas tendem a recorrer a abordagens mais reativas evitando custos fixos elevados associados a equipas especializadas, deste modo apenas 4 dos 7 entrevistados que mencionaram este mecanismo é que o implementam de facto. De uma forma complementar, outro mecanismo frequentemente referido como essencial para a capacitação de equipas antifraude e com alta taxa de implementação é o treino e sensibilizações dos colaboradores, principalmente nas equipas de atendimento ao cliente, logística e armazém pois são estes que entram em contacto direto com as encomendas a serem entregues ou devolvidas. A eficácia deste tipo de ação depende, contudo, da consistência dos programas formativos, da baixa rotatividade da força de trabalho e da disponibilidade de tempo e recursos despendidos em formação continua. Com base nos dados recolhidos, é possível auferir que o treino dos colaboradores é visto como uma das prioridades das empresas, indo deste modo de encontro com o proposto pela literatura, uma vez que, funcionários treinados conseguem identificar produtos devolvidos usados ou alterados, táticas de abuso recorrentes por parte de consumidores e tentativas de aplicação indevida de descontos.

Por fim, uma prática mencionada por todos os entrevistados é a necessidade de pagamento no ato da compra, uma prática comum no *e-commerce*, que reduz significativamente o risco de fraude associado a recusas de pagamento, fraudes de reembolsos em múltiplos canais, pois fica registado de forma clara o canal específico de compra, o que impede o cliente de alegar que pagou noutro canal para obter reembolsos duplicados, e fraudes de manipulação de endereço,

quando o intuito é manipular o local de entrega de modo a não pagar o item ou a taxa de entrega, modificando o endereço de entrega para um cacifo, por exemplo. Contudo, foi mencionada, de forma complementar, a necessidade, de por vezes, limitar os modos de pagamento em certas transações visto que, algumas plataformas de pagamento digitais, como o Paypal, podem representar um maior risco para os vendedores, uma vez que facilitam a abertura de disputas por parte dos clientes e, frequentemente, adotam políticas de proteção ao comprador. Isto pode levar a situações em que, mesmo com certas provas de entrega, a empresa perca o valor da venda devido a contestações ou fique com o valor congelado durante o processo de análise, afetando o fluxo de caixa do negócio. Deste modo, esta restrição poderá reduzir a ocorrências de fraudes como o *chargeback*.

Posto isto, é possível concluir que apesar da maioria dos mecanismos referidos pelos profissionais entrevistados encontrar respaldo na literatura, é constatável que algumas das soluções tecnológicas e estratégicas destacadas em estudos académicas e técnicos não foram mencionadas pelos entrevistados como mecanismos implementados. Esta ausência levanta questões relevantes sobre a distância entre o conhecimento teórico e a sua aplicação prática no contexto empresarial. Mecanismos como RFID (com e sem sensores), autenticação biométrica e a etiquetagem em locais externos já foram anteriormente discutidos devido à ausência da sua aplicação nas empresas estudadas, deste modo torna-se pertinente analisar as possíveis razões para a não adoção de outros mecanismos como o blockchain, entregas por drones, e externalização antifraude via contratação estratégica de 3PLs, os quais, embora apontados como promissores na mitigação de fraudes na última milha tanto na literatura tanto por alguns entrevistados, não emergiram nas respostas de nenhum profissional como mecanismos efetivamente implementados.

Relativamente à tecnologia blockchain, foi mencionada por um entrevistado que relatou a tentativa de aplicação deste mecanismo no seio da empresa que se efetivou como uma implementação falhada e com grades perdas económicas. De facto, embora a literatura destaque o potencial disruptivo de soluções como a blockchain para a rastreabilidade e verificação de integridade das entregas/devoluções, também ressalva os seus desafios de implementação, apoiando de certo modo a visão dos profissionais quanto a este mecanismo. A blockchain é vista como uma tecnologia de difícil integração e cujos custos de implementação, complexidade técnica e exigência de padronização de sistemas entre múltiplos *stakeholders* retarda, ou até mesmo impede, a sua adoção em ambientes logísticos reais. Através da análise dos dados recolhidos nas entrevistas é possível destacar a existência de uma inconsistência da unidade

transacional ao longo da cadeia de abastecimento como um dos maiores obstáculos à implementação deste mecanismo, visto que, os produtos podem ser desagregados, reagrupados ou transformados em diferentes formatos em cada etapa logística, o que provoca um aumento substancial dos dados registados e o que dificulta o rastreamento contínuo e preciso de cada um. Sem um sistema robusto para registar estas mudanças, a correspondência entre o identificador digital na blockchain e o bem físico torna-se frágil, comprometendo a eficácia do sistema na deteção de fraudes ou desvios nos pontos finais da distribuição.

Por sua vez, mecanismos como entregas por drones também foram alvo de discussão junto dos profissionais, contudo, as conclusões auferidas foram, de uma forma geral, semelhantes, refletindo-se como um mecanismo ineficaz na área da logística, tanto devido a restrições legais como a desafios de escalabilidade urbana. De facto, foi mencionado o problema relacionado à escalabilidade de custos uma vez que um drone não permite efetuar entregas/recolhas em larga escala, aumentando desta forma os custos associados à última milha, e por isso, não é apontada como uma prática adotada nem foi demonstrada intenção de futura implementação.

Como referido, apesar da literatura destacar a possibilidade de subcontratação de operadores logísticos especializados (3PLs) como uma estratégia para aumentar a eficiência e reforçar os mecanismos de mitigação de fraudes, nas entrevistas realizadas não foi mencionado como um mecanismo implementado. Contudo, é visto por alguns profissionais como uma solução eficaz num futuro em que as fraudes configurem um problema grave na empresa. Esta decisão de não externalizar o tratamento logístico, e consequentemente das fraudes, está relacionada sobretudo aos custos adicionais associados a esta contratação, uma vez que o impacto das fraudes não é considerado significativo não é um custo considerado necessário. Para além disso, esta externalização pode causar problemas associados à confidencialidade e proteção de dados bem como de uma possível perda de visibilidade e controlo sobre processos sensíveis associados à gestão de fraudes.

Posto isto, é evidente um ligeiro desalinhamento entre a viabilidade prática de alguns mecanismos e a exposta na literatura existente.

Na maioria dos casos, os entrevistados revelaram barreiras à adoção de mecanismos derivado a: (1) elevados custos de implementação e manutenção, principalmente de mecanismos tecnológicos, uma vez que podem comprometer a viabilidade económica do projeto, sobretudo em empresas com orçamentos limitados; (2) alta complexidade operacional devido à gestão de volumes elevados de dados, à integração de múltiplos sistemas e tecnologias,

à coordenação entre vários departamentos e parceiros e à necessidade de monitorização e controlo contínuos, o que no seu todo dificulta a integração e gestão eficiente dos mecanismos, exigindo maior coordenação e controlo; (3) interdependência de vários sistemas para garantir um *tracking* eficiente, tornando o sistema vulnerável a falhas em qualquer ponto da cadeia de abastecimento, comprometendo a rastreabilidade; (4) limitações técnicas relacionadas a desatualizações, a sistemas incompatíveis, a baixa capacidade de armazenamento e processamento e a baixa capacidade de cibersegurança o que pode impedir o funcionamento pleno dos mecanismos ou a compatibilidade com a infraestrutura existente; (5) falta de especialização, relacionada à falta de equipas especializadas ou altas taxas de rotatividade de trabalhadores, o que contribui para o desconhecimento ou a impossibilidade de implementação de boas práticas do setor; (6) dependência de terceiros (como de transportadoras) o que reduz o controlo direto sobre os processos, aumentando o risco de falhas e atrasos; (7) a necessidade de encontrar mecanismos que sejam coerentes com o nível de eficiência e experiência que a empresa pretende oferecer ao cliente exigindo que os sistemas implementados estejam totalmente alinhados com as expectativas do serviço prestado, o que pode limitar as opções de combate disponíveis, aumentar custos e exigir mais personalização e controlo.

4.2.4. Grau de adoção dos mecanismos antifraudes nas empresas portuguesas

No contexto do presente estudo, a taxa de adoção de mecanismos antifraudes é considerada (1) Elevada quando os mecanismos têm 6 ou mais aplicações efetivas (nº de implementações); (2) Moderada se detiver entre 3 e 5 (inclusive); (3) Baixa ou inexistente se for menor que 3 ou igual a 0, respetivamente. Este critério baseia-se na distribuição observada no estudo (número de vezes que cada mecanismo é implementado), servindo como uma métrica prática para avaliar o grau de adoção de cada solução nas operações das empresas com canal de *e-commerce* em Portugal.

Deste modo, a análise revela que, de forma geral, o grau de adoção dos mecanismos de mitigação de fraudes na última milha em Portugal é moderado, ou seja, parcialmente desenvolvido. Isto significa que, embora exista um conjunto razoável de práticas em uso, muitas delas de natureza processual, a adoção de mecanismos mais sofisticados, sobretudo tecnológico, permanece limitada e desigual entre empresas como é constatável na Tabela 4.3, onde são listados todos os mecanismos identificados tanto na literatura quanto nas entrevistas.

Tabela 4.3 - Grau de adoção dos mecanismos antifraudes existentes

Fonte: Elaboração Própria

Mecanismos existentes (Retirados das Entrevistas + Revisão da Literatura)		Nº de empresas que implementam (das 7 entrevistadas)	Mecanismos presentes na literatura	Tipo de mecanismo
IA		4	x	Tecnológico
ML		4	x	Tecnológico
Blacklist e construção de perfis de risco		7	x	Tecnológico/ Processual
IoT	RFID (com/sem sensores integrados)	0	x	Tecnológico
	GPS	2	x	Tecnológico
	Código de barras	7	x	Tecnológico
Portas de intrusão nos transportes		3		Tecnológico
Contratos com os parceiros logisticos com objetivos estabelecidos		5		Processual
Presença de pelo menos 2 funcionários no transporte		4		Processual
Sistema de *reviews* de clientes		3		Tecnológico
Processo de controlo de qualidade no processamento de encomendas		6		Processual
Tracking fotográfico tanto na entrega como em possíveis devoluções		0		Tecnológico
Sistema de autenticação de entrega	PIN, Assinatura	7	x	Tecnológico
	Qr code, Autenticação biométrica	0		Tecnológico
Registo fotográfico pontual na entrega, na recolha e à chegada armazém		2	x	Tecnológico
Preenchimento de formulários de controlo de última milha		6		Processual
Agendamento de entregas e/ou recolhas associadas a devoluções		3	x	Processual
Integração entre plataformas		7	x	Tecnológico
Integração omnicanal		7	x	Tecnológico
Colocação de etiquetas térmicas		0		Tecnológico
Política de reembolsos em vales ou cartões oferta		0	x	Processual
Imposição de restrições sazonais nos prazos de devolução		0		Processual
Exigência do comprovativo de compra para efetuar devolução		7	x	Processual
Verificação do produto no momento de devolução		7		Processual
Pagamento taxas de devolução		6	x	Processual
Auditorias de conformidade para deteção de anomalias		7	x	Processual
Equipas especializadas em análise de dados e fraudes		4	x	Processual
Treino e sensibilização de funcionários		7	x	Processual
Pagamento no ato da compra		6		Processual
Limitação dos tipos de pagamento online		1		Processual
Contratação de 3PL		0	x	Processual
Blockchain		0	x	Tecnológico
Etiquetagem em locais externos		0	x	Processual
Entrega por drones		0	x	Tecnológico
Câmaras nos locais de embalagem das encomendas		0	x	Tecnológico

Importa reconhecer que esta realidade está fortemente relacionada à perceção dos profissionais de que a incidência de fraudes na última milha é, ainda, residual. Esta mentalidade pode conduzir a uma menor urgência ou prioridade na implementação de soluções preventivas mais automatizadas, uma vez que o risco percebido não justifica, do ponto de vista de muitos profissionais, o investimento necessário.

De uma forma sucinta, a ausência de implementação de determinados mecanismos, que embora sejam amplamente referenciados na literatura, pode ter duas justificações: (1) mecanismos como RFID (com e sem sensores), autenticação biométrica e contratação 3PL, são mecanismos que na visão dos entrevistados, apesar de não serem implementados atualmente por nenhuma empresa da amostra, surgem como práticas promissoras e eficientes no combate à fraude, tal como defendido na literatura, contudo só reconhecem a necessidade de implementação caso se verifique um aumento das fraudes; (2) mecanismos como etiquetagem em locais externos, blockchain e entrega por drones, evidenciam a existência de um desalinhamento entre o potencial teórico e a viabilidade prática, configurando-se em mecanismos que, do ponto de vista dos entrevistados, se demonstram ineficientes e desajustados à realidade logística. Por sua vez, a prática de colocação de câmaras nos locais de embalagem das encomendas, foi identificado na literatura, mas não foi mencionado nas entrevistas não sendo assim possível determinar a sua eficiência real no combate às fraudes.

Desta forma, é possível aferir que embora a teoria aponte para a eficácia de sistemas integrados e soluções tecnológicas na prevenção de fraudes na última milha, a sua aplicação real no seio empresarial continua limitada, sendo o grau de adoção de mecanismos antifraudes desigual entre empresas. Contudo, os profissionais revelam consciência da possibilidade de riscos futuros. De momento, 3 dos 7 entrevistados demonstram estarem satisfeitos com os mecanismos já implementados, não vendo necessidade de efetuar mais investimentos para colocar em curso processos de implementação de mecanismos, justificando a decisão com base nas baixas incidências de fraudes, demonstrando-se, contudo, disponíveis e atentos a necessidades de atualizações e melhoria futura em consonância com o crescimento do *e-commerce* e consequentemente do aumento de tentativas fraudulentas. Por sua vez, os restantes profissionais, defendem que os mecanismos implementados atualmente, agregados aos que já detêm planos de implementação futura, configuram uma eficiência capaz de mitigar as fraudes das quais as empresas são alvo. De uma forma geral, os dados obtidos nas entrevistas revelam um esforço contínuo e atento por parte das empresas no combate às fraudes.

Em síntese, apesar da existência de boas práticas face ao cenário de fraudes atual e a sensibilização para o tema, o atual cenário aponta para uma adoção moderada e seletiva dos mecanismos disponíveis, destacando a utilização de mecanismos sobretudo processuais em detrimento de mecanismos tecnológicos, como IA, ML, RFID, GPS, que são amplamente referidas na literatura, mas com pouca aplicação prática no contexto nacional. De facto, a baixa perceção do risco de fraude combinada com barreiras de implementação tem contribuído para

esta realidade. A decisão de implementação está, portanto, condicionada a fatores como o grau de maturidade digital e operacional da empresa, o perfil do consumidor, os recursos financeiros e humanos disponíveis, o tipo de produto comercializado e o risco a fraudes inerentes ao negócio. Assim, empresas com maior maturidade, com mais recursos, com produtos de maior valor ou com maior risco ou incidência de fraudes, destacam-se pela utilização de mecanismos sobretudos tecnológicos, frequentemente integrados em plataformas logísticas e operacionais complexas, permitindo uma abordagem preditiva às fraudes. Esta estruturação tecnológica reflete a escala e complexidade dos seus processos bem como, uma maior capacidade de investimento em soluções especializadas. Por outro lado, empresas com menor maturidade, com menos recursos, com produtos de menor valor ou com menor risco ou incidência de fraudes tendem a adotar estratégias mais reativas e com um menor grau de automação, justificando a ausência de mecanismos mais sofisticados por meio de dois fatores, a baixa incidência de fraudes reportadas e/ou as limitações operacionais e financeiras.

Diferentes tipos de empresas justificam diferentes mecanismos antifraudes e, portanto, a ausência de uma solução única reforça a necessidade de uma abordagem estratégica, adaptada à realidade operacional de cada organização, para um combate eficaz às fraudes na última milha.

4.2.5. Recomendação de mecanismos por perfil de empresa e recursos disponíveis

Como visto, com o crescimento exponencial do *e-commerce*, é expectável que o número de tentativas de fraudes na última milha também denote um crescimento, especialmente em ambientes digitais mais expostos e com maiores valores transacionais. Assim, é essencial que as empresas portuguesas passem a adotar medidas preventivas proporcionais à sua maturidade digital e operacional, recursos disponíveis e ao tipo de produto comercializado de modo a antecipar cenários futuros.

Em primeira instância, é fundamental que cada empresa realize um diagnóstico interno que permita avaliar o grau de maturidade digital e operacional, a complexidade da sua cadeia logística e os principais pontos de vulnerabilidades nos processos de entrega e devolução. Esta avaliação permitirá uma escolha mais eficaz e faseada dos mecanismos a adotar.

Assim, é de extrema importância analisar o risco de fraude atual e futuro de modo a verificar se detêm os mecanismos necessários ou se necessitam de realizar mais investimentos,

permitindo não só agir de forma proativa, como também ajudar as empresas com menos recursos a redirecionar os seus investimentos, não despendendo dinheiro em mecanismos extras que não sejam necessários.

Assim, a recomendar mecanismos antifraude é necessário ter em conta o perfil de cada empresa, em termos de maturidade digital e operacional, e posteriormente a nível de recursos disponíveis para investimento. Deste modo, a Tabela 4.4, apresenta os diferentes perfis tendo em conta os diferentes níveis possíveis de maturidade digital e operacional. Esta classificação é relevante pois a maturidade condiciona o tipo de mecanismos que uma empresa pode ou deve implementar, devido à estrutura que detêm, tanto a nível tecnológicos quanto a nível de processos internos e logísticos, isto é, empresas com maturidade digital mais baixa não serão capazes de implementar tecnologias mais avançadas por falta de estrutura tecnológica e empresas com maturidade operacional baixa terá dificuldade em implementar mecanismos que sejam dependentes de processos mais robustos.

Tabela 4.4 - Perfis de empresas face à maturidade digital e operacional

Fonte: Elaboração Própria

	Maturidade **Operacional Alta** (MO+)	Maturidade **Operacional Baixa** (MO-)
Maturidade **Digital Alta** (MD+)	**Perfil A**: Empresas estruturadas, com forte integração tecnológica e processos internos e logísticos sólidos	**Perfil B**: Empresas com forte integração tecnológica mas com processos internos e logísticos frágeis e pouco estruturados
Maturidade **Digital Baixa** (MD-)	**Perfil C**: Empresas com baixa capacidade de integração tecnológica mas com processos internos e logísticos sólidos	**Perfil D**: Empresas com baixa capacidade de integração tecnológica e processos internos e logísticos frágeis e pouco estruturados

Posto isto, face aos desafios intrínsecos de cada mecanismo e pela análise dos dados obtidos nas entrevistas, foi possível a elaboração da Tabela 4.5 que demonstra, de forma sumária, os mecanismos possíveis de implementação face aos perfis existentes e à disponibilidade de recursos financeiros, tendo apenas em consideração os mecanismos, que da ótica dos entrevistados, se demonstram eficientes ou promissores no combate às fraudes na última milha. (No Anexo E, encontram-se as justificações da não recomendação de alguns mecanismos para certos perfis de empresas.)

Tabela 4.5 - Mecanismos antifraudes recomendados por perfil de empresa e recursos financeiros

Fonte: Elaboração Própria

	Mecanismos recomendados					
Mecanismos detalhados	Perfil A (MD+/MO+)	Perfil B (MD+/MO-)	Perfil C (MD-/MO+)	Perfil D (MD-/MO-)	Recursos Financeiros Altos/ Moderados	Recursos Financeiros Limitados
IA	x	x			x	
ML	x	x			x	
Blacklist e construção de perfis de risco	x	x	x	x	x	x
RFID (com ou sem sensores integrados)	x				x	
GPS	x	x	x		x	x [2]
Código de barras	x	x	x	x	x	x
Portas de intrusão nos transportes	x	x	x	x	x	x [2]
Contratos com os parceiros logísticos com objetivos estabelecidos	x	x	x	x	x	x
Presença de pelo menos 2 funcionários no transporte	x	x [2]	x	x [2]	x	x
Sistema de *reviews* de clientes	x	x			x	x
Processo de controlo de qualidade no processamento de encomendas	x	x	x		x	x
Tracking fotográfico tanto na entrega e na recolha	x	x	x		x	x
Autenticação de entrega por PIN/ assinatura/ Qr code	x	x	x	x	x	x
Autenticação de entrega por autenticação biométrica	x	x			x	
Registo fotográfico pontual na entrega, na recolha e à chegada ao armazém	x	x	x		x	x
Preenchimento de formulários de controlo de última milha	x	x	x	x	x	x
Agendamento de entregas e/ou recolhas associadas a devoluções	x				x	
Integração entre plataformas	x	x			x	
Integração omnicanal	x	x			x	
Colocação de etiquetas térmicas [1]	x	x	x	x	x	- [3]
Política de reembolsos em vales ou cartões oferta	x	x	x	x	x	x
Imposição de restrições sazonais nos prazos de devolução	x	x	x	x	x	x
Exigência do comprovativo de compra para efetuar devolução	x	x	x	x	x	x
Verificação do produto no momento de devolução	x	x	x	x	x	x
Pagamento taxas de devolução	x	x	x	x	x	x
Auditorias de conformidade para deteção de anomalias	x		x		x	x
Equipas especializadas em análise de dados e fraudes	x	x			x	
Treino e sensibilização de funcionários	x	x	x	x	x	x
Pagamento no ato da compra	x	x	x	x	x	x
Limitação dos tipos de pagamento online	x	x	x	x	x	x
Contratação de 3PL	x	x	x	x	x	

(1) Quando saírem da fase de teste e forem lançadas para o mercado

(2) Se forem implementados pelos parceiros logísticos

(3) Por estarem em fase de teste ainda não é possível auferir os seus custos de implementação ou manutenção

De uma forma geral, as recomendações apresentadas refletem a importância da implementação de uma abordagem estratégica, faseada e adaptada à realidade operacional e digital de cada empresa. De facto, a mitigação de fraudes na última milha não depende apenas de tecnologias de ponta, mas sim de uma combinação equilibrada entre processos robustos, cultura organizacional preventiva, capacitação de recursos humanos e, progressivamente, a incorporação de soluções mais automatizadas e digitais. A tabela evidencia que independentemente do perfil de uma empresa e dos com recursos financeiros disponíveis, todas as empresas dispõem de mecanismos viáveis para reforçar o controlo e a segurança nas etapas logísticas finais. A chave está na coerência entre o nível de maturidade, os recursos disponíveis para investimento, as fraudes incorridas e as medidas implementadas, permitindo desta forma garantir eficácia no combate às fraudes sem comprometer a sustentabilidade operacional.

Uma empresa tecnologicamente avançada e com processos internos e logísticos robustos e estruturados, como o perfil A, é capaz de adotar a maioria dos mecanismos, incluindo os mais exigentes, como IA, RFID e biometria. Por sua vez, empresas do perfil B (MD+/MO-) devem focar-se em aprimorar processos logísticos básicos antes de adotar mecanismos que dependam fortemente de operações estruturadas, mesmo que detenham uma estrutura com capacidade de integração tecnológica, uma vez que detém processos logísticos frágeis, passando a sua evolução pela integração gradual dos processos operacionais às tecnologias disponíveis. Já as empresas do perfil C (MD-, MO+), devem focar-se em introduzir a digitalização de forma progressiva, aproveitando a robustez dos seus processos internos e logísticos para implementar tecnologias simples como códigos de barras e sistemas básicos de *tracking*, evoluindo gradualmente para soluções mais integradas e automatizadas conforme a evolução da infraestrutura digital. Por fim, empresas do perfil D (MD-/MO-), devem focar-se em mecanismos essenciais e simples, sobretudo processuais e de baixo custo, evoluindo, de forma gradual, em consonância com o desenvolvimento da maturidade digital e operacional.

Além da maturidade digital e operacional, a avaliação da viabilidade por recursos completa esta análise, destacando que alguns mecanismos, ainda que adequados a um certo perfil, não são exequíveis sem os recursos financeiros necessários. Empresas com recursos limitados devem priorizar soluções econômicas e processuais, enquanto as com maior capacidade financeira podem investir em tecnologias sofisticadas.

Desta forma, a prevenção de fraudes na última milha deve ser vista como um esforço contínuo, multidisciplinar e proporcional, que evolui conforme o crescimento da empresa,

desenvolvimento dos processos internos, perceção do risco de fraude e a transformação digital. Posto isto, os mecanismos antifraudes implementados devem ser proporcionais ao risco presente e à perceção de risco futuro, que é influenciado tanto pela estrutura da empresa quanto pela natureza dos produtos comercializados, conjugando a tecnologia com o conhecimento e experiência de profissionais especializados para combater as fraudes de forma eficaz, indo assim de encontro ao sugerido na literatura. Para além disso, é importante ter em conta que nenhum mecanismo é por si só suficiente para mitigar as fraudes, necessitando, portanto, de estratégias que permitam a integração de diversos mecanismos complementares no combate às fraudes na última milha.

5. Conclusão

Por fim, no último capítulo apresentam-se as conclusões da investigação, reunindo as considerações finais com base nos objetivos definidos e nos dados recolhidos e analisados. Posteriormente identificam-se os contributos académicos e empresariais do estudo bem como as limitações identificadas no decorrer da investigação. Por último, propõe-se sugestões para investigações futuras, com o objetivo de coadjuvar no desenvolvimento do conhecimento na área de estudo.

5.1. Considerações finais

O presente estudo tem como foco compreender de que forma empresas com canal de *e-commerce* B2C em Portugal podem mitigar as fraudes na última milha. Para isto, a investigação teve como objetivos compreender os desafios enfrentados na última milha que contribuem para o aparecimento de fraudes, identificar os tipos de fraudes na última milha, bem como os mecanismos de mitigação existentes e os seus desafios de implementação, e por fim, perceber o grau de adoção destes mecanismos no seio empresarial.

Após a aplicação do estudo torna-se possível concluir que a última minha se configura de facto como uma fase onerosa, sobretudo no contexto atual de transformação digital do consumo, pela sua complexidade operacional e elevada exposição a riscos. Este estudo confirma que os desafios decorrem não só da crescente pressão por entregas rápidas e flexíveis, como também da necessidade de políticas de devolução flexíveis cada vez mais convenientes ao consumidor digital, devido à distância física entre o consumidor e o produto. Paralelamente, a necessidade de *tracking* e gestão de stocks em tempo real, amplificam os desafios logísticos e as vulnerabilidades das operações que podem ser exploradas por atores maliciosos. Adicionalmente, as empresas enfrentam desafios relacionados a comunicação e integração entre sistemas devido à existência de diversos intervenientes no processo logístico de última milha, exigindo assim um sistema unificado e capaz de registar e partilhar informações, o que representa um desafio para algumas empresas com uma estrutura digital menos desenvolvida.

Observou-se ainda que os modelos de entrega e de recolha intrínsecos do processo de última milha, influenciam o tipo de desafios e vulnerabilidades que um retalhista enfrenta. Foram verificadas diversas formas de entrega e de devolução de produtos, pois embora modelos de entrega e devolução em loja física apresentem menor exposição a fraudes na última milha,

devido à existência de um controlo mais direto, não são viáveis como solução única, dada a expectativa do consumidor por conveniência e múltiplas opções de entrega e devolução que configurem maior comodidade. Assim, tornou-se necessário a adoção de outros modelos de entrega/recolha como ao domicílio, pontos de recolha parceiros e cacifos.

Por sua vez, relativamente às principais fraudes na última milha no *e-commerce*, embora a literatura e os dados obtidos apontem para diversas tipologias de fraudes na última milha, o estudo identificou predominantemente as fraudes relacionadas à alegação de produto não recebido e roubo de encomendas como as mais transversais no contexto português. Em simultâneo, o estudo permitiu corroborar com a literatura quanto à defesa da heterogeneidade da origem das fraudes, podendo as mesmas ser de origem interna (realizada por colaboradores internos) ou externa.

O presente estudo revelou uma correlação entre o tipo de setor e a tipologia de fraude enfrentada, demonstrando que setores com altas operações logísticas e margens de lucro mais reduzidas estão mais expostos a fraudes operacionais, e setores que comercializam produtos de maior valor unitário estão sujeitos, sobretudo, a fraudes estratégicas e/ou comportamentais. É de ressalvar que a fraude é multidimensional e pode variar bastante entre empresas e mercados, a generalização é útil para entender tendências, mas deve ser sempre realizada uma análise caso a caso.

Para além disso, é constatável que a incidência de fraudes está frequentemente relacionada ao tipo de produtos comercializado e o volume de operações digitais, visto que, de forma geral, empresas com maior volume de produtos transacionadas e cujos produtos proporcionem maior lucro por fraude ao infrator tendem a ser maiores alvos de tentativas fraudulentas. Por sua vez, o sucesso das mesmas está relacionado à inexistência de mecanismos eficazes de mitigação.

De forma sumária, a ocorrência de fraudes representa riscos significativos tanto para as empresas quanto para os consumidores, comprometendo a confiança no *e-commerce* e a eficiência dos processos logísticos. E por isso, a identificação das principais fraudes na última milha é um ponto essencial para o desenvolvimento da pesquisa sobre mecanismos de mitigação de fraudes. Ao mapear as fraudes mais recorrentes, é possível direcionar as soluções e estratégias para problemas específicos, permitindo identificar mecanismos direcionados e eficientes para cada situação e necessidade. Estas conclusões evidenciam que as fraudes não podem ser vistas como um fenómeno homogéneo, exigindo uma análise segmentada e soluções personalizadas.

Adicionalmente é possível concluir que as empresas dispõem atualmente de um vasto leque de mecanismos de mitigação que permitem mitigar as principais fraudes na última milha, sendo mecanismos como *blacklist* e construção de perfis de risco; código de barras; verificação do produto no momento de devolução; sistema de autenticação de entrega por PIN e/ou assinatura; integração entre plataformas; integração omnicanal; exigência do comprovativo de compra para efetuar devolução; treino e sensibilização de funcionários e a realização de auditorias, os mais frequentemente utilizados pelas empresas no combate e prevenção das fraudes na última milha, demonstrando, de uma forma geral, um alinhamento parcial com a literatura, visto que a mesma destaca mecanismos tecnológicos, como IA, ML, RFID e blockchain, que não contemplam na lista dos mecanismos mais usados pelas empresas.

Apesar da realidade atual das empresas, a investigação permitiu identificar diversos mecanismos ao dispor das mesmas que poderão ser implementados para combater as fraudes, incluindo desde soluções tecnológicas avançadas, como IA, ML e RFID, até mecanismos processuais baseados na melhoria de procedimentos internos, capacitação de equipas e cultura organizacional preventiva, sendo que geralmente os mecanismos antifraudes são transversais aos diferentes setores de retalho e permitem combater e evitar diversas fraudes. No entanto, a escolha e aplicação destes mecanismos não podem ser generalizadas, pois dependem fortemente da maturidade digital, dos recursos financeiros e da maturidade e estrutura operacional de cada organização. Empresas com menor maturidade digital ou recursos financeiros limitados devem recorrer prioritariamente a mecanismos processuais e tecnológicos mais simples, visto que não detém uma estrutura que permita a integração tecnológica nem acesso a tecnologias de ponta devido aos elevados custos de investimento e manutenção, por outro lado, organizações com maior capacidade financeira e digital demonstram maior propensão à adoção de tecnologias disruptivas. Por sua vez empresas com menor maturidade operacional devem optar por mecanismos que não dependem fortemente de processos robustos, privilegiando assim mecanismos mais simples, priorizando a melhoria gradual dos processos e controlos internos.

Conclui-se, contudo, que a eficácia na mitigação de fraudes na última milha não está exclusivamente relacionada ao uso de tecnologia, mas sim a uma combinação equilibrada entre processos robustos, cultura organizacional preventiva, capacitação continua de recursos humanos e integração faseada de soluções digitais em consonância com o crescimento da empresa e da perceção do risco a fraudes. Esta abordagem assegura a coerência entre o risco de fraude, a estratégia de negócio e os mecanismos implementados, garantindo que a gestão de

fraudes seja proporcional à exposição e ao potencial impacto para a organização. Tal abordagem permite alinhar o investimento em mecanismos aos riscos e à realidade operacional, garantido eficácia e sustentabilidade na implementação.

Constata-se que, em Portugal, o grau de adoção de mecanismos antifraude na última milha é moderado. Esta limitação, apesar da crescente sofisticação dos mecanismos de prevenção e deteção de fraude no processo de entrega e devolução, decorre de desafios estratégicos, financeiros e operacionais, incluindo restrições orçamentais para investimentos tecnológicos, baixa maturidade digital e/ou operacional, lacunas de conhecimento sobre soluções disponíveis e prioridades organizacionais centradas no curto prazo. Muitas empresas ainda não percecionam as fraudes como ameaça atual significativa, seja pela eficácia dos mecanismos atuais, seja pelo baixo volume de operações online. Contudo, a tendência de crescimento acelerado do *e-commerce*, associada à sofisticação dos esquemas fraudulentos, reforça a necessidade de maior consciencialização, inovação tecnológica, integração de abordagem preventivas e integração de mecanismos tecnológicos de forma gradual, de modo a garantir a sustentabilidade operacional e competitiva no futuro.

Assim, embora o panorama prático atual reflita uma abordagem pragmática focados em mecanismos de mitigação já consolidados, há espaço significativo para evolução, sobretudo se as empresas investirem em inovação, integração tecnológica e capacitação continua. Deste modo, é reforçada a necessidade de uma abordagem holística e adaptativa à mitigação de fraudes na última milha, alinhando o estado da arte à realidade operacional. De facto, a adoção efetiva de mecanismos antifraude depende de fatores contextuais, organizacionais e económicos, o que exige abordagens realistas e adaptadas à maturidade e às capacidades de cada empresa. Trata-se, portanto, de um campo em evolução, no qual se espera uma maior adesão a soluções mais sofisticas e automatizadas à medida que as tecnologias se tornem mais acessíveis, os processos internos e logísticos se solidifiquem e os riscos de fraudes se intensifiquem.

Posto isto, é auferível que os objetivos de investigação endereçados foram alcançados, visto que foi possível identificar os desafios enfrentados na última etapa do processo logístico potenciadores de fraudes e os principais tipos de fraude na última milha, permitiu também identificar e avaliar os mecanismos disponíveis para o combate à fraude bem como os principais desafios na implementação destes mecanismos e, por fim, permitiu compreender o grau de adoção de mecanismos de combate à fraude por parte de empresas que utilizam o canal de *e-*

commerce. A presente investigação permitiu, portanto, responder às questões de investigação formuladas, bem como perceber de forma concreta como é que os retalhistas B2C em Portugal, que implementam no seu modelo de negócio o canal *e-commerce*, podem reduzir as fraudes na última milha, tendo em conta os desafios inerentes, as variadas tipologias de fraudes existentes e, claramente, os mecanismos ao seu dispor para combater o problema tendo em conta o grau de maturidade digital e operacional e recursos disponíveis.

5.2. Contribuições

Este estudo contribui para a consciencialização do problema de fraudes na última milha e a identificação de mecanismos antifraudes úteis para a sobrevivência das empresas no futuro do *e-commerce*. É importante ressalvar que não basta um conhecimento dos mecanismos existentes e uma consciencialização do problema se não forem adotadas estratégias adequadas para analisar a exposição ao risco e preparar a estrutura das empresas de modo a serem capazes de suportar os mecanismos antifraudes necessários. Mesmo que, atualmente, em Portugal, as fraudes na última milha no *e-commerce* não configurem um problema grave para a maioria das empresas, a realização desta investigação mantém toda a sua pertinência. A investigação académica deve desempenhar um papel prospetivo e preventivo, antecipando fenómenos que, embora ainda marginais, têm elevado potencial de crescimento num cenário de expansão digital. Assim, ao fornecer conhecimento estruturado sobre o tema, este estudo permite que as empresas estejam preparadas para responder de forma eficaz a estes desafios emergentes, permitindo em simultâneo colmatar a escassez da literatura sobre o tema, preenchendo a lacuna teórica sobre fraudes na última milha no *e-commerce*, sintetizando desafios, tipos de fraudes e mecanismos de mitigação, oferecendo bases para futuras investigações e para melhorias de práticas na gestão logística.

5.3. Limitações da investigação

Esta investigação apresenta como principal limitação a dimensão reduzida da amostra, constituída por 7 profissionais do mercado português. Este número limitado de participantes, ainda que de setores distintos, característica de estudos qualitativos exploratórios, restringe a generalização dos resultados, fornecendo indicações e perceções em detrimento de representatividade estatística.

Acrescenta-se que a natureza deste estudo, embora adequada ao objetivo da investigação, não permite quantificar o impacto real das fraudes na última milha no desempenho financeiros das empresas, nem o retorno sobre o investimento de cada mecanismo de mitigação identificado, nem o nível de risco a fraudes na última milha que cada tipo de retalho está exposto sendo estas análises fundamentais para decisões estratégicas mais robustas.

Adicionalmente, a presente investigação não aborda a relação entre as políticas antifraude e o comportamento ou satisfação do consumidor, o que constitui uma limitação ao não considerar o impacto destas medidas na experiência do cliente e na confiança no *e-commerce*. Para além disso, o foco exclusivo no contexto nacional limita a aplicabilidade direta das conclusões a mercados internacionais, cujas realidades logísticas e exposição a fraudes podem diferir significativamente.

Por fim, a rápida evolução tecnológica e a constante sofisticação das fraudes implicam que os resultados reflitam um cenário em transformação contínua, carecendo de atualizações constantes para manter a sua relevância prática.

5.4. Sugestões para investigações futuras

Considerando a amostra reduzida deste estudo, futuras investigações poderão expandir o número e a diversidade de participantes, incluindo diferentes tipos de empresas, operadores logísticos e mercados internacionais. Esta ampliação permitirá identificar diversas práticas e enriquecer a compreensão sobre a manifestação das fraudes na última milha e o seu combate em contextos distintos, proporcionando resultados possíveis de generalização e identificação de boas práticas transferíveis para o contexto português.

Outro aspeto que se destaca como lacuna é a inexistência de dados sobre o impacto real das fraudes, o retorno sobre o investimento dos mecanismos possíveis de implementação e o risco de cada setor a cada tipo de fraude. Assim, futuras investigações poderão avaliar o retorno sobre o investimento associado à implementação de mecanismos de combate a fraudes na última milha, permitindo que as organizações escolham soluções que maximizem a relação custo-benefício e consigam implementar estratégias de priorização de investimentos em segurança logística. Adicionalmente, futuras investigações poderão focar-se no desenvolvimento de *frameworks* que permitam identificar, medir e classificar os riscos de cada tipo de fraude na última milha por tipo de retalho de forma a apoiar a definição de estratégias de mitigação mais

eficazes. Paralelamente, recomenda-se a investigação do impacto dos mecanismos antifraudes no comportamento do consumidor digital, tendo em conta os diferentes tipos de retalho, permitindo assim revelar dimensões importantes sobre a adequabilidade e a sustentabilidade dos mecanismos identificados.

Por fim, dada à rápida evolução tecnológica e à crescentes sofisticação das fraudes, é recomendável a realização de estudos longitudinais que acompanhem as transformações digitais ao longo do tempo, garantindo que a literatura e as soluções propostas se mantenham atualizadas e eficazes frente a desafios do mercado futuro.

Referências Bibliográficas

5 Strategies for Retail Businesses to Reduce Last Mile Reverse Logistics Costs. (2022, November 11). *Business World*. https://www.proquest.com/magazines/5-strategies-retail-businesses-reduce-last-mile/docview/2735105187/se-2?accountid=38384

Adeniran, A. O., Akinsehinwa, F. O., & Olorunfemi, S. O. (2022). Factors influencing the acceptance and patronage of e-commerce logistics operations in Nigeria. *Bulletin of the National Research Centre*, *46*(1), 128. https://doi.org/10.1186/s42269-022-00816-x

Allen, J., Piecyk, M., Piotrowska, M., McLeod, F., Cherrett, T., Ghali, K., Nguyen, T., Bektas, T., Bates, O., Friday, A., Wise, S., & Austwick, M. (2018). Understanding the impact of e-commerce on last-mile light goods vehicle activity in urban areas: The case of London. *Transportation Research Part D: Transport and Environment*, *61*, 325–338. https://doi.org/10.1016/j.trd.2017.07.020

Alverhed, E., Hellgren, S., Isaksson, H., Olsson, L., Palmqvist, H., & Flodén, J. (2024). Autonomous last-mile delivery robots: A literature review. *European Transport Research Review*, *16*(1), 4. https://doi.org/10.1186/s12544-023-00629-7

ANANSI. (n.d.). *The rising tide of fraud in last-mile shipping*. Retrieved October 27, 2024, from https://withanansi.com/blog/the-rising-tide-of-fraud-in-last-mile-shipping

Association of Certified Fraud Examiners. (n.d.). *Fraud 101: What is fraud?* Retrieved October 27, 2024, from https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

Barabas, M. (2020, November 23). *Photo proof of delivery: Concerns and best practices*. Elite EXTRA. https://eliteextra.com/photo-proof-of-delivery-concerns-and-best-practices/

Bauer, R., Hoster, B., Nadel, M., Rose, J., Rutledge, K., & Williams, H. (2020). *Differentiating with last-mile delivery*.

Blackburn, J. D., Guide, V. D. R., Souza, G. C., & Van Wassenhove, L. N. (2004). Reverse supply chains for commercial returns. In *California Management Review* (Vol. 46, pp. 6–22). Haas School of Business. https://doi.org/10.2307/41166207

Capgemini. (2021, February). *The last-mile delivery challenge*. https://www.capgemini.com/wp-content/uploads/2021/02/Report-Digital-%E2%80%93-Last-Mile-Delivery-Challenge1-1-1.pdf

Cegarra-Navarro, J. G., Jiménez, D. J., & Martínez-Conesa, E. Á. (2007). Implementing e-business through organizational learning: An empirical investigation in SMEs. *International Journal of Information Management*, *27*(3), 173–186.

Cekerevac, Z., Bogavac, M., & Prigoda, L. (2024). A review of blockchain application in logistics and last-mile delivery. *MEST Journal*, *12*(1), 4–12. https://doi.org/10.12709/mest.12.12.01.02

Choi, T.-M. (2013). Optimal return service charging policy for a fashion mass customization program. *Service Science*, *5*(1), 56–68. https://doi.org/10.1287/serv.1120.0036

Coppola, D. (2024, May 22). *Global e-commerce share of retail sales 2024*. Statista. https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/

DahNAY. (2024, January 18). *Last Mile Logistics vs Last Mile Reverse Logistics - DahNay Logistics*. https://dahnay.com/last-mile-logistics-vs-last-mile-reverse-logistics/

Dima, A., Radu, E., Dobrota, E. M., Otoiu, A., & Saracu, A. F. (2023). Sustainable development of e-commerce in the post-COVID times: A mixed-methods analysis of pestle factors. *Amfiteatru Economic*, *25*(Special 17), 1095–1114. https://doi.org/10.24818/EA/2023/S17/1095

Forbes, L. P., Kelley, S. W., & Hoffman, K. D. (2005). Typologies of e-commerce retail failures and recovery strategies. *Journal of Services Marketing*, *19*(5), 280–292. https://doi.org/10.1108/08876040510609907

García, A., Seok Chang, Y., & Valverde, R. (2006). Impact of new identification and tracking technologies on a distribution center. *Computers & Industrial Engineering*, *51*(3), 542–552. https://doi.org/10.1016/j.cie.2006.08.013

Garg, V., & Bindewari, S. (2024). Fraud Prevention in New User Incentive Programs for Digital Retail. *International Journal of Research and Analytical Reviews*, *11*(4). www.ijrar.org

Gayam, S. R. (2020). AI-Driven fraud detection in e-commerce: Advanced techniques for anomaly detection, transaction monitoring, and risk mitigation. *Distributed Learning and Broad Applications in Scientific Research*, *6*, 124–151.

Gheorghiță, C.-A., Smada, D., Vevera, A.-V., Dumitrache, M., Sandu, I.-E., & Rotună, C.-I. (2023). Blacklists and whitelists in the framework of a domain reputation system. *Revista Română de Informatică Și Automatică*, *33*(4), 33–46. https://doi.org/10.33436/v33i4y202303

Gomes, A. C., De Lima Junior, F. B., Soliani, R. D., Oliveira, P. R. de S., De Oliveira, D. A., Siqueira, R. M., Nora, L. A. R. da S., & De Macêdo, J. J. S. (2023). Logistics management in e-commerce: Challenges and opportunities. *Revista de Gestão e Secretariado (Management and Administrative Professional Review)*, *14*(5), 7252–7272. https://doi.org/10.7769/gesec.v14i5.2119

Grover, V. (2015). Research aproach: An overview. *Golden Research Thoughts*, *4*(8), 1–8.

Hall, D. J., Huscroft, J. R., Hazen, B. T., & Hanna, J. B. (2013). Reverse logistics goals, metrics, and challenges: Perspectives from industry. *International Journal of Physical Distribution and Logistics Management*, *43*, 768–785. https://doi.org/10.1108/IJPDLM-02-2012-0052

Hanna, M. G., & Pantanowitz, L. (2015). Bar coding and tracking in pathology. *Surgical Pathology Clinics*, *8*(2), 123–135. https://doi.org/10.1016/j.path.2015.02.017

Harris, L. C. (2008). Fraudulent return proclivity: An empirical analysis. *Journal of Retailing*, *84*(4), 461–476. https://doi.org/10.1016/j.jretai.2008.09.003

Harris, L. C., & Ogbonna, E. (2006). Service sabotage: A study of antecedents and consequences. In *Journal of the Academy of Marketing Science*. https://doi.org/10.1177/0092070306287324

Hesse-Biber, S. N., & Leavy, P. (2011). *The practice of qualitative research* (2nd ed.). Sage.

Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, *89*, 23–34. https://doi.org/10.1016/j.compind.2017.04.002

Kalakota, R., & Whinston, A. B. (1997). *Electronic commerce: A manager's guide*. Addison-Wesley.

Khanday, S. A., & Khanam, D. (2019). The research design. *Journal of Critical Reviews*, *6*(3), 367–376.

Kleinheksel, A. J., Rockich-Winston, N., Tawfik, H., & Wyatt, T. R. (2020). Demystifying content analysis. *American Journal of Pharmaceutical Education*, *84*(1), 7113. https://doi.org/10.5688/ajpe7113

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*(1), 1–21. https://doi.org/10.1186/s40537-019-0268-2

Kunešová, H., & Eger, L. (2017). Evaluation and comparison of B2C e-commerce intensity in EU member states. *E+M Ekonomie a Management*, *20*(4), 151–167. https://doi.org/10.15240/tul/001/2017-4-011

Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors*, *20*(9), 2495. https://doi.org/10.3390/s20092495

Last Mile Logistics. (2023, October 2). *The importance of cyber security in logistics operations*. https://www.lastmilelogisticssolutions.com/the-importance-of-cyber-security-in-logistics-operations/

Lazić, A., Milić, S., & Vukmirović, D. (2024). The future of electronic commerce in the IoT environment. *Journal of Theoretical and Applied Electronic Commerce Research*, *19*(1), 172–187. https://doi.org/10.3390/jtaer19010010

Lee, I. (2012). *Electronic commerce management for business activities and global enterprises: Competitive advantages*. IGI Global.

Leeuw, J., Bukhsh, Z., & Zhang, Y. (2023). *Parcel loss prediction in last-mile delivery: deep and non-deep approaches with insights from Explainable AI*. http://arxiv.org/abs/2310.16602

Lim, S. F. W. T., Jin, X., & Srai, J. S. (2018). Consumer-driven e-commerce. *International Journal of Physical Distribution & Logistics Management*, *48*(3), 308–332. https://doi.org/10.1108/IJPDLM-02-2017-0081

Lison, P., & Mavroeidis, V. (2017). Neural reputation models learned from passive DNS data. *2017 IEEE International Conference on Big Data (Big Data)*, 3662–3671. https://doi.org/10.1109/BigData.2017.8258361

Liu, H., & Du, F. (2023). Research on e-Commerce platforms' return policies considering consumers abusing return policies. *Sustainability*, *15*(18), 13938. https://doi.org/10.3390/su151813938

Lu, Z., Cui, R., Sun, T., & Wu, L. (2023). The value of last-mile delivery in online retail. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4590356

Macioszek, E. (2018). First and last mile delivery – Problems and issues. In *Advanced Solutions of Transport Systems for Growing Mobility: 14th Scientific and Technical Conference" Transport Systems. Theory & Practice 2017" Selected Papers* (pp. 147–154). Springer International Publishing. https://doi.org/10.1007/978-3-319-62316-0_12

Min, H. (2015). *The essentials of supply chain management: New business concepts and applications*. Pearson Education Inc.

Min, H. (2023). Leveraging drone technology for last-mile deliveries in the e-tailing ecosystem. *Sustainability*, *15*(15), 11588. https://doi.org/10.3390/su151511588

Monday, T. U. (2020). Impacts of interview as research instrument of data collection in social sciences. *Journal of Digital Art & Humanities*, *1*(1), 15–24. https://doi.org/10.33847/2712-8148.1.1_2

Moraes, R. (1999). *Análise de conteúdo*. *22*(37), 7–32.

Ngai, E. W. T., & Wat, F. K. T. (2002). A literature review and classification of electronic commerce research. *Information & Management*, *39*(5), 415–429. https://doi.org/10.1016/S0378-7206(01)00107-0

Nguyen, D. H., Leeuw, S., & Dullaert, W. E. H. (2018). Consumer behaviour and order fulfilment in online retailing: A systematic review. *International Journal of Management Reviews*, *20*(2), 255–276. https://doi.org/10.1111/ijmr.12129

Oláh, J., Kitukutha, N., Haddad, H., Pakurár, M., Máté, D., & Popp, J. (2018). Achieving sustainable e-commerce in environmental, social and economic dimensions by taking possible trade-offs. *Sustainability*, *11*(1), 89. https://doi.org/10.3390/su11010089

Olaoye, F., & Potter, K. (2024). Blockchain technology for secure and transparent data sharing. *Journal of Cybersecurity*.

Organization for Economic Co-operation and Development. (2013). *OECD science, technology and industry scoreboard 2013*. https://doi.org/https://doi.org/10.1787/sti_scoreboard-2013-en

Pandey, P., & Pandey, M. M. (2015). *Research methodology tools and techniques*. Bridge Center.

Petrosyan, A. (2024, May 22). *Global number of internet users 2005-2023*. Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? Part 2: Introducing qualitative research methodologies and methods. *Manual Therapy*, *17*(5), 378–384. https://doi.org/10.1016/j.math.2012.03.004

Piron, F., & Young, M. (2000). Retail borrowing: Insights and implications on returning used merchandise. *International Journal of Retail & Distribution Management*, *28*(1), 27–36. https://doi.org/10.1108/09590550010306755

Pourrahmani, E., & Jaller, M. (2021). Crowdshipping in last mile deliveries: Operational challenges and research opportunities. *Socio-Economic Planning Sciences*, *78*, 101063. https://doi.org/10.1016/j.seps.2021.101063

Prasanna, K. R., & Hemalatha, M. (2012). RFID GPS and GSM based logistics vehicle load balancing and tracking mechanism. *Procedia Engineering*, *30*, 726–729. https://doi.org/10.1016/j.proeng.2012.01.920

Purolator. (2023, September 28). *13 types of e-commerce fraud and how to prevent them*. https://resources.purolator.com/ecommerce-shipping-fraud-prevention/

Reynolds, K. L., & Harris, L. C. (2005). When service failure is not service failure: an exploration of the forms and motives of “illegitimate” customer complaining. *Journal of Services Marketing*, *19*(5), 321–335. https://doi.org/10.1108/08876040510609934

Richards, G. (2017). *Warehouse management: a complete guide to improving efficiency and minimizing costs in the modern warehouse* (Gwynne Richards, Ed.; 1st ed.). Kogan Page Publishers.

Robson, C., & McCartan, K. (2016). *Real world research* (4th ed.). Wiley.

RTS Labs. (2024, April 12). *Revolutionizing last-mile delivery: How AI is transforming logistics.* https://rtslabs.com/last-mile-delivery-ai

Salem, S. F., & Alanadoly, A. B. (2024). Driving customer engagement and citizenship behaviour in omnichannel retailing: evidence from the fashion sector. *Spanish Journal of Marketing - ESIC*, *28*(1), 98–122. https://doi.org/10.1108/SJME-10-2022-0220

Sampaio, J. (2022, October 19). *Como se proteger de fraudes na devolução de produtos*. https://www.codimarc.pt/blog/como-se-proteger-de-fraudes-na-devolu%C3%A7%C3%A3o-de-produtos

Sehrawat, D., & Gill, N. S. (2019). Smart sensors: Analysis of different types of IoT sensors. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 523–528. https://doi.org/10.1109/ICOEI.2019.8862778

SEON. (n.d.). *Return fraud: What is it & how to prevent It*. Retrieved November 5, 2024, from https://seon.io/resources/how-to-fight-return-fraud/

Shih, D.-H., Huang, F.-C., Chieh, C.-Y., Shih, M.-H., & Wu, T.-W. (2021). Preventing return fraud in reverse logistics— A case study of ESPRES solution by Ethereum. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(6), 2170–2191. https://doi.org/10.3390/jtaer16060121

Silva, L. S., Soliani, R. D., Argoud, A. R. T. T., & Freitas, C. G. de. (2022). O papel de um Centro de Distribuição (CD) no setor supermercadista: uma revisão sistemática da literatura. *Research, Society and Development*, *11*(16), e503111638728. https://doi.org/10.33448/rsd-v11i16.38728

Stallmann, F., & Wegner, U. (2014). *Internationalisierung von e-commerce-geschäften: Bausteine, strategien, umsetzung*. Springer-Verlag.

Statista. (2024). *eCommerce - Portugal | Statista Market Forecast*. Https://Www.Statista.Com/Outlook/Emo/Ecommerce/Portugal#live-Commerce. https://www.statista.com/outlook/emo/ecommerce/portugal#live-commerc

Stefanova, M. G., & Stoyanova, A. (2023, September 6). Risks and challenges in last mile logistics: Exploring safety and security issues. *28th International Maritime Lecturers' Association Conference (IMLA 28) & The 33rd International Maritime English Conference (IMEC 33)*. https://www.researchgate.net/publication/378520336_risks_and_challenges_in_last_mile_logistics_exploring_safety_and_security_issues

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. https://doi.org/10.1016/j.jisa.2019.102407

Ülkü, M. A., & Gürler, Ü. (2018). The impact of abusing return policies: A newsvendor model with opportunistic consumers. *International Journal of Production Economics*, *203*, 124–133. https://doi.org/10.1016/j.ijpe.2018.05.016

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Evaluating deep learning approaches to characterize and classify malicious URL's. *Journal of Intelligent & Fuzzy Systems*, *34*(3), 1333–1343. https://doi.org/10.3233/JIFS-169429

Viu-Roig, M., & Alvarez-Palau, E. J. (2020). The impact of e-commerce-related last-mile logistics on cities: A systematic literature review. *Sustainability*, *12*(16), 6492. https://doi.org/10.3390/su12166492

Wang, C.-C., & Chen, C.-C. (2010). Electronic commerce research in latest decade: A literature review. *International Journal of Electronic Commerce Studies*, *1*(1), 1–14.

Wang, G., Zhang, X., Gao, Y., Yee, A. L., & Wang, X. (2023). The use of an internet of things data management system using data mining association algorithm in an e-commerce platform. *Journal of Organizational and End User Computing*, *35*(3), 1–19. https://doi.org/10.4018/JOEUC.322553

Wang, Y., Jia, F., Schoenherr, T., Gong, Y., & Chen, L. (2020). Cross-border e-commerce firms as supply chain integrators: The management of three flows. *Industrial Marketing Management*, *89*, 72–88. https://doi.org/10.1016/j.indmarman.2019.09.004

Westland, J. C. (2022). A comparative study of frequentist vs Bayesian A/B testing in the detection of e-commerce fraud. *Journal of Electronic Business & Digital Economics*, *1*(1/2), 3–23. https://doi.org/10.1108/JEBDE-07-2022-0020

Xu, Y., Guo, R., Liu, X., Luo, H., Dong, C., Yao, A., & Li, X. (2022). Efficient face recognition via Multi-UAV-Edge collaboration in UAV delivery service. *2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 676–683. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00092

Yan, R., & Pei, Z. (2019). Return policies and O2O coordination in the e-tailing age. *Journal of Retailing and Consumer Services*, *50*, 314–321. https://doi.org/10.1016/j.jretconser.2018.07.006

Yu, Y., Wang, X., Zhong, R. Y., & Huang, G. Q. (2017). E-commerce logistics in supply chain management. *Industrial Management & Data Systems*, *117*(10), 2263–2286. https://doi.org/10.1108/IMDS-09-2016-0398

Zhang, D., Bayer, S., Willis, G., Frei, G., Gerding, E., & Senyo, P. (2022). Using big data analytics to combat retail fraud. *Proceedings of the 4th International Conference on Finance, Economics, Management and IT Business*, 85–92. https://doi.org/10.5220/0011042600003206

Zhang, D., Frei, R., Senyo, P. K., Bayer, S., Gerding, E., Wills, G., & Beck, A. (2023). Understanding fraudulent returns and mitigation strategies in multichannel retailing. *Journal of Retailing and Consumer Services*, *70*, 103145. https://doi.org/10.1016/j.jretconser.2022.103145

Zhao, X., Hu, S., & Meng, X. (2020). Who should pay for return freight in the online retailing? Retailers or consumers. *Electronic Commerce Research*, *20*(2), 427–452. https://doi.org/10.1007/s10660-019-09360-9

Anexos

Anexo A - Tabela de estruturação do guião de entrevistas

Pontos principais de estudo	Perguntas auxiliares
1. Perceber a operação da logística de última milha e os desafios enfrentados na mesma.	1.1. Como é estruturada a operação de última milha na sua empresa? 1.2. Quais são os maiores desafios enfrentados atualmente na operação da última milha?
2. Identificar das fraudes de última milha ocorrentes no seio do negócio derivadas da utilização do canal de *e-commerce*.	2.1. Quais são as fraudes de última milha que enfrentam ou já enfrentaram? 2.2. Como é que essas fraudes impactam o negócio (tanto a nível operacional quanto financeiro)?
3. Identificar e analisar os mecanismos antifraudes implementados e os mecanismos ao dispor das empresas que não são utilizados.	3.1. Que mecanismos são aplicados para mitigar as fraudes? 3.2. De um modo geral como avalia a eficácia das estratégias aplicadas? 3.3. Existem outros mecanismos do seu conhecimento que poderiam ajudar a mitigar as fraudes, mas não são aplicados? Por que motivo?
4. Identificar os principais desafios enfrentados pela empresa relacionados à mitigação de fraudes.	4.1. Existem desafios internos que a empresa enfrenta aquando o combate às fraudes na última milha? 4.2. Considera que existem fatores externos à empresa que dificultam a implementação de mecanismos antifraudes?
5. Perceber as perspetivas futuras relativas à adoção de mecanismos antifraude.	5.1. A sua empresa pretende adotar novas tecnologias ou estratégias nos próximos anos para lidar com as fraudes? (Se sim: quais? Se não: porquê?)

Anexo B - Citações dos profissionais sobre as fraudes na última milha identificadas

Categoria	Código	Citações dos profissionais entrevistados
Fraudes na última milha	Fraude de Reembolso em múltiplos canais	" … já não é muito recorrente pois com o passar dos anos foram feitas melhorias na integração dos múltiplos canais, contudo já se registaram tentativas de fraudes em que os clientes tentavam obter diversos reembolsos , recorrendo à loja física e ao canal online."
	Jiffy Bag	"Há registos de falsas devoluções de produtos, isto é, devoluções com destino aos nossos armazém que chegam com as caixas vazias ou com pedras, invés do produto associado à devolução."
	Fraude de produto não recebido	" Das fraudes mais recorrentes posso citar a alegação de não recebimento do produto, embora tudo indique que o produto foi de facto entregue"
	Chargeback	"É raro mas já registamos casos de chargeback, isto é, o cliente após receber a encomenda, sem nos contactar previamente, pediu o reembolso ao seu banco diretamente, na tentativa de ficar com o produto e receber o dinheiro de volta. É uma situação bastante complicada caso o banco favoreça protamente o cliente"
	Bricking	" De forma menos recorrente, mas especialmente nos produtos mais caros, já se verificou a devolução de produtos sem as peças originais, tentando associar ao pedido de devolução um pedido de reembolso"
	Roubo de encomendas	"É do nosso conhecimento que por vez há a ocorrência de roubos de encomendas, tanto por parte de colaboradores internos ou parceiros "
	Fraude por manipulação de endereços	" Já ocorreram entregas em moradas "não reais", o que nos leva a querer que tenha existido manipulação da morada após a confirmação da compra."
	Wardrobing	"É do meu conhecimento a existência de fraudes onde o cliente faz uso de roupa e acessórios para eventos e a posterior devolução"
	Fraude de descontos	" Nas campanhas leve 3 pague 2 há clientes que postermente devolvem 1 dos artigos na tentativa de serem reembolsados na totalidade por esse artigo mesmo não devolvendo o artigo gratuíto"; " por vezes os clientes numa campanha de fidelização efetuam compras para atingir o valor que lhes permite receber créditos para futuras compras, após a compra usam o crédito na sua totalidade e por fim devolvem as peças compradas inicialmente, ficando apenas com as que foram compradas com o crédito fornecido pela loja"
	Fraude de reembolso entre retalhistas	"Em produtos de maior valor já se verificaram tentativas de devolução de artigo que não perticiam à empresa em causa"
	Fraude por falsificação do estado logístico de entrega	" Posso citar a ocorrência de falsas entregas realizadas, ou seja, o transportador dá a entega como entregue ao destinatário, mas a mesma nunca ocorreu"
	Fraude exploratória por encomendas de teste	"Muitas vezes acontecia algumas pessoas menos bem intencionadas acabarem por fazer encomendas de teste com um valor menor para testar e perceber como é processada a operação, para depois fazerem uma encomenda mais avultada já com um esquema fraudulento montado"
	Fraude de troca de mercadorias	"Apesar de forma menos recorrente, já se verificaram situações onde eram devolvidos produtos diferentes aos que eram de facto comprados e geralmente nestes casos o cliente associava à devolução um pedido de reembolso"

Anexo C – Mecanismos de mitigação de fraudes na última milha: Fraudes mitigadas e modo de atuação

Mecanismos codificados	Fraudes na última milha possíveis de mitigar	Como é que os mecanismos permitem mitigar as fraudes
Mecanismos de prevenção através de análise de dados	Fraudes de reembolso em múltiplos canais; Chargeback; Fraude de produto não recebido; *Bricking;* Fraude por manipulação de endereços; Fraude de descontos; Fraude de reembolso entre retalhistas; *wardrobing* e Fraudes exploratórias por encomendas testes	Identifica padrões anômalos nos pedidos de encomendas/devoluções, promoções (com IA e ML). A criação de perfis de risco permite o cruzamento de dados permitindo assim sinalizar possíveis fraudes antes de efetuar a entrega/ reembolsos e agir de forma proativa. Em caso de um cliente incorrer em sucessivas tentativas de fraude é colocado na blacklist, de modo a impedi-lo de realizar mais compras no site do retalhista em causa
IoT	Fraude de produto não recebido; *Jiffy bag;* Roubo de encomendas; Fraude por falsificação do estado logístico de entrega e Fraude de troca de mercadorias	Garante a identificação correta dos itens de forma individual (RFID) ou do tipo de produto (código de barras) e o seu posicionamento constante (GPS) reduzindo desvios e erros no processo de última milha
Protocolo de segurança e contrato com parceiros de transporte	Roubo de encomendas; Fraude de produto não recebidos; Fraude por falsificação do estado logístico de entrega.	Permite alinhar objetivos, usufruir de mecanismos das transportadoras como GPS e portas de intrusão nos transportes, integração eficiente de sistemas, permitindo a comunicação e rastreabilidade contínua, e desencentivo de fraudes cometidas pelos funcionários de transporte devido ao estabelecimento de objetivos
Sistema de reviews de clientes	Fraude de produto não recebido; Fraude de manipução do estado logístico de entrega; roubo de encomendas; Fraude de troca de mercadorias	Permite recolha de feedback dos clientes sobre o processo de entrega e/ou devolução, permitindo a escolha de transportadores com menores incidencias. adicionalmente, permite um contacto direto com o cliente, permitindo a recolha e monitorização ativa de avaliações por parte dos clientes, o que pode ajudar a sinalizar padrões de comportamento suspeito, como contas que sistematicamente alegam problemas com as entregas ou com os produtos, permitindo construir perfis de risco
Processo de controlo de qualidade no processamento de encomendas	Fraude de produto não recebido e Fraude de troca de mercadorias	Garante a qualidade do processamento de encomendas, evitando encomendas com produtos defeitusos ou incompletas, permitindo garantir a integridade da mesma
Comprovativo de prova de entrega/recolha	Roubo de encomendas; Fraude por manipulação do estado de entrega; B*ricking; Jiffy bag;* Fraude de troca de mercadores e Fraude de produto não recebido	Comprova a entrega e/ou recolha de um produto e permite identificar os envolvidos na transação, desde o retalhista ao cliente (ou vice-versa)
Agendamento de entregas e/ou recolhas associadas a devoluções	Fraude de produto não recebido; Roubo de encomendas e Falsificação do estado logístico de entrega	Reforça a validação no ato de entrega/recolha e evita deslocações desnecessárias permitindo deste modo reduzir os custos associados à última milha e minimizar o espaço aberto a tentativas de fraudes
Plataformas unificadas	Fraude de reembolso em múltiplos canais; Fraude manipulação de endereços; Fraude de reembolso entre retalhistas; Fraude de troca de mercadorias; *Chargeback* ; Fraude de descontos	A integração omnicanal permite uma coerência entre os diversos canais da empresa (site, app, loja física,central de antendimento telefónico) permitindo um cruzamento de dados dos canais de vendas, permitindo deter informações sobre uma compra, devolução ou cliente independentemente do canal utilizado. Por sua vez, a integração entre plataformas permite o compartilhamento de dados e ações em tempo real entre plataformas internas e externas, permitindo combinar informações de múltiplas fontes
Colocação de etiquetas térmicas *(Não é um mecanismo possível de implementar no momento uma vez que ainda se encontra em fases de teste)*	*Wardrobing*	A mundança irreversível da coloração da etiqueta a partir do contacto contínuo com o corpo permite ao retalhista verficar se o produto já foi utilizado
Políticas de devoluções antifraude	*Wardrobing* ; Fraude de descontos; Fraude reembolso entre retalhistas; Roubo de encomendas; Fraude de troca de mercadorias e Fraude de reembolso em múltiplos canais; *Jiffy bag* ; *Bricking*	Desincentiva os clientes a efetuar devoluções fraudulentas, através de imposições de prazos sazonais e pagamento de taxas de devolução. Para além disso, a obrigatoriedade de verificação dos produtos devolvidos também permite garantir a conformidade do mesmo antes de proceder a reembolsos/trocas que possam estar ligados a devoluções fraudulentas. Adicionalmente, o estabelecimento de políticas claras de reembolso e contestação protege a empresa e o cliente de má-fé
Auditorias de conformidade para deteção de anomalias	Todas as fraudes em geral, mas agem de forma reativa ao identificar fraudes que já ocorreram permitindo identificar vulnarabilidades e estabeler estratégias de modo a agir no futuro de forma preventiva sobre fraudes semelhantes	Permite identificar padrões anómalos, abusos e falhas nos processos, através da análise sistemática de registos, transações e procedimentos de modo a verificar se estes estão a ser efetuados corretamente
Capacitação de equipas antifraude	Todas as fraudes em geral	O treino dos colaboradores facilita a deteção de fraudes no momento de entregas e devoluções, evitando que as mesmas se concretizem. Adicionalmente a criação de equipas especializadas em análise de dados e fraudes permite identificar padrões suspeitos, analisar transações em tempo real, investigar comportamentos anómalos e implementar rapidamente medidas de bloqueio ou prevenção, permitindo mitigar fraudes na última milha com maior eficácia e agilidade
Pagamento seguro e antecipado	*Chargeback;* Fraude de reembolso em múltiplos canais; Fraude de manipulação de endereços	Exige o pagamento no ato da compra para evitar recusas ou esquemas para não pagar após o recebimento da encomenda. A limitação dos meios de pagamento também é importante para as empresas pois garante que a empresa não sai projudicada pela má-fe dos clientes que se aproveitam de bancos que detenham politicas de *chargeback* facilitadoras
3PL	Externeliza o tratamento do problema das fraudes, contudo, a empresa contratada terá de aplicar algum dos mecanismos acima descritos.	Permite combater as fraudes ao externalizar a componente logística e consequentemente os problemas logísticos, continuando com foco na atividade core da empresa, permitindo usufruir dos conhecimentos aprofundados da empresa contratada

Anexo D – Restrições sumarizadas dos mecanismos antifraudes identificados

Mecanismos codificados	Restrições sumarizadas dos mecanismos
Mecanismos de prevenção através de análise de dados	A implementação de IA e ML requer altos custos de implementação e manutenção; exige uma estrutura digital bem desenvolvida capaz de suportar estas tecnologias; exige equipas capacitadas e detêm uma alta dependencia de dados de qualidade
IoT	RFID tem grandes custos de implementação o que pode levar a um custo-benefício negativo. Código de barras não permite leituras em massa nem atualizações automáticas
Protocolo de segurança e contrato com parceiros de transporte	Exige a escolha de parceiros logísticos com sistemas adequados para suportar as medidas antifraudes estabelecidas
Sistema de reviews de clientes	Exige uma equipa dedicada à analise do feedback ou então investimento em ML para analisar os dados das reviews e posterior uso de IA ou de uma equipa para redigir relatórios com a informação da análise
Processo de controlo de qualidade no processamento de encomendas	Exige mais tempo no processamento de encomendas, o que pode ser dificil no ambiente fernético e exigente por entregas rápidas
Comprovativo de prova de entrega/recolha	Exige uma integração entre sistemas internos e externos de modo a haver partilha de informação para posterior cruzamento de dados
Agendamento de entregas e/ou recolhas associadas a devoluções	Exige a integração com sistemas logisticos que permitam atualizações em tempo real
Plataformas unificadas	Destaca-se como um desafio nas empresas com menor maturidade digital uma vez que estas empresas possuem geralmente sistemas isolados, processos pouco digitalizados e falta de infraestrutura tecnológica unificada, o que dificulta a conexão consistente entre canais
Colocação de etiquetas térmicas *(Não é um mecanismo possível de implementar no momento uma vez que ainda se encontra em fases de teste)*	Ainda está em fase de testes e por isso não são conhecidas ainda as restrições associadas a este mecanismo
Políticas de devoluções antifraude	O pagamento de taxas de devolução pode desencorajar as compras dos clientes digitais que agem de boa-fé
Auditorias de conformidade para deteção de anomalias	Agem de forma reativa e caso sejam realizadas continuamente podem representar custos elevados
Capacitação de equipas antifraude	A eficácia do treino e sensibilização de funcionários depende da consistência dos programas formativos, da baixa rotatividade da força de trabalho e da disponibilidade de tempo e recursos despendidos em formação continua, A criação de equipas pode ser muito dispendioso,exige recursos humanos qualificados, tempo de monitorização contínuo, e a integração entre plataformas, o que pode ser mais dificl para empresas com menor maturidade digital
Pagamento seguro e antecipado	Podem reduzir a conveniência para o cliente o que pode causar potenciais perdas de vendas (clientes sem meios de pagamento aceites não concluem a compra). Exige flexibilidade para ajustar os métodos de pagamento conforme tendências e riscos
3PL	Acarreta custos adicionais associados a esta contratação; pode gerar problemas associados à confidencialidade e proteção de dados bem como de uma possível perda de visibilidade e controlo sobre processos sensíveis associados à gestão de fraudes

Anexo E - Justificação dos mecanismos não recomendados para certos perfis de empresas e recursos

Mecanismos Detalhados	Perfis não recomendados	Justificação
IA	Perfil C; Perfil D; Recursos Financeiros Limitados	A Inteligência Artificial requer elevada maturidade digital e capacidade de investimento, o que empresas com baixa maturidade digital ou poucos recursos não conseguem assegurar.
ML	Perfil C; Perfil D; Recursos Limitados	O ML exige dados estruturados, infraestrutura tecnológica avançada e equipas especializadas, elementos indisponíveis para empresas com maturidade digital baixa ou recursos escassos.
Blacklist e construção de perfis de risco	-	Possível de implementar em todos os perfis pois é possível o uso de ML (para empresas com maior maturidade digital) ou de forma manual. Mais desafiantes para empresas com processos pouco estruturados que não tenham estruturas digitais consolidas (perfil D).
RFID (com ou sem sensores integrados)	Perfil B; Perfil C; Perfil D; Recursos Limitados	RFID implica custos elevados em tecnologia e logística (etiquetas, leitores, integração de sistemas) e requer processos logísticos maduros, exigindo elevados iniciais e de manutenção elevados. Não justificáveis para empresas com baixa maturidade digital ou operacional ou baixa capacidade financeira.
GPS	Perfil C; Perfil D; Recursos Limitados	Requer infraestrutura tecnológica para monitorizar em tempo real e integração com sistemas operacionais, requer recursos consideráveis para implementação, manutenção e integração, o que se torna difícil para empresas com maturidade digital baixo ou recursos financeiros limitados. Caso o transporte seja terceirizado o retalhista pode usufruir deste mecanismos (se maturidade digital alta) por meio de contrato com o parceiro logístico.
Código de barras	-	Recomendável para todos os perfis pois é uma tecnologia de baixo custo e facilmente integrável mesmo com sistemas simples. Contudo, em perfis A, deve-se, se possível financeiramente, optar por RFID.
Portas de intrusão nos transportes	-	Caso o transporte seja terceirizado o retalhista deve procurar parceiros logisticos capazes de satisfazer esta exigencia, aproveitando-se assim das práticas já usadas pela empresa parceira para mitigar fraudes. Ou seja pode ser um mecanismos aplicado contratualmente ao parceiro logístico.
Contratos com parceiros logísticos com objetivos definidos	-	Recurso contratual e estratégico que não exige investimentos tecnológicos ou processos internos ou logísticos complexos.
Presença de pelo menos 2 funcionários no transporte	-	Caso o transporte seja terceirizado o retalhista deve procurar parceiros logisticos capazes de satisfazer esta exigencia. Ou seja pode ser um mecanismos aplicado contratualmente com o parceiro logístico.
Sistema de reviews de clientes	Perfil C; Perfil D	Requer uma plataforma digital adequada, processos organizacionais para gestão dos feedbacks e equipas capacitadas para analisar e responder às avaliações, tornando se inviáveis para empresas com baixa maturidade digital. É recomendável ao perfil B mas, poderão existir dificuldades em agir rapidamente sobre os feedbacks devido à baixa maturidade operacional.
Processo de controlo de qualidade no processamento de encomendas	Perfil D	Envolve procedimentos estruturados e formação, ou seja MO+. (Apesar do perfil B ter maturidade operacional baixa, como tem maturidade digital alta, pode usar soluções digitais para compensar processos logísticos frágies).
Tracking fotográfico (entrega e recolha)	Perfil D	Requer disciplina operacional na recolha e armazenamento das fotos e tecnologias capazes de registar imagens sistematicamente (Apesar do perfil B maturidade operacional baixa, como tem maturidade digital alta, pode usar soluções digitais para compensar processos logísticos frágies; o perfil C tem maturidade digital baixa mas pode usar processos mais simples, como uso de smartphones com associação à encomenda feita de forma manual)
Autenticação de entrega por PIN/assinatura/QR code	-	Todos os perfis são capazes de realizar autenticação de entregas, contudo perfis com mais dificuldade de integração tecnológica devem adotar por meios mais simples como assinatura.
Autenticação de entrega por biometria	Perfil C, Perfil D, Recursos Limitados	Solução de custo elevado, de difícil implementação e que exige infraestrutura tecnológica e maturidade digital elevada, ausente nestes perfis.
Registo fotográfico pontual (entrega, recolha ou armazém)	Perfil D	Requer processos estruturados e ferramentas tecnológicas, o que torna difícil até mesmo a aplicação pontual para perfis como o D, porque não detem nem meios digitais para executar o registo nem tem estrutura organizacional sólida para aplicar registos manuais ou com equipamentos básicos. Pode ser possível com muito esforço, mas não é recomendado como prioritário.
Prenchimento de formulários de controlo de última milha	-	Todos os perfis podem implementar formulários de controlo, de forma digital ou manual, adaptando-se à sua maturidade. É um mecanismo flexível e escalável, ideal para qualquer grau de maturidade.
Agendamento de entregas e/ou recolhas associadas devoluções	Perfil B; Perfil C; Perfil D; Recursos Limitados	Exige coordenação entre sistemas digitais e capacidade processual. Assim, só é recomendável para empresas com ambos os níveis de maturidade elevados. Requer investimentos em ferramentas digitais, manutenção ou integrações com parceiros logísticos.
Integração entre plataformas	Perfil C; Perfil D; Recursos Limitados	Implica conhecimento técnico e investimento em software para permitir a integração entre sistemas, o que não é acessível para empresas com baixa maturidade digital.ou recursos limitados.
Integração omnicanal	Perfil C, Perfil D, Recursos Limitados	Necessita de elevada maturidade digital para conectar e sincronizar os canais de venda eficientemente. Apesar de num contexto de e-commerce a integração omnicanal ser importante para todos os retalhistas, empresas com baixa maturidade digital devem começar com integrações mais simples e parciais, focando-se em soluções que necessitem de menos investimento e complexidade, para depois evoluir.

Colocação de etiquetas térmicas	-	É difícil apurar os recursos necessários para a implementação deste mecanismos uma vez que ainda se encontra em fases de teste. Por isso é uma informação a atualizar!
Política de reembolso em vales/cartões oferta	-	Esta política necessita apenas de definições estratégicas e comunicação ao cliente, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Imposição de restrições sazonais nos prazos de devolução	-	Esta política necessita apenas de definições estratégicas e comunicação ao cliente.
Exigência de comprovativo de compra para devolução	-	Procedimento operacional simples que pode ser adotado sem custo, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Verificação do produto no momento da devolução	-	Processo manual que pode ser feito com formação básica e organização, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Pagamento de taxa de devolução	-	Política definida pela empresa, não requer investimento financeiro necessitando apenas de comunicação ao cliente, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Auditorias de conformidade para deteção de anomalias	Perfil B; Perfil D	Requer planeamento, métricas, e pessoal qualificado, monstrando-se como indisponível em contextos com baixa maturidade operacional. Apesar de deter limitações, pode ser realizada em contextos aixa maturidade digital, aproveitando processos sólidos realizando auditorias manuais (perfil C). Em caso de recursos financeiros limitados devem ser realizadas auditorias básicas e manuais, mas com menor frequência e profundidade.
Equipas especializadas em análise de dados e fraudes	Perfil C; Perfil D; Recursos Limitados	Empresas com fraca maturidade digital e poucos recursos, limitam a capacidade de usar ferramentas avançadas, tornando difícil formar/manter equipas especializadas.
Treino e sensibilização de funcionários	-	Formação interna ou com apoio de entidades externas, possível mesmo com orçamento limitado, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Pagamento no ato da compra	-	Prática operacional comum, não requer investimento adicional, , não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Limitação dos tipos de pagamento online	-	Decisão estratégica facilmente configurável nas plataformas de venda, não dependendo da maturidade digital ou operacional de uma empresa para a sua aplicabilidade.
Contratação de 3PL	Recursos Financeiros Limitados	Implica custos significativos.