U.PORTO

**SEGUNDO CICLO DE ESTUDOS**
CRIMINOLOGIA

# Fraudes no Comércio Online: Das Pistas Visuais aos Discursos de Confiança em Websites de Comércio

Rúben Miguel Pereira Pinto

**M**

**2026**

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para obtenção do grau de Mestre em Criminologia elaborada sob orientação das Professoras Doutoras Rita Faria e Inês Sousa Guedes

# EPÍGRAFE

"*Se podes olhar, vê.*

*Se podes ver, repara.*"

(Saramago, 1995)

# RESUMO

A digitalização da sociedade e a expansão do comércio *online* transforaram os comportamentos de consumo, mas potenciaram a proliferação de fraudes ao consumidor *online*. Em particular, destacam-se os *websites* de comércio fraudulentos, que reproduzem a aparência e as funcionalidades dos *websites* legítimos para induzir os consumidores em erro, provocando graves prejuízos patrimoniais e emocionais. Apesar da relevância deste fenómeno, permanece limitado o conhecimento sobre a forma como os consumidores distribuem a sua atenção e interpretam os elementos visuais dos *websites* de comércio.

Partindo dos pressupostos da Criminologia Visual, esta dissertação desenvolveu um estudo de metodologias mistas para analisar, através de técnicas de *eye-tracking*, os padrões visuais dos consumidores, associando-os à suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos, e explorar, por meio de técnicas de *photo-elicitation*, os significados atribuídos às pistas visuais dos *websites* de comércio.

Participaram 66 indivíduos que haviam realizado compras *online* nos 12 meses anteriores, sendo distribuídos por dois grupos experimentais para responderem a um questionário sociodemográfico e visualizarem um conjunto de 16 *websites* de comércio (8 legítimos e 8 fraudulentos). Complementarmente, entrevistaram-se 12 participantes para aprofundar os processos interpretativos das imagens observadas.

Os resultados quantitativos demonstraram que os participantes suscetíveis à cibervitimação dirigiram menos atenção aos indicadores de legitimidade, como o URL, concentrando-a nos produtos comerciais. A análise qualitativa revelou que a suscetibilidade à cibervitimação nos *websites* fraudulentos depende da forma como as pistas visuais são interpretadas pelos consumidores, em função de conhecimentos prévios, experiências de consumo e discursos socioculturais. Propõe-se um modelo sequencial em que a atenção visual antecede a atribuição de significados, da qual emergem os juízos de legitimidade e risco que influenciam a confiança e a intenção de compra *online*.

Esta investigação contribui para o desenvolvimento da Criminologia Visual aplicada à cibercriminalidade e ao comércio *online*, evidenciando o potencial de articulação entre técnicas de *eye-tracking* e de *photo-elicitation* para compreender os processos visuais, cognitivos e interpretativos subjacentes à suscetibilidade à fraude ao consumidor *online*.



**Palavras-chave:** Criminologia Visual; *Eye-Tracking*; Fraude ao Consumidor *Online*; *Photo-Elicitation*; Suscetibilidade à Cibervitimação nos *Websites* Fraudulentos

## ABSTRACT

The digitalization of society and the expansion of e-commerce have transformed consumer behavior, but have also contributed to the proliferation of online consumer fraud. In particular, fraudulent e-commerce websites stand out by replicating the appearance and functionality of legitimate websites to deceive consumers, causing serious financial and emotional harm. Despite the relevance of this phenomenon, knowledge about how consumers distribute their attention and interpret the visual elements of e-commerce websites remains limited.

Based on the assumptions of Visual Criminology, this dissertation developed a mixed-methods study to analyze consumers´ visual patterns through eye-tracking techniques, associating them with susceptibility to cybervictimization on fraudulent e-commerce websites, and to explore, through photo-elicitation techniques, the meanings attributed to the visual cues of e-commerce websites.

A total of 66 individuals who had made online purchases in the previous 12 months participated, being distributed into two experimental groups to answer a sociodemographic questionnaire and view a set of 16 e-commerce websites (8 legitimate and 8 fraudulent). Additionally, 12 participants were interviewed to further explore the interpretative processes associated with the observed images.

The quantitative results showed that participants who were susceptible to cybervictimization directed less attention to indicators of legitimacy, such as the URL, and concentrated their attention on commercial products. The qualitative analysis revealed that susceptibility to cybervictimization on fraudulent websites depends on how consumers interpret visual cues, which is influenced by prior knowledge, consumption experiences, and sociocultural discourses. A sequential model is proposed in which visual attention precedes the attribution of meanings, from which judgments of legitimacy and risk emerge, ultimately influencing trust and online purchase intention.

This research contributes to the development of Visual Criminology applied to cybercrime and e-commerce, highlighting the potential of combining eye-tracking and photo-elicitation techniques to understand the visual, cognitive, and interpretative processes underlying susceptibility to online consumer fraud.



**Keywords:** Eye-Tracking; Online Consumer Fraud; Photo-Elicitation; Susceptibility to Cybervictimization on Fraudulent Websites; Visual Criminology

## AGRADECIMENTOS

Esta dissertação representa o culminar de um percurso pessoal e académico repleto de desafios, aprendizagens e emoções. Embora seja o fim de um ciclo, tenho a certeza que começará um novo capítulo na minha vida. Resta-me agradecer o apoio, a orientação e o incentivo de diversas pessoas, às quais expresso a minha mais sincera gratidão.

À Professora Doutora Rita Faria, minha orientadora, expresso o mais profundo agradecimento por me ter desafiado, desde o primeiro momento, a realizar um projeto inovador e cientificamente ambicioso. Quero agradecer-lhe a disponibilidade constante, a confiança que depositou em mim e a exigência que me motivou a ser e fazer melhor, superando diversos obstáculos. O seu apoio foi fundamental para a concretização deste projeto e para o meu crescimento enquanto investigador ou "cientista".

À Professora Doutora Inês Guedes, minha coorientadora, agradeço os contributos científicos, a disponibilidade, as sugestões e o apoio prestado ao longo deste percurso, que enriqueceram este trabalho.

A todos os docentes da Faculdade de Direito da Universidade do Porto com os quais tive a oportunidade de aprender e evoluir. Em particular, à Professora Doutora Carla Cardoso, por me orientar desde o Seminário e incentivar a dar os primeiros passos na construção deste projeto.

À minha família, agradeço o apoio incondicional e por acreditarem sempre em mim. Em especial, à minha mãe, pelo amor e por nunca me deixar desistir dos meus objetivos. Ao meu avô, que partiu recentemente, deixo uma palavra de saudade. Gostaria que estivesses presente para celebrarmos esta conquista, mas tenho a certeza de que estarias profundamente orgulhoso do meu percurso e da pessoa que me tornei.

À Maria, pelo apoio, pela paciência, pelas palavras de incentivo nos momentos mais difíceis e por celebrares cada pequena conquista. A tua companhia tornou esta jornada mais leve e, de certa forma, fazes parte desta conquista.

Por fim, agradeço a todos os amigos e aos participantes deste estudo. A vossa disponibilidade e colaboração contribuíram decisivamente para a concretização desta investigação.

## LISTA DE ABREVIATURAS E ACRÓNIMOS

ACD – Análise Crítica do Discurso

AOI – *Areas of Interest*

APAV – Associação Portuguesa de Apoio à Vítima

CP – Código Penal

FDUP – Faculdade de Direito da Universidade do Porto

IA – Inteligência Artificial

LC – Lei do Cibercrime

LEC-FDUP – Laboratório da Escola de Criminologia da Faculdade de Direito da Universidade do Porto

MHS – Modelo Heurístico-Sistemático

PGR – Procuradoria-Geral da República

TAR – Teoria das Atividades de Rotina

TCC – Teoria da Cultura do Consumidor

TCP – Teoria do Comportamento Planeado

UE – União Europeia

UP – Universidade do Porto

URL – *Uniform Resource Locator*

# ÍNDICE GERAL

INTRODUÇÃO ..... 1
CAPÍTULO I – REVISÃO DA LITERATURA ..... 2
1. Criminologia Visual ..... 2
1.1 Métodos Visuais na Tradição Criminológica ..... 4
1.2 Métodos Visuais na Era Digital ..... 6
2. Cibercriminalidade ..... 7
2.1 Tipologias de Cibercrime ..... 8
2.2 Fraudes: Do *Offline* ao *Online* ..... 9
3. Cultura de Consumo Contemporânea e Fraudes ao Consumidor *Online* ..... 12
3.1 Enquadramento da Fraude ao Consumidor *Online* ..... 15
3.2 Os *Websites* de Comércio Fraudulentos ..... 17
3.3 Riscos e Danos para Vítimas e Sociedade ..... 19
4. Teorias Explicativas da Suscetibilidade à Fraude ao Consumidor *Online* ..... 20
4.1 Teoria das Atividades de Rotina ..... 21
4.2 Modelo Heurístico-Sistemático ..... 22
4.3 Da Teoria do Comportamento Planeado à Teoria da Cultura do Consumidor 23
5. Outros Fatores Explicativos da Suscetibilidade ..... 25
5.1 Fatores Individuais ..... 25
5.2 Fatores Contextuais ..... 28
6. *Eye-Tracking* e o Estudo da Atenção Seletiva em *Websites* ..... 32
CAPÍTULO II – ESTUDO EMPÍRICO ..... 35
1. Enquadramento Metodológico ..... 36
2. Objetivos, Hipóteses e Questões de Investigação ..... 37
3. Constituição da Amostra e Procedimentos de Recolha de Dados ..... 39
4. Instrumentos e Operacionalização ..... 40
4.1 Questionário Sociodemográfico ..... 41
4.2 *Eye Tracker* ..... 41
4.3 Guião de Entrevista Semiestruturada ..... 46
5. Procedimentos de Análise de Dados ..... 48
5.1 Análises Estatísticas ..... 48
5.2 Análise Temática do Discurso ..... 49

CAPÍTULO III – RESULTADOS EMPÍRICOS ..... 51
PARTE I: RESULTADOS QUANTITATIVOS ..... 51
1. Caracterização Sociodemográfica da Amostra ..... 52
2. Intenção de Compra nos *Websites* de Comércio ..... 53
3. Atenção Seletiva às AOI dos *Websites* de Comércio ..... 53
3.1 Comparação entre *Websites* Fraudulentos e Legítimos ..... 54
3.2 Análise Visual dos Mapas de Calor ..... 55
4. Relação entre a Atenção Seletiva e a Suscetibilidade à Cibervitimação ..... 55
4.1 Atenção Seletiva e Suscetibilidade dos Participantes ..... 55
4.2 Análise Visual dos Mapas de Calor ..... 57
5. Associação entre Características Sociodemográficas e Suscetibilidade à Cibervitimação ..... 58
PARTE II: RESULTADOS QUALITATIVOS ..... 59
1. Cultura de Consumo Contemporânea ..... 59
2. Pistas Visuais de Legitimidade dos *Websites* ..... 61
3. Construção de Confiança nos *Websites* de Comércio ..... 62
4. Perceção dos Riscos ..... 63
5. Recomendações ..... 65
CAPÍTULO IV – DISCUSSÃO DOS RESULTADOS ..... 65
1. Atenção Seletiva, Confiança e Intenção de Compra *Online* ..... 66
2. Limitações e Pistas Futuras ..... 69
CONCLUSÃO ..... 70
REFERÊNCIAS BIBLIOGRÁFICAS ..... 71
ANEXOS ..... 81
ANEXO A – *Flyer* para a Participação no Estudo ..... 82
ANEXO B – Formulário de Inscrição no Estudo ..... 83
ANEXO C – Termo de Consentimento Informado ..... 86
ANEXO D – Protocolo de Recolha de Dados ..... 87
ANEXO E – Grupo 1 de *Websites* ..... 88
ANEXO F – Grupo 2 de *Websites* ..... 92
ANEXO G – Estratégias de Manipulação dos *Websites* ..... 96
ANEXO H – Guião de Entrevista Semiestruturada ..... 97
ANEXO I – Mapas de Calor dos *Websites* Legítimos e Fraudulentos ..... 99

ANEXO J – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI de cada *Website* Fraudulento ..... 101

ANEXO K – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI dos *Websites* Legítimos ..... 103

ANEXO L – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI de cada *Website* Legítimo ..... 104

ANEXO M – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis ..... 106

ANEXO N – *Mind Map* das Entrevistas ..... 108

ANEXO O – Modelo Sequencial de Construção da Confiança ..... 109

## INDÍCE DE TABELAS

Tabela 1 – Caracterização dos Estímulos ..... 44
Tabela 2 – Caracterização Sociodemográfica da Amostra (N=66)..... 52
Tabela 3 – Intenção de Compra nos *Websites*..... 53
Tabela 4 – Comparação da duração média das fixações, número total médio de fixações e latência nas AOI dos *Websites* (Teste *Friedman*)..... 53
Tabela 5 – Comparação da duração média das fixações, do número total médio de fixações e da latência nas AOI entre *Websites* Fraudulentos e *Websites* Legítimos ..... 54
Tabela 6 – Comparação da duração média das fixações, número total médio de fixações e latência nas AOI dos *Websites* Fraudulentos entre Participantes Não Suscetíveis e Suscetíveis ..... 56
Tabela 7 – Associação entre Variáveis Sociodemográficas e Suscetibilidade à Cibervitimação..... 58

## INDÍCE DE FIGURAS

Figura 1 – Esquema do Protocolo Experimental ..... 44
Figura 2 – Mapas de Calor do *Website* Legitimo 6 e *Website* Fraudulento 8 ..... 55
Figura 3 – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis no F8 (respetivamente) ..... 57
Figura 4 – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis no F1 (respetivamente) ..... 58

# INTRODUÇÃO

Desde o mapeamento geográfico do crime pela Escola Cartográfica no séc. XIX e o registo ilustrativo dos criminosos por Lombroso, as representações visuais permeiam inúmeros conhecimentos criminológicos. Contudo, os materiais visuais destacaram-se na análise de fenómenos criminógenos com o desenvolvimento da Criminologia Visual que pretende discernir os elementos socioculturais, simbólicos e comunicacionais das representações visuais sobre a vitimação, o crime e o seu controlo (Carrabine, 2012; Margolis & Zunjarwad, 2018; Pauwels, 2017; Wheeldon & Harris, 2015).

A importância atribuída ao "universo visual" ascendeu na era digital, na medida em que a expansão desmesurada da *Internet* consolidou a transposição de uma variedade comportamentos para o contexto *online* (Comissão Europeia, 2020; Jahankhani, 2009; Wall, 2001; Yar, 2006) e, consequentemente, transformou a forma como os indivíduos interpretam a realidade social e os estímulos visuais (Brown & Carrabine, 2019; Wheeldon & Harris, 2015; Yar, 2006).

A crescente digitalização da sociedade e os contextos socioculturais, como o da pandemia *Covid-19*, impulsionaram o consumo *online* em massa (Fonseca *et al.*, 2022; Gillespie & Magor, 2020; Theodorou *et al.*, 2023). A aquisição de bens e serviços tornou-se mais cómoda devido às vantagens do comércio *online*, como a rapidez das transações e a variedade de produtos (Edwards *et al.*, 2025; Rose *et al.*, 2011; van Wilsem, 2013). Todavia, assistiu-se ao aumento de fraudes ao consumidor *online*, destacando-se a proliferação de *websites* de comércio fraudulentos que provocam prejuízos patrimoniais e contribuem para a erosão da confiança nos ambientes digitais (Associação Portuguesa de Apoio à Vítima [APAV], 2020; Carpineto & Romano, 2017; Procuradoria-Geral da República [PGR], 2025; Whittaker *et al.*, 2023). Embora qualquer consumidor possa tornar-se vítima, a suscetibilidade à fraude ao consumidor *online* depende da forma como os consumidores percecionam e interpretam os elementos visuais dos *websites* (Chen *et al.*, 2017; Kelley & Bertenthal, 2016; Leukfeldt & Yar, 2016; Waqas *et al.*, 2021).

Perante as lacunas da literatura científica sobre a interseção entre os padrões visuais, a suscetibilidade à fraude ao consumidor *online* e a atribuição de significados aos *websites* de comércio, a presente investigação adotou uma metodologia mista que combina técnicas de *eye-tracking* e de *photo-elicitation* para aprofundar a compreensão dos padrões visuais e dos significados que os indivíduos atribuem aos *websites* de comércio. Desta forma, espera-se que os conhecimentos científicos produzidos contribuam para estratégias preventivas mais eficazes, melhorando a confiança no comércio *online*.

Esta dissertação estrutura-se em quatro capítulos. O Capítulo I apresenta o enquadramento teórico-empírico desta dissertação, delimitando-se, através de uma revisão da literatura, os pressupostos da Criminologia Visual, as evidências científicas sobre o cibercrime e as fraudes *online* (especificamente, as fraudes ao consumidor) e a aplicação das técnicas de *eye-tracking* ao comércio *online*. O Capítulo II, por sua vez, descreve o desenho metodológico do estudo empírico, explicitando os objetivos, as opções metodológicas, os instrumentos de recolha de dados e os procedimentos de análise dos dados. O Capítulo III expõe os resultados obtidos e no Capítulo IV discute-se a integração das evidências quantitativas e qualitativas, bem como as limitações e as pistas para futuros estudos. Por fim, apresentam-se as principais conclusões da investigação.

# CAPÍTULO I – REVISÃO DA LITERATURA

O presente capítulo apresenta o enquadramento teórico-empírico da investigação, incidindo sobre a Criminologia Visual, as fraudes ao consumidor *online*, os fatores associados à suscetibilidade à cibervitimação no comércio *online* e a aplicação das técnicas de *eye-tracking* ao estudo destes fenómenos. Este trabalho comporta a sua originalidade no modo como as componentes visuais são articuladas, pelo que se procederá à justificação desta abordagem no estudo das fraudes ao consumidor *online*.

## 1. Criminologia Visual

A Criminologia Visual consolidou-se como uma subárea da Criminologia na última década, acompanhando o desenvolvimento de pressupostos teóricos, ferramentas metodológicas e técnicas de investigação orientadas para a análise dos significados das representações visuais da criminalidade (Brown & Carrabine, 2019; McClanahan, 2021; Wheeldon, 2021). Assente na premissa de que a observação e as representações visuais constituem fontes de produção de conhecimento sobre fenómenos e contextos socioculturais específicos, esta perspetiva inspirou-se na investigação visual naturalista desenvolvida noutras ciências e aplicou-a ao estudo do crime e do controlo social (Brown & Carrabine, 2019; Margolis & Zunjarwad, 2018; Pauwels, 2017).

A Criminologia Visual ultrapassa a mera descrição das representações visuais associadas a contextos desviantes e criminais, procurando compreender os processos interpretativos através dos quais essas representações adquirem sentido em função das experiências, dos conhecimentos e dos referenciais socioculturais dos indivíduos (Brown & Carrabine, 2019; Carrabine, 2012; Pauwels, 2017; Wheeldon & Harris, 2015).

Consequentemente, as representações visuais não influenciam apenas a forma como o crime é percecionado, mas também a construção de discursos, significados e práticas sociais que lhes estão associadas (Brown & Carrabine, 2019; Hayward, 2010; McClanahan, 2021; Wheeldon & Harris, 2015).

O campo de estudo da Criminologia Visual carece ainda de uma delimitação conceptual consensual. Enquanto alguns autores privilegiam a análise de representações gráficas da criminalidade, outros adotam perspetivas críticas focadas nos mecanismos de poder, vigilância e controlo social (Brown & Carrabine, 2019; Pauwels, 2017; Wheeldon, 2021). Nesta dissertação, a Criminologia Visual é definida como o "uso de qualquer imagem (incluindo, mas não se limitando a pinturas, fotografias, desenhos, mapas, diagramas, gráficos, tabelas e outras abordagens visuais/gráficas) para: recolher informações dos participantes; descrever, apresentar e analisar dados; e/ou analisar ou questionar o(s) significado(s) desses dados" (Wheeldon & Harris, 2015, p. 145). Desta forma, alega-se que o presente trabalho se enquadra na Criminologia Visual já que, como será explicitado, as representações visuais, como imagens e mapas, vão assumir um papel central na recolha, análise e interpretação dos dados.

Os elementos visuais sempre constituíram um dos pilares de análise da Criminologia. Por conseguinte, a Criminologia Visual estabelece estreitas relações com outras áreas criminológicas, como a Criminologia Crítica e a Criminologia Cultural (Hayward, 2010; McClanahan, 2021).

A Criminologia Crítica assenta numa perspetiva sociopolítica da criminalidade, interpretando o fenómeno criminal como um produto das desigualdades sociais, das estruturas de poder e dos mecanismos de controlo (Brown & Carrabine, 2019; McClanahan, 2021). Neste sentido, a Criminologia Visual amplia a análise crítica ao explorar a forma como os elementos visuais e simbólicos participam na construção e na reprodução de relações sociais marcadas por controlo, resistência, violência e exclusão (Brown & Carrabine, 2019; Wheeldon & Harris, 2015; Wheeldon, 2021).

Por sua vez, a Criminologia Cultural defende que as interações humanas, as práticas culturais e as relações de poder moldam os significados atribuídos ao crime, ao desvio e ao controlo social (Hayward, 2010). Por esta razão, a Criminologia Visual partilha o interesse pelos processos simbólicos, pelas representações sociais e pela "imaginação criminológica", procurando compreender de que modo os contextos socioculturais influenciam a interpretação das representações visuais (Hayward, 2010; McClanahan, 2021; Pauwels, 2017).

Nas sociedades contemporâneas, a omnipresença de imagens demonstra a centralidade das representações visuais na construção da realidade social. Os seres humanos dependem da visão para interpretarem os estímulos do mundo que os rodeia e orientarem os seus comportamentos (Margolis & Zunjarwad, 2018). Neste sentido, as representações visuais não constituem elementos meramente ilustrativos, mas formas comunicacionais capazes de persuadir o espectador a assimilar valores, significados e discursos que despertam respostas emocionais e comportamentais (Brown & Carrabine, 2019; Wheeldon & Harris, 2015). Um exemplo paradigmático é o comércio, onde os estímulos visuais, como as publicidades, moldam as perceções dos consumidores e influenciam a intenção de compra (Arnould & Thompson, 2005; McClanahan, 2021; Zahari *et al.*, 2019).

A natureza polissémica das imagens permite-lhes assumir em simultâneo um carácter interpretativo e científico que amplia as possibilidades analíticas da Criminologia Visual. Por um lado, encontram-se sujeitas a inúmeros significados condicionados pelos contextos socioculturais e pelas experiências individuais. Por outro, constituem materiais empíricos passíveis de observação e análise científica (Margolis & Zunjarwad, 2018; McClanahan, 2021). Esta natureza dual acarreta uma diversidade metodológica característica da Criminologia Visual, que recorre a diferentes métodos para analisar as representações visuais e os significados que lhes são atribuídos, o que será detalhado nas secções seguintes.

### 1.1 Métodos Visuais na Tradição Criminológica

A diversidade metodológica da Criminologia Visual reflete a natureza subjetiva e interpretativa dos estudos visuais, exigindo a seleção de métodos, instrumentos e procedimentos adequados às características do objeto de estudo, dos participantes e do contexto sociocultural (McClanahan, 2021; Sun & Benson, 2022). Por exemplo, a utilização de registos estáticos (e.g., fotografias) ou dinâmicos (e.g., vídeos) depende dos objetivos de investigação e do tipo de informação que se pretende extrair, como também do fenómeno sob análise (Pauwels, 2017). Neste sentido, importa rever, desde já, as principais metodologias visuais que fundamentam as opções metodológicas da presente investigação.

A literatura científica destaca quatro abordagens tradicionais de recolha e análise de dados visuais: (i) a produção de imagens originais pelos investigadores; (ii) a produção de imagens pelos participantes; (iii) a análise de imagens fictícias; e (iv) a análise de imagens pré-existentes.

A primeira abordagem refere-se à criação de imagens pelos investigadores através de fotografias documentais obtidas em contextos etnográficos, permitindo registar espaços urbanos e práticas desviantes relevantes para a investigação criminológica, embora suscite desafios éticos relacionados com a privacidade e o consentimento dos sujeitos retratados (Carrabine, 2012; McClanahan, 2021; Pauwels, 2017; Wheeldon & Harris, 2015). A segunda abordagem desloca, parcialmente, o controlo da produção de dados para os participantes, valorizando a sua colaboração ativa na construção de representações visuais que retratem experiências e contextos de vida (McClanahan, 2021; Wheeldon & Harris, 2015), como sucede na técnica de *photo-voice* (foto-voz), em que as imagens são acompanhadas pelas narrativas dos próprios participantes para reduzir interpretações descontextualizadas (McClanahan, 2021; Pauwels, 2017). A terceira abordagem incide na análise de imagens fictícias, como filmes e videojogos, permitindo explorar de que forma os discursos mediáticos e culturais constroem significados sobre o crime, a justiça e o controlo social (Carrabine, 2012; McClanahan, 2021; Pauwels, 2017). Por último, a quarta abordagem constitui um dos métodos mais utilizados devido à ampla disponibilidade de materiais visuais provenientes de arquivos, meios de comunicação social e plataformas digitais, apesar de suscitar questões ético-legais relacionadas, por exemplo, com o direito à imagem e a utilização de registos de videovigilância (CCTV) (McClanahan, 2021; Pauwels, 2017).

Face às limitações de cada método, a produção de conhecimentos tem-se concretizado por meio de processos de criatividade e reflexividade. As técnicas de *photo-elicitation* são particularmente relevantes para o presente estudo, consistindo na utilização de imagens – produzidas pelos investigadores, pelos participantes ou previamente existentes – como estímulos visuais integrados em entrevistas qualitativas (Gill, 2024; Pauwels, 2017). A articulação entre imagens e discursos permite explorar, de forma aprofundada, as experiências, as perceções e os significados que dificilmente emergiriam por outras vias de comunicação verbal (Gill, 2024; Pauwels, 2017; Wheeldon & Harris, 2015), materializando um dos objetivos da Criminologia Visual. No contexto do comércio *online*, esta abordagem tem permitido desconstruir fenomenologicamente as perceções e as experiências dos consumidores, interpretando-se os significados atribuídos às práticas de consumo (Boardman & Mccormick, 2022; Kawaf & Tagg, 2017).

Como veremos de seguida, as tecnologias como o *eye-tracking* ampliaram as possibilidades metodológicas da Criminologia Visual, transformando diversos materiais

em instrumentos híbridos de recolha, análise e interpretação dos dados visuais (Brown & Carrabine, 2019; Hayward, 2010; Pauwels, 2017).

### 1.2 Métodos Visuais na Era Digital

Incontornavelmente, tal como Wall (2001) mencionou, o final do século precedente marcou o surgimento de um novo espaço que coexiste com o mundo físico: o ciberespaço. Este pode ser concebido como "o espaço ou ambiente interacional criado pela ligação de computadores numa rede de comunicação" (Yar, 2006, p. 155). Segundo Sade-Beck (2004), os últimos anos refletiram um processo de "domesticação" (p. 48), ou como prefiro denominar "tecnodomesticação", da população mundial, caracterizado pela crescente incorporação das tecnologias digitais nas rotinas quotidianas e pela progressiva transposição de atividades tradicionalmente presenciais para o ciberespaço. A maior praticidade e rapidez proporcionadas pelas tecnologias transformaram atividades como as comunicações interpessoais e as transações económicas (Edwards *et al.*, 2025; Rose *et al.*, 2011; Theodorou *et al.*, 2023; van Wilsem, 2013; Yar, 2006). Atualmente, estima-se que cerca de 6 mil milhões de pessoas utilizam a *Internet*, o equivalente a 74% da população mundial (International Telecommunication Union, 2025).

O ciberespaço caracteriza-se pela sua natureza imediata, dinâmica e multidimensional, permitindo que os estudos criminológicos o explorem enquanto espaço criminógeno ou método de investigação (Sade-Beck, 2004; Yar, 2006). Por um lado, enquanto objeto de estudo, o ciberespaço constitui o contexto onde são perpetrados diferentes tipos de cibercriminalidade. Por outro lado, enquanto método, os ambientes virtuais armazenam um vasto conjunto de dados e pegadas digitais, incluindo imagens e vídeos, que podem ser recolhidos e analisados cientificamente (Brown & Carrabine, 2019; McClanahan, 2021; Sade-Beck, 2004).

As inovações tecnológicas promoveram novas formas de pensar, agir e interagir, ampliando o potencial de investigação da Criminologia Visual. Os novos dispositivos tecnológicos, como os *smart glasses* e os *eye trackers*, passaram a ser utilizados em cenários naturais ou experimentais com diferentes objetivos como, por exemplo, o estudo da atenção seletiva dos indivíduos nos ambientes digitais ou nos espaços citadinos associados à insegurança (Barreto, 2012; Boardman & Mccormick, 2022; Pauwels, 2017). Em particular, os *eye trackers*, portáteis ou remotos, utilizam sensores infravermelhos e câmaras de vídeo capazes de registar a localização e a duração da atenção visual, permitindo compreender os padrões visuais perante diferentes estímulos

visuais (Barreto, 2012; Darwish & Bataineh, 2012; Semmelmann & Weigelt, 2017; Tobii Pro, 2021).

Desta forma, as tecnologias modificaram a natureza dos fenómenos sociais e criminológicos, assim como providenciaram novos instrumentos para a sua investigação (Hollingworth & Bahle, 2019; Wheeldon & Harris, 2015; Wong *et al.*, 2014). Entre esses fenómenos, destaca-se a cibercriminalidade, que será abordada na secção seguinte.

## 2. Cibercriminalidade

O desenvolvimento das tecnologias digitais e das interfaces informáticas criou um espaço de vigilância e de acesso a informações privadas, onde circulam dados pessoais e bancários, que anteriormente permaneciam inacessíveis a terceiros desconhecidos (Brown & Carrabine, 2019; Comissão Europeia, 2020; Edwards *et al.*, 2025; Sun, 2002). Se é consensual que a *Internet* proporcionou inúmeras oportunidades legítimas, não é menos verdade que a mesma facilitou "novos caminhos" associados a oportunidades criminais. A perpetração de crimes *online* (ou cibercrimes) traduz-se numa criminalidade inovadora, quer pela adaptação da prática de crimes tradicionais ao ciberespaço, quer pelo surgimento de novos ilícitos que dependem da *Internet* para serem consumados (Furnell, 2001; Guedes *et al.*, 2021; Wall, 2001).

Atualmente, a cibercriminalidade representa um fenómeno ubíquo e uma das principais ameaças transfronteiriças a nível global, à qual Portugal não é exceção (Comissão Europeia, 2020; Sistema de Segurança Interna [SSI], 2025; Venâncio, 2021). Neste contexto, a proteção dos cidadãos no ciberespaço tem vindo a assumir crescente relevância jurídica e político-criminal. A Lei n.º 51/2023, de 28 de agosto, que definiu objetivos, prioridades e orientações da política criminal para o biénio 2023-2025 classificou a cibercriminalidade como criminalidade de prevenção e investigação prioritária. Esta orientação é reforçada na Lei n.º 35/2026, de 27 de julho, relativa às prioridades da política criminal para o biénio 2026-2028, que reafirma a cibercriminalidade como um dos fenómenos criminais prioritários, na prevenção e investigação, e prevê o reforço dos mecanismos de coordenação e investigação criminal.

Apesar dos esforços institucionais, legislativos e de outra natureza para combater a cibercriminalidade, este fenómeno revela-se bastante exigente para a investigação criminal e científica. Tal como Yar (2006) referiu, a cibercriminalidade compreende um "conjunto de atividades ilegais e ilícitas que partilham em comum o ambiente eletrónico único ("ciberespaço") em que ocorrem" (p. 5). Apesar da abrangência e uniformidade

demonstradas nesta designação, não podemos ignorar que a cibercriminalidade engloba diversos crimes com características distintas que exigem conhecimentos técnicos por parte das autoridades e dos académicos. No domínio científico, persistem dificuldades conceptuais e metodológicas decorrentes da coexistência de diferentes designações e definições. Às noções alternativas (e.g., "crime informático") somam-se as explicações com elementos díspares que requerem metodologias de investigação diferenciadas em função do objeto de estudo ou do tipo de cibercrime em questão (Furnell, 2001; Guedes *et al.*, 2021; Leukfeldt & Yar, 2016).

### 2.1 Tipologias de Cibercrime

A diversidade de ilícitos que podem ser perpetrados no ciberespaço conduziu diversos autores à elaboração de tipologias destinadas a sistematizar e a compreender as diversas manifestações da cibercriminalidade (Furnell, 2001; Wall, 2001).

Furnell (2001) apresentou uma das distinções mais importantes nesta matéria, diferenciando "infrações assistidas por computador" das "infrações focadas no computador", de acordo com o papel da tecnologia na prática do crime. As primeiras correspondem a crimes que existiam antes da *Internet*, mas que passaram a ser facilitados pela mesma, surgindo novos meios para a sua perpetração como, por exemplo, as fraudes. As segundas referem-se a crimes que dependem da existência de redes e sistemas informáticos para serem consumados, não sendo concebíveis fora do ciberespaço, como o *hacking* (ou acesso ilegítimo a sistemas informáticos).

Wall (2001) elaborou uma tipologia mais abrangente baseada em quatro áreas de condutas prejudiciais praticadas no ciberespaço. A primeira área é denominada de "*cybertrespass*" e corresponde a atividades destinadas ao acesso não autorizado a sistemas informáticos alheios, como o *hacking*. A segunda área designa-se de "*cyberdeceptions/thefts*" e abarca comportamentos aquisitivos ou patrimoniais, incluindo as fraudes *online* associadas a cartões de crédito. A terceira área corresponde à "*cyberpornography/obscenity*", integrando a divulgação ou a disseminação de conteúdos sexuais ofensivos e ilegais como a pornografia de menores. A quarta área denomina-se de "*cyberviolence*" e refere-se à manifestação de conteúdos sociopolíticos suscetíveis de provocar danos psicológicos, emocionais ou sociais, como o *cyberbullying*.

A nível internacional, a Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste), que teve como finalidade promover a proteção da sociedade no ciberespaço, propôs a seguinte tipologia da cibercriminalidade: (i) as infrações contra

a confidencialidade, integridade e disponibilidade de dados informáticos, como o "acesso ilegítimo" (art.º 2.º); (ii) as infrações relacionadas com computadores, como a "burla informática" (art.º 8.º); (iii) as infrações relacionadas com o conteúdo, concretamente associadas à "pornografia infantil" (art.º 9.º); e (iv) as infrações relacionadas com a violação de direitos de autor e direitos conexos (art.º 10.º) (Conselho da Europa, 2001).

Em Portugal, a atual Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro) resultou da ratificação, pelo Estado português, da Convenção sobre o Cibercrime e da adoção da Decisão Quadro n.º 2005/222/JAI15, do Conselho da Europa, de 24 de fevereiro, relativa a ataques contra sistemas de informação, revogando a Lei n.º 109/91. Apesar do Código Penal (CP) sancionar condutas informáticas, como a "burla informática e nas comunicações" (art.º 221.º) que será abordada adiante, a Lei do Cibercrime (LC) consagrou novas disposições penais, nomeadamente a "falsidade informática" (art.º 3.º), o "dano relativo a programas ou outros dados informáticos" (art.º 4.ª), a "sabotagem informática" (art.º 5.º), o "acesso ilegítimo" (art.º 6.º), a "interceção ilegítima" (art.º 7.º) e a "reprodução ilegítima de programa protegido" (art.º 8.º).

Perante as diferentes tipologias apresentadas, realça-se que não existe uma classificação universalmente aceite. Estas tipologias não devem ser entendidas como classificações concorrentes, mas enquadramentos complementares que revelam que a cibercriminalidade constitui um fenómeno heterogéneo e em permanente adaptação às transformações tecnológicas e sociais. Com o agravamento do contexto geopolítico internacional e a crescente digitalização, as entidades portuguesas reforçaram a preocupação securitária no ciberespaço de interesse nacional perante o aumento significativo de cibercrimes perpetrados por agentes independentes ou redes organizadas, destacando-se a evolução técnica por Inteligência Artificial (IA), a complexidade e a frequência destas práticas, particularmente das fraudes *online* (SSI, 2023, 2025). Por esse motivo, a secção seguinte centra-se no fenómeno destas fraudes.

### 2.2 Fraudes: Do *Offline* ao *Online*

A fraude constitui um fenómeno com raízes históricas profundas, precedendo a existência da *Internet* (Dadà *et al.*, 2025; Gillespie & Magor, 2020; Sofo *et al.*, 2010; Whitty, 2020). Segundo Titus *et al.* (1995), as fraudes envolvem "a deturpação de factos e a intenção deliberada de enganar com a promessa de bens, serviços ou outros benefícios financeiros que de facto não existem ou que nunca se pretendeu que fossem fornecidos" (p. 54), configurando a versatilidade e o engano como características nucleares.

Por um lado, a fraude não constitui uma prática homogénea, mas apresenta várias ramificações de atividades ilícitas distintas (Beals *et al.*, 2015; Dadà *et al.*, 2025; Kemp & Pérez, 2023), pelo que será conceptualizada, na presente dissertação, como um termo "guarda-chuva". Perante esta complexidade, Beals *et al.* (2015) propuseram uma taxonomia da fraude financeira constituída por sete categorias que diferenciam ações económico-financeiras em função dos benefícios esperados pelos indivíduos, nomeadamente: (i) a fraude de investimentos, que envolve a promessa enganosa de elevados retornos financeiros mediante investimentos (e.g., esquemas *Ponzi*); (ii) a fraude de produtos e serviços de consumo, que se refere à venda de produtos inexistentes ou adulterados; (iii) a fraude no emprego, na qual se oferecem falsas oportunidades de emprego para solicitar pagamentos prévios; (iv) a fraude de prémios e subsídios, em que se instigam ações financeiras em troca de prémios ou subsídios fictícios; (v) a fraude de cobrança de dívidas fantasma, que consiste em tentativas de cobrar dívidas inexistentes; (vi) a fraude de caridade, em que se solicitam pagamentos para causas sociais ou organizações inexistentes; e (vii) a fraude de relacionamento e confiança, que explora vínculos emocionais e afetivos para obter benefícios financeiros (e.g., fraude romântica).

Independentemente da sua modalidade, o engano constitui o denominador comum das fraudes, que compreendem estratégias de manipulação destinadas a induzir a potencial vítima em erro, participando em transações económicas que não seriam concretizadas se a verdade fosse esclarecida (Beals *et al.*, 2015; Dadà *et al.*, 2025; Whittaker *et al.*, 2025; Yar, 2006).

Embora as fraudes assentem em práticas enganosas, nem todos os enganos configuram fraudes, pelo que importa averiguar os enquadramentos jurídicos. No ordenamento jurídico português, a fraude pode ser tipificada como "burla", prevista no art.º 217.º do CP[1]. A interpretação desta norma permite elencar quatro elementos deste fenómeno, a saber: (i) a intenção de "obter para si ou para terceiro enriquecimento ilegítimo"; (ii) o meio através de "erro ou engano"; (iii) a ação da vítima com a "prática de atos que lhe causem, ou causem a outra pessoa" prejuízo; e (iv) as consequências traduzidas num "prejuízo patrimonial". Posto isto, estamos perante um crime cujo bem jurídico protegido consiste no património, recobrindo situações em que um agente, com intenção de enriquecimento ilegítimo (próprio ou alheio), induz outra pessoa em erro para que esta pratique atos que causem a si (ou a terceiros) prejuízos patrimoniais (Costa, 2020).

[1] O agente que praticar tais atos pode ser punido com pena de prisão até três anos ou com pena de multa. A tentativa punível nos termos do n.º 2.

Tal como sucedeu com outros crimes, a fraude transitou para o ciberespaço, surgindo as designações de "fraude *online*" (Cross *et al.*, 2014) ou "fraude cibernética ou na *Internet*" (Beals *et al.*, 2015). Nesta dissertação, adota-se o primeiro termo para referir "a experiência de alguém que respondeu, através da *Internet*, a um convite, notificação ou oferta desonesta, fornecendo informações pessoais ou dinheiro que levou a uma perda ou impacto financeiro ou não financeiro de algum tipo" (Cross *et al.*, 2014, p. 1).

As fraudes *online* incluem cibercrimes heterogéneos, tais como as fraudes ao consumidor em *websites* e as fraudes românticas nas redes sociais, caracterizando-se pela utilização de meios informáticos para divulgar anúncios, estabelecer contacto com as vítimas ou concretizar transações financeiras (Beals *et al.*, 2015; Button *et al.*, 2014; Gillespie & Magor, 2020; Jahankhani, 2009; Whitty, 2020; Yar, 2006).

Face às múltiplas manifestações deste fenómeno, a Convenção sobre o Cibercrime estabeleceu, no art.º 8.º, a necessidade de os Estados adotarem medidas legislativas ou outras para concretizar como ilícito penal as ações intencionais que visem obter enriquecimento ilegítimo através de prejuízos patrimoniais a terceiros por meio de sistemas informáticos (Conselho da Europa, 2001). As normas internacionais foram transpostas para o ordenamento jurídico português e as fraudes *online* podem corresponder a duas figuras de delito que consubstanciam crimes contra o património (Costa, 2020), nomeadamente a burla (art.º 217.º do CP) e a burla informática e nas comunicações (art.º 221.º do CP)[2], que contempla, no n.º 1, a burla informática e, no n.º 2, a burla nas telecomunicações. Estes tipos legais diferenciam-se quanto aos meios e à forma de concretização do dano. Enquanto as burlas correspondem a ações ou relações enganosas que culminam na atuação da vítima consoante uma vontade minada, como as burlas românticas, as burlas informáticas materializam-se através do uso incorreto de meios informáticos com o *animus* do enriquecimento, como a criação de *websites* fraudulentos ou, também, denominados de "*websites phishing*"[3] (APAV, 2020; Costa, 2020).

Nas últimas décadas, a doutrina e a jurisprudência portuguesas divergiram quanto à possibilidade de concurso aparente ou efetivo entre a burla informática e a falsidade

[2] O agente que praticar tais atos incorre na mesma moldura penal, prevendo-se pena de prisão até três anos ou pena de multa. A tentativa é punível nos termos do n.º 3.

[3] O *phishing* consiste em técnicas através das quais os ofensores recorrem a comunicações enganosas, como *e-mails* e *websites* fraudulentos, que simulam entidades legítimas com o objetivo de induzir os indivíduos a divulgarem dados pessoais ou bancários (Brody *et al.*, 2007; Darwish & Bataineh, 2012; Whittaker *et al.*, 2025).

informática[4], que visa proteger a integridade/funcionalidade dos sistemas informáticos (Costa, 2020; Venâncio, 2021). Enquanto alguma jurisprudência, admite o concurso efetivo por entender que ambos conservam relevância autónoma e protegem bens jurídicos diferentes (Venâncio, 2021), Costa (2020) defende o concurso aparente, legal ou de normas, considerando que a falsidade informática constitui um meio para efetivar a burla informática e é, por isso, absorvida por esta.

A crescente digitalização do consumo potenciou a perpetração de fraudes nos *websites* de comércio, tornando este fenómeno uma grave problemática por comportar vários riscos e danos para as vítimas e a sociedade geral, como serão explicitados adiante. Por esse motivo, a secção seguinte centra-se na fraude ao consumidor *online*.

## 3. Cultura de Consumo Contemporânea e Fraudes ao Consumidor *Online*

O progresso tecnológico e a expansão da *Internet* transformaram profundamente as práticas de consumo, impulsionando o crescimento do comércio *online* (também denominado de "comércio eletrónico" ou "*e-commerce"*). Atualmente, esta modalidade permite a aquisição rápida de bens e serviços através da aproximação de vendedores e consumidores no ciberespaço, eliminando limitações espaciais e temporais do comércio físico (Bangun & Handra, 2021; Izogo & Jayawardhena, 2018; Jahankhani, 2009; Rana & Baria, 2015; Whittaker *et al.*, 2025; Yar, 2006).

Apesar de partilharem o mesmo propósito comercial, o comércio *online* distingue-se do comércio tradicional ou físico. Em primeiro lugar, caracteriza-se pela conveniência de acesso a produtos e serviços sem restrições espácio-temporais, ao passo que o comércio tradicional permanece condicionado por horários de funcionamento e pela localização geográfica dos estabelecimentos (Bangun & Handra, 2021; Fonseca *et al.*, 2022; Rose *et al.*, 2011; Sun, 2002; van Wilsem, 2013). Em segundo lugar, o comércio *online* disponibiliza informações detalhadas sobre os produtos através de formatos (áudio)visuais, como fotografias e vídeos, que facilitam a avaliação e a comparação dos produtos disponíveis, enquanto no comércio físico as informações tendem a ser limitadas e dependentes de pósteres, folhetos ou etiquetas (Bangun & Handra, 2021; Rose *et al.*, 2011). Por fim, o contacto interpessoal assume uma expressão reduzida no comércio *online*, predominando plataformas digitais e sistemas de atendimento automático, ao contrário do comércio tradicional em que a interação com funcionários e os estímulos

[4] De acordo com o art.º 3.º da LC, a falsidade informática comtempla condutas em que o agente pratica a ação de "introduzir, modificar, apagar ou suprimir dados ou programas informáticos" ou "interferir num tratamento informáticos de dados" com o efeito de produzir "dados ou documentos não genuínos".

sensoriais do espaço físico influenciam a experiência e a intenção de compra (Rose *et al.*, 2011; van Wilsem, 2013).

A ascensão global do comércio *online* não resulta apenas das inovações tecnológicas ou das estratégias comerciais das empresas. Trata-se, também, de uma evolução sociocultural impulsionada pela globalização económica, pela concorrência entre mercados e pela livre circulação de bens (Arnould & Thompson, 2005; Edwards *et al.*, 2025; Jahankhani, 2009). Este crescimento intensificou-se durante a pandemia do *Covid-19*, um período em que o encerramento de lojas físicas e as restrições geográficas à mobilidade dos cidadãos aceleraram a integração de práticas de consumo *online* nas rotinas quotidianas (Apau & Koranteng, 2020; Cross *et al.*, 2022; Edwards *et al.*, 2025; Theodorou *at al.*, 2023; Whittaker *et al.*, 2025).

Estas transformações enquadram-se na cultura de consumo contemporânea caracterizada pela produção em massa, pela digitalização dos mercados, pela valorização da conveniência e pela procura de satisfação imediata das necessidades dos consumidores (Arnould & Thompson, 2005; Edwards *et al.*, 2025). Segundo, Arnould e Thompson (2005), a cultura do consumidor denota um sistema interconectado de discursos, práticas e identidades que se traduzem num "arranjo social no qual as relações entre cultura vivida e recursos sociais, e entre modos de vida significativos e os recursos simbólicos e materiais dos quais dependem, são mediadas por meio de mercados" (p. 869). Consequentemente, o consumo contemporâneo assume uma natureza híbrida, conjugando motivações utilitárias, associadas à satisfação das necessidades práticas através da aquisição de bens, e motivações hedónicas, relacionadas com o prazer, a experiência sensorial, a gratificação emocional e os significados atribuídos às práticas de consumo *online* (Cross *et al.*, 2022; Kawaf & Tagg, 2017; Whittaker *et al.*, 2023).

Com a consolidação destas dinâmicas, o comércio *online* constitui uma pedra basilar da vida moderna na União Europeia (UE). Os dados mais recentes revelam um aumento contínuo do número de indivíduos que realizam compras *online*, sobretudo a população jovem-adulta entre os 25 e os 34 anos com níveis de escolaridade mais elevados, uma tendência desde os 18 aos 54 anos (Conselho Europeu, 2025).

À semelhança de outros Estados-Membros da UE, Portugal registou uma tendência crescente do comércio *online*. No ano de 2025, 50% da população residente em Portugal com idades compreendidas entre os 16 e os 74 anos efetuou compras na *Internet*, observando-se uma maior prevalência de indivíduos com menos de 55 anos, estudantes e empregados detentores de níveis de escolaridade mais elevados (Autoridade Nacional de

Comunicações [ANACOM], 2025). Nos últimos três anos, o volume de compras *online* ultrapassou os 6 mil milhões de euros, destacando-se as categorias do vestuário e dos produtos eletrónicos (ANACOM, 2025; CTT, 2024). Entre os principais fatores apontados pelos consumidores portugueses para a adesão ao comércio *online*, salientam-se a facilidade de compra e os preços mais reduzidos, privilegiando plataformas internacionais amplamente difundidas, como a *Shein*, a *Temu* e a *Amazon* (CTT, 2024).

As características estruturais do comércio *online* convergem na experiência do consumidor, que corresponde a "um estado cognitivo e afetivo que surge de significados culturais atribuídos ao conjunto de interações entre um cliente e um objeto" (Waqas *et al.*, 2021, p. 139). Embora os ambientes digitais possam apresentar características semelhantes, estes são interpretados de forma distinta em função das experiências, dos conhecimentos e dos contextos socioculturais de cada indivíduo (Bangun & Handra, 2021; Izogo & Jayawardhena, 2018; Kawaf & Tagg, 2017; Rose *et al.*, 2011; Waqas *et al.*, 2021).

A crescente complexidade das relações de consumo *online*, como a distância entre as partes, justificou o desenvolvimento de instrumentos jurídicos interdisciplinares destinados a regular o ciberespaço e a proteger os consumidores (PGR, 2025). O Regulamento (UE) 2022/2065, do Parlamento Europeu e do Conselho, de 19 de outubro, intitulado Regulamento dos Serviços Digitais, estabelece um quadro normativo direcionado para a criação de ambientes digitais mais seguros, transparentes e competitivos, introduzindo-se exigências de rigor das relações comerciais, de proteção dos consumidores contra conteúdos nocivos e fraudes, e de responsabilização das plataformas no combate à venda de produtos ilegais. Em Portugal, o regime legal aplicável à defesa dos consumidores (Lei n.º 24/96, de 31 de julho) consagra no art.º 2.º a definição de consumidor, constando no art.º 3.º direitos, como a proteção dos interesses económicos e a proteção jurídica, e no art.º 12.º o direito à reparação dos danos. Esta proteção já se encontra vertida no art.º 60.º da Constituição da República Portuguesa, que estabelece os direitos dos consumidores, tais como os direitos à qualidade dos bens e serviços consumidos, à formação e à informação, à proteção da saúde, da segurança e dos seus interesses económicos, bem como à reparação de danos.

Embora indispensável, a proteção jurídica revela-se insuficiente para garantir, por si só, a segurança[5] das transações *online*, uma vez que a constante adaptação das práticas fraudulentas às novas tecnologias amplia as oportunidades de atuação dos ofensores e coloca desafios aos consumidores, às empresas e às autoridades (APAV, 2020; Yar, 2006).

Neste contexto, importa aprofundar o fenómeno das fraudes ao consumidor *online*. Antes da próxima secção, ressalva-se que as tendências de consumo *online* e, por consequência, os padrões de cometimento destas fraudes podem sofrer alterações em resultado da recente aprovação do Regulamento (UE) 2026/382, do Conselho. Este diploma prevê a aplicação, entre 1 de julho de 2026 a 1 de julho de 2028, de um direito aduaneiro de 3€ por artigo cujo valor intrínseco não exceda um total de 150€, procurando reforçar o controlo sobre as importações de reduzido valor provenientes de países terceiros e reduzir parte das vantagens competitivas associadas às plataformas de comércio *online* extracomunitárias.

### 3.1 Enquadramento da Fraude ao Consumidor *Online*

A cibervitimação por fraude ao consumidor *online* pode ser definida como o ato de "pagar por um produto *online* que nunca foi entregue, bem como receber um produto muito diferente do esperado, geralmente de qualidade inferior ou uma falsificação" (Cross *et al.*, 2022, p. 7). Trata-se, assim, de uma situação em que os consumidores efetuam encomendas e pagamentos através da *Internet*, mas os bens adquiridos não são entregues ou apresentam características substancialmente distintas das prometidas, originando prejuízos patrimoniais e a violação das expectativas negociais (Button *et al.*, 2014; Comissão Europeia, 2020; Leukfeldt & Yar, 2016; Pinjarkar *et al.*, 2024; van Wilsem, 2013; Whittaker *et al.*, 2023; Yar, 2006).

Do ponto de vista criminológico, a fraude ao consumidor *online* constitui uma forma de criminalidade económica devido à obtenção de vantagens patrimoniais ilícitas pelos ofensores através da exploração da confiança dos consumidores (e.g., Beals *et al.*, 2015; Carpineto & Romano, 2017; Holtfreter *et al.*, 2008; Whittaker *et al.*, 2025). Simultaneamente, enquadra-se em diferentes tipologias de cibercrime. Por um lado, corresponde a uma *cyberdeception/theft* (Wall, 2001) por envolver comportamentos aquisitivos fraudulentos orientados para o lucro económico mediante o logro das vítimas (Carpineto & Romano, 2017; Fonseca *et al.*, 2022). Por outro, configura uma ofensa

[5] Neste contexto, a segurança diz respeito à perceção de que o *website* dispõe de mecanismos técnicos capazes de proteger as informações pessoais e financeiras dos consumidores durante o processo de compra *online* (Abbasi & Chen, 2009; Jahankhani, 2009; Zahari *et al.*, 2019).

assistida por computador (Furnell, 2001), na medida em que transpõe práticas fraudulentas já existentes para o ciberespaço, permitindo aos ofensores beneficiar da distância física, do anonimato e do alcance proporcionado pela *Internet* (Reisig & Holtfreter, 2013; Sofo *et al.*, 2010; Whittaker *et al.*, 2025; Yar, 2006).

A expansão substancial do comércio *online*, particularmente durante a pandemia do *Covid*-19, aumentou exponencialmente as oportunidades para a prática destas fraudes e o número de potenciais vítimas nos mercados virtuais (Cross *et al.*, 2022; Edwards *et al.*, 2025; Fonseca *et al.*, 2022). Em 2020, estimava-se que as fraudes ao consumidor *online* representavam cerca de 38% das fraudes denunciadas no mundo (Gillespie & Magor, 2020).

Pese embora a relevância das fraudes ao consumidor *online*, as estatísticas oficiais nacionais denotam limitações relativas à sua medição, prejudicando o rigor da quantificação estatística. Quanto aos crimes registados pelas autoridades policiais, este fenómeno não surge como uma categoria autónoma ou independente, uma vez que estas condutas são registadas sob diferentes tipos legais, nomeadamente a burla ou a burla informática. Segundo Venâncio (2021), a autonomização da burla informática exprime a relevância da promoção do comércio *online* e das transações eletrónicas, observando-se, assim, que o dano patrimonial da vítima e o enriquecimento do agente são operados no ambiente digital, ou seja, o *iter criminis* desenrola-se no ciberespaço (Costa, 2020). Acresce que as entidades responsáveis pelo registo dos crimes não diferenciam os contextos *offline* e *online*, agregando ocorrências sob categorias genéricas, como sucede com a burla com fraude bancária.

Estima-se ainda que as cifras negras sejam elevadas já que a subnotificação é um problema transversal às fraudes *online* e a verdadeira dimensão da prevalência e da incidência permanece difícil de determinar (Button *et al.*, 2014; Williams *et al.*, 2017; Yar, 2006). Tal como ocorre com outras formas de cibercriminalidade ou criminalidade económica, a maioria das vítimas não reporta os factos às autoridades policiais ou prefere comunicá-los a instituições alternativas (Fonseca *et al.*, 2022). Alguns lesados experienciam sentimentos de vergonha e preferem esquecer a situação, sobretudo em situações de quase cibervitimação[6] (Button *et al.*, 2014; Cross *et al.*, 2022; Edwards *et al.*, 2025; Yar, 2006), enquanto outros demonstram pouca confiança no trabalho da polícia

[6] Neste contexto, a quase cibervitimação designa uma situação em que o individuo esteve próximo de ser vítima, mas desistiu do processo de compra *online*, geralmente após identificar indícios de suspeição do *website*, como a solicitação injustificada de dados pessoais (Cross *et al.*, 2022; Edwards *et al.*, 2025).

para recuperar os valores perdidos, principalmente quando os montantes envolvidos são reduzidos (Button *et al.*, 2014; Comissão Europeia, 2020; Fonseca *et al.*, 2022; PGR, 2025; Yar, 2006).

No contexto português, os resultados de Fonseca *et al.* (2022) ilustram baixas taxas de denúncia à polícia, verificando-se que apenas 10% dos participantes reportaram as fraudes ao consumidor *online* a esta entidade. Em contraste, 62% das vítimas não reportou a cibervitimação e 28% recorreram a outras instituições, justificando essa decisão com a reduzida confiança na atuação da polícia e do Sistema de Justiça.

Dados complementares sobre a cibervitimação têm sido recolhidos por instituições alternativas como a APAV e a Associação Portuguesa para a Defesa do Consumidor (DECO). De acordo com a Linha Internet Segura da APAV (2025), a burla constituiu um dos principais tipos legais reportados no último ano, registando-se 247 ocorrências, das quais 40 correspondiam a fraudes ao consumidor *online*.

Se, outrora, a perpetração destas fraudes assentava em promessas enganosas do envio de produtos mediante pagamentos, os avanços tecnológicos complexificaram as estratégias fraudulentas e, atualmente, os ofensores recorrem a *websites* fraudulentos com o objetivo de ludibriarem os consumidores e obterem vantagens financeiras ilícitas. É precisamente sobre estes *websites* que incide a secção seguinte.

### 3.2 Os *Websites* de Comércio Fraudulentos

Em poucos anos, os *websites* transformaram-se em montras comerciais globais que viabilizaram a comercialização de bens e serviços por parte de empresas e outros atores económicos, expandindo as oportunidades de consumo (Gillespie & Magor, 2020; Jahankhani, 2009; van Wilsem, 2013; Whittaker *et al.*, 2023). Ao eliminarem barreiras geográficas e temporais, estas plataformas digitais possibilitaram o contacto imediato entre vendedores e consumidores em diferentes partes do mundo, tornando qualquer cibernauta num potencial consumidor (APAV, 2020, 2025; Jahankhani, 2009; Yar, 2006).

Não obstante as vantagens proporcionadas para a aquisição de produtos ou serviços, os *websites* constituem contextos propícios para a ocorrência de fraudes ao consumidor *online*. Entre as práticas mais comuns, destacam-se as fraudes em *websites* de vendas públicas, onde qualquer pessoa pode anunciar produtos que efetivamente serão entregues, como também produtos inexistentes ou que, apesar de serem entregues, diferem das características anunciadas (Cross *et al.*, 2022; Edwards *et al.*, 2025; Whittaker *et al.*, 2023; Yar, 2006).

Ultimamente, assistiu-se à proliferação de *websites* fraudulentos que simulam plataformas legítimas através da manipulação dos seus elementos visuais, estruturais e funcionais como, por exemplo, imagens adulteradas de produtos comerciais (Bitaab *et al.*, 2023; Cross *et al.*, 2022; Edwards *et al.*, 2025; Rana & Baria, 2015; Whittaker *et al.*, 2025). Esta evolução denota a adaptabilidade das práticas criminosas às novas tecnologias. Para esse efeito, os ofensores recorrem a técnicas de *web spoofing*, que consistem na reprodução total ou parcial da aparência de *websites* legítimos com o objetivo de criar uma falsa perceção de autenticidade e induzir os consumidores em erro na concretização de transações económicas fraudulentas (Bitaab *et al.*, 2023; Darwish & Bataineh, 2012; Pinjarkar *et al.*, 2024; SSI, 2023; Whittaker *et al.*, 2023; Yar, 2006). Os *marketplaces* internacionais, como o *eBay* e a *Amazon*, tendem a ser os mais adulterados devido ao elevado grau de familiaridade que estas marcas despertam nos consumidores (Chen *et al.*, 2017; Cross *et al.*, 2022; Kelley *et al.*, 2023; Pinjarkar *et al.*, 2024; Whittaker *et al.*, 2023; Wong *et al.*, 2014).

Neste âmbito, importa distinguir dois conceitos centrais. A legitimidade corresponde ao juízo acerca da autenticidade do *website* enquanto montra digital de uma empresa genuína que opera de forma legal (Dhamija *et al.*, 2006; Kelley *et al.*, 2023; Whittaker *et al.*, 2023; Yar, 2006; Zahari *et al.*, 2019). Já a confiança traduz a expectativa de credibilidade em relação ao *website*, na medida em que as pessoas acreditam que a empresa que o sustenta irá atuar de forma honesta durante todo o processo de compra, respeitando as obrigações e os deveres inerentes ao papel de vendedor (Carpineto & Romano, 2017; Jahankhani, 2009; Rose *et al.*, 2011; Yar, 2006; Zahari *et al.*, 2019).

Em Portugal, os *websites* fraudulentos constituem uma particular preocupação, uma vez que vários cidadãos realizam compras nos *websites* das empresas de comércio (ANACOM, 2025; CTT, 2024). Com o aumento destes esquemas fraudulentos, o Gabinete do Cibercrime da PGR instaurou, nos últimos dois anos, mais de 30 inquéritos relacionados com *websites* fraudulentos de marcas de vestuário destinados à obtenção de pagamentos por produtos que não seriam entregues (PGR, 2025).

Apesar dos esforços desenvolvidos, a identificação e o combate a estes *websites* continuam a representar um desafio para as autoridades e para a comunidade académica. Por um lado, estas plataformas permanecem, frequentemente, ativas durante curtos períodos, sendo removidas ou substituídas pouco tempo após a criação para evitar a deteção (Bitaab *et al.*, 2023; Pinjarkar *et al.*, 2024). Por outro lado, podem integrar campanhas de *e-mails phishing* que encaminham as potenciais vítimas para *websites*

fraudulentos (Beals *et al.*, 2015; Brody *et al.*, 2007; Darwish & Bataineh, 2012; Sofo *et al.*, 2010; Whittaker *et al.*, 2025). Consequentemente, estas práticas provocam riscos e danos significativos aos consumidores e à sociedade geral, como será abordado a seguir.

### 3.3 Riscos e Danos para Vítimas e Sociedade

Apesar dos mecanismos jurídicos e institucionais destinados a regular o comércio *online*, as compras na *Internet* não estão isentas de riscos e de possíveis consequências adversas para os consumidores e os restantes membros da sociedade.

Segundo Jahankhani (2009), estes riscos podem ser agrupados em seis categorias. Primeiro, o risco financeiro refere-se à possibilidade de perdas económicas decorrentes do não recebimento dos produtos ou da aquisição de bens que não correspondem ao valor pago. Segundo, o risco físico corresponde a potenciais danos para a saúde ou o bem-estar causados pela utilização de produtos contrafeitos ou perigosos. Terceiro, o risco funcional diz respeito à incerteza sobre o desempenho ou a qualidade dos produtos face às expectativas criadas. Quarto, o risco psicológico envolve sentimentos de insatisfação e frustração provocados pela aquisição de produtos incompatíveis com as preferências ou necessidades do consumidor. Quinto, o risco social está associado à preocupação de que os produtos adquiridos comprometam a imagem que os indivíduos pretendem transmitir aos outros. Por último, o risco de perda de tempo resulta dos recursos temporais investidos na procura, aquisição, devolução ou substituição dos produtos.

Embora estes riscos sejam antecipados antes da compra, a consciencialização dos mesmos surge quando ocorrem fraudes. Os estudos vêm demonstrando que o risco financeiro é a principal preocupação dos consumidores, dado que o prejuízo patrimonial constitui uma consequência imediata e tangível da cibervitimação (Button *et al.*, 2014; Cross *et al.*, 2022; Dadà *et al.*, 2025; Edwards *et al.*, 2025). A Comissão Europeia (2020) estimou que os cidadãos da UE perderam, cumulativamente, cerca de 24 mil milhões de euros em compras *online* fraudulentas. Todavia, a literatura científica alerta para a necessidade de interpretar estes prejuízos à luz das condições socioeconómicas das vítimas, uma vez que perdas relativamente reduzidas podem despoletar consequências gravosas para indivíduos com menores rendimentos (APAV, 2020; Cross *et al.*, 2022).

Aos prejuízos patrimoniais diretos acrescem outros, nomeadamente psicológicos, que conduzem à erosão da confiança nos *websites* de comércio, fragilizando o progresso económico das empresas e, em última instância, dos países (Apau & Koranteng, 2020; Dadà *et al.*, 2025; Izogo & Jayawardhena, 2018; Jahankhani, 2009; SSI, 2023; van

Wilsem, 2013). Em muitos casos, os lesados responsabilizam as empresas comerciais pelas perdas sofridas e descrevem insatisfação perante os mecanismos de apoio ao cliente ou de reembolso (Cross *et al.*, 2022; Edwards *et al.*, 2025).

Independentemente de terem sido enganados ou não, muitos consumidores relatam sentimentos de medo, desconfiança e insegurança em relação aos *websites* de comércio (APAV, 2020; Brody *et al.*, 2007; Cross *et al.*, 2022; Edwards *et al.*, 2025; van Wilsem, 2013). Por exemplo, Kemp e Pérez (2023), através de um estudo com cerca de 26 mil participantes, procuraram analisar os impactos da (ciber)vitimação por fraudes ao consumidor entre diferentes grupos etários e verificaram que os adultos mais velhos experienciaram com maior frequência consequências emocionais e físicas, como raiva, frustração, vergonha e deterioração do bem-estar. De forma convergente, a revisão sistemática de Dadà *et al.* (2025) concluiu que os mais velhos apresentam reações emocionais mais intensas do que os jovens, incluindo raiva, desilusão e vergonha.

Paradoxalmente, a perceção destes riscos pode promover comportamentos de autoproteção na *Internet*, incluindo a procura de informações sobre *websites* desconhecidos e a verificação dos indicadores de legitimidade (Bangun & Handra, 2021; Comissão Europeia, 2020; Cross *et al.*, 2022; Edwards *et al.*, 2025). Assim, os múltiplos riscos das fraudes no comércio *online* reforçam a necessidade de promover estratégias de prevenção e sensibilização que permitam fortalecer a coesão social e a confiança da sociedade num comércio *online* mais seguro. Para esse efeito, revela-se crucial compreender que fatores explicam a suscetibilidade às fraudes no comércio *online*.

## 4. Teorias Explicativas da Suscetibilidade à Fraude ao Consumidor *Online*

A expansão global da *Internet* alargou significativamente o universo de potenciais vítimas de fraude ao consumidor *online*, embora alguns indivíduos apresentem maior grau de suscetibilidade à cibervitimação (APAV, 2020; Dadà *et al.*, 2025; Dhamija *et al.*, 2006; Leukfeldt & Yar, 2016; Pratt *et al.*, 2010). Enquanto a cibervitimação por fraude ao consumidor *online* diz respeito à experiência efetiva de se ser enganado ou prejudicado no contexto das compras *online* (Cross *et al.*, 2022; Pinjarkar *et al.*, 2024; van Wilsem, 2013), a suscetibilidade corresponde à predisposição ou probabilidade de um indivíduo ser enganado neste tipo de fraude, mesmo sem uma cibervitimação efetiva (Kelley *et al.*, 2023; Norris *et al.*, 2019; Williams *et al.*, 2017).

A literatura tem revelado que a suscetibilidade às fraudes no comércio *online* resulta da interação entre fatores individuais, cognitivos, comportamentais e socioculturais.

Assim, esta secção apresenta quadros teóricos explicativos dessa suscetibilidade: (i) a Teoria das Atividades de Rotina; (ii) o Modelo Heurístico-Sistemático; (iii) a Teoria do Comportamento Planeado; e (iv) a Teoria da Cultura do Consumidor.

### 4.1 Teoria das Atividades de Rotina

Cohen e Felson (1979) desenvolveram a Teoria das Atividades de Rotina (TAR) para explicar a ocorrência de crimes predatórios associados às mudanças ocorridas nos estilos de vida contemporâneos. Segundo os autores, a crescente participação no mercado de trabalho, a multiplicação de relações interpessoais e a enorme movimentação de bens de consumo e transações ampliaram as oportunidades criminais. A TAR postula que o crime resulta da convergência, no tempo e no espaço, de três elementos em simultâneo: (i) o ofensor motivado, alguém com intenção e capacidade para delinquir; (ii) o alvo adequado, uma pessoa ou um objeto com características atrativas para o ofensor; e (iii) a ausência de guardiões eficazes, que poderiam dissuadir e prevenir o crime. Assim, na confluência destes elementos, dá-se o risco de vitimação (Reyns, 2013), mas a ausência de apenas um elemento pode "evitar que tais infrações ocorram" (Cohen & Felson, 1979, p. 590).

Embora concebida para explicar os crimes tradicionais, a TAR tem sido adaptada à cibercriminalidade, argumentando-se que as oportunidades criminais surgem num espaço e num tempo que não envolvem a proximidade física entre as vítimas e os ofensores (Holtfreter *et al.*, 2008; Leukfeldt & Yar, 2016; Pratt *et al.*, 2010; Reyns, 2013). Neste contexto, a exposição ao ofensor motivado tem sido operacionalizada pelo tempo despendido *online* (e.g., Fonseca *et al.*, 2022; Pratt *et al.*, 2010), pela utilização quotidiana de serviços digitais, como o uso do *e-mail* (e.g., Chen *et al.*, 2017), pela frequência de compras *online* (e.g., van Wilsem, 2013), entre outros indicadores. O alvo adequado tem sido associado à realização de atividades de maior risco, como a interação com desconhecidos em fóruns digitais (e.g., Reyns, 2013) e a utilização de *websites* inseguros (e.g., Reisig & Holtfreter, 2013). Por fim, a ausência de guardiões eficazes tem sido relacionada com a insuficiência de mecanismos de proteção técnica e de competências digitais, como a inexistência de *softwares* antivírus (e.g., Chen *et al.*, 2017) e os níveis reduzidos de literacia digital[7] (e.g., Leukfeldt & Yar, 2016).

As evidências empíricas demostram que uma maior frequência de compras *online* aumenta a exposição a oportunidades fraudulentas e, consequentemente, a probabilidade

[7] Entendida como o conjunto de conhecimentos e competências de cada individuo que permitem utilizar as tecnologias digitais de forma segura e reduzir a exposição aos riscos *online* (Leukfeldt & Yar, 2016).

de cibervitimação (Chen *et al.*, 2017; Kemp & Pérez, 2023; Leukfeldt & Yar, 2016; Pratt *et al.*, 2010; Reyns, 2013; van Wilsem, 2013). Ademais, a utilização de *websites* inseguros e a divulgação de informações pessoais e bancárias sem a devida verificação da legitimidade das plataformas digitais aumentam significativamente a suscetibilidade às fraudes no comércio *online* (Chen *et al.*, 2017; Fonseca *et al.*, 2022; Reisig & Holtfreter, 2013; van Wilsem, 2013).

Apesar do contributo da TAR para explicar as oportunidades de cibervitimação, esta teoria dá primazia aos fatores situacionais, atribuindo menor relevância aos processos cognitivos relacionados com a interpretação dos estímulos visuais. Porém, a literatura recente sugere que a suscetibilidade não depende apenas da exposição ao risco, mas também da forma como os indivíduos processam e avaliam a informação disponível no contexto *online* (e.g., Leukfeldt & Yar, 2016). Desta forma, esta teoria pode ser enriquecida com a integração de modelos explicativos do processamento da informação, como o explicitado na secção seguinte.

### 4.2 Modelo Heurístico-Sistemático

Proposto por Chaiken (1980), o Modelo Heurístico-Sistemático (MHS) explica a construção de perceções, juízos e atitudes a partir do processamento de informações. Segundo este modelo dual, os indivíduos adaptam o seu estilo de raciocínio às circunstâncias e aos recursos cognitivos disponíveis, existindo dois modos de processamento – o heurístico e o sistemático – que podem ocorrer em simultâneo, mas diferem quanto ao grau de esforço e análise (Chaiken, 1980; Todorov *et al.*, 2002).

O processamento heurístico caracteriza-se por uma avaliação rápida e superficial da informação, baseada em regras simples ou *scripts* (Chaiken, 1980; Todorov *et al.*, 2002), que permitem selecionar atalhos cognitivos e tomar decisões com pouco esforço (Kelley *et al.*, 2023; Shang *et al.*, 2023). Este modo é ativado quando os indivíduos dispõem de pouco tempo, apresentam baixa motivação ou possuem recursos cognitivos limitados para desconstruir as informações, recorrendo a um número reduzido de pistas heurísticas para formar juízos (Todorov *et al.*, 2002). Em contraste, o processamento sistemático envolve uma análise deliberada, lógica e aprofundada da informação disponível, exigindo maior esforço cognitivo (Chaiken, 1980; Todorov *et al.*, 2002). Este modo ocorre quando as pessoas estão motivadas para avaliar criticamente os estímulos e as informações recolhidas (Kelley *et al.*, 2023; Shang *et al.*, 2023; Todorov *et al.*, 2002).

Os diferentes níveis de atenção e de processamento da informação conduzem a distintos graus de suscetibilidade à cibervitimação. A evidência empírica demonstra que o processamento heurístico tende a aumentar a probabilidade de os consumidores confiarem em *websites* fraudulentos, uma vez que favorece a rapidez da análise de informações em detrimento da avaliação crítica das pistas disponíveis (Chen *et al.*, 2017; Kelley *et al.*, 2023; Shang *et al.*, 2023; Sun, 2002). A sobreposição destes processos a mecanismos racionais de avaliação da informação é mais acentuada entre consumidores com reduzidos níveis de literacia digital, dado que estes tendem a basear os seus juízos em pistas visuais superficiais (e.g., logótipos e cores fluorescentes), revelando maior dificuldade em distinguir indicadores de segurança digital de estratégias enganosas (Chen *et al.*, 2017; Kelley & Bertenthal, 2016; Leukfeldt & Yar, 2016). Esta identificação seria possível com o processamento sistemático que permitiria uma avaliação mais deliberada e aprofundada dos *websites*, possibilitando a detetação de sinais de suspeição (Kelley *et al.*, 2023; Shang *et al.*, 2023; Sun, 2002).

A revisão sistemática realizada por Shang *et al.* (2023) centrou-se nos mecanismos cognitivos subjacentes à cibervitimação por fraudes, reforçando esta perspetiva ao evidenciar que determinadas características do contexto tecnológico, como a utilização de dispositivos móveis, podem favorecer o processamento heurístico. A rapidez das interações e as limitações associadas à menor dimensão dos ecrãs reduzem a profundidade da análise, aumentando a probabilidade de os consumidores utilizarem atalhos cognitivos e, consequentemente, a sua suscetibilidade.

Não obstante a sua pertinência, o MHS atribui menor relevância aos fatores motivacionais e socioculturais que influenciam a intenção de compra *online* e os significados atribuídos às práticas de consumo (Rose *et al.*, 2011; Waqas *et al.*, 2021). Por esse motivo, estes fatores serão abordados de forma integrada na próxima secção.

### 4.3 Da Teoria do Comportamento Planeado à Teoria da Cultura do Consumidor

Como veremos de seguida, a intenção de compra *online* resulta da interação entre processos individuais, que orientam as escolhas dos indivíduos, e contextos socioculturais, que moldam as crenças, as expectativas e as práticas de consumo. Neste sentido, decidiu-se articular a Teoria do Comportamento Planeado (TCP) e a Teoria da Cultura do Consumidor (TCC) por constituírem, a nosso ver, abordagens teóricas complementares para compreender a suscetibilidade à fraude ao consumidor *online*.

Derivada da Teoria da Ação Racional, a TCP procura explicar e prever comportamentos humanos através da associação entre as intenções e as ações dos indivíduos. Segundo Ajzen (1991), o comportamento resulta diretamente da intenção de o realizar e esta, por sua vez, é influenciada por três elementos: (i) a atitude em relação ao comportamento[8]; (ii) as normas subjetivas[9]; e (iii) o controlo comportamental percebido[10]. A intenção só se manifesta em comportamento quando o indivíduo dispõe de um suficiente "controlo volitivo" (Ajzen, 1991, p. 181), ou seja, quando possui a capacidade e a oportunidade para agir. No contexto do comércio *online*, a TCP tem sido utilizada para explicar a intenção de compra *online*, que pode ser entendida como a predisposição dos indivíduos para realizarem compras na *Internet* (e.g., Apau & Koranteng, 2020; Bangun & Handra, 2021; Izogo & Jayawardhena, 2018; Theodorou *et al.*, 2023). As evidências empíricas demostram que esta intenção é influenciada pelas atitudes face às compras *online*, pelos benefícios percebidos das transações, pela facilidade de utilização de tecnologias e pelas normas sociais, incluindo as recomendações ou as opiniões de terceiros (Apau & Koranteng, 2020; Bangun & Handra, 2021; Izogo & Jayawardhena, 2018; Rose *et al.*, 2011).

Embora a TCP explique a formação das intenções comportamentais, não esclarece os processos sociais e culturais que sustentam os significados e as práticas de consumo. Neste âmbito, a Teoria da Cultura do Consumidor (TCC), proposta por Arnould e Thompson (2005), complementa esta perspetiva ao interpretar o consumo como uma prática social e culturalmente produzida. Entende-se que os seres humanos são atores socioculturais que constroem identidades, interpretando as dinâmicas dos mercados em função de valores e discursos resultantes da interação entre as macroestruturas sociais e as microestruturas das experiências quotidianas (Arnould & Thompson, 2005; van Dijk, 2009).

No comércio *online*, os *websites* constituem ambientes simbólicos que difundem valores, estilos de vida e significados associados ao consumo, influenciando a forma como os consumidores interpretam os estímulos visuais e constroem intenções de compra (Button *et al.*, 2014; Waqas *et al.*, 2021). Paralelamente, as estratégias comerciais das

[8] Apreciação favorável ou desfavorável quanto à realização de determinado comportamento (Ajzen, 1991; Bangun & Handra, 2021; Theodorou *et al.*, 2023).
[9] Crenças relativamente a comportamentos específicos resultantes da pressão ou opinião de grupos próximos, como a família e os amigos (Ajzen, 1991; Bangun & Handra, 2021; Theodorou *et al.*, 2023).
[10] Perceção de facilidade ou dificuldade em realizar determinado comportamento (Ajzen, 1991; Bangun & Handra, 2021; Theodorou *et al.*, 2023).

empresas articulam-se com as crenças, as motivações e as expectativas individuais, contribuindo para a normalização do comércio *online* e potenciando decisões impulsivas (Button *et al.*, 2014; Holtfreter *et al.*, 2008; Sofo *et al.*, 2010). Assim, os consumidores que valorizam a rapidez, a conveniência e a satisfação imediata dos seus interesses tendem a privilegiar pistas visuais apelativas, podendo tornar-se mais suscetíveis quando esses elementos são estrategicamente manipulados pelos ofensores em *websites* fraudulentos (Chen *et al.*, 2017; Holtfreter *et al.*, 2008; Izogo & Jayawardhena, 2018; Sun, 2002; van Wilsem, 2013; Waqas *et al.*, 2021).

Embora a TCP e a TCC possam oferecer um enquadramento explicativo para compreender que a intenção de compra *online* resulta da articulação entre condições individuais, sociais e culturais, a literatura demonstra que a interpretação dos estímulos visuais, a construção da confiança e a suscetibilidade à fraude ao consumidor *online* variam em função de outros aspetos, como as experiências prévias e os conhecimentos adquiridos durante as interações *online*, que serão desenvolvidos na secção seguinte.

## 5. Outros Fatores Explicativos da Suscetibilidade

Embora os enquadramentos teóricos anteriormente apresentados contribuam para explicar a suscetibilidade às fraudes ao consumidor *online*, estes não esgotam a complexidade do fenómeno. As evidências científicas demonstram que a suscetibilidade não se distribuí de forma homogénea entre os consumidores, mas varia consoante fatores individuais, que se encontram relacionados com características sociodemográficas, perceções e experiências prévias, e fatores contextuais, que estão associados à interação dos indivíduos com o ambiente digital (Dadà *et al.*, 2025; Norris *et al.*, 2019; Williams *et al.*, 2017). A seguir, serão revistos alguns trabalhos sobre a influência destes fatores na suscetibilidade à cibervitimação por fraude ao consumidor *online*.

### 5.1 Fatores Individuais

A literatura tem analisado de que modo as características sociodemográficas, as experiências prévias de consumo *online*, a literacia digital e a perceção do risco de cibervitimação influenciam esta suscetibilidade específica.

#### 5.1.1 Características Sociodemográficas

A investigação científica tem correlacionado a idade, o género, as habilitações literárias e os rendimentos dos participantes com a suscetibilidade às fraudes no comércio *online*. Embora não exista consenso, os principais resultados revelam que os homens mais

velhos com rendimentos mais elevados são 60% mais suscetíveis de serem vítimas (e.g., Reyns, 2013).

Os estudos também revelam que os mais jovens são mais propensos à cibervitimação devido ao maior tempo despendido na *Internet*, o que aumenta as oportunidades de contacto com ofensores e de realização de compras *online* (e.g., Pratt *et al.*, 2010; van Wilsem, 2013). Contudo, outros autores encontraram uma relação positiva entre a idade e a cibervitimação, argumentando que os adultos mais velhos têm maior probabilidade de serem vítimas, o que pode ser explicado, entre várias razões, pelas menores competências digitais e, consequentemente, pela maior dificuldade em identificar estratégias fraudulentas (e.g., Reyns, 2013; Whitty, 2020). Já Kemp e Pérez (2023) identificaram uma maior suscetibilidade entre indivíduos dos 35 aos 49 anos, eventualmente devido à maior capacidade económica para realizar compras *online*.

Embora alguns estudos apontem que as mulheres são mais suscetíveis à cibervitmação (Whitty, 2020), outros demonstram que os homens apresentam maior probabilidade de serem vítimas de fraudes ao consumidor *online* devido a padrões socioculturais associados à propensão para assumir riscos na *Internet* (e.g., Holtfreter *et al.*, 2008; Reyns, 2013). Contudo, diversos resultados não identificaram diferenças significativas entre o género e a cibervitimação (e.g., Edwards *et al.*, 2025; van Wilsem, 2013).

Quanto às habilitações literárias, a literatura sugere que os menores níveis de escolaridade estão positivamente associados à suscetibilidade, visto que menores conhecimentos académicos e informáticos dificultam a avaliação crítica dos *websites* de comércio (e.g., Leukfeldt & Yar, 2016; Shang *et al.*, 2023; Whitty, 2020). Todavia, Pratt *et al.* (2010) e van Wilsem (2013) verificaram resultados paradoxais: os mais escolarizados revelaram um elevado grau de suscetibilidade, eventualmente devido ao excesso de confiança na sua segurança *online*.

Por fim, no que respeita aos rendimentos, algumas investigações indicam que os indivíduos com rendimentos mais elevados apresentam maior probabilidade de se tornarem vítimas devido ao poder económico para uma maior frequência de compras *online* (e.g., Reyns, 2013). Pelo contrário, a perceção de dificuldades financeiras pode reduzir a intenção de compra *online* e, consequentemente, diminuir a exposição ao risco. Outros estudos referem que as condições financeiras não exercem influência significativa na probabilidade de cibervitimação (e.g., Fonseca *et al.*, 2022; Leukfeldt & Yar, 2016).

Os resultados encontrados sobre as características sociodemográficas e a suscetibilidade à fraude ao consumidor *online* são inconclusivos. Em vários estudos, estas

variáveis revelam associações reduzidas ou inexistentes (Dhamija *et al.*, 2006; Fonseca *et al.*, 2022; Reisig & Holtfreter, 2013). Isto sugere que a suscetibilidade dificilmente pode ser explicada por fatores sociodemográficos considerados isoladamente (Titus *et al.*, 1995; Whitty, 2020). Estes resultados reforçam a necessidade de considerar outros fatores cognitivos, comportamentais e contextuais.

### 5.1.2 Experiências Prévias de Consumo *Online*

As experiências prévias refletem o grau de familiaridade dos indivíduos com o comércio *online*, influenciando os juízos de legitimidade, confiança e risco associados às compras na *Internet*. De forma geral, as experiências positivas reforçam a confiança e aumentam a predisposição para o consumo nos *websites*, reduzindo incertezas inerentes às transações digitais (Jahankhani, 2009; Rose *et al.*, 2011; Zahari *et al.*, 2019).

A reiteração de compras bem-sucedidas favorece processos de habituação e de normalização dos padrões de consumo *online*, conduzindo os consumidores a interpretarem os *websites* como plataformas digitais previsíveis, familiares e seguras (Jahankhani, 2009; Kawaf & Tagg, 2017). Contudo, esta familiaridade pode aumentar a suscetibilidade à cibervitimação. A confiança acumulada reduz os comportamentos de vigilância perante potenciais ameaças *online*, levando os indivíduos a recorrerem a processos heurísticos na avaliação dos *websites* (Kelley & Bertenthal, 2016; Zahari *et al.*, 2019). Neste sentido, Kelley e Bertenthal (2016) realizaram um estudo com participantes que acederam a diferentes *websites* (legítimos e fraudulentos) e responderam a um questionário auto-reportado sobre o seu conhecimento da segurança digital, verificando que os indivíduos mais familiarizados com determinados *websites* apresentavam menor probabilidade de confirmar elementos de segurança digital devido à criação de padrões visuais automáticos e às expectativas de credibilidade relativamente a *websites* similares.

Em contrapartida, experiências negativas de consumo *online*, particularmente quando associadas à cibervitimação, tendem a comprometer a confiança nos *websites* e a reduzir a intenção de compra *online*, sobretudo devido aos prejuízos patrimoniais ou à exposição de informações pessoais e bancárias (Cross *et al.*, 2022; Rose *et al.*, 2011). Paralelamente, concebe-se que aqueles que experienciaram situações de engano podem adotar comportamentos cautelosos, tornando-se potencialmente menos suscetíveis a novas tentativas de fraudes no comércio *online* (Cross *et al.*, 2022; Edwards *et al.*, 2025).

Em síntese, as experiências prévias podem constituir um fator de risco ou proteção à suscetibilidade à fraude ao consumidor *online*. Enquanto as experiências positivas podem promover uma confiança excessiva e diminuir comportamentos de vigilância, as

experiências negativas tendem a reforçar a perceção dos riscos e a incentivar estratégias de proteção *online*. Estes processos remetem para a relevância da perceção dos riscos na redução da suscetibilidade à cibervitimação, um aspeto que será abordado a seguir.

### 5.1.3 Riscos Percebidos e Literacia Digital

A literatura realça que inúmeros consumidores avaliam as compras *online* através da ponderação entre os potenciais riscos (e.g., perdas financeiras) e os benefícios esperados (e.g., a variedade de produtos) (Bangun & Handra, 2021; Jahankhani, 2009). Concretamente, os estudos demonstram que indivíduos que já foram enganados no comércio *online* percecionam mais riscos quanto a esta modalidade de consumo (Bangun & Handra, 2021; Cross *et al.*, 2022; Edwards *et al.*, 2025). A maioria das evidências científicas revela uma associação positiva entre os riscos percebidos e a adoção de comportamentos de precaução no ciberespaço, sugerindo que quem perceciona mais riscos irá evitar *websites* considerados inseguros (Bangun & Handra, 2021; Edwards *et al.*, 2025; Jahankhani, 2009; Leukfeldt & Yar, 2016).

A perceção dos riscos encontra-se estreitamente associada à literacia digital. A evidência científica demonstra que a literacia digital é um fator de resiliência à cibervitimação no comércio *online*, uma vez que os indivíduos com mais conhecimentos e competências digitais possuem capacidades cognitivas e técnicas que permitem identificar mais facilmente pistas fraudulentas e adotar comportamentos de proteção nas plataformas digitais (Chen *et al.*, 2017; Leukfeldt & Yar, 2016; Norris *et al.*, 2019). Em contrapartida, os indivíduos com reduzidas competências informáticas tendem a adotar comportamentos impulsivos, porque percecionam menos riscos e não detetam informações enganosas, tornando-se mais suscetíveis (Kelley & Bertenthal, 2016; Shang *et al.*, 2023).

Assim, a intenção de compra *online* pode resultar do equilíbrio entre as vantagens percebidas das transações *online* e os riscos que lhes são associados. Neste sentido, estas dimensões serão integradas no estudo, de modo a compreender a sua influência nos padrões visuais, na interpretação dos *websites* e na suscetibilidade à cibervitimação.

## 5.2 Fatores Contextuais

A suscetibilidade à cibervitimação pode resultar das interações estabelecidas entre os indivíduos e as interfaces digitais. Neste contexto, a literatura tem recorrido ao conceito

de engenharia social[11] para explicar os mecanismos de manipulação dos ofensores, explorando vulnerabilidades humanas e tecnológicas. Segundo Jahankhani (2009), a engenharia social pode assumir duas modalidades. Por um lado, o engano baseado na pessoa, em que os ofensores procuram persuadir as potenciais vítimas, aproveitando-se da falta de conhecimentos e da predisposição para cooperar. Por outro, o engano baseado na tecnologia, que envolve a manipulação de recursos tecnológicos para induzir os indivíduos a acreditar que estão a interagir com um sistema ou uma plataforma verídica.

Neste trabalho adota-se uma abordagem lata de engenharia social, entendendo-a como o conjunto de estratégias que combinam técnicas de manipulação psicológica e recursos tecnológicos com o propósito de induzir os indivíduos em erro (e.g., Whittaker *et al.*, 2023). Estas estratégias serão apresentadas agora com mais pormenor.

### 5.2.1 Estratégias Persuasivas

A literatura sublinha a importância de se compreender as estratégias persuasivas dos ofensores, de forma a se poder avaliar as ameaças e a construir estratégias de prevenção mais eficazes contra as fraudes no comércio *online* (Brody *et al.*, 2007; Dhamija *et al.*, 2006; Holtfreter *et al.*, 2008; Norris *et al.*, 2019; Pratt *et al.*, 2010; Whittaker *et al.*, 2023).

A maioria dos estudos científicos revela que os ofensores deste tipo de fraude são homens adultos, motivados pela obtenção de lucros económicos (Carpineto & Romano, 2017; Cross *et al.*, 2014; Edwards *et al.*, 2025). Contudo, algumas evidências sugerem que também procuram experiências de excitação e gratificação emocional associadas à manipulação e ao controlo das vítimas (Whittaker *et al.*, 2025). Neste sentido, estes esquemas fraudulentos são concebidos para ludibriar um público alargado, induzindo à divulgação de dados pessoais (e.g., números de cartões de crédito) e à participação em transações fraudulentas (Brody *et al.*, 2007; Pinjarkar *et al.*, 2024; Williams *et al.*, 2017).

Neste contexto, os princípios de influência propostos por Cialdini (2007) constituem um enquadramento útil para compreender os principais indutores psicológicos utilizados pelos ofensores. A literatura destaca seis mecanismos que influenciam comportamentos por impulso. Primeiro, a autoridade é construída mediante a apropriação e a exibição de elementos distintivos de empresas comerciais reconhecidas, como os logótipos (Dhamija *et al.*, 2006; Pinjarkar *et al.*, 2024; Sofo *et al.*, 2010; Williams *et al.*, 2017; Yar, 2006). Segundo, a prova social assenta na premissa de que o ser humano procura agir de acordo

[11] Conjunto de estratégias utilizadas para influenciar os indivíduos a se envolverem em comportamentos de risco, como transações *online* inseguras (Pinjarkar *et al.*, 2024; Williams *et al.*, 2017).

com a maioria, verificando-se a partilha de históricos de compras recentes e de testemunhos positivos que apresentam o consumo *online* como uma prática comum e socialmente aceitável (Bitaab *et al.*, 2023; Button *et al.*, 2014; Williams *et al.*, 2017). Terceiro, o compromisso é explorado mediante o incentivo a ações que aumentam a probabilidade de concluir a compra, como a criação de conta de utilizador e a adição de produtos ao carrinho (Button *et al.*, 2014; Carpineto & Romano, 2017; Sun, 2002). Quarto, a reciprocidade manifesta-se na promessa de recompensas ou benefícios emocionais, como a satisfação, após a realização de compras *online* (Button *et al.*, 2014; Rose *et al.*, 2011; Williams *et al.*, 2017). Quinto, a simpatia traduz-se na utilização de uma linguagem acolhedora, como mensagens de boas-vindas ao *website*, e na exposição de conteúdos de consumo adaptados aos interesses dos consumidores (PGR, 2025; Pinjarkar *et al.*, 2024; Sun, 2002). Por fim, a escassez, através da qual os ofensores exploram heurísticas cognitivas e emocionais com a menção da urgência, por meio de promoções por tempo limitado e últimas oportunidades, procurando desencadear o receio da perda de oportunidades de aquisição (Bitaab *et al.*, 2023; Button *et al.*, 2014; Dadà *et al.*, 2025; Kelley *et al.*, 2023; Sofo *et al.*, 2010; Williams *et al.*, 2017).

Além destes mecanismos de persuasão, os preços constituem uma das estratégias mais eficazes para aumentar a atratividade dos *websites* fraudulentos. Embora procurem reproduzir uma aparência semelhante aos *websites* legítimos, estes *websites* anunciam produtos com preços significativamente inferiores aos praticados no mercado (por vezes, cerca de 80% do preço de base), aumentando a intenção de compra *online* (Bitaab *et al.*, 2023; Carpineto & Romano, 2017; Kelley *et al.*, 2023; PGR, 2025; Pinjarkar *et al.*, 2024; Rana & Baria, 2015; Whittaker *et al.*, 2025).

Por fim, as avaliações *online* podem ser cruciais na construção da confiança e na intenção de realizar compras na *Internet*. O ciberespaço disponibiliza múltiplos canais de interação virtual, onde os consumidores publicam comentários (ou *feedbacks*) acerca das suas experiências, podendo influenciar os comportamentos de outros indivíduos, sobretudo quando são utilizadas expressões emocionais de satisfação e felicidade (Izogo & Jayawardhena, 2018; Jahankhani, 2009; Sun, 2002; Yar, 2006). Ainda que as experiências negativas se encontrem associadas à maior disposição para a partilha de testemunhos (Izogo & Jayawardhena, 2018), a aparência legítima dos *websites* fraudulentos pode ser complementada com a publicação de avaliações falsas dos produtos. Estas avaliações podem ser produzidas por vendedores ou terceiros com o intuito de simular opiniões de "consumidores reais", reforçar artificialmente a

credibilidade dos *websites* e impulsionar a venda dos produtos (Hu *et al.*, 2010; Pinjarkar *et al.*, 2024; Whittaker *et al.*, 2023; Yar, 2006). Neste âmbito, Hu *et al.* (2010) concluíram que as avaliações dos produtos de menor qualidade são alvo de manipulações frequentes para compensar a reduzida atratividade real e inflacionar a procura.

### 5.2.2 Construção das Interfaces e Pistas Fraudulentas

A diferenciação entre *websites* legítimos e fraudulentos revela-se cada vez mais difícil, uma vez que estes últimos apresentam funcionalidades, elementos visuais e recursos característicos dos *websites* legítimos, incluindo a barra de pesquisa dos produtos, os logótipos e até os métodos de pagamento aparentemente seguros (Abbasi & Chen, 2009; Bitaab *et al.*, 2023; Carpineto & Romano, 2017; Dhamija *et al*., 2006; Hu *et al.*, 2010).

Esta semelhança resulta de um duplo processo. Por um lado, os *websites* legítimos têm vindo a conceber interfaces mais sofisticadas para proporcionar experiências de consumo *online* intuitivas e emocionalmente apelativas (Boardman & Mccormick, 2022; Kawaf & Tagg, 2017; Sun, 2002; Wong *et al.*, 2014). Por outro, os ofensores apropriam-se dessas características visuais e estruturais, reproduzindo identidades gráficas idênticas às de empresas reconhecidas, conferindo uma aparência profissional aos *websites* fraudulentos (Abbasi & Chen, 2009; Bitaab *et al.*, 2023; Carpineto & Romano, 2017; Dhamija *et al.*, 2006; Pinjarkar *et al.*, 2024; Rana & Baria, 2015; Yar, 2006).

Neste contexto, importa desconstruir a ideia de que os *websites* fraudulentos se caracterizam por interfaces rudimentares, erros evidentes e reduzida qualidade gráfica. A literatura demonstra que muitos destes *websites* apresentam um elevado nível de qualidade visual, recorrendo a cores apelativas e imagens de alta resolução que suscitam respostas emocionais positivas, aumentando a predisposição para efetuar compras *online* e, portanto, a suscetibilidade à cibervitimação (Abbasi & Chen, 2009; Dhamija, 2006; Pinjarkar *et al.*, 2024; Sun, 2002; Whittaker *et al.*, 2023).

A suscetibilidade às fraudes nos *websites* de comércio pode ainda ser potenciada pela reduzida atenção ou pelo desconhecimento dos consumidores relativamente aos indicadores de segurança digital. Embora estes indicadores auxiliem os indivíduos a atribuírem juízos ou avaliações de legitimidade às plataformas digitais, a sua presença constitui um sinal meramente indicativo de segurança e não uma garantia absoluta de legitimidade, uma vez que podem ser manipulados pelos ofensores (Darwish & Bataineh, 2012; Dhamija *et al.*, 2006; Kelley & Bertenthal, 2016; Whittaker *et al.*, 2023). Um dos principais elementos que contribui para a atribuição da legitimidade corresponde ao endereço URL (do inglês "*Uniform Resource Locator*"), localizado na barra do navegador

e responsável pela identificação de recursos na *Internet*, como páginas *web*. Este endereço é composto pelo protocolo HTTPS e pelo nome de domínio da entidade, mas pode ser alvo de manipulações subtis que passam despercebidas aos consumidores menos atentos (Abbasi & Chen, 2009; Carpineto & Romano, 2017; Darwish & Bataineh, 2012).

Também existem outras pistas que podem sinalizar *websites* fraudulentos. Em primeiro lugar, os conteúdos textuais podem apresentar uma linguagem descuidada, erros ortográficos e/ou gramaticais e traduções incoerentes (Abbasi & Chen, 2009; APAV, 2020; Dhamija *et al.*, 2006; Kelley *et al.*, 2023). Em segundo, é comum existirem variações dos nomes de domínio de marcas reconhecidas – por exemplo, "*vvish*" em vez de "*wish*" – com vista a induzir os consumidores em erro através da semelhança visual (Bitaab *et al.*, 2023; Dhamija *et al.*, 2006; Kelley & Bertenthal, 2016; Kelley *et al.*, 2023). Em terceiro, a ausência do protocolo de segurança HTTPS e/ou do ícone de ligação segura representado na forma de cadeado pode indicar que as comunicações não se encontram protegidas por encriptação, sendo comum nestes casos a utilização do protocolo HTTP ou a apresentação de avisos de (in)segurança (Abbasi & Chen, 2009; APAV, 2020; Carpineto & Romano, 2017; Darwish & Bataineh, 2012; Dhamija *et al.*, 2006; Kelley & Bertenthal, 2016; Kelley *et al.*, 2023). Por fim, muitos *websites* fraudulentos não apresentam informações complementares ou disponibilizam dados falsos sobre políticas de privacidade, contactos da empresa ou outras informações institucionais (Bitaab *et al.*, 2023; Carpineto & Romano, 2017; Kelley *et al.*, 2023; PGR, 2025; Pinjarkar *et al.*, 2024).

Deste modo, o conhecimento e a identificação destas pistas fraudulentas podem reduzir a suscetibilidade à cibervitimação no comércio *online*. Todavia, reconhecer a importância destes elementos não significa, necessariamente, que os consumidores lhes prestem atenção durante a interação com o *website*. Assim, a próxima secção aborda as técnicas de *eye-tracking*, que permitem compreender quais são os elementos visuais dos *websites* que recebem maior atenção dos indivíduos e quais tendem a ser ignorados.

## 6. *Eye-Tracking* e o Estudo da Atenção Seletiva em *Websites*

A tecnologia de *eye-tracking* tem vindo a assumir relevância em diversas áreas de investigação científica, e particularmente na Criminologia, porque permite analisar objetivamente os padrões visuais e inferir os processos cognitivos subjacentes à tomada de decisão, à perceção do risco e às interações em ambientes digitais (Akshay *et al.*, 2020; Barreto, 2012; Gordieiev *et al.*, 2021; Wong *et al.*, 2014).

As técnicas de *eye-tracking* consistem na monotorização dos movimentos oculares dos indivíduos durante a observação de estímulos visuais, como imagens de *websites*, permitindo registar as propriedades espácio-temporais da atenção seletiva e identificar padrões visuais dificilmente observáveis por outros métodos (Barreto, 2012; Darwish & Bataineh, 2012; Gordieiev *et al.*, 2021; Hollingworth & Bahle, 2019).

No contexto *online*, o *eye-tracking* tem sido utilizado para compreender a forma como os consumidores distribuem a sua atenção pelos diferentes elementos visuais que compõem os *websites*, em diversas categorias de produtos e dispositivos tecnológicos (Akshay *et al.*, 2020; Darwish & Bataineh, 2012; Wong *et al.*, 2014). Para esse efeito, delimitam-se áreas de interesse (AOI – do inglês "*Areas of Interest*"), que correspondem a zonas específicas do estímulo visual sob análise, incluindo os logótipos, os produtos e o URL, permitindo comparar a atenção dirigida a cada uma dessas áreas (Barreto, 2012; Boardman & Mccormick, 2022; Darwish & Bataineh, 2012; Gordieiev *et al.*, 2021).

Entre as principais métricas analisadas, destacam-se as fixações[12], representadas por círculos com dimensão proporcional ao tempo de atenção dedicado a uma área do estímulo, permitindo inferir os elementos que exigem maior processamento cognitivo ou despertam maior interesse visual (Barreto, 2012; Darwish & Bataineh, 2012; Gordieiev *et al.*, 2021). Estudos prévios têm analisado as fixações através de indicadores como o número total[13], a duração total[14] e a latência[15] (e.g., Darwish & Bataineh, 2012). Adicionalmente, podem ser analisadas as sacadas[16], definidas por linhas que conectam os círculos das fixações, demonstrando a sequência da inspeção visual (Barreto, 2012; Gordieiev *et al.*, 2021). Já as regressões[17] podem indicar a reavaliação da informação ou o maior esforço durante o processamento do estímulo (Barreto, 2012).

Os dados obtidos podem ainda ser representados através de *heat maps* (ou mapas de calor), que sintetizam graficamente a distribuição da atenção mediante uma escala cromática (Barreto, 2012; Boardman & Mccormick, 2022; Guedes, 2016; Hollingworth & Bahle, 2019; Wong *et al.*, 2014). Geralmente, as áreas representadas a vermelho

[12] Estado imóvel dos olhos em determinado ponto, assimilando ou descodificando a informação (Buscher *et al.*, 2009; Gordieiev *et al.*, 2021; Shokishalov & Wang, 2019).
[13] Somatória de fixações em cada AOI (Guedes, 2016; Hollingworth & Bahle, 2019).
[14] Remete para a "duração cumulativa e localização espacial média de uma série de fixações consecutivas dentro de uma área de interesse" (Barreto, 2012, p. 176), mais concretamente o tempo de fixação despendido em determinada AOI (Darwish & Bataineh, 2012).
[15] Intervalo de tempo entre o aparecimento do estímulo e a primeira fixação em determinada AOI (Buscher *et al.*, 2009; Darwish & Bataineh, 2012; Guedes, 2016).
[16] Movimentos oculares rápidos de uma fixação para outra (Buscher *et al.*, 2009; Gordieiev *et al.*, 2021).
[17] Retorno a área(s) já visualizada(s) (Barreto, 2012).

correspondem às zonas que concentraram maior número ou duração de fixações, podendo revelar as áreas que despertaram mais interesse para os indivíduos. As áreas a verde indicam as áreas com menor duração de fixações e as áreas sem cor poderão indicar regiões sem fixações registadas (Barreto, 2012; Boardman & Mccormick, 2022; Shokishalov & Wang, 2019; Wong *et al.*, 2014).

Embora ainda escassos, alguns estudos empíricos recorreram ao *eye-tracking* para analisar os padrões visuais e comportamentais na interação com *websites*. Por exemplo, Buscher *et al.* (2009) desenvolveram um estudo quantitativo experimental com 20 participantes aos quais foram atribuídas duas tarefas em mais de 300 *websites*: (i) a recolha de informações; e (ii) o reconhecimento da legitimidade. Os investigadores analisaram medidas relacionadas com o número total de fixações e a latência. Quanto à primeira tarefa, as regiões centrais dos *websites* assumiram maior relevância devido aos principais conteúdos informativos, particularmente no caso dos homens e dos mais jovens. Quanto à segunda tarefa, as regiões superiores esquerdas captaram a atenção mais precocemente devido à localização de indicadores associados à legitimidade dos *websites*, como os logótipos e o URL. Nesta tarefa, constataram que as mulheres, os participantes mais velhos e com menores competências informáticas distribuíram a sua atenção por um maior número de áreas e durante mais tempo, sugerindo um processamento visual mais cauteloso e menos automatizado.

Noutro estudo, Darwish e Bataineh (2012) analisaram os padrões visuais perante 6 *websites* (legítimos e fraudulentos). Com base numa amostra intencional de 36 participantes entre 18 e 55 anos, os autores recolheram dados relativos ao número total de fixações, à duração total das fixações e à latência. Os resultados demonstraram que a estrutura dos *websites* influenciou significativamente a atenção seletiva dos indivíduos, mesmo daqueles que identificaram pistas fraudulentas. Embora o URL estivesse associado ao reconhecimento da legitimidade dos *websites*, esta área recebeu menos atenção do que os produtos, reduzindo a probabilidade de deteção de pistas fraudulentas.

Mais recentemente, Boardman e Mccormick (2022) combinaram técnicas de *eye-tracking* com entrevistas semiestruturadas para analisar a influência das interfaces digitais nos estados emocionais e nos comportamentos de consumo *online* dos participantes. O estudo envolveu uma amostra intencional de 52 indivíduos, entre os 20 e 70 anos, que haviam realizado compras *online* nos 12 meses anteriores. Os resultados demonstraram uma concentração inicial das fixações nas imagens dos produtos, seguindo-se a visualização de elementos localizados no canto superior esquerdo, como o URL. As

entrevistas aprofundaram os dados do *eye-tracking*, revelando que a atenção era orientada pelos interesses e pelas motivações dos participantes, que valorizaram características facilitadoras de uma experiência de consumo *online* mais fácil, rápida e agradável, como as recomendações personalizadas de produtos comerciais. Estes resultados corroboram outras investigações que demonstraram que, durante os primeiros 5 segundos de observação, a atenção tende a concentrar-se nas áreas percecionadas como mais atrativas (Gordieiev *et al.*, 2021).

Em síntese, a literatura demonstra que os padrões visuais em *websites* não ocorrem de forma aleatória, mas dependem de características visuais das plataformas digitais, de interesses individuais e de processamentos cognitivos da informação. Neste sentido, as técnicas de *eye-tracking* constituem uma ferramenta adequada para compreender a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos, permitindo identificar os elementos que orientam a atenção e influenciam os processos de avaliação da legitimidade, do risco e da confiança.

Partindo da revisão da literatura apresentada, a suscetibilidade à cibervitimação por fraude ao consumidor *online* permanece uma realidade complexa ainda insuficientemente compreendida. A maioria das investigações tem recorrido a questionários e medidas de autorrelato que pouco esclarecem acerca da relação entre processos atencionais e interpretativos mobilizados durante a observação dos *websites*. Consequentemente, continua por esclarecer de que modo os consumidores distribuem a atenção pelos diferentes elementos visuais, como interpretam pistas visuais associadas à legitimidade, ao risco e à confiança e como esses processos influenciam a intenção de compra *online*. Acresce que a aplicação da Criminologia Visual ao estudo da suscetibilidade à cibervitimação continua incipiente e, no contexto português, são escassas as investigações que recorrem a metodologias mistas para uma compreensão integrada deste fenómeno. Em seguida, será apresentado o presente estudo empírico, que procura colmatar as lacunas enunciadas e, simultaneamente, contribuir para o desenvolvimento de pressupostos da Criminologia Visual aplicados ao comércio *online* e à cibervitimação.

# CAPÍTULO II – ESTUDO EMPÍRICO

Este capítulo divide-se em cinco secções: (i) o enquadramento metodológico; (ii) os objetivos, as hipóteses e as questões de investigação; (iii) a constituição da amostra e os procedimentos de recolha de dados: (iv) os instrumentos utilizados na recolha de dados; e (v) os procedimentos de análise dos mesmos.

## 1. Enquadramento Metodológico

Face à complexidade irredutível do fenómeno em análise e às lacunas científicas sobre os padrões visuais e os discursos associados ao comércio *online*, a presente investigação assume um carácter exploratório e inovador, na medida em que se procura aprofundar um tema ainda escassamente estudado, sobretudo no contexto português.

Tendo isto em consideração, delineou-se uma investigação multimetodológica (ou metodologias mistas). As metodologias mistas definem-se pela combinação de "técnicas, métodos, abordagens, conceitos ou linguagem da investigação quantitativa e qualitativa num único estudo" (Johnson & Onwuegbuzie, 2004, p. 17), articulando elementos, *insights* e procedimentos de ambas as abordagens na produção de um projeto geral (Maruna, 2010; Johnson & Onwuegbuzie, 2004; Sun & Benson, 2022; Wilkes *et al.*, 2021). Na presente investigação, complementou-se abordagens quantitativas e qualitativas, mais concretamente técnicas de *eye-tracking* e de *photo-elicitation* que constituem, a nosso ver, métodos tradicionais e inovadores da Criminologia Visual.

Pese embora a metodologia mista apresente desafios de planificação, recolha e análise dos dados, como o facto de se afigurar mais demorada, a sua principal vantagem reside na produção de conhecimentos científicos robustos (Maruna, 2010; Sun & Benson, 2022), na medida em que permite articular tendências quantitativas com interpretações qualitativas para analisar o mesmo fenómeno, favorecendo uma compreensão holística da realidade estudada (Trahan & Stewart, 2013; Wilkes *et al.*, 2021; Wincup, 2017).

Adotou-se um desenho quantitativo-qualitativo sequencial, iniciado pela recolha dados quantitativos, seguindo-se a recolha de dados qualitativos para aprofundar, contextualizar e interpretar os resultados. Assim, a recolha inicial orientou as recolhas subsequentes, permitindo que as inferências finais resultassem da integração dos dois conjuntos de evidências empíricas (Maruna, 2010; Sun & Benson, 2022; Wilkes *et al.*, 2021).

Na primeira fase do estudo, de natureza quantitativa e experimental, recorreu-se à tecnologia *eye-tracking* com o objetivo de analisar os padrões visuais dos participantes durante a observação de imagens de *websites* de comércio pré-existentes e criadas pelo investigador, complementando-se esta recolha com um questionário sociodemográfico. Esta fase decorreu em contexto laboratorial, controlando-se variáveis externas potencialmente influentes com vista a aumentar a precisão e a validade interna dos resultados obtidos (Pauwels, 2017; Semmelmann & Weigelt, 2017).

Na segunda fase foram realizadas entrevistas semiestruturadas para ultrapassar as limitações das técnicas de *eye-tracking* na compreensão do que orienta a atenção dos

sujeitos. A integração de entrevistas qualitativas justifica-se pela possibilidade de aprofundar o processamento de informações cognitivas, os sentimentos e os significados atribuídos pelos indivíduos (Boardman & Mccormick, 2022; Johnson & Onwuegbuzie, 2004; Wilkes *et al.*, 2021; Wincup, 2017; Wong *et al.*, 2014). Para esse fim, recorreu-se a técnicas de *photo-elicitation,* utilizando-se as mesmas imagens como estímulos visuais para desencadear interpretações dos participantes quanto às pistas visuais e aprofundar os resultados do *eye-tracking* (Gill, 2024; Pauwels, 2017; Wheeldon & Harris, 2015).

Deste modo, os dados qualitativos conferem significado aos dados quantitativos e expandem o conhecimento criminológico por meio de descrições e interpretações densas acerca dos padrões visuais e dos significados atribuídos aos estímulos visualizados (Boeri & Lamonica, 2015; Gill, 2020; Maruna, 2010; Wincup, 2017). Adiante, serão detalhados os procedimentos metodológicos.

## 2. Objetivos, Hipóteses e Questões de Investigação

Tendo em conta a natureza distinta das fases que compõem a investigação, definiram-se objetivos gerais e específicos para cada uma delas.

Na primeira fase, procurou-se descrever e comparar, por meio de técnicas de *eye-tracking*, os padrões visuais dos participantes perante *websites* de comércio legítimos e fraudulentos, assim como analisar a sua suscetibilidade à cibervitimação nos *websites* fraudulentos. Especificamente, pretendeu-se: (i) identificar as principais áreas de interesse visual dos participantes nos *websites* de comércio; (ii) analisar a relação entre os padrões visuais e a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos; e (iii) perceber se a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos difere consoante as características sociodemográficas dos participantes (idade, género, habilitações literárias e rendimento do agregado familiar).

Com base nas evidências empíricas sobre os padrões visuais em *websites* (e.g., Buscher *et al.*, 2009; Darwish & Bataineh, 2012), formularam-se as seguintes hipóteses para os objetivos específicos (i) e (ii):

H1: Os indivíduos dirigem mais atenção aos produtos comerciais nos *websites* legítimos do que nos *websites* fraudulentos.

H2: Os indivíduos mais suscetíveis à cibervitimação nos *websites* de comércio fraudulentos dirigem mais atenção aos produtos comerciais do que os indivíduos menos suscetíveis.

H3: Os indivíduos menos suscetíveis à cibervitimação nos *websites* de comércio fraudulentos dirigem mais atenção para o URL do que os indivíduos mais suscetíveis.

Quanto ao objetivo específico (iii), e apesar da falta de consenso científico, enunciam-se as seguintes hipóteses a testar em função dos trabalhos revistos (e.g., Reyns, 2013):

H4: Os indivíduos mais velhos são mais suscetíveis à cibervitimação nos *websites* de comércio fraudulentos do que os indivíduos mais jovens.

H5: Os homens são mais suscetíveis à cibervitimação nos *websites* de comércio fraudulentos do que as mulheres.

H6: Os indivíduos com menores níveis de escolaridade são mais suscetíveis à cibervitimação nos *websites* de comércio fraudulentos do que os indivíduos com maiores níveis de escolaridade.

H7: Os indivíduos mais satisfeitos com o rendimento do agregado familiar são mais suscetíveis à cibervitimação nos *websites* de comércio fraudulentos do que os indivíduos menos satisfeitos.

Na segunda fase do estudo, procurou-se explorar, a partir de técnicas de *photo-elicitation*, os significados atribuídos pelos participantes aos *websites* de comércio, bem como interpretar os seus discursos à luz da cultura de consumo contemporânea. A partir de investigações anteriores (e.g., Boardman & Mccormick, 2022), pretendeu-se, especificamente: (i) enquadrar as experiências de comércio *online* na atual cultura de consumo; (ii) compreender de que modo os participantes atribuem juízos de legitimidade e a confiança aos *websites* de comércio; (iii) descrever os principais riscos percebidos pelos participantes nos *websites* de comércio; e (iv) identificar as recomendações dos participantes para melhorar a confiança em *websites* de comércio legítimos.

Tendo em conta os objetivos, elaboraram-se as seguintes questões de investigação:

1) De que forma as experiências de comércio *online* dos participantes se enquadram na atual cultura de consumo?
2) De que modo os participantes atribuem legitimidade aos *websites* de comércio?
3) Como é que os participantes atribuem confiança aos *websites* de comércio?
4) Quais são os riscos identificados pelos participantes em *websites* de comércio?
5) Quais são as recomendações dos participantes para melhorar a confiança nos *websites* de comércio legítimos?

## 3. Constituição da Amostra e Procedimentos de Recolha de Dados

Previamente à recolha de dados, realizaram-se pré-testes com uma amostra de conveniência (Boeri & Lamonica, 2015) constituída por 4 estudantes da Faculdade de Direito da Universidade do Porto (FDUP) para determinar a adequação da metodologia e proceder a melhorias. Num primeiro momento, 2 estudantes deslocaram-se ao Laboratório da Escola de Criminologia da Faculdade de Direito da Universidade do Porto (LEC-FDUP) para aferir a clareza dos itens do questionário, a viabilidade do protocolo experimental e a adequação dos estímulos visuais utilizados na tarefa de *eye-tracking*. Num segundo momento, realizaram-se entrevistas-piloto com outros 2 estudantes para avaliar o guião de entrevista, testar a aplicação das técnicas de *photo-elicitation* e definir orientações para a condução das entrevistas.

O pré-teste permitiu definir o tempo de exposição de cada estímulo visual em 10 segundos, reformular algumas questões do guião de entrevista para reduzir ambiguidades e estimar a duração total da participação em 5 minutos para a tarefa de *eye-tracking* e aproximadamente 40 minutos para a participação em ambas as fases.

A recolha de dados iniciou-se após o parecer positivo da Comissão de Ética da FDUP acerca dos procedimentos da investigação. O recrutamento de participantes foi efetuado através de duas estratégias: (i) a distribuição de *flyers* com códigos QR (Anexo A) para acesso ao formulário de inscrição (Anexo B), por zonas próximas do local de recolha de dados, como a Rua de Cedofeita; e (ii) a divulgação nas redes sociais (e.g., *Instagram* e *LinkedIn*). Estas estratégias procuraram maximizar o número de participantes, garantindo uma amostra heterogénea e adequada para realizar as análises estatísticas e as entrevistas.

À semelhança de outros estudos (e.g., Boardman & Mccormick, 2022; Darwish & Bataineh, 2012), optou-se por uma amostra intencional (não probabilística) que permitiu selecionar os participantes em função de critérios de inclusão e exclusão relevantes para os objetivos da investigação (Boeri & Lamonica, 2015; Gill, 2020; Kawaf & Tagg, 2017). Como critérios de inclusão, definiram-se: (i) a idade igual ou superior a 18 anos; e (ii) a experiência na realização de uma ou mais compras de produtos em *websites* de comércio nos últimos 12 meses. Por motivos técnicos associados à tecnologia *eye-tracking*, excluíram-se indivíduos submetidos a intervenções cirúrgicas oculares e portadores de óculos com lentes bifocais (Barreto, 2012).

Após a inscrição, os participantes deslocaram-se ao LEC-FDUP, onde lhes foi disponibilizado o Termo de Consentimento Informado (Anexo C) e prestados esclarecimentos sobre os objetivos da investigação, as atividades a realizar e os princípios

éticos aprovados: (i) a confidencialidade, assegurando-se o armazenamento seguro dos dados; (ii) o anonimato, atribuindo um código alfanumérico a cada participante (a letra "P" e a ordem de participação) para proteger a sua identidade; (iii) a voluntariedade da participação; e (iv) a possibilidade de desistência a qualquer momento.

De acordo com o protocolo de recolha de dados (Anexo D), os participantes responderam aos itens do questionário sociodemográfico auto-reportado (em papel). De seguida, já sentados numa cadeira em frente a um computador, receberam instruções relativas à tarefa experimental, sendo-lhes solicitado que observassem um conjunto de 8 imagens de *websites* de comércio. Após cada uma, surgia uma questão sobre a intenção de compra, devendo olhar para o monitor para marcar a resposta "sim" ou "não".

Após o esclarecimento de dúvidas, iniciou-se o processo de calibração individual do equipamento *Tobii Pro*, com duração de 10 segundos. Considerando que o olho humano apresenta variações individuais naturais na sua forma e geometria, procurou-se ajustar os parâmetros de registo às características fisiológicas dos movimentos oculares de cada participante através da fixação sucessiva de pontos apresentados no ecrã (Akshay *et al.*, 2020; Barreto, 2012; Guedes, 2016; Tobii Pro, 2021). Após a validação da calibração, iniciou-se a recolha dos dados de *eye-tracking*. Os participantes foram distribuídos, aleatoriamente, por dois grupos experimentais (G1 e G2) pela ordem de participação, o que significa que o primeiro participante observou as imagens do G1, o segundo as imagens do G2, o terceiro as imagens do G1 e assim por diante.

Concluída esta tarefa, os 12 primeiros participantes foram encaminhados para outra sala, onde realizaram as entrevistas. No final das entrevistas, empregou-se a estratégia de *snowball* (ou bola de neve), solicitando-se a recomendação de outros indivíduos para aumentar a amostra (Gill, 2020). A recolha qualitativa foi interrompida ao alcançar a saturação empírica[18], após a qual se prosseguiu com a recolha quantitativa. No final, obteve-se uma amostra de 66 participantes (N=66), considerada adequada para a realização das análises estatísticas previstas e consistente com estudos anteriores.

## 4. Instrumentos e Operacionalização

Nesta secção descrevem-se o questionário sociodemográfico, o equipamento *eye tracker* e o guião de entrevista semiestruturada, explicitando-se a sua finalidade e aplicação no contexto da investigação.

[18] Ocorre quando novas entrevistas deixam de acrescentar informações substancialmente distintas às já obtidas (Boeri & Lamonica, 2015; Kawaf & Tagg, 2017).

## 4.1 Questionário Sociodemográfico

Para operacionalizar as variáveis sociodemográficas, aplicou-se um curto questionário, baseado nas investigações científicas consultadas, que permitiu caracterizar a amostra da investigação, nomeadamente a "idade", o "género", as "habilitações literárias" e o "rendimento do agregado familiar".

Similarmente a estudos revistos, a idade (variável contínua) foi medida em número de anos em função do momento em que os participantes responderam ao questionário (e.g., Fonseca *et al.*, 2022; Holtfreter *et al.*, 2008; Pratt *et al.*, 2010). Quanto ao género, esta variável foi codificada de forma dicotómica (0 = feminino; 1 = masculino), em consonância com a operacionalização adotada em estudos científicos (e.g., Holtfreter *et al.*, 2008; Pratt *et al.*, 2010; Reyns, 2013). No que concerne às habilitações literárias, considerou-se o último nível completado no momento da resposta consoante seis opções adaptadas de outros estudos (e.g., Whitty, 2020): (1) "Ensino Básico"; (2) "Ensino Secundário"; (3) "Licenciatura"; (4) "Pós-graduação"; (5) "Mestrado"; e (6) "Doutoramento". Esta variável foi recodificada como *dummy* com base na mediana "2", dicotomizando-se os itens em "Até ao Ensino Secundário" (0 = Ensino Básico e Ensino Secundário) e "Ensino Superior" (1 = Licenciatura e restantes). A situação profissional foi determinada através de seis opções: (1) "Estudante"; (2) "Trabalhador-estudante"; (3) "Empregado(a) por conta própria"; (4) "Empregado(a) por conta de outrem"; (5) "Desempregado(a)"; e (6) "Outro". Por fim, com base no *European Social Survey* (2010), questionou-se "*Qual das seguintes descrições se aproxima mais ao que sente relativamente ao rendimento atual do seu agregado familiar?*" para averiguar o grau de satisfação quanto ao rendimento do agregado familiar, variando as respostas entre (1) "É muito difícil viver com o rendimento atual", (2) "É difícil viver com o rendimento atual", (3) "O rendimento atual dá para viver" e (4) "O rendimento atual permite viver confortavelmente". Também esta variável foi recodificada como *dummy*, considerando-se "menor satisfação" (0 = muito difícil e difícil viver com o rendimento atual) e maior satisfação (1 = o rendimento atual dá para viver e permite viver confortavelmente).

## 4.2 *Eye Tracker*

Os estímulos visuais (*websites* legítimos e fraudulentos) foram apresentados através do monitor e do computador presentes no LEC-FDUP. Os movimentos oculares dos

participantes foram registados pelo *Eye Tracker Tobii Pro Fusion*[19], equipamento que permite captar, com uma boa precisão, diferentes dimensões da atenção, como as fixações dirigidas aos elementos visuais dos *websites* (Barreto, 2012; Gordieiev *et al.*, 2021; Tobii Pro, 2021). Este equipamento é composto por duas câmaras e dois modos de rastrear a pupila numa velocidade de até 250 Hz, permitindo configurar a recolha de dados a diferentes indivíduos e contextos de investigação (Akshay *et al.*, 2020; Tobii Pro, 2021). Foi, ainda, utilizado o *software Tobii Pro Lab* para controlar a recolha e exportar os dados para outros *softwares* de análise estatística, como o *Excel* e o *SPSS*.

O *Eye Tracker* caracteriza-se por ser um equipamento não invasivo que permite que os participantes tenham reações espontâneas, reduzindo enviesamentos e aumentando a validade interna. Acresce que as técnicas de *eye-tracking* não exigem um treino intensivo, possibilitando a realização de estudos sobre o comportamento visual em *websites* de forma rápida e económica (Barreto, 2012; Semmelmann & Weigelt, 2017). Entre as suas vantagens, destaca-se a capacidade de recolher informação objetiva sobre os elementos visuais que orientam a atenção das pessoas, depreendendo-se a relação entre o processamento de informações e as pistas visuais (Barreto, 2012; Darwish & Bataineh, 2012; Guedes, 2016; Semmelmann & Weigelt, 2017). A utilização desta tecnologia assenta na hipótese "*strong eye-mind*", segundo a qual a visualização de estímulos tende a ser acompanhada por um processo cognitivo (Barreto, 2012). Aliás, os estudos comprovam que os estímulos visuais são processados a partir de informações ou detalhes (Barreto, 2012; Buscher *et al.*, 2009; Wong *et al.*, 2014). Como Barreto (2012) indica, as fixações não esclarecem as associações cognitivas concretas, pelo que se optou por integrar protocolos verbais. Sempre que pertinente, os mapas de calor foram apresentados durante as entrevistas para estimular a reflexão dos participantes sobre a atenção seletiva dirigida a determinadas AOI, como será explicado na secção do guião de entrevista.

### 4.2.1 Estímulos Visuais Utilizados e Protocolo Experimental

Nas investigações experimentais, a seleção criteriosa de estímulos visuais é fundamental para assegurar a validade e a fiabilidade dos resultados obtidos (Boardman & Mccormick, 2022; Darwish & Bataineh, 2012; Guedes, 2016). Neste sentido, procedeu-se a uma análise prévia de *websites* de *comércio* para selecionar um conjunto de estímulos adequado aos objetivos da investigação.

[19] Este dispositivo utiliza iluminadores infravermelhos para gerar padrões de reflexão nas córneas dos olhos do participante. Este processo decorre de algoritmos complexos de processamento de imagem que permitem definir a posição 3D dos olhos relativamente ao seu ponto de fixação (Tobii Pro, 2021).

Optou-se por utilizar imagens de *websites* de *marketplaces* e similares, tais como a *Amazon* e o *eBay*, por serem os mais adulterados (Cross *et al.*, 2022; Kelley *et al.*, 2023; Pinjarkar *et al.*, 2024; Whittaker *et al.*, 2023). Atendendo à complexidade estrutural dos *websites* e à diversidade dos seus elementos visuais, como os produtos e as categorias comerciais (Boardman & Mccormick, 2022; Buscher *et al.*, 2009), definiram-se quatro critérios de seleção. Em primeiro, a uniformidade do *design*, assegurando a localização equivalente dos principais elementos visuais[20], reduzindo a variabilidade dos estímulos visualizados. Em segundo, a diversidade de categorias de produtos, incluindo vestuário e equipamentos eletrónicos. Em terceiro, a adequação dos conteúdos a diferentes perfis de consumidores, abrangendo diferentes géneros e faixas etárias. Por último, a apresentação de preços compatíveis com os habitualmente praticados no comércio *online*.

Após a averiguação destes critérios, selecionaram-se 8 *websites* legítimos, realizando-se uma captura de ecrã com dimensões semelhantes para controlar possíveis efeitos do tamanho na atenção seletiva. Cada imagem foi duplicada e editada pelo investigador, introduzindo-se alterações inspiradas nas estratégias fraudulentas descritas na literatura e em exemplos de *websites phishing*[21] disponibilizados pela APAV. Emparelharam-se 16 estímulos, correspondentes a 8 *websites* legítimos (L1-L8) e a 8 *websites* fraudulentos (F1-F8), distribuídos aleatoriamente por dois grupos experimentais, designados G1 (Anexo E) e G2 (Anexo F), que incluem 4 *websites* legítimos e 4 *websites* fraudulentos. A ordem dos estímulos foi aleatorizada para cada participante do mesmo grupo, reduzindo ameaças à validade interna (Kelley & Bertenthal, 2016).

Com base na literatura (e.g., Buscher *et al.*, 2009; Darwish & Bataineh, 2012), definiram-se sete AOI (Tabela 1). As quatro AOI comuns corresponderam: (i) à Área do Utilizador, que inclui os ícones da conta, carrinho de compras e favoritos; (ii) aos Produtos Comerciais, abrangendo as imagens, as descrições, os preços e as avaliações; (iii) à Marca, relacionada com o logótipo; e (iv) ao URL, que integra o nome de domínio, o cadeado de segurança e o protocolo HTTPS. Sempre que presentes, analisaram-se três AOI complementares: (v) a Pesquisa, que inclui a barra de pesquisa, as categorias comerciais e os filtros de navegação; (vi) a Informação Comercial relativa ao envio, aos descontos, à devolução e aos *downloads*; e (vii) as Pistas Fraudulentas, como os erros ortográficos ou gramaticais. Por exemplo, os estímulos F5 e F8 apresentam as mesmas AOI, mas apenas o F5 integra as AOI Informação Comercial e a Pesquisa.

[20] Por exemplo, os logótipos das empresas comerciais no canto superior esquerdo.
[21] Estes *websites* não foram utilizados por não cumprirem os critérios de seleção.

Tabela 1 – Caracterização dos Estímulos

| Grupo | *Website* | Código | Principais Áreas de Interesse (AOI) | | | | Outras AOI | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Área do Utilizador | Produtos Comerciais | Marca | URL | Informação Comercial | Pesquisa | Pistas Fraudulentas |
| 1 | *Joom* | L1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *Wish* | F2 | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | *Shein* | L3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *Temu* | L4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *AliExpress* | F5 | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | *Amazon* | F6 | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| | *eBay* | F7 | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| | OLX | L8 | ✓ | ✓ | ✓ | ✓ | - | - | - |
| 2 | *Joom* | F1 | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| | *Wish* | L2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *Shein* | F3 | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| | *Temu* | F4 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| | *AliExpress* | L5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *Amazon* | L6 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | *eBay* | L7 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| | OLX | F8 | ✓ | ✗ | ✓ | ✗ | - | - | ✗ |

Nota: ✗ = Manipulação; ✓ = Original; - = Ausência de AOI

O protocolo experimental do *eye-tracking* foi adaptado de estudos prévios (e.g., Guedes, 2016; Shokishalov & Wang, 2019), estruturando-se em três fases sucessivas até ao fim da experiência (Figura 1). Primeiro, surgiu um ponto de fixação (5 segundos) para centrar a atenção das participantes no monitor e minimizar distrações. Seguidamente, apresentou-se o estímulo visual (10 segundos) e a questão "*Estaria disposto/a a realizar compras neste website?*" (5 segundos), cujo propósito será explicado na próxima secção.

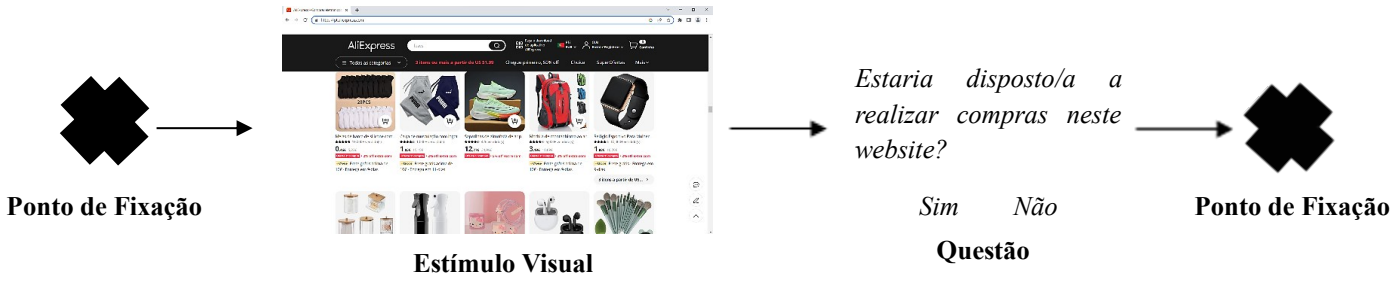



Figura 1 – Esquema do Protocolo Experimental

### 4.2.2 Variáveis Dependentes e Independentes

Considerando os objetivos e as hipóteses formuladas para a fase quantitativa, procede-se à identificação das variáveis e à respetiva operacionalização.

A variável independente[22] correspondeu ao tipo de *website* apresentado aos participantes, operacionalizado em duas condições experimentais: (i) *websites* legítimos; e (ii) *websites* fraudulentos. Os *websites* legítimos correspondiam a interfaces digitais autênticas, tendo sido efetuados ajustamentos para simplificar a apresentação visual e eliminar informações pessoais do investigador. Por sua vez, os *websites* fraudulentos resultaram da manipulação[23] dos elementos visuais dos *websites* legítimos (Anexo G).

Para analisar a associação entre as características dos participantes e as restantes variáveis em estudo, as características sociodemográficas foram consideradas variáveis independentes individuais. A sua operacionalização foi efetuada através do questionário sociodemográfico aplicado previamente à experiência e já explicado na secção anterior.

As variáveis dependentes[24] foram a atenção seletiva e a suscetibilidade à cibervitimação nos *websites* fraudulentos. A atenção seletiva foi operacionalizada através da duração total das fixações em milissegundos (ms) em cada AOI do *website*, considerada a principal métrica do estudo por refletir a quantidade de atenção e o processamento cognitivo dedicados aos diferentes elementos visuais (Barreto, 2012; Gordieiev *et al.*, 2021). Como métricas complementares, analisaram-se o número total de fixações em cada AOI do *website* e a latência (ms). A suscetibilidade foi operacionalizada através da intenção de compra nos *websites* fraudulentos e as respostas afirmativas ("sim") constituíram indicadores de suscetibilidade. Com base neste critério, os participantes foram classificados como "não suscetíveis" (0), quando não manifestaram intenção de compra nos quatro *websites* fraudulentos, ou "suscetíveis" (1), quando responderam afirmativamente a pelo menos um *website* fraudulento.

As métricas do *eye-tracking* foram obtidas através do *software Tobii Pro Lab*, sendo complementadas pela análise dos mapas de calor. A duração total das fixações correspondeu ao tempo médio durante o qual o olhar permaneceu sobre cada AOI. O número total de fixações correspondeu à soma das vezes que cada participante direcionou o olhar para determinada AOI. À semelhança de estudos prévios, a primeira fixação foi excluída por se considerar a primeira aceitação e processamento do estímulo, entendendo-

[22] Variáveis que resultam da manipulação do investigador (Buscher *et al.*, 2009; Guedes, 2016).
[23] Para realizar as manipulações, recorreu-se a técnicas de edição de imagens (*Paint*).
[24] Os resultados diretamente medidos das técnicas de *eye-tracking* (Gordieiev *et al.*, 2021; Guedes, 2016).

se como primeira fixação aquela que ocorre após a sacada inicial (Buscher *et al.*, 2009; Guedes, 2016). A latência correspondeu ao tempo médio decorrido entre a apresentação do estímulo e a primeira fixação numa AOI específica, permitindo identificar os elementos que captam mais rapidamente a atenção (Barreto, 2012; Guedes, 2016).

### 4.3 Guião de Entrevista Semiestruturada

Para responder às questões de investigação da fase qualitativa, realizaram-se entrevistas semiestruturadas devido à flexibilidade e à capacidade de aprofundar as experiências, as perceções e os significados atribuídos pelos participantes ao fenómeno em estudo (Sun & Benson, 2022; Zahari *et al.*, 2019). Este tipo de entrevista assenta num conjunto de tópicos e questões abertas previamente definidas, permitindo explorar temas emergentes e aspetos considerados relevantes durante a interação com os participantes (Roulston, 2013; Sun & Benson, 2022).

O guião de entrevista foi elaborado com base nas questões de investigação e na revisão da literatura, organizando-se em quatro dimensões: (i) *Experiências Prévias nos Websites de Comércio*; (ii) *Perceções e Significados atribuídos aos Websites Visualizados*; (iii) *Riscos Percebidos e Cibervitimação*; e (iv) *Recomendações*. Atendendo ao carácter semiestruturado das entrevistas, serão apresentadas apenas as questões consideradas mais representativas de cada dimensão, remetendo-se o guião completo para o Anexo H.

Antes do início da entrevista, os participantes foram novamente informados sobre os procedimentos éticos em curso. Após o consentimento para a gravação áudio, iniciou-se a entrevista com uma questão de abertura (*icebreaker*) – "*Como é que se sentiu na realização das tarefas de eye-tracking?*" – inspirada no estudo de Boardman e Mccormick (2022). Esta questão teve como objetivo estabelecer a proximidade com o entrevistado e promover um ambiente propício à partilha de experiências, perceções e significados ao longo da entrevista (Boardman & Mccormick, 2022; Sun & Benson, 2022).

A primeira dimensão – *Experiências Prévias nos Websites de Comércio* – decorre da primeira questão de investigação e inclui as subdimensões *Diferenças Online-Offline*, *Experiências e Familiaridade,* e *Cultura de Consumo Online*. Esta formulação fundamenta-se na evidência de que as vantagens percebidas do comércio *online*, as experiências prévias e as influências sociais moldam os comportamentos de consumo e a forma como os indivíduos interpretam os *websites* (Cross *et al.*, 2022; Izogo & Jayawardhena, 2018; Kawaf & Tagg, 2017; Reyns, 2013). Para esse efeito, colocaram-se questões como: "*Na sua opinião, o que difere o comércio online do comércio em lojas*

*físicas?*" e "*Recordando os últimos meses, como descreve as suas experiências no comércio online?*". Estas questões foram complementadas por perguntas *follow-up*[25] relativas aos hábitos de consumo *online*, à familiaridade e às influências sociais.

De seguida, recorreu-se à técnica de *photo-elicitation*, apresentando-se aos participantes, aleatoriamente, duas imagens de *websites* visualizados na tarefa de *eye-tracking* (1 legítimo e 1 fraudulento). A aplicação desta técnica fundamentou-se na Criminologia Visual, que sustenta que as imagens funcionam como estímulos visuais capazes de desencadear emoções, memórias e perceções dificilmente acessíveis através do discurso verbal isolado (Gill, 2024; Pauwels, 2017; Wheeldon & Harris, 2015).

A segunda dimensão – *Perceções e Significados atribuídos aos Websites Visualizados* – procurou responder à segunda e à terceira questões de investigação, englobando as subdimensões *Segurança*, *Legitimidade* e *Confiança*. A literatura demonstra que os juízos são construídos a partir da perceção e da interpretação de pistas visuais, como o *design*, os indicadores de segurança digital e os logótipos (Bitaab *et al.*, 2023; Boardman & Mccormick, 2022; Darwish & Bataineh, 2012; Kelley & Bertenthal, 2016). Deste modo, as questões centrais incidiram sobre os processos de atribuição de segurança, legitimidade e confiança aos *websites*: "*Ao observar as imagens, quais foram os elementos visuais que associou aos websites seguros?*" e "*O que o/a levou a confiar nos websites?*". Estas questões foram aprofundadas por perguntas *follow-up* relacionadas com a divulgação de dados bancários em *websites* e as razões que justificaram a atenção dirigida a determinadas áreas das plataformas digitais.

A terceira dimensão – *Riscos Percebidos e Cibervitimação* – relaciona-se com a quarta questão de investigação e incluiu as subdimensões *Tipos de Riscos*, *Experiências de Cibervitimação* e *Literacia Digital*. As investigações prévias demonstram que os riscos percebidos influenciam a confiança e a intenção de compra, principalmente entre indivíduos que experienciaram situações de engano (Cross *et al.*, 2022; Edwards *et al.*, 2025; Jahankhani, 2009; Reyns, 2013). Assim, procurou-se descrever os riscos associados pelos participantes às compras nos *websites* através da seguinte questão: "*Quais são os riscos que associa às compras nos websites?*". Esta questão foi aprofundada por perguntas *follow-up* relativas às eventuais experiências de cibervitimação no comércio *online* e aos comportamentos de autoproteção *online*.

[25] Estas questões permitiram aprofundar informações consideradas pertinentes.

A quarta e última dimensão – *Recomendações* – está associada à quinta questão de investigação e integrou as subdimensões *Mudanças nos Websites* e *Conselhos Interpessoais*. Com esta dimensão procurou-se identificar as sugestões dos participantes para melhorar a sua confiança nos *websites* legítimos.

Por fim, a entrevista terminou com uma questão prospetiva – "*No futuro, o que poderá influenciar as suas compras nos websites de comércio?"* – permitindo a reflexão global sobre os temas abordados e a exposição de aspetos adicionais. Importa realçar que, mantendo-se a estrutura geral do guião, algumas questões *follow-up* foram adaptadas durante a recolha de dados para aprofundar temas que emergiram dos discursos dos participantes, como a ética das empresas comerciais, a denúncia da cibervitimação às autoridades e o impacto da IA na evolução das fraudes no comércio *online*.

## 5. Procedimentos de Análise de Dados

Nesta secção descrevem-se, primeiramente, os procedimentos da análise quantitativa e, posteriormente, as etapas da análise qualitativa.

### 5.1 Análises Estatísticas

A análise dos dados estatísticos desenvolveu-se em três etapas: (i) a análise indutiva dos mapas de calor; (ii) a análise estatística descritiva; e (iii) análise estatística inferencial.

Na primeira etapa, os mapas de calor gerados pelo *software Pro Lab* foram extraídos e analisados através da observação e da descrição da distribuição da atenção seletiva pelas AOI dos *websites*. Posteriormente, os dados do *eye-tracking* foram exportados para uma base de dados em ficheiro CVS (*Excel*), realizando-se um *data screening* para identificar possíveis erros. Posteriormente, esses dados foram importados para uma base de dados SPSS e analisados através do *software IBM SPSS Statistic 30*. Repetiu-se este procedimento para os dados do questionário, criando-se, assim, duas bases de dados SPSS para possibilitar a análise estatística das diferentes variáveis. Foi, ainda, criada uma base de dados única para realizar testes estatísticos entre os dados de ambas as bases.

Seguiram-se procedimentos de análise estatística descritiva com recurso a medidas de tendência central e medidas de dispersão. Quanto às variáveis quantitativas (e.g., idade), a média (M) foi utilizada como medida de tendência central e o desvio-padrão (*Std. Deviation* [SD]) como medida de dispersão. Nas variáveis categóricas (e.g., género), recorreu-se a outras medidas, como a moda, para a averiguar as frequências absolutas e relativas. Considerando o número da amostra, a normalidade dos dados foi analisada com

o teste *Kolmogorov-Smirnov* (n>30). Tendo-se verificado que os dados não seguiam uma distribuição normal (p<.001), recorreu-se a testes não paramétricos.

Para testar a hipótese 1, realizou-se o teste de *Friedman* para comparar as distribuições das medidas da atenção seletiva (duração total das fixações, número total de fixações e latência) entre as AOI observadas pelos mesmos participantes. Sempre que se verificaram diferenças estatisticamente significativas, recorreu-se a testes pós-hoc de *Wilcoxon*, de forma a identificar especificamente quais as AOI que diferiam entre si.

As hipóteses 2, 3 e 4 foram testadas através do teste U de *Mann-Whitney*, comparando os participantes classificados como não suscetíveis e suscetíveis à cibervitimação relativamente às métricas da atenção seletiva e à idade.

As hipóteses 5, 6 e 7 foram testadas com recurso ao teste Qui-Quadrado, analisando-se a associação entre a suscetibilidade à cibervitimação e as variáveis sociodemográficas categóricas. A força da associação foi estimada através do coeficiente φ (*phi*), por se tratar de tabelas de contingência 2x2, sendo ainda calculado o *odds ratio* (OR) e o respetivo intervalo de confiança a 95% para associações estatisticamente significativas.

Em todas as análises foi considerado o nível de significância de $\alpha = .05$, utilizando-se o valor do *p-value* ($p \leq .05$) para resultados estatisticamente significativos.

### 5.2 Análise Temática do Discurso

Os dados qualitativos foram submetidos a uma Análise Temática do Discurso. A articulação dos princípios da Análise Temática com os pressupostos da Análise Crítica do Discurso (ACD) permite identificar os padrões temáticos nos dados e compreender as estratégias discursivas através das quais os participantes constroem e mobilizam significados (Petintseva, 2022; Trahan & Stewart, 2013; Willig, 2013).

Por um lado, a Análise Temática constitui uma abordagem amplamente utilizada na investigação qualitativa, assumindo particular relevância em áreas ainda pouco estudadas, como no presente estudo. Segundo Braun e Clarke (2006), esta metodologia permite "identificar, analisar e divulgar padrões (temas) nos dados" (p. 79), caracterizando-se pela possibilidade de integrar processos de análise dedutivos e indutivos (Braun & Clarke, 2006; Trahan & Stewart, 2013).

Por outro lado, a ACD parte do pressuposto de que a linguagem constitui uma prática social através da qual os indivíduos constroem e atribuem significados às suas experiências sociais (Petintseva, 2022; Willig, 2013). A sua integração nesta investigação justifica-se pelo facto de que as perceções acerca do comércio *online* refletem discursos

socioculturais que orientam a interpretação dos *websites* e, consequentemente, os comportamentos de consumo. Estas interpretações não devem ser entendidas como meramente subjetivas, mas como construções discursivas ancoradas em contextos históricos e socioculturais (Petintseva, 2022; van Dijk, 2009; Willig, 2013). Deste modo, a ACD permite articular as estratégias discursivas mobilizadas pelos participantes ao nível micro com os macrodiscursos que estruturam as práticas de consumo *online* e influenciam a interpretação dos estímulos visuais (Petintseva, 2022; van Dijk, 2009).

As etapas de análise destas abordagens são congruentes e complementares, possibilitando procedimentos mais rigorosos, claros e transparentes (Petintseva, 2022). Assim, a presente investigação assumiu uma orientação essencialista, ao descrever os significados atribuídos pelos participantes, e construcionista, ao interpretar esses significados como produtos de discursos que operam na sociedade (Braun & Clarke, 2006; Willig, 2013).

Antes da análise dos dados propriamente dita, todas as entrevistas foram transcritas manualmente, registando-se os elementos discursivos e paralinguísticos considerados relevantes para a interpretação dos dados, como pausas e risos (Kowal & O´Connell, 2013; Petintseva, 2022; Trahan & Stewart, 2013; van Dijk, 2009; Willig, 2013).

Após a transcrição, a análise foi realizada em sete etapas. A primeira consistiu na familiarização com os dados recolhidos através de leituras minuciosas das transcrições e da elaboração de resumos de cada entrevista, permitindo identificar padrões e significados preliminares (Braun & Clarke, 2006; Petintseva, 2022; Roulston, 2013). Na segunda, procedeu-se à codificação manual e sistemática dos dados, atribuindo códigos (e.g., "*facilidade de compra*") aos segmentos discursivos relevantes para os objetivos de investigação (Maruna, 2010). Embora a codificação tenha seguido uma lógica indutiva a partir dos dados recolhidos (*data-driven*), outros códigos surgiram da revisão da literatura científica. Os excertos considerados mais representativos foram selecionados para ilustrar as categorias analíticas e sustentar a interpretação dos resultados (Roulston, 2013).

Na terceira etapa, os códigos foram agrupados em categorias temáticas abrangentes, permitindo a construção de temas e subtemas (Braun & Clarke, 2006). Para facilitar a organização e a interpretação dos dados, recorreu-se a representações visuais, como tabelas e esquemas (Trahan & Stewart, 2013; Wheeldon & Harris, 2015). Na quarta e quinta etapas, os temas foram revistos e refinados para avaliar a sua coerência e adequação a todo o conjunto de dados. Este processo culminou num "mapa temático" que sintetizou a estrutura conceptual da análise (Braun & Clarke, 2006).

A sexta etapa correspondeu à interpretação dos temas à luz da ACD, identificando-se as estratégias discursivas utilizadas pelos participantes na atribuição de significados aos estímulos visuais. A análise incidiu sobre as estratégias de (des)legitimação[26] e de normalização[27] por serem amplamente discutidas na literatura enquanto mecanismos de construção da realidade social (Fairclough, 1992; van Leeuwen, 2008) Para a análise das estratégias de legitimação recorreu-se ao modelo de van Leeuwen (2008), mais concretamente as categorias de autorização[28], avaliação moral[29] e a racionalização[30] por terem surgido de forma mais consistente nos discursos dos participantes. Posteriormente, estas estratégias discursivas (nível micro) foram articuladas com os processos interpretativos dos participantes (nível meso) e com os discursos socioculturais (nível macro) que enquadram o comércio *online* (Petintseva, 2022; van Dijk, 2009; Willig, 2013). Na sétima etapa, os resultados foram organizados em função das questões de investigação e articulados com a literatura científica (Braun & Clarke, 2006).

Finalizada a descrição metodológica, apresentam-se a seguir os resultados empíricos.

## CAPÍTULO III – RESULTADOS EMPÍRICOS

Este capítulo apresenta os resultados empíricos em duas partes. A primeira expõe os resultados quantitativos relativos às métricas do *eye-tracking*, à suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos e aos mapas de calor. A segunda apresenta os resultados qualitativos, analisando-se as estratégias discursivas mobilizadas pelos participantes na atribuição de significados aos *websites* e ao comércio *online*.

### PARTE I: RESULTADOS QUANTITATIVOS

A apresentação dos resultados quantitativos organiza-se em eixos descritivos (caracterização sociodemográfica da amostra e intenção de compra nos *websites*) e inferenciais (atenção seletiva às AOI dos *websites*, relação entre atenção seletiva e suscetibilidade, e associação entre variáveis sociodemográficas e suscetibilidade).

---

[26] Processo através do qual práticas são percebidas como (i)legítimas, (in)apropriadas ou (in)aceitáveis socialmente (Petintseva, 2022; van Leeuwen, 2008).

[27] Processo através do qual as práticas socais são entendidas como habituais, naturais e socialmente expectáveis, contribuindo para o consenso (Fairclough, 1992; van Dijk, 2009; van Leeuwen, 2008).

[28] Legitimação através da referência a uma autoridade reconhecida, que pode assumir a forma de autoridade pessoal (e.g., especialistas), impessoal (e.g., normas ou leis), tradicional (e.g., costumes) ou de conformidade, baseada no comportamento ou opinião da maioria (van Leeuwen, 2008).

[29] Legitimação ocorre por referência a sistemas de valores morais, éticos, religiosos, culturais ou ideológicos, classificando práticas ou comportamentos como corretos ou incorretos (van Leeuwen, 2008).

[30] Legitimação de uma prática social através de argumentos lógicos, utilitários ou instrumentais, justificando-a pelos seus objetivos, benefícios, funções ou consequências (van Leeuwen, 2008).

## 1. Caracterização Sociodemográfica da Amostra

A tabela 2 apresenta a descrição estatística das características sociodemográficas. Relativamente à idade, os participantes apresentaram uma média de 24.98 anos e desvio padrão de 11.01, com idade mínima de 18 anos e máxima de 70 anos. Quanto ao género, houve maior prevalência do feminino (71.2%) face ao masculino (28.8%). Em relação às habilitações literárias, a maioria dos participantes concluiu o Ensino Secundário (65.2%) e a Licenciatura (24.2%), seguindo-se o Ensino Básico (6.1%) e o Mestrado (4.5%). No que respeita à situação profissional, participaram estudantes (65.2%), trabalhadores-estudantes (16.7%), empregados por conta de outrem (12.1%) e empregados por conta própria (6.1%). Quanto ao rendimento do agregado familiar, a maioria dos participantes (59.1%) reportou que o mesmo permite viver confortavelmente comparativamente a uma minoria (7.6%) que reportou que é difícil viver.

Tabela 2 – Caracterização Sociodemográfica da Amostra (N=66)

| | N | % | M±SD | Min-Max |
|---|---|---|---|---|
| Género | | | | |
| Feminino | 47 | 71.2 | | |
| Masculino | 19 | 28.8 | | |
| Idade | | | 24.98±11.01 | 18-70 |
| ≤ 25 | 56 | 84.9 | | |
| 26-45 | 3 | 4.5 | | |
| 46-65 | 6 | 9 | | |
| ≥ 66 | 1 | 1.5 | | |
| Habilitações Literárias | | | | |
| Ensino Básico | 4 | 6.1 | | |
| Ensino Secundário | 43 | 65.2 | | |
| Licenciatura | 16 | 24.2 | | |
| Pós-Graduação | 0 | 0 | | |
| Mestrado | 3 | 4.5 | | |
| Doutoramento | 0 | 0 | | |
| Situação Profissional | | | | |
| Estudante | 43 | 65.2 | | |
| Trabalhador-Estudante | 11 | 16.7 | | |
| Empregado por conta própria | 4 | 6.1 | | |
| Empregado por conta de outrem | 8 | 12.1 | | |
| Rendimento Agregado Familiar | | | | |
| Muito difícil viver | 0 | 0 | | |
| É difícil viver | 5 | 7.6 | | |
| Dá para viver | 22 | 33.3 | | |
| Permite viver confortavelmente | 39 | 59.1 | | |

Nota: N = Número de Participantes; M = Média; SD = *Std. Deviation*; Min.-Máx. = Mínimo e Máximo

## 2. Intenção de Compra nos *Websites* de Comércio

A tabela 3 apresenta o número e a percentagem de participantes que manifestaram intenção de compra em cada *website*. De forma geral, verificou-se uma maior intenção de compra nos *websites* legítimos (56%) do que nos *websites* fraudulentos (32%). Entre os *websites* legítimos, o L6 registou maior intenção de compra (73%), seguindo-se o L3, o L4 e o L8 (67% em todos), enquanto o L1 (45%) e o L2 (21%) apresentaram menores valores. Relativamente aos *websites* fraudulentos, a maior intenção de compra – que, na presente dissertação, corresponde a uma maior suscetibilidade à cibervitimação – verificou-se no F8 (64%) e F3 (48%), ao passo que o F2 (15%) e F1 (12%) registaram menores percentagens.

Tabela 3 – Intenção de Compra nos *Websites*

| Fraudulentos | | | Legítimos | | |
|---|---|---|---|---|---|
| *Website* | N | % | *Website* | N | % |
| F1 | 4 | 12 | L1 | 15 | 45 |
| F2 | 5 | 15 | L2 | 7 | 21 |
| F3 | 16 | 48 | L3 | 22 | 67 |
| F4 | 8 | 24 | L4 | 22 | 67 |
| F5 | 14 | 42 | L5 | 16 | 48 |
| F6 | 13 | 39 | L6 | 24 | 73 |
| F7 | 5 | 15 | L7 | 19 | 58 |
| F8 | 21 | 64 | L8 | 22 | 67 |
| Média (%) | | 32 | | | 56 |

Nota: N = Número de Participantes; % = Percentagem de Participantes

## 3. Atenção Seletiva às AOI dos *Websites* de Comércio

Para comparar a atenção dirigida às AOI, independentemente da legitimidade dos *websites*, recorreu-se ao teste *Friedman*, cujos resultados são apresentados na tabela 4.

Tabela 4 – Comparação da duração média das fixações, número total médio de fixações e latência nas AOI dos *Websites* (*Teste Friedman*)

| | Duração média das Fixações (ms) | | Número total médio das Fixações | | Latência (ms) | |
|---|---|---|---|---|---|---|
| | M ± SD | MR | M ± SD | MR | M ± SD | MR |
| AOI | | | | | | |
| Área do Utilizador | .22 ± .20 | 2.61 | 1.00 ± .84 | 2.56 | 5.30 ± 1.43 | 6.11 |
| Produtos Comerciais | 3.80 ± 1.56 | 6.83 | 18.05 ± 6.85 | 6.86 | 1.08 ± 0.73 | 1.69 |
| Marca | .39 ± .25 | 3.63 | 1.52 ± .88 | 3.50 | 2.19 ± 1.29 | 3.33 |
| URL | .52 ± .80 | 3.21 | 1.69 ± 2.28 | 3.02 | 3.00 ± 2.07 | 3.98 |
| Informação Comercial | .38 ± .25 | 3.78 | 1.84 ± 1.10 | 4.01 | 3.33 ± 1.80 | 4.29 |
| Pesquisa | 1.56 ± .52 | 5.92 | 7.69 ± 2.43 | 6.02 | 1.74 ± .87 | 2.89 |
| Pistas Fraudulentas | .16 ± .17 | 2.01 | .72 ± 0.72 | 2.03 | 5.33 ± 2.58 | 5.71 |
| *p-value* | **<.001** | | **<.001** | | **<.001** | |

Nota: M = Média; SD = *Std. Deviation*; MR = *Mean Rank*

O teste *Friedman* revelou diferenças estatisticamente significativas entre as AOI quanto à duração média das fixações ($X^2(6) = 261.70$, p<.001). A AOI Produtos Comerciais apresentou maior *Mean Rank* (MR=6.83), o que indica que os participantes observaram durante mais tempo os produtos disponíveis nos *websites* de comércio. As comparações pós-hoc do teste *Wilcoxon* permitiram concluir que esta AOI apresentou valores significativamente superiores às restantes AOI (p<.001).

### 3.1 Comparação entre *Websites* Fraudulentos e Legítimos

Para comparar a atenção dirigida às AOI entre *websites* legítimos e fraudulentos, utilizou-se o teste *Wicoxon*, cujos resultados se encontram na tabela 5.

Tabela 5 – Comparação da duração média das fixações, do número total médio de fixações e da latência nas AOI entre *Websites* Fraudulentos e *Websites* Legítimos

| | Fraudulentos | Legítimos | p |
|---|---|---|---|
| | M ± SD | M ± SD | |
| Duração Média das Fixações (ms) | | | |
| Área do Utilizador | .19 ± .19 | .25 ± .26 | .101 |
| Produtos Comerciais | 3.67 ± 1.59 | 3.94 ± 1.66 | **.011** |
| Marca | .43 ± .35 | .35 ± .25 | .167 |
| URL | .56 ± .89 | .47 ± .77 | .226 |
| Informação Comercial | .35 ± .29 | .40 ± .31 | .149 |
| Pesquisa | 1.57 ± .62 | 1.54 ± .64 | .853 |
| Número Médio das Fixações | | | |
| Área do Utilizador | .89 ± .86 | 1.11 ± 1.07 | .132 |
| Produtos Comerciais | 17.55 ± 7.10 | 18.56 ± 7.33 | .156 |
| Marca | 1.55 ± 1.11 | 1.48 ± .90 | .905 |
| URL | 1.69 ± 2.61 | 1.68 ± 2.26 | .887 |
| Informação Comercial | 1.72 ± 1.36 | 1.95 ± 1.33 | .199 |
| Pesquisa | 7.53 ± 2.71 | 7.85 ± 3.01 | .294 |
| Latência (ms) | | | |
| Área do Utilizador | 6.42 ± 1.57 | 4.82 ± 1.58 | **.010** |
| Produtos Comerciais | 1.34 ± .99 | .99 ± .76 | .163 |
| Marca | 2.37 ± 1.80 | 1.61 ± .89 | .166 |
| URL | 2.20 ± 1.69 | 3.25 ± 2.35 | **.020** |
| Informação Comercial | 3.52 ± 2.21 | 3.24 ± 2.10 | .148 |
| Pesquisa | 1.73 ± .85 | 1.71 ± 1.11 | .185 |

Nota: M = Média; SD = *Std. Deviation*; p = *p-value* referente ao teste *Wilcoxon*

Verificaram-se diferenças estatisticamente significativas na duração média das fixações dirigidas à AOI Produtos Comerciais entre *websites* fraudulentos e legítimos (Z= -2.539, p=.011). Concretamente, os participantes dirigiram mais atenção aos produtos comerciais nos *websites* legítimos (M=3.94; SD=1.66) em comparação com os *websites* fraudulentos (M=3.67; SD=1.59). Foram, ainda, registadas diferenças estatisticamente

significativas quanto à latência para as AOI Área do Utilizador (Z = -2.574, p=.010) e URL (Z = -2.326, p=.020). Os participantes fixaram mais rapidamente a atenção na Área do Utilizador dos *websites* legítimos (M=4.82; SD=1.58), enquanto o URL foi visualizado mais precocemente nos *websites* fraudulentos (M=2.20; SD=1.69).

### 3.2 Análise Visual dos Mapas de Calor

Face ao elevado número de mapas de calor gerados, apresentam-se apenas aqueles correspondentes aos *websites* legítimos e fraudulentos que registaram maior intenção de compra (Figura 2), complementando os resultados da análise estatística. Os restantes mapas de calor podem ser consultados no Anexo I.

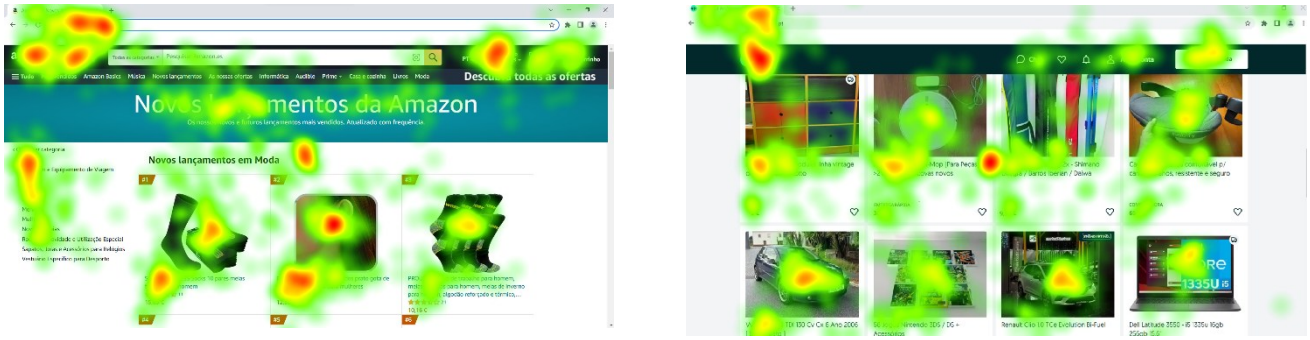



Figura 2 – Mapas de Calor do *Website* Legitimo 6 e *Website* Fraudulento 8

De forma geral, observaram-se ligeiras diferenças nos padrões visuais entre os *websites* legítimos e fraudulentos. Os dois mapas de calor corroboram os resultados quantitativos para a AOI Produtos Comerciais, evidenciando uma maior intensidade de observação nos produtos, sobretudo nas imagens e nas descrições dos artigos dos *websites* legítimos. Ademais, verificou-se uma elevada intensidade de observação nas áreas superiores esquerdas, onde se localizam elementos como o logótipo e o URL.

## 4. Relação entre a Atenção Seletiva e a Suscetibilidade à Cibervitimação

Dos 66 participantes, 42 foram classificados como suscetíveis e 24 como não suscetíveis à cibervitimação nos *websites* de comércio fraudulentos. Para comparar as diferenças entre ambos os grupos nas AOI dos *websites*, realizou-se o teste U de *Mann-Whitney*, complementando-se a interpretação dos dados com a análise dos mapas de calor.

### 4.1 Atenção Seletiva e Suscetibilidade dos Participantes

A tabela 5 apresenta os resultados estatísticos da comparação entre participantes não suscetíveis e suscetíveis nas AOI dos *websites* fraudulentos.

Tabela 6 – Comparação da duração média das fixações, número total médio de fixações e latência nas AOI dos *Websites* Fraudulentos entre Participantes Não Suscetíveis e Suscetíveis

| | Não Suscetíveis | | | Suscetíveis | | | p |
|---|---|---|---|---|---|---|---|
| | N | M ± SD | MR | N | M ± SD | MR | |
| Duração Média das Fixações (ms) | 24 | | | 42 | | | |
| Área do Utilizador | | .24 ± .23 | 37.52 | | .16 ± .16 | 31.20 | .197 |
| Produtos Comerciais | | 2.25 ± 1.24 | 16.71 | | 4.48 ± 1.15 | 43.10 | **<.001** |
| Marca | | .57 ± .40 | 41.33 | | .34 ± .30 | 29.02 | **.012** |
| URL | | 1.32 ± 1.07 | 50.46 | | .13 ± .26 | 23.81 | **<.001** |
| Informação Comercial | | .38 ± .33 | 34.69 | | .34 ± .27 | 32.82 | .704 |
| Pesquisa | | 1.35 ± .47 | 27.00 | | 1.70 ± .67 | 37.21 | **.038** |
| Pistas Fraudulentas | | .23 ± .23 | 38.63 | | .12 ± .11 | 30.57 | .099 |
| Número Total Médio das Fixações | | | | | | | |
| Área do Utilizador | | 1.08 ± 1.02 | 36.58 | | .78 ± .74 | 31.74 | .319 |
| Produtos Comerciais | | 11.43 ± 6.11 | 17.06 | | 21.04 ± 4.96 | 42.89 | **<.001** |
| Marca | | 1.95 ± 1.27 | 40.00 | | 1.33 ± .95 | 29.79 | **.037** |
| URL | | 3.94 ± 3.38 | 49.02 | | .58 ± .93 | 24.63 | **<.001** |
| Informação Comercial | | 1.79 ± 1.46 | 34.13 | | 1.67 ± 1.32 | 33.14 | .841 |
| Pesquisa | | 6.82 ± 1.77 | 29.56 | | 7.94 ± 3.07 | 35.75 | .207 |
| Pistas Fraudulentas | | .86 ± .76 | 37.06 | | .64 ± .69 | 31.46 | .249 |
| Latência (ms) | | | | | | | |
| Área do Utilizador | | 5.59 ± 2.10 | 28.12 | | 5.42 ± 2.13 | 27.11 | .818 |
| Produtos Comerciais | | 1.74 ± .93 | 47.10 | | .73 ± .72 | 25.73 | **<.001** |
| Marca | | 2.54 ± 1.36 | 37.91 | | 2.07 ± 1.75 | 27.98 | **.038** |
| URL | | 2.08 ± 1.64 | 21.55 | | 2.73 ± 2.21 | 25.29 | .344 |
| Informação Comercial | | 4.13 ± 1.90 | 34.58 | | 3.23 ± 2.50 | 25.99 | .062 |
| Pesquisa | | 2.13 ± .99 | 37.67 | | 1.82 ± 1.08 | 31.12 | .183 |
| Pistas Fraudulentas | | 4.55 ± 2.36 | 23.35 | | 5.35 ± 2.81 | 28.47 | .236 |

Nota: N = Número de Participantes; M = Média; SD = *Std. Deviation*; MR = *Mean Rank*; p = *p-value* referente ao teste U de *Mann-Whitney*

Os resultados evidenciaram diferenças estatisticamente significativas entre participantes não suscetíveis e suscetíveis quanto aos padrões visuais nos *websites* fraudulentos. Em termos de duração média das fixações, os participantes suscetíveis apresentaram *Mean Ranks* superiores nas AOI Pesquisa (MR=27.00 vs. MR=37.21, U=348.00, p=.038) e Produtos Comerciais (MR=16.71 vs. MR=43.10, U=101.00, p<.001). Por sua vez, os participantes não suscetíveis observaram durante mais tempo as AOI Marca (MR=41.33 vs. MR=29.02, U=316.00, p=.012) e URL (MR=50.46 vs. MR=23.81, U=97.00, p<.001). A análise individual dos *websites* fraudulentos (Anexo J)

revelou que o F8 registou a maior duração média das fixações na AOI Produtos Comerciais (M=6.33; SD=1.53) e o F2 na AOI URL (M=1.96; SD=1.35).

Verificaram-se, ainda, diferenças estatisticamente significativas no número médio de fixações e na latência. Enquanto os participantes não suscetíveis realizaram mais fixações nas AOI Marca (MR=40.00 vs. MR=29.79, U=348.00, p=.037) e URL (MR=49.02 vs. MR=24.63, U=131.50, p<.001), os participantes suscetíveis concentraram um maior número de fixações na AOI Produtos Comerciais (MR=17.06 vs. MR=42.09, U=109.50, p<.001). Quanto à latência, os participantes suscetíveis dirigiram a sua atenção mais precocemente para as AOI Produtos Comerciais (MR=47.10 vs. MR=25.73, U=177.50, p<.001) e Marca (MR= 37.91 vs. MR= 27.98, U=299.00, p=.038).

Embora não constituísse um objetivo específico da investigação, observaram-se padrões visuais semelhantes nos *websites* legítimos (Anexos K e L). Enquanto os participantes suscetíveis dedicaram mais tempo da sua atenção na AOI Produtos Comerciais (MR=20.88 vs. MR=40.71, U=201.00, p<.001), os não suscetíveis dirigiram maior atenção à AOI URL (MR=50.79 vs. MR=23.62, U=89.00, p<.001), constatando-se a maior duração média das fixações nesta área no L1 (M=1.42; SD=1.48).

### 4.2 Análise Visual dos Mapas de Calor

Para complementar os resultados estatísticos, serão apresentados os mapas de calor dos *websites* fraudulentos que suscitaram maior e menor predisposição para a compra (Figura 3 e 4, respetivamente). Os restantes mapas de calor encontram-se no Anexo M.

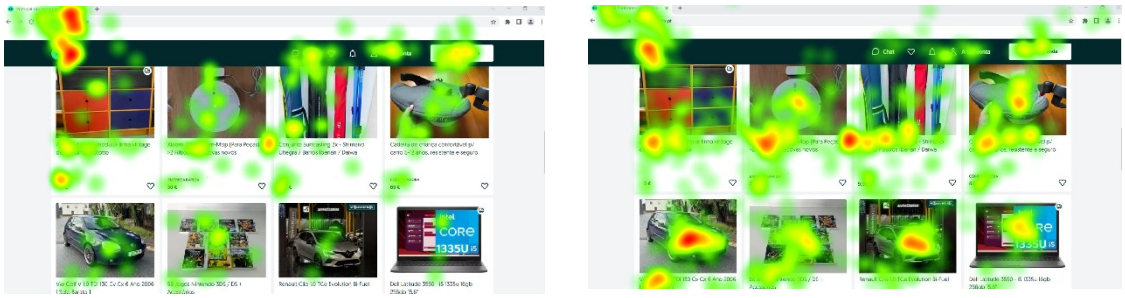


Figura 3 – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis no F8 (respetivamente)

No *website* fraudulento 8, verificou-se que os participantes não suscetíveis observaram com maior intensidade o URL e o logótipo do *website*. Pelo contrário, os participantes suscetíveis despenderam mais atenção nas imagens e descrições dos produtos, observando de forma moderada o logótipo e dedicando reduzida atenção ao URL.

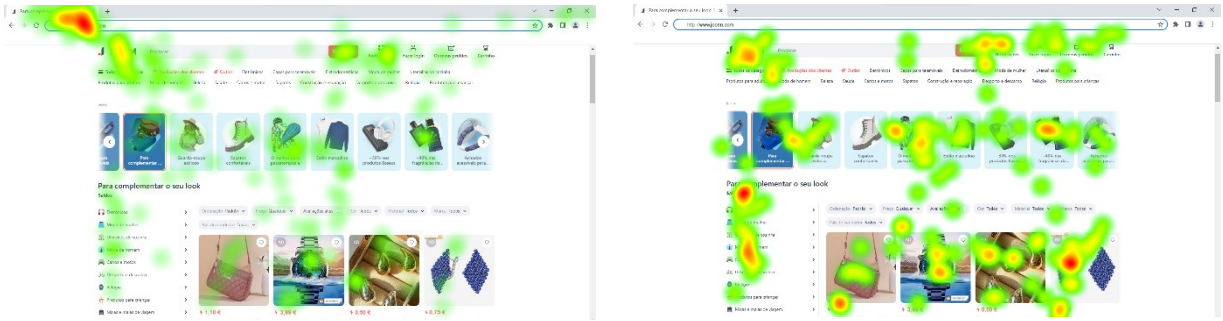


Figura 4 – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis no F1 (respetivamente)

No *website* fraudulento 1, os participantes não suscetíveis observaram o URL durante mais tempo comparativamente às restantes áreas. Já os suscetíveis ignoraram, completamente, a área do URL e concentraram a sua atenção nas imagens dos produtos, seguindo-se as categorias de pesquisa e o logótipo com uma duração moderada.

## 5. Associação entre Características Sociodemográficas e Suscetibilidade à Cibervitimação

A tabela 6 mostra os resultados estatísticos da associação entre as características sociodemográficas e a suscetibilidade à cibervitimação.

Tabela 7 – Associação entre Variáveis Sociodemográficas e Suscetibilidade à Cibervitimação

| | Não Suscetíveis | | Suscetíveis | | U | $X^2$ | p |
|---|---|---|---|---|---|---|---|
| | N (%) | M±SD | N (%) | M±SD | | | |
| Idade | | 24.71±9.92 | | 25.14±11.70 | 401.50 | | .169 |
| Género | | | | | | .264 | .607 |
| Feminino | 18 (38) | | 29 (62) | | | | |
| Masculino | 6 (32) | | 13 (68) | | | | |
| Habilitações Literárias | | | | | | 5.345 | **.021** |
| Até Ensino Secundário | 13 (28) | | 34 (72) | | | | |
| Ensino Superior | 11 (58) | | 8 (42) | | | | |
| Rendimento Familiar | | | | | | .031 | .860 |
| Menor Satisfação | 2 (40) | | 3 (60) | | | | |
| Maior Satisfação | 22 (36) | | 39 (64) | | | | |

Nota: N (%) = Número de Participantes e Percentagem; M = Média; SD = *Std. Deviation*; U = valor do teste *Mann-Whitney*; $X^2$ = valor do teste Qui-quadrado; p = *p-value*

O teste U de *Mann-Whitney* não revelou uma associação estatisticamente significativa entre a suscetibilidade e a idade (p=.169). Do mesmo modo, o teste Qui-Quadrado não evidenciou associações estatisticamente significativas com o género (p=.607) ou o rendimento familiar atual (p=.860). Em contraste, as habilitações literárias associaram-se

significativamente à suscetibilidade ($X^2(1) = 5.35$, p=.021) com um tamanho de efeito moderado (φ=.285). Os participantes com escolaridade até ao Ensino Secundário apresentaram uma probabilidade 3,60 vezes superior de serem suscetíveis em comparação aos participantes com Ensino Superior (OR=3.60; IC=95%: 1.18 – 10.99).

## PARTE II: RESULTADOS QUALITATIVOS

A amostra de 12 participantes do estudo qualitativo incluiu 7 do sexo feminino e 5 do sexo masculino, com idades entre os 19 e os 50 anos, mas maioritariamente entre os 19 e os 25 anos. Quanto às habilitações literárias, 3 concluíram o Ensino Básio, 4 completaram o Ensino Secundário e 4 finalizaram a Licenciatura. Ressalva-se que 3 participantes já tinham experienciado algum tipo de cibervitimação nos *websites* de comércio e 7 foram considerados suscetíveis na tarefa do *eye-tracking*.

De forma a responder às questões de investigação, os resultados organizam-se em cinco eixos temáticos: (i) a Cultura de Consumo Contemporânea; (ii) as Pistas Visuais de Legitimidade dos *Websites*; (iii) a Construção de Confiança nos *Websites* de Comércio; (iv) a Perceção dos Riscos; e (v) as Recomendações. Para facilitar a compreensão dos mesmos, elaborou-se um *mind map* (Anexo N) e os vários temas serão fundamentados com excertos das transcrições consideradas mais relevantes para exemplificar os resultados obtidos.

### 1. Cultura de Consumo Contemporânea

Os participantes recorreram a estratégias discursivas de racionalização e normalização para justificar o consumo *online* enquanto uma prática profundamente integrada nas rotinas quotidianas e enraizada na cultura de consumo contemporânea.

Em primeiro lugar, sobressaiu a estratégia de racionalização instrumental para justificar os benefícios utilitários e económicos proporcionados pelo comércio *online*, nomeadamente a facilidade de compra, a variedade da oferta, a comodidade de adquirir produtos sem deslocação física e os preços mais reduzidos, considerados particularmente atrativos perante as atuais exigências financeiras. Esta estratégia é ilustrada pelas seguintes afirmações: "*é mais fácil comprar online devido ao maior grau de variedade de produtos*" (P7); "*fazemos compras sem sair de casa*" (P5) e "*com o ordenado atual, torna-se muito mais barato comprar online*" (P10). Simultaneamente, emergiu uma dimensão hedónica do consumo, expressa em afirmações como "*não é que precisasse de comprar roupa, mas compro, porque gosto*" (P10), revelando que as compras *online* são associadas à satisfação dos desejos e interesses pessoais. Neste contexto, a preferência

por "*sites mais baratos*" (P12) ou plataformas *low-cost*, tais como "*Shein*" (P9), "*Temu*" (P5) e "*AliExpress*" (P4), evidencia uma racionalidade económica orientada para a maximização da relação custo-benefício, na qual o preço assume maior relevância do que a qualidade dos produtos, como se torna evidente no seguinte excerto: "*em termos de uma relação qualidade-preço sinto-me melhor com um preço mais baixo*" (P6).

Os participantes utilizaram ainda estratégias discursivas de normalização, retratando o comércio *online* como uma consequência natural e inevitável do progresso tecnológico e dos estilos de vida contemporâneos. A afirmação "*tornou-se muito raro comprar coisas em lojas físicas*" (P1) mostra que o comércio *online* assume o papel outrora desempenhado pelo comércio físico. Esta normalização é reforçada por formas linguísticas de consenso e generalização através da utilização recorrente da primeira pessoa do plural em expressões como "*faz parte das nossas vidas, porque fazemos muitas compras online*" (P4) e "*vivemos numa sociedade onde o consumismo é uma coisa tão banalizada*" (P7), deslocando o consumo *online* da esfera individual para uma realidade coletiva. Além do exposto, a oposição discursiva entre "nós" (consumidores) e "eles" (*websites*) em expressões como "*os sites mostram o que não sabíamos que precisávamos*" (P8) e "*os sites querem que tu compres*" (P9) revela a responsabilização das plataformas digitais pela criação de estratégias comerciais deliberadas para estimular o consumo, como "*promoções e contagens decrescentes para incentivar o agora ou nunca*" (P7).

Paralelamente, os participantes mobilizaram estratégias de autoridade por conformidade, justificando a intenção de compra *online* com base nas experiências e recomendações de outros consumidores, o que reflete o crescente viralismo deste consumo. A importância atribuída a familiares, amigos, comunidades digitais e redes sociais demonstra que a intenção de compra foi construída por processos de observação e imitação social, como ilustram as afirmações: "*tento encomendar de websites que os meus amigos aconselharam*" (P6) e "*vemos pessoas a publicarem roupas no Instagram e sentimos pressão para comprar*" (P12). Ademais, a utilização de estrangeirismos, como "*influencers*" (P7), "*click*" (P6) e "*red flag*" (P4), evidencia a apropriação de um léxico característico da cultura digital no discurso quotidiano dos participantes.

Em suma, os discursos evidenciaram que o comércio *online* é justificado por argumentos de utilidade, racionalidade económica, conformidade social e normalização, sugerindo que, além de um comportamento individual, constitui uma prática sociocultural sustentada por significados, normas e valores coletivamente partilhados.

## 2. Pistas Visuais de Legitimidade dos *Websites*

Os participantes interpretaram as pistas visuais dos *websites* através da atribuição de significados de autenticidade (contacto com uma empresa de comércio genuína), segurança *online* (proteção das transações económicas e dos dados pessoais) ou suspeição (possibilidade de fraude).

Elementos técnicos, como o URL, o protocolo HTTPS e o cadeado de segurança, e elementos simbólicos, como o logótipo da marca, foram associados à autenticidade e à segurança *online*, como demonstra a afirmação: "*observei o link, porque esse é o elemento que verifico para considerar um website fidedigno*" (P2). Pelo contrário, os erros ortográficos e as alterações no URL, como "*não é OLX, mas O1X*" (P2), os preços irrealisticamente reduzidos, ilustrados por "*preços demasiado baratos para este tipo de coisas à venda*" (P6), e as imagens adulteradas, expressas em "*as imagens são falsas e editadas*" (P11), foram interpretados como sinais de potencial fraude.

A atribuição destes significados traduziu-se em estratégias discursivas de avaliação moral, através das quais os participantes formularam juízos de legitimidade. Os *websites* considerados legítimos foram descritos por adjetivos como "*fidedigno*" (P2), "*verdadeiro*" (P3), "*bom*" (P6) e "*seguro*" (P8). Em contraste, os *websites* considerados fraudulentos foram caracterizados como "*estranho*" (P4), "*duvidoso*" (P6), "*enganador*" (P10) e "*falso*" (P11). Paralelamente, o recurso a verbos de ação (e.g., "observar" e "verificar") realçou a ideia de que o consumo *online* implica um processo ativo de inspeção das pistas visuais presentes nos *websites*, como se constata pela seguinte afirmação: "*verifiquei os logótipos para perceber o site em que estou a comprar*" (P8).

Os participantes recorreram, também, a estratégias discursivas de racionalização teórica, autoridade impessoal e autoridade por conformidade, fundamentando os seus juízos de legitimidade em conhecimentos previamente adquiridos, normas de segurança digital e valores socialmente partilhados, tal como demonstram as afirmações: "*o HTTPS indica que estou perante um website verdadeiro*" (P1); "*tenho conhecimento e é da opinião geral que existem links duvidosos e, por isso, essa é a primeira coisa que tento verificar*" (P6); e "*foi-me dito que devo ter atenção ao HTTPS nos sites*" (P7).

Em síntese, os discursos demonstraram que a interpretação das pistas visuais dos *websites* resulta da atribuição de significados que conduzem à formulação de juízos de legitimidade sustentados por estratégias de avaliação moral, racionalização e autorização. Simultaneamente, o consumo *online* acarreta a aplicação de conhecimentos previamente adquiridos, atribuindo-se aos consumidores a responsabilidade pela sua segurança *online*.

## 3. Construção de Confiança nos *Websites* de Comércio

Relativamente à confiança atribuída aos *websites* de comércio, os participantes fundamentaram-na em diferentes indicadores relacionados com a segurança percebida das transações digitais, a aparência visual dos *websites*, as experiências prévias de consumo *online* e a validação social obtida por outros consumidores.

No que respeita à segurança percebida das transações digitais, os participantes mobilizaram estratégias discursivas de autoridade impessoal, atribuindo particular relevância à presença de métodos de pagamento considerados seguros para sustentar a expectativa de que os *websites* cumprirão as promessas assumidas durante a transação económica (credibilidade). A expressão "*só compro se um site tiver as opções de MB WAY, MB NET ou Apple Pay, porque torna-se mais seguro*" (P4) revela que estes métodos constituem uma condição prévia para a realização de compras em *websites*. Simultaneamente, a afirmação "*faço o pagamento por MB WAY para proteger os dados bancários*" (P9) sugere uma racionalização instrumental, na qual a escolha do método de pagamento é justificada pela expectativa de proteção dos dados financeiros e de redução dos riscos inerentes às transações *online*.

Paralelamente, a aparência visual dos *websites* foi associada à credibilidade. A organização das interfaces, a estética apelativa e a estrutura semelhante com plataformas digitais familiares reforçaram a confiança dos consumidores. Excertos como "*a interface mais limpa e clara ajuda imenso na decisão de compra*" (P7) e "*a estrutura dos sites que confio é a mesma com vários produtos organizados por categorias*" (P3) revelam uma avaliação moral, através da qual determinadas características visuais são valorizadas positivamente por recurso a adjetivos como "*bonito*" e "*interessante*". Esta avaliação traduziu-se na maior predisposição para permanecer e comprar nos *websites*, como ilustrado em: "*se um website for mais bonito, tenho mais vontade de estar lá*" (P1) e "*ver o que está a ser vendido acaba por ser interessante e capta mais a atenção*" (P5).

As experiências prévias de consumo *online* constituíram igualmente um importante fundamento da confiança. Afirmações como "*confio, porque conheço o site e já comprei várias vezes*" (P8) ou "*nunca tive problemas com websites que já utilizo e, por isso, sei que posso comprar*" (P5) revelam estratégias discursivas de racionalização através das quais a familiaridade e a repetição de experiências positivas foram utilizadas para justificar a expectativa de que futuras compras decorrerão de forma previsível e segura.

Os participantes mobilizaram ainda estratégias discursivas de autoridade por conformidade, sustentando a confiança nos *websites* nos comentários *online* de outros

consumidores, em avaliações dos produtos e na reputação das marcas. Afirmações como "*se encontrar comentários negativos, isso é o suficiente para me dissuadir de realizar compras*" (P1) e "*toda a gente sabe que as marcas mais conhecidas, como a Nike, têm menos problemas*" (P12) demonstram que a confiança não assenta apenas na experiência individual, mas também na reputação e nas opiniões socialmente partilhadas.

Os juízos de confiança em torno dos *websites* refletiram-se em consequências comportamentais. Quando as experiências próprias ou de terceiros correspondiam às expectativas, os participantes recorreram à racionalização instrumental para justificar a repetição de compras e a fidelização, como P3 mencionou: "*compro há 2 anos, porque dão-me garantias que vou receber os produtos*". Pelo contrário, as experiências negativas, como atrasos ou incumprimentos na entrega, deram origem a estratégias discursivas de deslegitimação traduzidas no abandono dos *websites*. Neste sentido, destaca-se o advérbio "*nunca*" na afirmação "*se algo correr mal, como o atraso da entrega dos produtos da Primor, nunca mais farei compras naquele website*" (P1), que demonstra uma rutura definitiva com a plataforma digital. Similarmente, a afirmação "*se não corresponder às expectativas, tentarei outro website numa ocasião futura*" (P2) demonstra que a perda de confiança conduz à procura de alternativas.

Assim, a confiança nos *websites* foi construída através de estratégias discursivas de autorização, racionalização e avaliação moral. A interpretação dos elementos visuais, as experiências anteriores e a validação social contribuíram para a credibilidade atribuída aos *websites*, condicionando a continuidade ou o abandono das plataformas digitais.

### 4. Perceção dos Riscos

Apesar das vantagens atribuídas ao comércio *online*, os participantes reconheceram que os *websites* constituem potenciais ambientes de risco, destacando-se os incumprimentos contratuais, as perdas financeiras e a apropriação indevida de dados.

Os riscos contratuais surgiram associados à possibilidade de os produtos recebidos não corresponderem ao anunciado ou não serem entregues, como demonstram as afirmações: "*pode chegar um produto diferente daquele que comprei*" (P11) e "*a encomenda pode não chegar à morada*" (P5). Estas interpretações configuram estratégias de deslegitimação por racionalização, através das quais a perda de confiança foi justificada pela antecipação de consequências negativas decorrentes do incumprimento das obrigações assumidas pelos vendedores e da violação do princípio da boa-fé contratual.

Os prejuízos patrimoniais decorrentes de fraudes constituíram um dos principais riscos antecipados, independentemente de experiências prévias de cibervitimação. Os participantes recorreram a estratégias discursivas de avaliação moral negativa, atribuindo intenções maliciosas aos *websites* fraudulentos, tal como ilustram os seguintes excertos: "*os websites fraudulentos de certas marcas querem retirar o dinheiro às pessoas*" (P4) e "*há fraudes e podemos ficar sem o nosso dinheiro, mas acredito que aconteça apenas em alguns sites*" (P10). Contudo, a gravidade de uma potencial cibervitimação foi relativizada em função do valor económico da perda. Alguns participantes minimizaram os prejuízos de valor reduzido, considerando-os insuficientes para justificar uma reação formal, como P3 exemplificou: "*se fosse uma quantia mínima ou insignificante de 2€, provavelmente não faria nada*". Em contrapartida, as perdas mais elevadas foram associadas à necessidade de recorrer a mecanismos de denúncia, reclamação ou reparação, conforme P9 referiu: "*se fosse um valor exorbitante, como 100 ou 200€, talvez compensasse apresentar queixa*". Estes discursos evidenciam uma racionalização instrumental, através da qual a decisão de agir perante uma fraude resultou da ponderação de custos e benefícios associados à reação.

Os participantes identificaram, ainda, riscos relacionados com a divulgação e a utilização indevida de dados pessoais e bancários, recorrendo a avaliações morais que classificam estas práticas como violações éticas e legais, através das seguintes expressões: "*roubo dos dados do cartão de crédito*" (P2); "*furto de identidade*" (P6); e "*podem utilizar os meus dados para outras coisas que eu não consenti*" (P8).

O recurso a expressões na primeira pessoa do singular e os advérbios (e.g., "*bastante*") permitiram intensificar sentimentos de medo, receio e ansiedade perante potenciais fraudes, como ilustram as seguintes afirmações: "*tenho receio que haja fraudes*" (P10); "*tenho bastante medo de que fiquem com a minha informação bancária*" (P9); e "*fico ansiosa para saber se a encomenda chega a casa sem problemas*" (P5). Simultaneamente, os participantes mobilizaram estratégias de autoridade impessoal, descrevendo comportamentos de autoproteção *online* baseados em normas de segurança digital, como "*evito colocar dados pessoais ou dos cartões de crédito na Internet*" (P1).

Em síntese, os discursos demonstraram que a perceção dos riscos resulta da articulação entre estratégias discursivas de racionalização, avaliação moral e autorização, sendo sustentada por avaliações cognitivas e respostas emocionais que influenciam a confiança e a intenção de compra nos *websites* de comércio.

### 5. Recomendações

Quando convidados a refletir sobre mudanças para melhorar a confiança nos *websites* de comércio legítimos, os participantes mobilizaram estratégias discursivas de racionalização instrumental e de autoridade impessoal, formulando recomendações dirigidas às plataformas digitais e aos consumidores.

Quanto às primeiras, propuseram interfaces mais simples e organizadas, bem como a disponibilização de imagens realistas dos produtos comerciais e de mecanismos de apoio ao cliente acessíveis, justificando estas medidas pela expectativa de redução das incertezas. Tal é ilustrado pelos seguintes excertos: "*os websites devem ser mais simples e menos estimulantes*" (P3); "*menos Photoshop e mais imagens com pessoas reais a vestir as roupas*" (P11); e "*deveria existir uma linha de contacto com pessoas para falar sobre as encomendas*" (P6). Estes discursos traduzem, também, estratégias de avaliação moral ao apresentarem a aparência visual e a interação humana como características desejáveis no comércio *online*.

No que respeita aos consumidores, os participantes recomendaram comportamentos de autoproteção *online*, como a verificação do URL e a proteção dos dados pessoais. As expressões "*evitem*" e "*devemos*" patentes em afirmações como "*evitem colocar os dados pessoais ou dos cartões na Internet*" (P1) e "*devemos sensibilizar os consumidores para o conhecimento dos endereços*" (P4) tomam o aspeto de prescrições normativas.

Assim, os participantes parecem sugerir que a melhoria da confiança nos *websites* de comércio constitui uma responsabilidade partilhada entre plataformas e consumidores, sustentada por princípios de autenticidade, segurança e literacia digital.

## CAPÍTULO IV – DISCUSSÃO DOS RESULTADOS

Como já referido, esta investigação recorreu a metodologias mistas que implicam a integração dos resultados provenientes de etapas assentes em métodos e pressupostos epistemológicos distintos. É na discussão que os dados devem dialogar para aprofundar o conhecimento criminológico sobre a problemática em análise.

Para compreendermos as implicações deste estudo, esta secção apresenta, numa primeira instância, uma discussão integrada dos resultados quantitativos e qualitativos, confrontando-os com a literatura científica. Posteriormente, expõem-se as limitações da investigação e as pistas para estudos futuros.

## 1. Atenção Seletiva, Confiança e Intenção de Compra *Online*

Os resultados demonstraram que a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos resulta de um processo sequencial, que integra padrões visuais, processos interpretativos e discursos socioculturais.

Num primeiro momento, os participantes dirigiram predominantemente a sua atenção para os produtos à venda, sobretudo nos *websites* legítimos, corroborando a hipótese 1 e os resultados de estudos prévios (e.g., Darwish & Bataineh, 2012). Contudo, as entrevistas revelaram que a atenção seletiva foi orientada pelos significados atribuídos às diferentes pistas visuais. Quando os participantes reconheceram indicadores de legitimidade, como o HTTPS ou um logótipo reconhecido, atribuíram precocemente confiança ao *website* e a atenção permaneceu centrada nos produtos comerciais. Em contrapartida, perante sinais de suspeição, como erros ortográficos e imagens adulteradas, a atenção deslocou-se para outros elementos de validação da autenticidade.

Estes resultados vão ao encontro de conclusões de estudos que demonstram a importância das heurísticas visuais na atribuição de confiança aos *websites* (Boardman & Mccormick, 2022; Buscher *et al.*, 2009; Darwish & Bataineh, 2012), sugerindo que a atenção seletiva constitui a primeira etapa de um processo interpretativo dos estímulos observados. Estas evidências sustentam os pressupostos da Criminologia Visual, segundo os quais as representações visuais constituem formas de comunicação que produzem significados, moldam perceções e orientam comportamentos (Brown & Carrabine, 2019; McClanahan, 2021). Paralelamente, a elevada intenção de compra observada em determinados *websites* fraudulentos com ligeiras modificações no URL (e.g., "*www.sh£in.com*") e erros ortográficos discretos (e.g., "*emtrega*") demonstra que a eficácia destas fraudes reside na reprodução de elementos visuais semelhantes aos de plataformas digitais legítimas, explorando heurísticas e significados previamente adquiridos pelos consumidores (Bitaab *et al.*, 2023; Carpineto & Romano, 2017; Dhamija *et al.*, 2006).

As diferenças observadas entre participantes suscetíveis e não suscetíveis reforçam esta interpretação. Os participantes mais suscetíveis concentraram significativamente a sua atenção nos produtos comerciais, o que confirmou a hipótese 2, justificando a sua intenção de compra *online* através de racionalizações económicas associadas à atratividade dos produtos. Em contraste, os participantes menos suscetíveis dirigiram mais atenção para o URL e o logótipo, o que corroborou a hipótese 3, interpretando estes elementos como indicadores de autenticidade através de estratégias discursivas de

autorização impessoal e racionalização teórica (van Leeuwen, 2008). Curiosamente, o reconhecimento espontâneo de um "limiar de preço" sugere que preços excessivamente reduzidos funcionam como indicadores de suspeição. Em conjunto, estes resultados demonstram que a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos depende da prioridade atribuída aos diferentes elementos visuais durante a interpretação dos *websites*, constituindo um dos principais contributos deste estudo.

A atribuição de significados conduziu à formulação de juízos de legitimidade e risco que sustentam a construção da confiança. Além de associarem determinados elementos técnicos e simbólicos à legitimidade, os participantes recorreram a estratégias discursivas de deslegitimação e avaliação moral negativa (van Leeuwen, 2008), através das quais reconheceram riscos instrumentais, como os prejuízos patrimoniais, e emocionais, como os sentimentos de medo e ansiedade, confirmando evidências prévias (Cross *et al.*, 2022; Edwards *et al.*, 2025; Jahankhani, 2009). Paralelamente, a confiança revelou-se uma construção dinâmica assente em pistas visuais, experiências anteriores e validação social. A familiaridade com determinados *websites*, as experiências de compras bem-sucedidas e a reputação derivada das avaliações e dos comentários *online* foram mobilizadas para atribuir credibilidade às plataformas digitais através de estratégias discursivas de racionalização instrumental e de autorização por conformidade (van Leeuwen, 2008), corroborando estudos prévios (Hu *et al.*, 2010; Izogo & Jayawardhena, 2018; Whittaker *et al.*, 2023). Paradoxalmente, à luz da Teoria das Atividades de Rotina (Cohen & Felson, 1979), esta familiaridade pode reduzir os comportamentos de vigilância e aumentar a exposição a oportunidades fraudulentas (Kelley & Bertenthal, 2016; Zahari *et al.*, 2019). Desta forma, a confiança pode aumentar a suscetibilidade à cibervitimação quando decorre da familiaridade e não de uma avaliação crítica dos *websites*.

A interpretação dos *websites* foi enquadrada por macrodiscursos que orientaram a perceção visual e a formulação de juízos. Os participantes abordaram o comércio *online* através de estratégias discursivas de normalização (Fairclough, 1992), racionalização instrumental e autorização por conformidade (van Leeuwen, 2008), descrevendo-o como uma prática conveniente, economicamente vantajosa e socialmente disseminada. Estes resultados encontram suporte na Teoria da Cultura do Consumidor (Arnould & Thompson, 2005), segundo a qual as práticas de consumo resultam da interação entre os interesses individuais, as condições económicas e os discursos culturais. Assim, os consumidores recorrem a conhecimentos, expectativas e normas previamente aprendidas

que condicionam a atribuição de significados ao comércio *online* (Button *et al.*, 2014; Waqas *et al.*, 2021).

Apesar de os participantes afirmarem adotar comportamentos de autoproteção *online*, observou-se uma discrepância entre o discurso e o comportamento: embora os participantes mais suscetíveis afirmassem verificar elementos de segurança, estes não observaram os principais indicadores de legitimidade, demonstrando que o conhecimento declarado nem sempre se traduz em comportamentos visuais efetivos. Por outro lado, enquanto o consumo *online* foi descrito como uma prática coletiva, a cibervitimação sofrida ou antecipada foi descrita como uma experiência individual, predominantemente na primeira pessoa do singular. Em conjunto com a reduzida predisposição para denunciar fraudes de menor valor económico, esta construção discursiva sugere que uma parte significativa destes episódios permanece por denunciar, contribuindo para elevadas cifras negras da fraude ao consumidor *online* (Fonseca *et al.*, 2022).

Relativamente às características sociodemográficas, apenas as habilitações literárias apresentaram uma associação significativa com a suscetibilidade à cibervitimação nos *websites* fraudulentos, corroborando a hipótese 6 e estudos anteriores (e.g., Leukfeldt & Yar, 2016; Shang *et al.*, 2023; Whitty, 2020). Embora esta variável não constitua uma medida direta da literacia digital, os resultados sugerem que os níveis mais elevados de escolaridade favorecem um processamento mais sistemático da informação, o que se revela consistente com o Modelo Heurístico-Sistemático (Chaiken, 1980). Em contraste, a idade, o género e a satisfação com o rendimento do agregado familiar não apresentaram associações significativas, refutando-se as hipóteses 4, 5 e 7. Estes resultados reforçam a ideia de que a cibervitimação no comércio *online* constitui um risco transversal, tal como revela a literatura (APAV, 2020; Dhamija *et al.*, 2006; Leukfeldt & Yar, 2016; Pratt *et al.*, 2010), dependendo sobretudo das competências individuais de avaliação crítica.

As recomendações dos participantes refletiram estratégias discursivas idênticas às identificadas ao longo do estudo. Os resultados reforçam a necessidade de promover a literacia digital e de desenvolver interfaces que atribuam maior saliência visual aos indicadores de legitimidade, de forma a facilitar processos interpretativos mais críticos e a reduzir a suscetibilidade à cibervitimação nos *websites* de comércio fraudulentos.

Em síntese, a integração dos dados quantitativos e qualitativos permitiu propor um modelo sequencial de construção da confiança nos *websites* de comércio (Anexo O). Este modelo sugere que os contextos individuais e socioeconómicos influenciam a interação inicial com os *websites*. Essa interação inicia-se pela atenção dirigida aos elementos

visuais, prosseguindo com a atribuição de significados sustentados pelos conhecimentos prévios, pelas experiências anteriores de consumo e pelos contextos socioculturais. O processo culmina na formulação de juízos de legitimidade e risco que influenciam a confiança e, consequentemente, a intenção de compra *online*.

## 2. Limitações e Pistas Futuras

Esta investigação não está isenta de limitações que devem ser consideradas na interpretação dos resultados. Embora se tenha procurado recrutar uma amostra heterogénea, a necessidade de deslocação dos participantes ao LEC-FDUP poderá ter condicionado a dimensão e a composição da amostra, verificando-se uma maior representatividade de participantes jovens, estudantes e do sexo feminino. Assim, os resultados devem ser interpretados no âmbito da amostra analisada, não sendo passiveis de generalização estatística à população. Acresce que, devido à demora da recolha e da análise dos dados, não foi possível integrar outras variáveis potencialmente relevantes, como o autocontrolo ou a frequência de compras *online*, que permitiriam compreender de forma mais completa a associação entre as características individuais, a atenção visual, os processos interpretativos e a suscetibilidade em causa. Também não foi possível determinar, em todos os casos, se a decisão de não comprar resultou da identificação do *website* como fraudulento ou de outros fatores alheios à perceção da sua legitimidade, como a ausência de interesse nos produtos comerciais. Embora as entrevistas semiestruturadas com recurso à *photo-elicitation* tenham permitido aprofundar os significados atribuídos pelos participantes às pistas visuais dos *websites*, os discursos poderão refletir processos de racionalização *a posteriori* e de desejabilidade social. Por fim, a utilização de imagens estáticas não reproduz a experiência interativa nos *websites*, limitando a observação dos comportamentos em contexto real de compra.

Não obstante estas limitações, a presente investigação encontra-se inacabada e abre pistas inovadoras para estudos futuros. Em primeiro lugar, recomenda-se a recolha de dados com amostras mais alargadas e diversificadas, permitindo aumentar a representatividade estatística e explorar outras perspetivas. Em segundo lugar, importa integrar variáveis individuais adicionais, como o autocontrolo, a frequência de compras *online* e a perceção de legitimidade dos *websites*, de modo a construir modelos explicativos mais abrangentes da suscetibilidade à cibervitimação por fraude ao consumidor *online*. Em terceiro lugar, futuros estudos poderão recorrer a tecnologias que permitam simular contextos de compra mais realistas, como a interação em tempo real

(*scrolling*) ou a ambientes de realidade virtual. Por último, seria pertinente alargar o foco da investigação à perspetiva dos ofensores e de profissionais das áreas da Investigação Criminal e da Cibersegurança, aprofundando o conhecimento sobre as estratégias de manipulação visual utilizadas nas fraudes ao consumidor *online*.

## CONCLUSÃO

A tecnologia ocupa um papel de central nas rotinas quotidianas, proporcionando novas oportunidades de consumo, mas também novos desafios associados às fraudes no comércio *online*. Neste contexto, compreender como os consumidores constroem juízos de legitimidade, risco e confiança perante *websites* de comércio revela-se fundamental para reduzir a suscetibilidade a esta cibermitimação.

Esta investigação constituiu uma abordagem metodológica inovadora em Portugal ao integrar técnicas de *eye-tracking* e *photo-elicitation* no estudo da suscetibilidade às fraudes ao consumidor *online*. Os resultados demonstraram que esta suscetibilidade não depende apenas das características sociodemográficas nem dos elementos visuais, mas da forma como estes são interpretados pelos consumidores. A integração dos dados quantitativos e qualitativos demonstrou que os padrões visuais e a construção discursiva dos significados são indissociáveis na compreensão deste fenómeno.

As diferenças entre participantes suscetíveis e não suscetíveis, bem como a associação entre níveis mais elevados de escolaridade e a menor suscetibilidade reforçam a necessidade de se promover medidas preventivas orientadas para a sensibilização, a formação e o treino de competências de literacia digital. À medida que os *websites* de comércio fraudulentos se tornam mais convincentes, torna-se imprescindível articular soluções tecnológicas com competências de avaliação crítica que permitam aos consumidores interpretar adequadamente os indicadores de legitimidade e reconhecer estratégias de engenharia social, nomeadamente através da verificação do HTTPS. Paralelamente, as plataformas digitais devem assumir um papel ativo na conceção de interfaces seguras e informativas, facilitando práticas de consumo mais conscientes.

Em suma, a prevenção das fraudes ao consumidor *online*, particularmente nos *websites*, constitui uma responsabilidade partilhada entre consumidores, empresas, autoridades e políticos. Espera-se que esta investigação contribua para o aprofundamento do conhecimento científico acerca da suscetibilidade à cibervitimação nos *websites* de comércio e sirvam de base para o desenvolvimento de estratégias de prevenção e de literacia digital que promovam experiências de consumo *online* mais seguras.

# REFERÊNCIAS BIBLIOGRÁFICAS


Abbasi, A., & Chen, H. (2009). A comparison of fraud cues and classification methods for fake escrow website detection. *Information Technology and Management*, *10*, 83-101. https://doi.org/10.1007/s10799-009-0059-0

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Akshay, S., Megha, Y. J., & Shetty, C. B. (2020). Machine learning algorithm to identify eye movement metrics using raw eye tracking data. In Institute of Electrical and Electronics Engineers (Coord.), *2020 Third International Conference on Smart Systems and Inventive Technology* (pp. 949-955). IEEE. https://doi.org/10.1109/ICSSIT48917.2020.9214290

Apau, R., & Koranteng, F. N. (2020). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber Criminology*, *13*(2), 228-254. https://doi.org/10.5281/zenodo.3697886

Arnould, E. J., & Thompson, C. J. (2005). Consumer Culture Theory (CCT): Twenty Years of Research. *Journal of Consumer Research*, *31*(4), 868–882. https://doi.org/10.1086/426626

Associação Portuguesa de Apoio à Vítima. (2020). *Burlas online*. https://apav.pt/apav_v3/images/pdf/FI_BO_2020.pdf

Associação Portuguesa de Apoio à Vítima. (2025). *Estatísticas APAV – Linha Internet Segura 2024*. https://apav.pt/estatisticas-apav-linha-internet-segura-2024/

Autoridade Nacional de Comunicações. (2025). *O comércio eletrónico em Portugal e na União Europeia em 2025 - segmento residencial e empresarial*. https://anacom.pt/render.jsp?contentId=1827576

Bangun, C. S., & Handra, T. (2021). How theory of planned behavior and perceived risk affect online shopping behavior. *Aptisi Transactions on Management (ATM)*, *5*(2), 169-179. https://doi.org/10.33050/atm.v5i2.1594

Barreto, A. M. (2012). Eye tracking como método de investigação aplicado às ciências da comunicação. *Revista Comunicando*, *1*(1), 168-186. https://doi.org/10.58050/comunicando.v1i1.126

Beals, M., DeLiema, M., & Deevy, M. (2015). *Framework for a taxonomy of fraud*. Financial Fraud Research Center.

https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf

Bitaab, M., Cho, H., Oest, A., Lyu, Z., Wang, W., Abraham, J., Wang, R., Bao, T., Shoshitaishvili, Y., & Doupé, A. (2023). BEYOND PHISH: Toward Detecting Fraudulent e-Commerce Websites at Scale. In L. O'Conner (Ed.), *44th IEEE Symposium on Security and Privacy* (pp. 2566-2583). IEEE. https://doi.org/10.1109/SP46215.2023.10179461

Boardman, R., & Mccormick, H. (2022). Attention and behaviour on fashion retail websites: an eye-tracking study. *Information Technology & People*, *35*(7), 2219-2240. https://doi.org/10.1108/ITP-08-2020-0580

Boeri, M., & Lamonica, A. K. (2015). Sampling designs and issues in qualitative criminology. In H. Copes & J. M. Miller (Eds.), *The Routledge Handbook of Qualitative Criminology* (pp. 125-143). Routledge.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brody, R. G., Mulig, E., & Kimball, V. (2007). PHISHING, PHARMING AND IDENTITY THEFT. *Academy of Accounting & Financial Studies Journal*, *11*(3). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c3f9bedf86614a9ca7cf18197bfbb978f56e6e56v

Brown, M., & Carrabine, E. (2019). The critical foundations of visual criminology: The state, crisis, and the sensory. *Critical Criminology*, *27*(1), 191-205. https://doi.org/10.1007/s10612-019-09439-7

Buscher, G., Cutrell, E., & Morris, M. R. (2009). What do you see when you're surfing? Using eye tracking to predict salient regions of web pages. In D. R. Olsen, R. B. Arthur, K. Hinckley, M. R. Morris, S. Hudson, & S. Greenberg (Eds.), *CHI '09: Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 21-30). Association for Computing Machinery. https://doi.org/10.1145/1518701.1518705

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology*, *47*(3), 391-408. https://doi.org/10.1177/0004865814521224

Carpineto, C., & Romano, G. (2017). Learning to detect and measure fake ecommerce websites in search-engine results. In A. Sheth, A. Ngonga, Y. Wang, E. Chang, D. Ślęzak, B. Franczyk, R. Alt, & X. Tao (Eds.), *WI '17: Proceedings of the international*

*conference on web intelligence* (pp. 403-410). Association for Computing Machinery. https://doi.org/10.1145/3106426.3106441

Carrabine, E. (2012). Just images: Aesthetics, ethics and visual criminology. *The British Journal of Criminology*, *52*(3), 463-489. https://doi.org/10.1093/bjc/azr089

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of personality and social psychology*, *39*(5), 752. https://doi.org/10.1037/0022-3514.39.5.752

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in human behavior, *70*, 291-302. https://doi.org/10.1016/j.chb.2017.01.003

Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. HarperCollins.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Comissão Europeia. (2020). *Survey on "Scams and fraud experienced by consumers"*. https://commission.europa.eu/system/files/2020-01/factsheet_fraud_survey.final_.pdf

Conselho da Europa. (2001). *Convenção sobre o Cibercrime*. https://rm.coe.int/16802fa428

Conselho Europeu. (2025), *Comércio eletrónico na UE*. https://www.consilium.europa.eu/pt/infographics/e-commerce/

Costa, A. M. A. (2020). *A burla no Código Penal Português*. Almedina.

Cross, C., Edwards, M., Button, M., & Whittaker, J. M. (2022). *Online shopping fraud victimisation in Australia*. University of Surrey.

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimization in Australia. *Trends and Issues in Crime and Criminal Justice*, *474*, 1–6. https://search.informit.org/doi/abs/10.3316/informit.312913302944818

CTT. (2024). *O panorama ibérico do e-Commerce em 2024*. https://www.ctt.pt/blog/o-panorama-iberico-do-e-commerce-em-2024

Dadà, C. B., Colautti, L., Rosi, A., Cavallini, E., Antonietti, A., & Iannello, P. (2025). Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review. *Computers in Human Behavior*, *172*, 108734. https://doi.org/10.1016/j.chb.2025.108734

Darwish, A., & Bataineh, E. (2012). Eye tracking analysis of browser security indicators. In American University of Sharjah (Coord.), *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCSII.2012.6454330

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. In R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, & G. Olson (Eds.), *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581–590). Association for Computing Machinery. https://doi.org/10.1145/1124772.1124861

Edwards, M., Whittaker, J. M., Cross, C., & Button, M. (2025). An exploratory study of victimisation and near misses in online shopping fraud. *Global Crime*, *26*(1), 69-89. https://doi.org/10.1080/17440572.2024.2423918

European Social Survey. (2010). *Round 5 - Module on Trust in the Police & Courts – Final Question Design Template*. London: Centre for Comparative Social Surveys – City University London.

Fairclough, N. (1992). *Discourse and social change*. Polity Press.

Fonseca, C., Moreira, S., & Guedes, I. (2022). Online consumer fraud victimization and reporting: A quantitative study of the predictors and motives. *Victims & Offenders*, *17*(5), 756-780. https://doi.org/10.1080/15564886.2021.2015031

Furnell, S. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, *1*(2), 35-44. https://www.jstor.org/stable/26486092

Gill, S. L. (2020). Qualitative sampling methods. *Journal of Human Lactation*, *36*(4), 579-581. https://doi.org/10.1177/089033442094921

Gill, S. L. (2024). About research-qualitative data collection: Photo elicitation. *Journal of Human Lactation*, *40*(4), 503-505. https://doi.org/10.1177/08903344241273863

Gillespie, A. A., & Magor, S. (2020). Tackling online fraud. *ERA Forum*, *20*, 439–454. https://doi.org/10.1007/s12027-019-00580-y

Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., & Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. *International Journal of Safety and Security Engineering*, *11*(4), 361-367. https://doi.org/10.18280/ijsse.110409

Guedes, I. M. E. S. (2016). *Medo do Crime: Emergência, Reações Emocionais e Dircursos. Contributos para a Utilização de Multi-Metodologias*. [Doctoral thesis,

Faculdade de Direito da Universidade do Porto]. Repositório Aberto da Universidade do Porto. https://hdl.handle.net/10216/90609

Guedes, I. S., Moreira, S., & Cardoso, C. (2021). Cibercrime: Conceptualização, desafios e perceções públicas. In I. S. Guedes & M. A. M. Gomes (Eds.), *Cibercriminalidade: novos desafios, ofensas e soluções* (pp. 3-23). Pactor Editora.

Hayward, K. (2010). Opening the lens: Cultural criminology and the image. In K. Hayward & M. Presdee (Eds.), *Framing Crime* (pp. 13-28). Routledge-Cavendish. https://doi.org/10.4324/9780203880753

Hollingworth, A., & Bahle, B. (2019). Eye Tracking in Visual Search Experiments. In S. Pollmann (Ed.), *Spatial Learning and Attention Guidance* (pp. 23-35). Humana Press. https://doi.org/10.1007/7657_2019_30

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Hu, N., Liu, L., & Sambamurthy, V. (2010). Fraud detection in online consumer reviews. *Decision Support Systems*, *50*(3), 614-626. https://doi.org/10.1016/j.dss.2010.08.012

International Telecommunication Union. (2025). *Statistics*. ITU: Committed to connecting the world. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Izogo, E. E., & Jayawardhena, C. (2018). Online shopping experience in an emerging e-retailing market. *Journal of Research in Interactive Marketing*, *12*(2), 193-214. https://doi.org/10.1108/JRIM-02-2017-0015

Jahankhani, H. (2009). The behaviour and perceptions of on-line consumers: Risk, risk perception and trust. *International Journal of Information Science and Technology, International Journal of Information Science and Management*, *7*(1), 79-90.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, *33*(7), 14-26. https://doi.org/10.3102/0013189X033007014

Kawaf, F., & Tagg, S. (2017). The construction of online shopping experience: A repertory grid approach. *Computers in Human Behavior*, 72, 222-232. https://doi.org/10.1016/j.chb.2017.02.055

Kelley, N. J., Hurley-Wallace, A. L., Warner, K. L., & Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. *Computers in Human Behavior*, *142*, 107648. https://doi.org/10.1016/j.chb.2022.107648

Kelley, T., & Bertenthal, B. I. (2016). Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. *Information & Computer Security*, *24*(2), 164-176. https://doi.org/10.1108/ICS-01-2016-0002

Kemp, S., & Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health*, *20*(7), 5404. https://doi.org/10.3390/ijerph20075404

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Margolis, E., & Zunjarwad, R. (2018). Visual research. In N. Denzin & Y. Lincoln, *The SAGE handbook of qualitative research* (pp. 600-626). SAGE.

Maruna, S. (2010). Mixed method research in criminology: Why not go both ways? In A. Piquero & D. Weisburd (Eds.), *Handbook of quantitative criminology* (pp. 123–140). New York: Springer. https://doi.org/10.1007/978-0-387-77650-7_7

McClanahan, B. (2021). Visual Methods in Criminology. In B. McClanahan (Ed.), *Visual Criminology* (pp. 37-50). Bristol University Press.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5

Pauwels, L. (2017). Key methods of visual criminology. In M. Brown & E. Carrabine (Eds.), *Routledge International Handbook of Visual Criminology* (pp. 62-73). Routledge.

Petintseva, O. (2022). Language matters: Doing systematic (critical) discourse analysis. In In R. Faria & M. Dodge (Eds.), *Qualitative Research in Criminology: Cutting-Edge Methods* (pp. 199-210). Springer. https://doi.org/10.1007/978-3-031-18401-7_12

Pinjarkar, L., Hete, P. R., Mattada, M., Nejakar, S., Agrawal, P., & Kaur, G. (2024). An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In M. Kannan (Ed.), *Second International Conference on Advances in Information Technology* (pp. 1-6). IEEE. https://doi.org/10.1109/ICAIT61638.2024.10690377

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of research in crime and delinquency*, *47*(3), 267-296. https://doi.org/10.1177/0022427810365903

Procuradoria-Geral da República. (2025). *Cibercrime: Denúncias Recebidas 2025*. https://cibercrime.ministeriopublico.pt/sites/default/files/2026-02/2026.02.11-denuncias-de-cibercrime-2025.pdf

Rana, P. J., & Baria, J. (2015). A survey on fraud detection techniques in ecommerce. *International Journal of Computer Applications*, *113*(14). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2534fe9a8221e042996d024192064a1aa2ecad47

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*(3), 324-337. https://doi.org/10.1108/JFC-03-2013-0014

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of research in crime and delinquency*, *50*(2), 216-238. https://doi.org/10.1177/0022427811425539

Rose, S., Hair, N., & Clark, M. (2011). Online customer experience: A review of the business-to-consumer online purchase context. *International Journal of Management Reviews*, *13*(1), 24-39. https://doi.org/10.1111/j.1468-2370.2010.00280.x

Roulston, K. (2013). Analysing Interviews. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 297-312). SAGE. https://doi.org/10.4135/9781446282243

Sade-Beck, L. (2004). Internet ethnography: Online and offline. *International journal of qualitative methods*, *3*(2), 45-51. https://doi.org/10.1177/160940690400300204

Semmelmann, K., & Weigelt, S. (2018). Online webcam-based eye tracking in cognitive science: A first look. *Behavior Research Methods*, *50*, 451-465. https://doi.org/10.3758/s13428-017-0913-7

Shang, Y., Wang, K., Tian, Y., Zhou, Y., Ma, B., & Liu, S. (2023). Theoretical basis and occurrence of internet fraud victimisation: Based on two systems in decision-making and reasoning. *Frontiers in Psychology*, *14*, 1087463. https://doi.org/10.3389/fpsyg.2023.1087463

Shokishalov, Z. H., & Wang, H. (2019). Applying eye tracking in information security. *Procedia Computer Science*, *150*, 347-351. https://doi.org/10.1016/j.procs.2019.02.062

Sistema de Segurança Interna. (2023). *Relatório Anual de Segurança Interna – Ano 2023*.

Sistema de Segurança Interna. (2025). *Relatório Anual de Segurança Interna – Ano 2025*.

Sofo, F., Berzins, M., Ammirato, S., & Volpentesta, A. P. (2010). Investigating the relationship between consumers' style of thinking and online victimization in scamming. *International Journal of Digital Content Technology and its Applications*, *4*(7), 38-49. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=35bca870c1581d1e129824b12940a42a795fc63a

Sun, L. S. (2002). The experiential dimensions of internet shopping: an ethnographic analysis of online store websites. *Asian Journal of Communication*, *12*(2), 79-99. https://doi.org/10.1080/01292980209364824

Sun, D., & Benson, M. L. (2022). Mixed Methods: A Justification, Explication, and Example. In R. Faria & M. Dodge (Eds.), *Qualitative Research in Criminology: Cutting-Edge Methods* (pp. 37-49). Springer. https://doi.org/10.1007/978-3-031-18401-7_3

Theodorou, A., Hatzithomas, L., Fotiadis, T., Diamantidis, A., & Gasteratos, A. (2023). The impact of the COVID-19 pandemic on online consumer behavior: applying the theory of planned behavior. *Sustainability*, *15*(3), 2545. https://doi.org/10.3390/su15032545

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency*, *41*(1), 54-72. https://doi.org/10.1177/0011128795041001004

Tobii Pro. (2021). *Pro Fusion User Manual*. Tobii Pro AB.

Trahan, A., & Stewart, D. M. (2013). Toward a Pragmatic Framework for Mixed-Methods Research in Criminal Justice and Criminology. *Applied Psychology in Criminal Justice*, *9*(1). https://dev.cjcenter.org/_files/apcj/apcjspring2013trahan.pdf_1368481261.pdf

Todorov, A., Chaiken, S., & Henderson, M. D. (2002). The heuristic-systematic model of social information processing. *The persuasion handbook: Developments in theory and practice*, *23*, 195-211. https://doi.org/10.4135/9781412976046.n11

van Dijk, T. A. (2009). Critical discourse studies: A sociocognitive approach. In R. Wodak & M. Meyer (Eds.), *Methods of Critical Discourse Analysis* (pp. 62-86). SAGE.

van Leeuwen, T. (2008). *Discourse and Pratice: New Tools for Crtitical Discourse Analysis*. Oxford University Press

van Wilsem, J. (2013). 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European sociological review*, *29*(2), 168-178. https://doi.org/10.1093/esr/jcr053

Venâncio, P. D. (2021). Tipos legais de crimes informáticos. In I. S. Guedes & M. A. M. Gomes (Eds.), *Cibercriminalidade: novos desafios, ofensas e soluções* (pp. 75-97). Pactor Editora.

Wall, D. (2001). Cybercrimes and the Internet. In D. Wall (Ed.), *Crime and the Internet* (pp. 1-17). Routledge.

Waqas, M., Hamzah, Z. L. B., & Salleh, N. A. M. (2021). Customer experience: a systematic literature review and consumer culture theory-based conceptualisation. *Management Review Quarterly*, *71*(1), 135-176. https://doi.org/10.1007/s11301-020-00182-w

Wheeldon, J. (Ed.). (2021). *Visual criminology: From history and methods to critique and policy translation*. Routledge.

Wheeldon, J., & Harris, D. (2015). Expanding visual criminology: Definitions, data and dissemination. *Current Issues in Criminal Justice*, *27*(2), 141-162. https://doi.org/10.1080/10345329.2015.12036038

Whittaker, J. M., Edwards, M., Cross, C., & Button, M. (2023). "I have only checked after the event": Consumer approaches to safe online shopping. *Victims & offenders*, *18*(7), 1259-1281. https://doi.org/10.1080/15564886.2022.2130486

Whittaker, J. M., McGuire, M. R., & Lazarus, S. (2025). Conversations with deviant website developers: A case study of online shopping fraud enablers. *Journal of Criminology*, 1-18. https://doi.org/10.1177/26338076251321844

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, *26*(3), 399-409. https://doi.org/10.1007/s10610-020-09458-z

Wilkes, N., Anderson, V. R., Johnson, C. L., & Bedell, L. M. (2021). Mixed methods research in criminology and criminal justice: A systematic review. *American journal of criminal justice*, 1-21. https://doi.org/10.1007/s12103-020-09593-7

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412-421. https://doi.org/10.1016/j.chb.2017.03.002

Willig, C. (2013). Discourses and Discourse Analysis. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 297-312). SAGE. https://doi.org/10.4135/9781446282243

Wincup, E. (2017). *Criminological research: Understanding qualitative methods*. SAGE.

Wong, W., Bartels, M., & Chrobot, N. (2014). Practical eye tracking of the ecommerce website user experience. In C. Stephanidis & M. Antona (Eds.), *Universal Access in Human-Computer Interaction: Design for All and Accessibility Practice* (pp. 109-118). Springer. https://doi.org/10.1007/978-3-319-07509-9_11

Yar, M. (2006). *Cybercrime and society* (1st ed.). SAGE Publications. https://dx.doi.org/10.4135/9781446212196

Zahari, A. I., Bilu, R., & Said, J. (2019). The role of familiarity, trust and awareness towards online fraud. *Journal of Research and Opinion*, *6*(9), 2470-2480. https://researchopinion.in/index.php/jro/article/view/23

***Fontes Legais***

Código Penal Português, Lei n.º 48/95, de 15 de março. (1995). Diário da República n.º 246, Série I de 2025-12-23. https://diariodarepublica.pt/dr/detalhe/lei/72-2025-992402106

Constituição da República Portuguesa, Lei Constitucional n.º 1/2005, de 12 de agosto, da Assembleia da República. (2005). Diário da República n.º 155, Série I-A de 2005-08-12. https://diariodarepublica.pt/dr/detalhe/lei-constitucional/1-2005-243729

Lei n.º 24/96, de 31 de julho, da Assembleia da República. (1996). Diário da República n.º 176, Série I-A de 1996-07-31. https://diariodarepublica.pt/dr/detalhe/lei/24-1996-406882

Lei n.º 109/2009, de 15 de setembro, da Assembleia da República. (2009). Diário da República n.º 179, Série I de 2009-09-15. https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693

Lei n.º 51/2023, de 28 de agosto, da Assembleia da República. (2023). Diário da República n.º 166, Série I de 2023-08-28. https://diariodarepublica.pt/dr/detalhe/lei/51-2023-220949538

Lei n.º 35/2026, de 27 de julho, da Assembleia da República. (2026). Diário da República n.º 143, Série I de 2026-07-27. https://diariodarepublica.pt/dr/detalhe/lei/35-2026-1152409208

Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho. (2022). Jornal Oficial da União Europeia de 2022-10-19. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/por

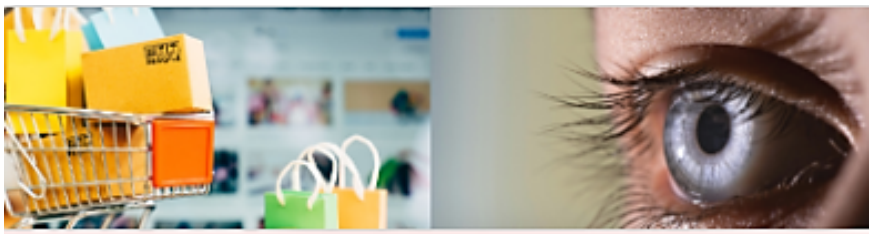
Regulamento (UE) 2026/382 do Conselho. (2026). Jornal Oficial da União Europeia de 2026-2-11. https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=OJ:L_202600382

# ANEXOS

**ANEXO A – *Flyer* para a Participação no Estudo**



## ANEXO B – Formulário de Inscrição no Estudo



# Inscrição no Estudo

O meu nome é Rúben Pinto e encontro-me a realizar a minha dissertação de Mestrado em Criminologia, na Faculdade de Direito da Universidade do Porto. Gostaria de o/a convidar a colaborar nas atividades da nossa investigação.

**Quais são as finalidades deste estudo?**

Pretendo compreender o comportamento visual e a intenção de compra em websites de comércio.

**Quem pode participar?**

Podem participar pessoas com idade igual ou superior a 18 anos e que nos últimos 12 meses realizaram pelo menos uma compra de produtos em websites de comércio (e.g., vestuário, equipamentos eletrónicos e informáticos, etc.).

Por motivos técnicos, não poderão participar indivíduos que tenham sido alvo de intervenções cirúrgicas oculares, nem que utilizam óculos com lentes bifocais.

**O que vai acontecer, onde e quanto tempo duram as atividades?**

Caso aceite colaborar, só precisa de visualizar um conjunto de imagens de websites de comércio (5 minutos) e participar numa entrevista (30 minutos aproximadamente)

Deve deslocar-se ao Laboratório da Escola de Criminologia da Faculdade de Direito da Universidade do Porto.

**Quais são as implicações da minha participação?**

A sua participação é voluntária e confidencial. Assim, poderá desistir a qualquer momento (sem nenhum prejuízo). Além disso, todos os dados recolhidos serão apenas utilizados para fins académicos e científicos, pelo que não serão recolhidas informações que permitam identificar a sua identificação. O estudo foi aprovado pela Comissão de Ética da Universidade do Porto no dia 5 de fevereiro de 2026.

Posteriormente, entraremos em contacto consigo para procedermos ao agendamento.

No caso de existirem dúvidas, poderá contactar-me através do seguinte e-mail: rpinto@direito.up.pt

Agradeço, desde já, a sua colaboração! A sua participação será fundamental e contribuirá para a produção de conhecimento científico.

Rúben Pinto

* Indica uma pergunta obrigatória

**1. Idade** *

Sua resposta

**2. E-mail de contacto** *

Sua resposta

**3. Nos últimos 12 meses, realizou uma ou mais compras de produtos em websites de comércio?** *

- ◯ Sim
- ◯ Não

**4. Foi alvo de intervenções cirúrgicas oculares ou utiliza óculos com lentes bifocais?** *

- ◯ Não
- ◯ Sim
- ◯ Outro:

**5. Selecione a semana que tem disponibilidade para participar** *

- ☐ Semana 09/03 - 13/03
- ☐ Semana 16/03 - 20/03
- ☐ Semana 23/03 - 27/03
- ☐ Semana 07/04 - 10/04
- ☐ Semana 13/04 - 17/04
- ☐ Semana 20/04 - 24/04
- ☐ Semana 27/04 - 01/05
- ☐ Semana 04/05 - 08/05
- ☐ Semana 11/05 - 15/05
- ☐ Semana 18/05 - 22/05

**6. Selecione o(s) dia(s) da semana mais conveniente(s) para si** *

- ☐ Segunda-feira
- ☐ Terça-feira
- ☐ Quarta-feira
- ☐ Quinta-feira
- ☐ Sexta-feira

**7. Selecione, pelo menos, dois horários mais convenientes para si** *

- [ ] 9h30
- [ ] 10h
- [ ] 10h30
- [ ] 11h
- [ ] 11h30
- [ ] 12h
- [ ] 12h30
- [ ] 13h30
- [ ] 14h
- [ ] 14h30
- [ ] 15h
- [ ] 15h30
- [ ] 16h
- [ ] 16h30
- [ ] 17h
- [ ] 17h30
- [ ] 18h
- [ ] 18h30

**8. Caso considere relevante, indique outras informações**

Sua resposta

**ANEXO C – Termo de Consentimento Informado**

Exmo/a. Participante,

Eu, Rúben Pinto, encontro-me a realizar uma investigação científica na Faculdade de Direito da Universidade do Porto, no âmbito do Mestrado em Criminologia, em que procuro compreender o comportamento visual e a intenção de compra nos *websites* de comércio.

Concretamente, pretende-se compreender se existem diferenças nos padrões visuais e nas intenções de compra dos indivíduos através da visualização, por meio de técnicas *eye-tracking*, de um conjunto de imagens de *websites* de comércio (5 minutos) e da participação numa entrevista (30 minutos aproximadamente).

Importa salientar que a sua participação é totalmente voluntária, pelo que poderá aceitar ou recusar participar e, no primeiro caso, poderá desistir a qualquer momento, sem prejuízo de qualquer natureza.

Por fim, todos os dados recolhidos serão armazenados de forma segura e protegidos por palavra-passe. Estas informações serão confidenciais e anónimas, pelo que serão apenas utilizadas para fins académicos e não serão recolhidos dados de identificação pessoal como, por exemplo, o seu nome.

Agradeço a sua colaboração,

_____

Depois de receber as informações acima referidas, declaro que:

i) Li e compreendi a informação presente neste documento, ficando esclarecido sobre os objetivos e condições da investigação;

ii) Pude realizar perguntas para ficar elucidado acerca de outras particularidades;

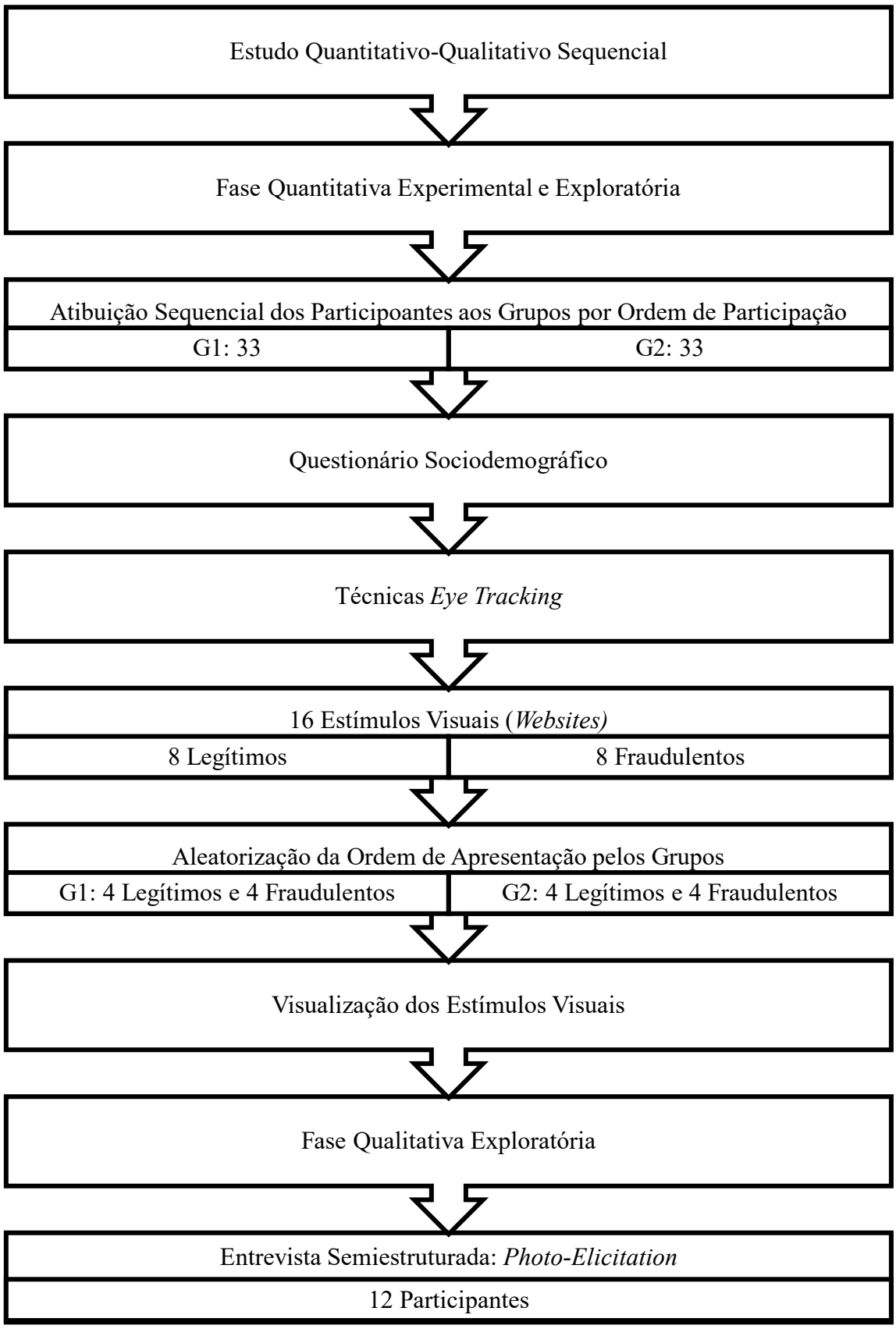
iii) Sou capaz de tomar esta decisão;

iv) Autorizo a gravação áudio da entrevista (assinalar com X a opção)
[ ] Sim [ ] Não

Data: _____

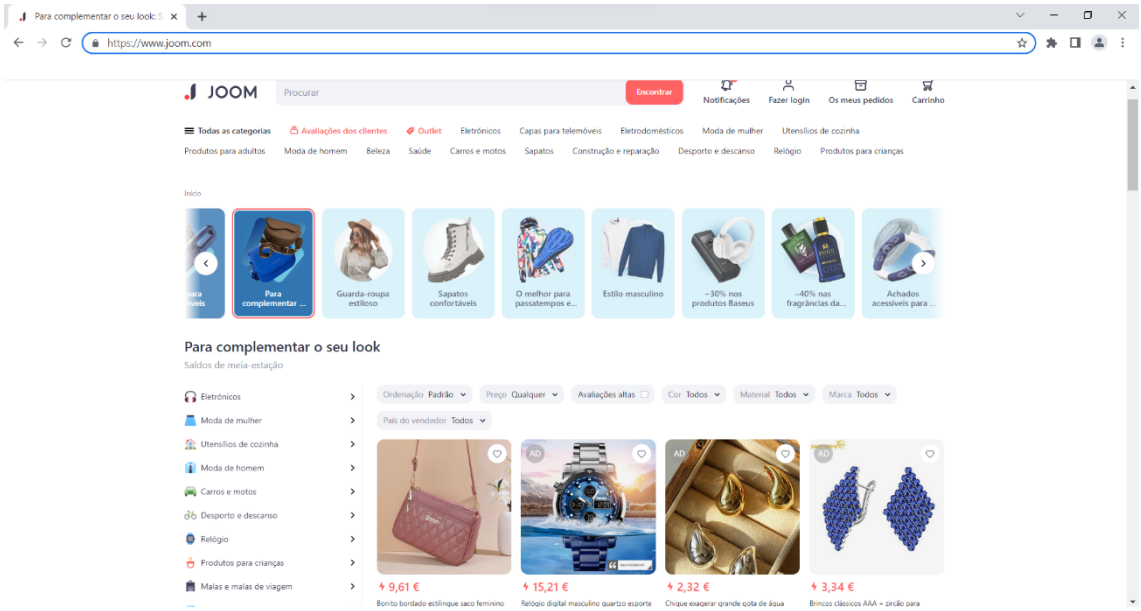
Assinatura/Rubrica do Participante: _____

**ANEXO D – Protocolo de Recolha de Dados**

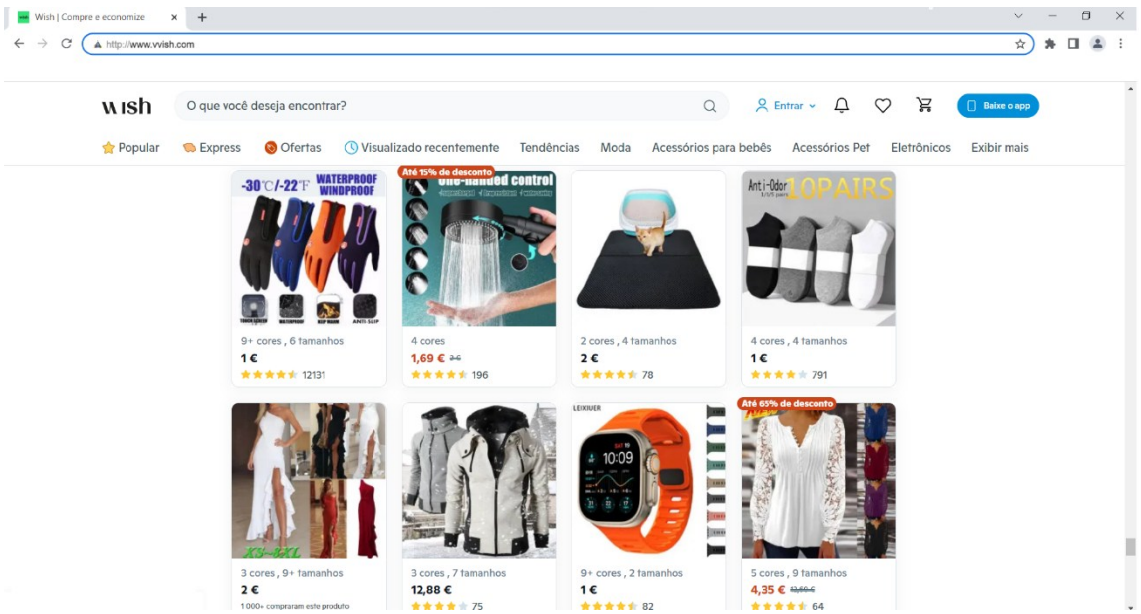


## ANEXO E – Grupo 1 de *Websites*

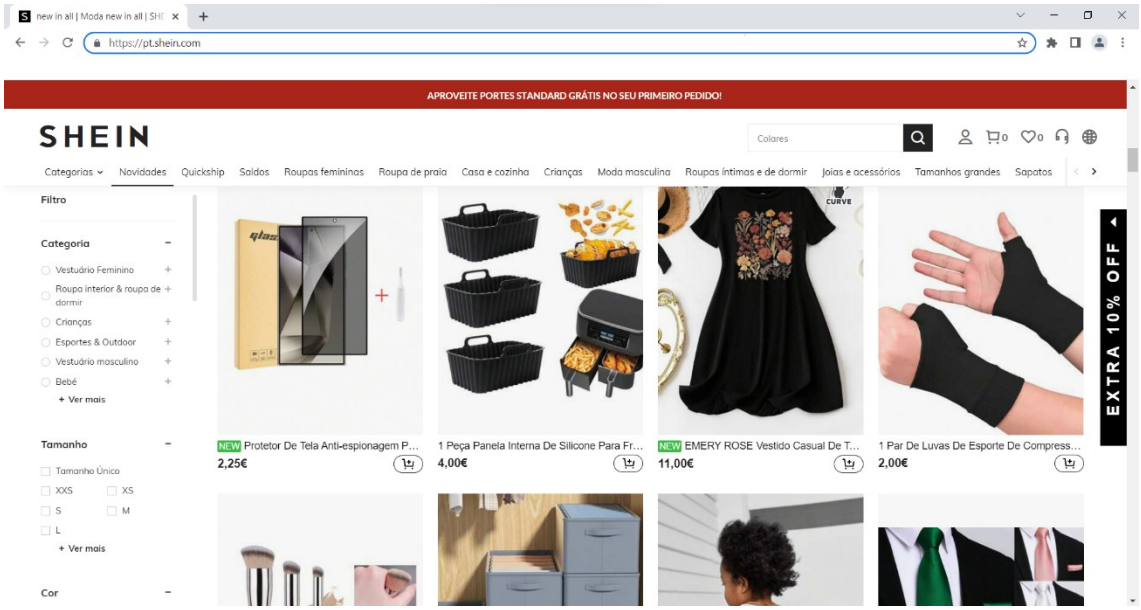
| L1 |
|---|



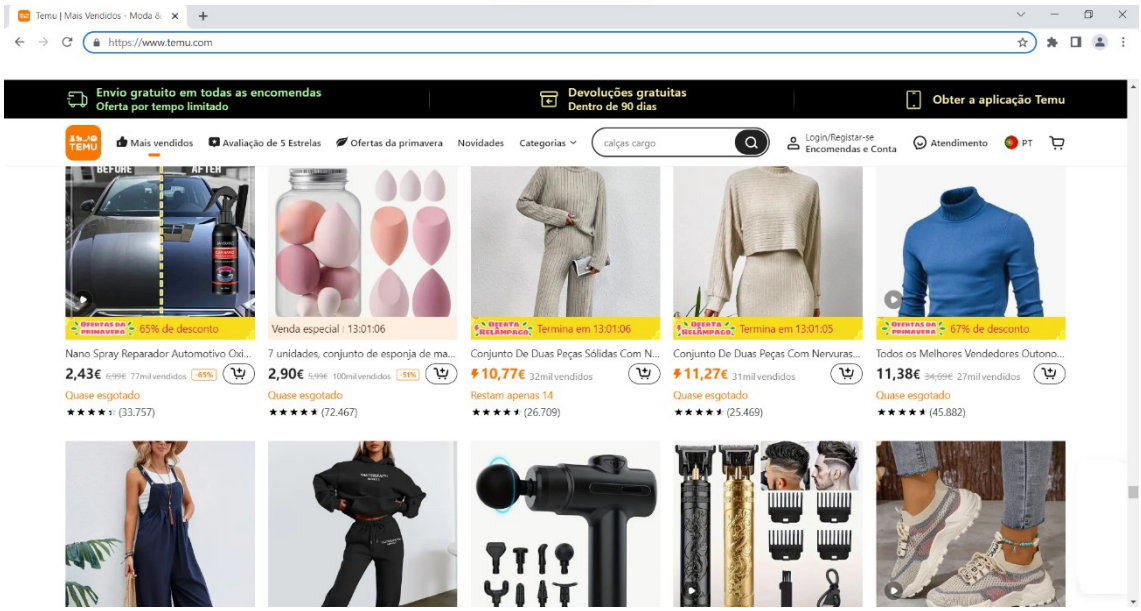

| F2 |
|---|



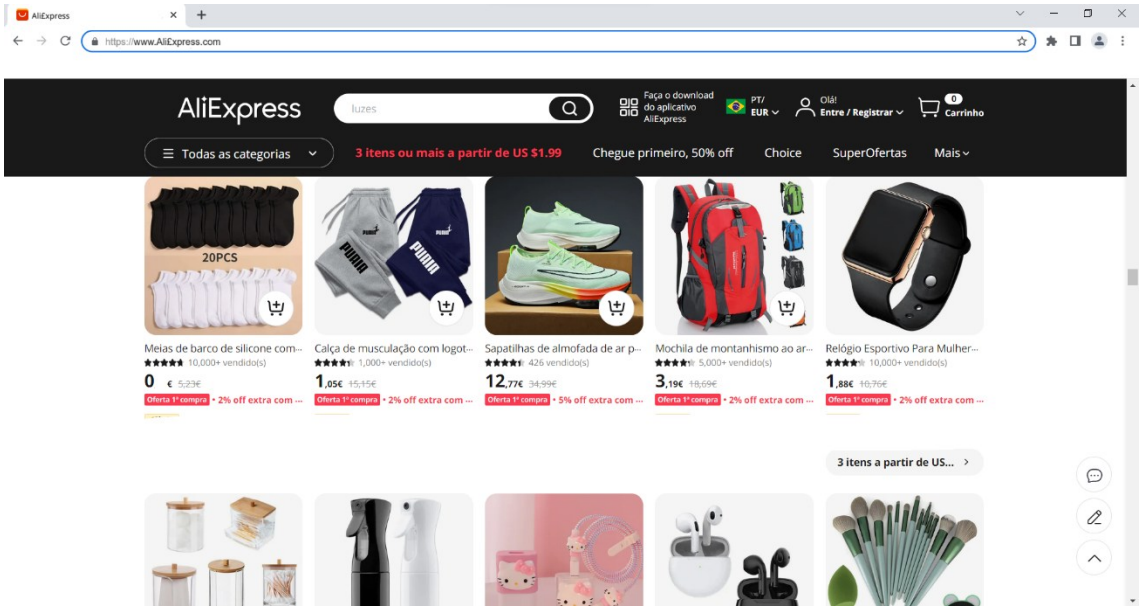
## L3


https://pt.shein.com
APROVEITE PORTES STANDARD GRÁTIS NO SEU PRIMEIRO PEDIDO!
SHEIN
Categorias
Novidades
Quickship
Saldos
Roupas femininas
Roupa de praia
Casa e cozinha
Crianças
Moda masculina
Roupas íntimas e de dormir
Joias e acessórios
Tamanhos grandes
Sapatos
Filtro
Categoria
Vestuário Feminino
Roupa interior & roupa de dormir
Crianças
Esportes & Outdoor
Vestuário masculino
Bebé
+ Ver mais
Tamanho
Tamanho Único
XXS
XS
S
M
L
+ Ver mais
Cor
NEW Protetor De Tela Anti-espionagem P...
2,25€
1 Peça Panela Interna De Silicone Para Fr...
4,00€
NEW EMERY ROSE Vestido Casual De T...
11,00€
1 Par De Luvas De Esporte De Compress...
2,00€
EXTRA 10% OFF

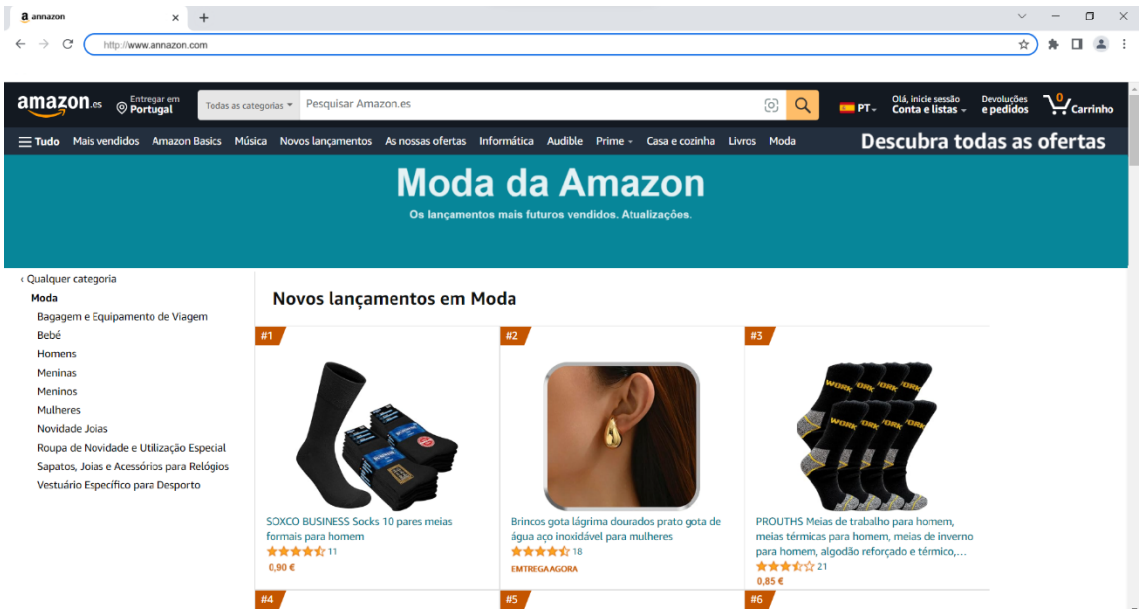
## L4


https://www.temu.com
Envio gratuito em todas as encomendas
Oferta por tempo limitado
Devoluções gratuitas
Dentro de 90 dias
Obter a aplicação Temu
Mais vendidos
Avaliação de 5 Estrelas
Ofertas da primavera
Novidades
Categorias
calças cargo
Login/Registar-se
Encomendas e Conta
Atendimento
PT
65% de desconto
Nano Spray Reparador Automotivo Oxi...
2,43€
Quase esgotado
(33.757)
Venda especial | 13:01:06
7 unidades, conjunto de esponja de ma...
2,90€
Quase esgotado
(72.467)
Termina em 13:01:06
Conjunto De Duas Peças Sólidas Com N...
10,77€
32mil vendidos
Restam apenas 14
(26.709)
Termina em 13:01:05
Conjunto De Duas Peças Com Nervuras...
11,27€
31mil vendidos
Quase esgotado
(25.469)
67% de desconto
Todos os Melhores Vendedores Outono...
11,38€
27mil vendidos
Quase esgotado
(45.882)

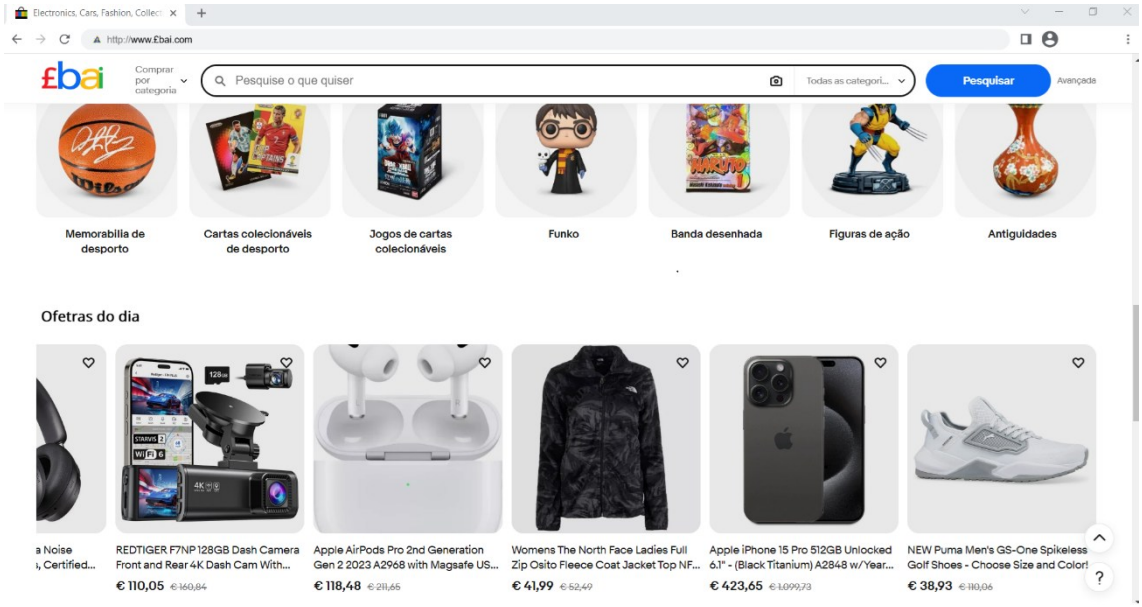
## F5


AliExpress
https://www.AliExpress.com
AliExpress
luzes
Faça o download do aplicativo AliExpress
PT/ EUR
Olá! Entre / Registrar
Carrinho
Todas as categorias
3 itens ou mais a partir de US $1.99
Chegue primeiro, 50% off
Choice
SuperOfertas
Mais
20PCS
Meias de barco de silicone com...
Calça de musculação com logot...
Sapatilhas de almofada de ar p...
Mochila de montanhismo ao ar...
Relógio Esportivo Para Mulher...
3 itens a partir de US...

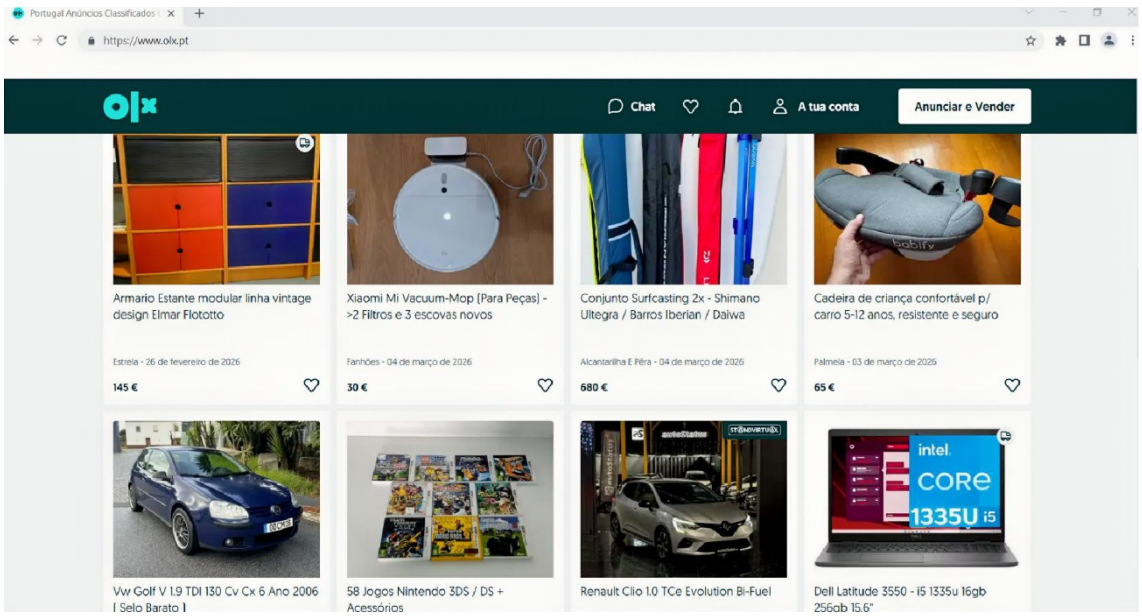
## F6


annazon
http://www.annazon.com
amazon.es
Entregar em Portugal
Todas as categorias
Pesquisar Amazon.es
PT
Olá, inicie sessão Conta e listas
Devoluções e pedidos
Carrinho
Tudo
Mais vendidos
Amazon Basics
Música
Novos lançamentos
As nossas ofertas
Informática
Audible
Prime
Casa e cozinha
Livros
Moda
Descubra todas as ofertas
Moda da Amazon
Os lançamentos mais futuros vendidos. Atualizações.
‹ Qualquer categoria
Moda
Bagagem e Equipamento de Viagem
Bebé
Homens
Meninas
Meninos
Mulheres
Novidade Joias
Roupa de Novidade e Utilização Especial
Sapatos, Joias e Acessórios para Relógios
Vestuário Específico para Desporto
Novos lançamentos em Moda
#1
SOXCO BUSINESS Socks 10 pares meias formais para homem
0,90 €
#2
Brincos gota lágrima dourados prato gota de água aço inoxidável para mulheres
EMTREGAAGORA
#3
PROUTHS Meias de trabalho para homem, meias térmicas para homem, meias de inverno para homem, algodão reforçado e térmico,...
0,85 €
#4
#5
#6

## F7

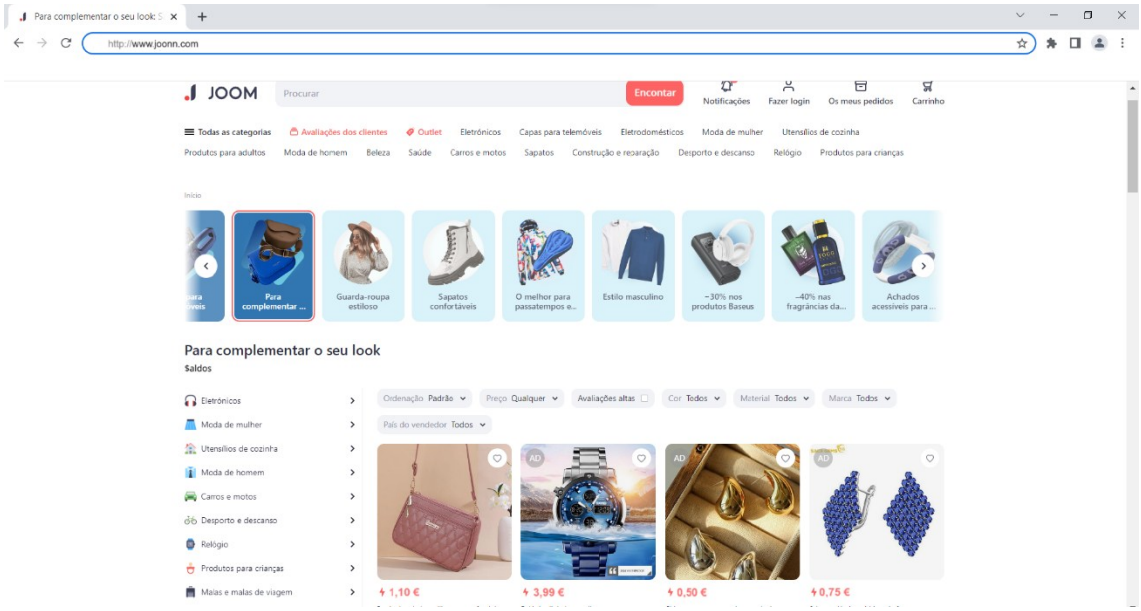

Electronics, Cars, Fashion, Collect
http://www.£bai.com
£bai
Comprar por categoria
Pesquise o que quiser
Todas as categori...
Pesquisar
Avançada
Memorabilia de desporto
Cartas colecionáveis de desporto
Jogos de cartas colecionáveis
Funko
Banda desenhada
Figuras de ação
Antiguidades
Ofetras do dia
a Noise
, Certified...
REDTIGER F7NP 128GB Dash Camera Front and Rear 4K Dash Cam With...
€ 110,05 € 160,84
Apple AirPods Pro 2nd Generation Gen 2 2023 A2968 with Magsafe US...
€ 118,48 € 211,65
Womens The North Face Ladies Full Zip Osito Fleece Coat Jacket Top NF...
€ 41,99 € 52,49
Apple iPhone 15 Pro 512GB Unlocked 6.1" - (Black Titanium) A2848 w/Year...
€ 423,65 € 1.099,73
NEW Puma Men's GS-One Spikeless Golf Shoes - Choose Size and Color!
€ 38,93 € 110,06

## L8

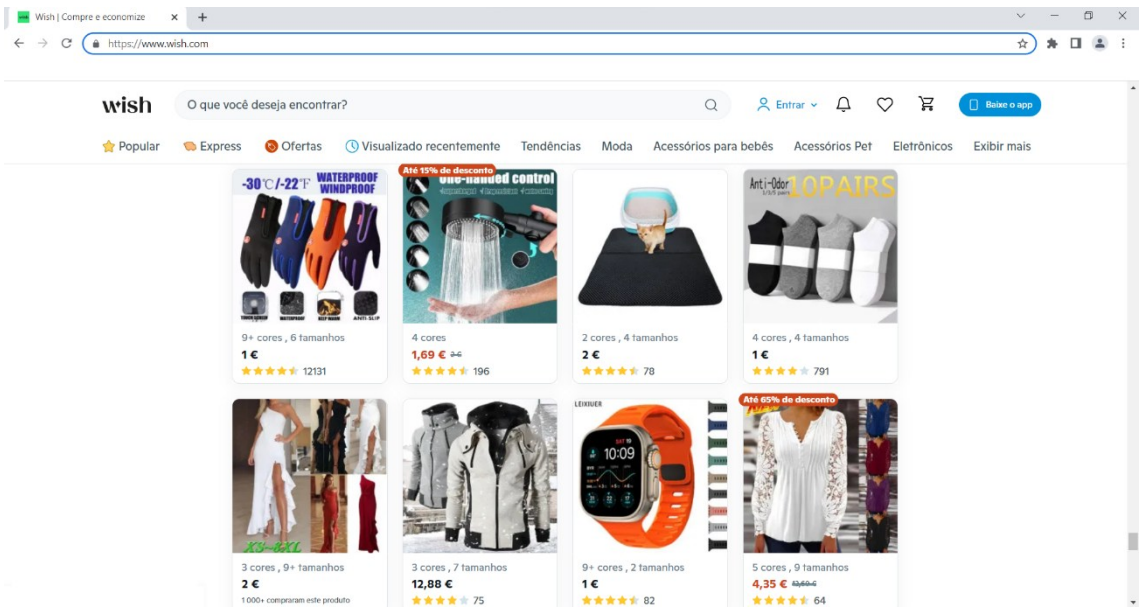

Portugal Anúncios Classificados
https://www.olx.pt
olx
Chat
A tua conta
Anunciar e Vender
Armario Estante modular linha vintage design Elmar Flototto
Estrela - 26 de fevereiro de 2026
145 €
Xiaomi Mi Vacuum-Mop [Para Peças] - >2 Filtros e 3 escovas novos
Fanhões - 04 de março de 2026
30 €
Conjunto Surfcasting 2x - Shimano Ultegra / Barros Iberian / Daiwa
Alcantarilha E Pêra - 04 de março de 2026
680 €
Cadeira de criança confortável p/ carro 5-12 anos, resistente e seguro
Palmela - 03 de março de 2026
65 €
Vw Golf V 1.9 TDI 130 Cv Cx 6 Ano 2006 | Selo Barato |
58 Jogos Nintendo 3DS / DS + Acessórios
Renault Clio 1.0 TCe Evolution Bi-Fuel
Dell Latitude 3550 - i5 1335u 16gb 256gb 15.6"
intel.
CORE
1335U i5

## ANEXO F – Grupo 2 de *Websites*

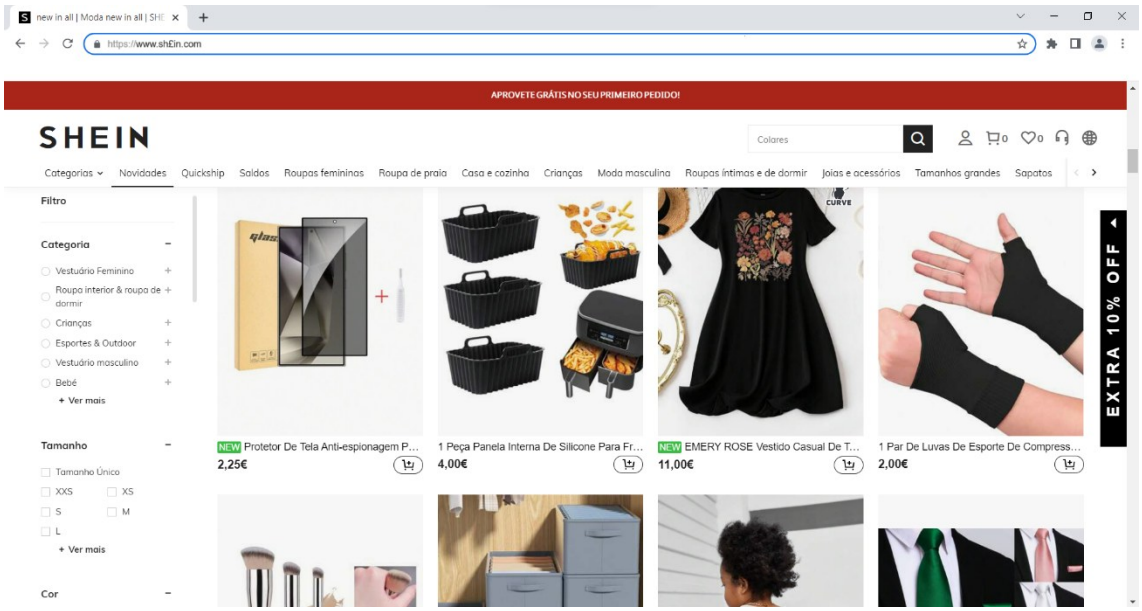
| F1 |
|---|



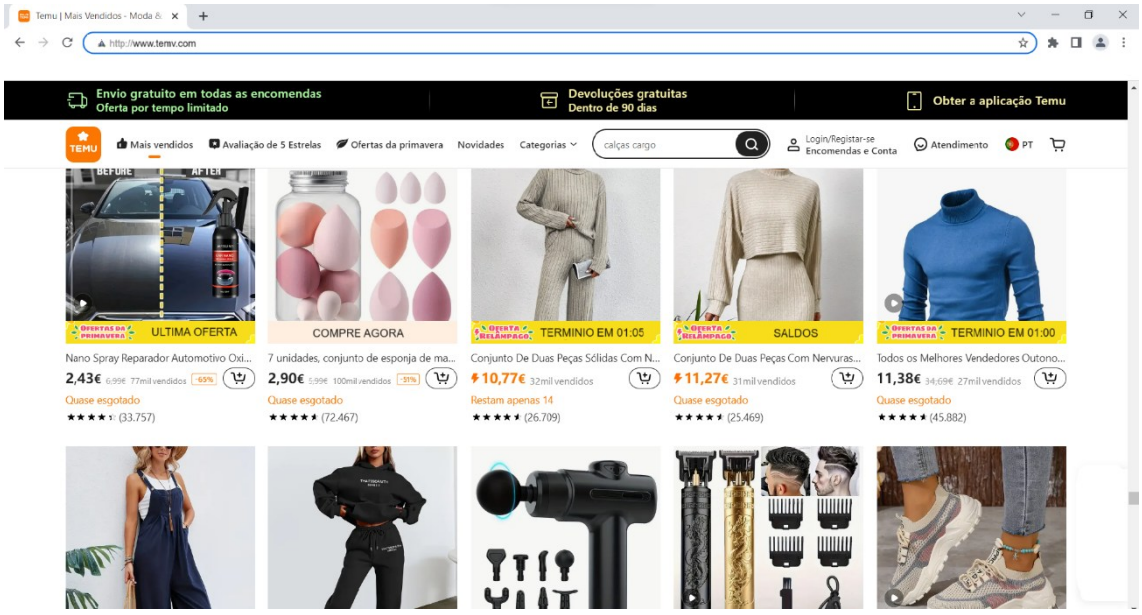

| L2 |
|---|



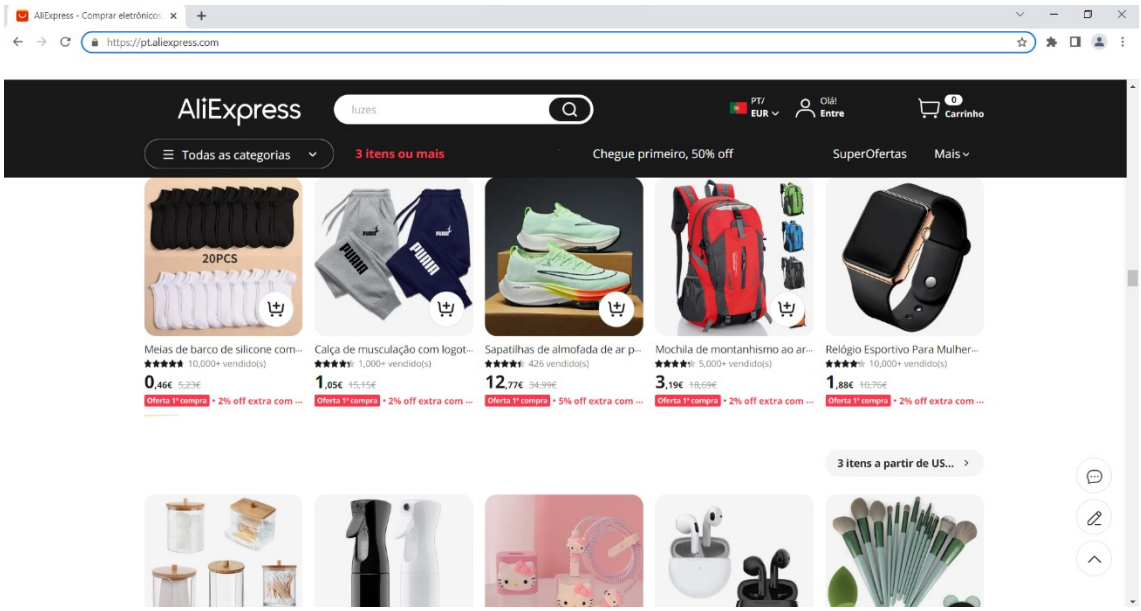
## F3


APROVETE GRÁTIS NO SEU PRIMEIRO PEDIDO!
SHEIN
Categorias
Novidades
Quickship
Saldos
Roupas femininas
Roupa de praia
Casa e cozinha
Crianças
Moda masculina
Roupas íntimas e de dormir
Joias e acessórios
Tamanhos grandes
Sapatos
Filtro
Categoria
Tamanho
Cor
EXTRA 10% OFF
2,25€
4,00€
11,00€
2,00€

## F4


Envio gratuito em todas as encomendas
Oferta por tempo limitado
Devoluções gratuitas
Dentro de 90 dias
Obter a aplicação Temu
Mais vendidos
Avaliação de 5 Estrelas
Ofertas da primavera
Novidades
Categorias
ULTIMA OFERTA
COMPRE AGORA
TERMINIO EM 01:05
SALDOS
TERMINIO EM 01:00
2,43€
2,90€
10,77€
11,27€
11,38€
Quase esgotado
Restam apenas 14

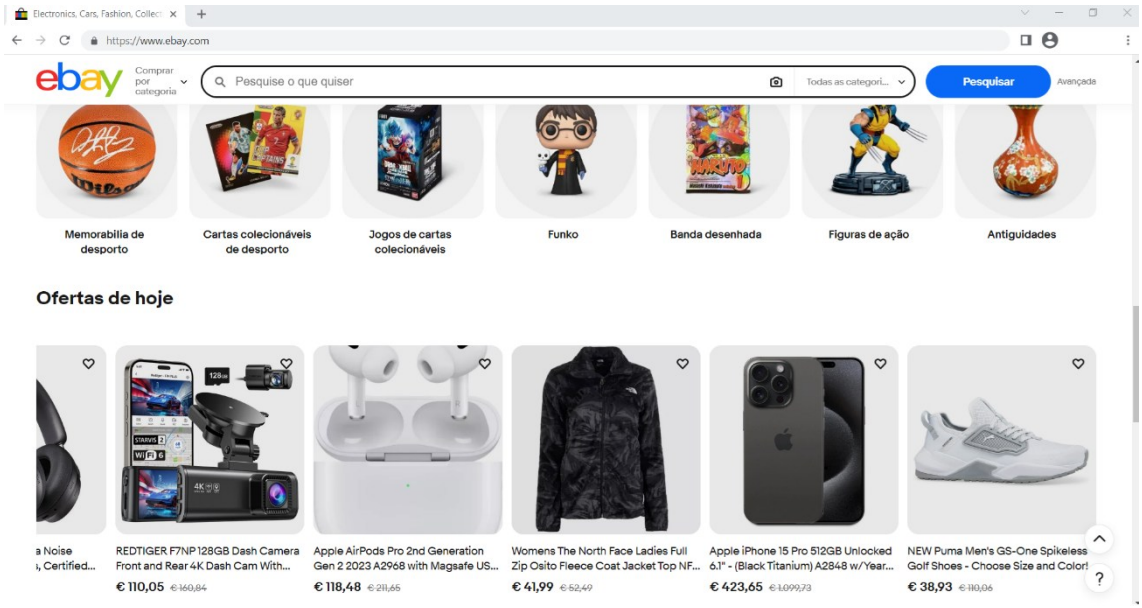
## L5


AliExpress - Comprar eletrónicos
https://pt.aliexpress.com
AliExpress
luzes
PT/ EUR
Olá! Entre
Carrinho
Todas as categorias
3 itens ou mais
Chegue primeiro, 50% off
SuperOfertas
Mais
20PCS
Meias de barco de silicone com...
Calça de musculação com logot...
Sapatilhas de almofada de ar p...
Mochila de montanhismo ao ar...
Relógio Esportivo Para Mulher...
0,46€ 5,23€
1,05€ 15,15€
12,77€ 34,99€
3,19€ 18,69€
1,88€ 10,76€
Oferta 1ª compra • 2% off extra com ...
Oferta 1ª compra • 5% off extra com ...
3 itens a partir de US...

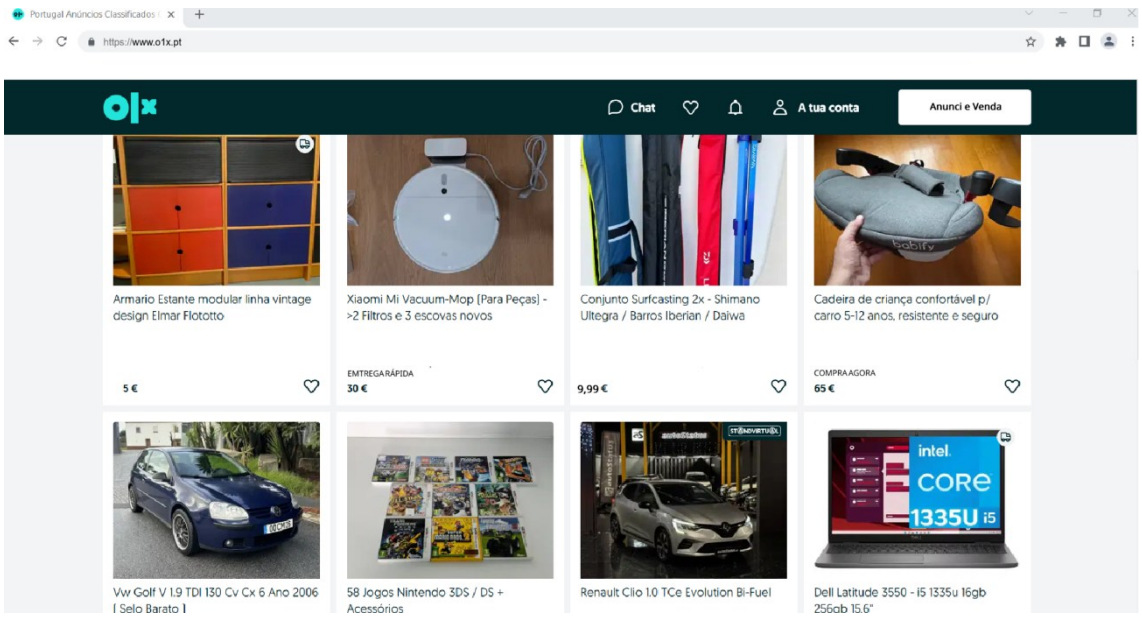
## L6


Amazon.es Novos lançamentos:
https://www.amazon.es
amazon.es
Entregar em Portugal
Todas as categorias
Pesquisar Amazon.es
PT
Olá, inicie sessão Conta e listas
Devoluções e pedidos
Carrinho
Tudo
Mais vendidos
Amazon Basics
Música
Novos lançamentos
As nossas ofertas
Informática
Audible
Prime
Casa e cozinha
Livros
Moda
Descubra todas as ofertas
Novos lançamentos da Amazon
Os nossos novos e futuros lançamentos mais vendidos. Atualizado com frequência.
‹ Qualquer categoria
Moda
Bagagem e Equipamento de Viagem
Bebé
Homens
Meninas
Meninos
Mulheres
Novidade Joias
Roupa de Novidade e Utilização Especial
Sapatos, Joias e Acessórios para Relógios
Vestuário Específico para Desporto
Novos lançamentos em Moda
#1
SOXCO BUSINESS Socks 10 pares meias formais para homem
15,69 €
#2
Brincos gota lágrima dourados prato gota de água aço inoxidável para mulheres
12,99 €
#3
PROUTHS Meias de trabalho para homem, meias térmicas para homem, meias de inverno para homem, algodão reforçado e térmico,...
10,16 €
#4
#5
#6

## L7


https://www.ebay.com
Pesquise o que quiser
Pesquisar
Memorabilia de desporto
Cartas colecionáveis de desporto
Jogos de cartas colecionáveis
Funko
Banda desenhada
Figuras de ação
Antiguidades
Ofertas de hoje
REDTIGER F7NP 128GB Dash Camera Front and Rear 4K Dash Cam With...
€ 110,05 € 160,84
Apple AirPods Pro 2nd Generation Gen 2 2023 A2968 with Magsafe US...
€ 118,48 € 211,65
Womens The North Face Ladies Full Zip Osito Fleece Coat Jacket Top NF...
€ 41,99 € 52,49
Apple iPhone 15 Pro 512GB Unlocked 6.1" - (Black Titanium) A2848 w/Year...
€ 423,65 € 1.099,73
NEW Puma Men's GS-One Spikeless Golf Shoes - Choose Size and Color!
€ 38,93 € 110,06

## F8


https://www.olx.pt
Chat
A tua conta
Anunci e Venda
Armario Estante modular linha vintage design Elmar Flototto
5 €
Xiaomi Mi Vacuum-Mop [Para Peças] - >2 Filtros e 3 escovas novos
ENTREGA RÁPIDA
30 €
Conjunto Surfcasting 2x - Shimano Ultegra / Barros Iberian / Daiwa
9,99 €
Cadeira de criança confortável p/ carro 5-12 anos, resistente e seguro
COMPRA AGORA
65 €
Vw Golf V 1.9 TDI 130 Cv Cx 6 Ano 2006 | Selo Barato |
58 Jogos Nintendo 3DS / DS + Acessórios
Renault Clio 1.0 TCe Evolution Bi-Fuel
Dell Latitude 3550 - i5 1335u 16gb 256gb 15.6"

**ANEXO G – Estratégias de Manipulação dos *Websites***

| Grupo | *Website* | Código | Manipulações |
|---|---|---|---|
| 2 | *Joom* | F1 | Alteração do Certificado Digital (“http://”)<br>Alteração do Nome de Domínio (“www.joonn.com”)<br>Ausência do Cadeado de Segurança<br>Redução dos Preços<br>Erros Ortográficos (“$aldos”) |
| 1 | *Wish* | F2 | Logótipo Falso<br>Símbolo de Ligação Insegura<br>Alteração do Certificado Digital (“http://”)<br>Alteração do Nome de Domínio (“www.vvish.com”)<br>Erros Gramaticais (“Baixe a app”) |
| 2 | *Shein* | F3 | Alteração do Nome de Domínio (“www.sh£in.com”)<br>Erros Ortográficos e Gramaticais (“Aprovete”) |
| 2 | *Temu* | F4 | Logótipo Falso<br>Símbolo de Ligação Insegura<br>Alteração do Certificado Digital (“http://”)<br>Alteração do Nome de Domínio (“www.temv.com”)<br>Erros Ortográficos (“Terminio”) |
| 1 | *AliExpress* | F5 | Alteração do Nome de Domínio (“www.Ali£xpress.com”)<br>Erro Idioma (“PT” e símbolo do Brasil)<br>Redução dos Preços |
| 1 | *Amazon* | F6 | Ausência do Cadeado de Segurança<br>Alteração do Certificado Digital (“http://”)<br>Alteração do Nome de Domínio (“www.annazon.com”)<br>Redução dos Preços<br>Erros Ortográficos e Gramaticais (“EMTREGA” e “lançamentos mais futuros vendidos”) |
| 1 | *eBay* | F7 | Logótipo Falso<br>Símbolo de Ligação Insegura<br>Alteração do Certificado Digital (“http://”)<br>Alteração do Nome de Domínio (“www.£bai.com”) |
| 2 | OLX | F8 | Alteração do Nome de Domínio (“www.o1x.pt”)<br>Redução dos Preços<br>Erros Ortográficos (“EMTREGA” e “Anunci”) |

**ANEXO H – Guião de Entrevista Semiestruturada**

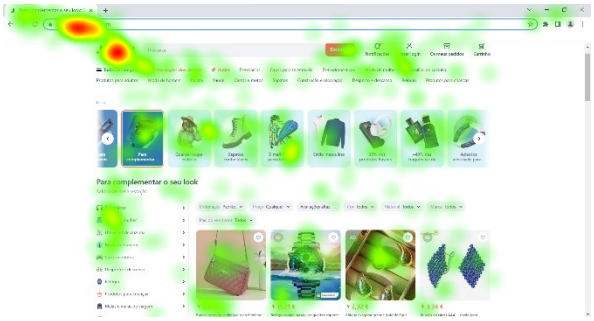
<table>
<tr><th colspan="4">Guião de Entrevista Semiestruturada</th></tr>
<tr><td colspan="4">Participante:<br>Data:<br>Duração:</td></tr>
<tr><td colspan="4">Caro/a Participante,<br>Em primeiro lugar, agradeço a sua disponibilidade para participar nesta entrevista.<br>Como referido anteriormente, sou estudante de Mestrado em Criminologia na Faculdade de Direito da Universidade do Porto e encontro-me a realizar um estudo sobre o comportamento visual e a intenção de compra nos websites de comércio.<br>Esta entrevista enquadra-se na metodologia selecionada para a investigação que tem como principal objetivo explorar os significados que atribui ao comércio online e aos elementos visuais dos websites de comércio. Para tal, abordarei a sua experiência ao visualizar as imagens dos websites.<br>Como mencionado anteriormente no termo de consentimento informado, a sua participação é totalmente voluntária, pelo que poderá retirar-se a qualquer momento sem nenhuma consequência e não tem obrigação de responder a todas as questões, apenas as que se sentir confortável.<br>Para efeitos de tratamento de dados, informo que esta entrevista será gravada, se assim autorizar, e posteriormente analisada. Realço que a gravação pode ser interrompida a qualquer momento se assim entender. Para garantir a sua segurança, a informação será tratada de forma anónima. Importa, ainda, referir que toda a informação partilhada será confidencial e apenas utilizada para fins académicos, pelo que algum material (e.g., gravações áudio) será eliminado após a conclusão do estudo.</td></tr>
<tr><td colspan="4">Antes de iniciarmos a entrevista, gostaria de perceber se tem alguma dúvida.<br>Com todas as informações esclarecidas, começo por questionar: Como é que descreve as tarefas de eye-tracking?<br>Obrigado pela partilha!</td></tr>
<tr><th>Dimensões</th><th>Subdimensões</th><th>Questões</th><th>Questões Follow-up</th></tr>
<tr><td rowspan="2">I. Experiências Prévias nos Websites de Comércio</td><td rowspan="2">Diferenças Online-Offline<br>Experiências e Familiaridade<br>Cultura de Consumo Online</td><td>1. Na sua opinião, o que difere o comércio online do comércio em lojas físicas?</td><td>a. O que costuma comprar nos websites de comércio? E para que fins?<br>b. Que meios de pagamento utiliza? Porquê?</td></tr>
<tr><td>2. Recordando os últimos meses, como descreve as suas experiências nos websites de comércio?</td><td>a. Qual é o papel dos websites de comércio no seu dia-a-dia?<br>b. De que forma as opiniões de outras pessoas acerca dos websites influenciam as suas compras online?</td></tr>
<tr><td colspan="4">PHOTO-ELICITATION – 2 IMAGENS<br>Agora peço que observe estas duas imagens de websites já visualizados</td></tr>
<tr><td></td><td></td><td>3. Ao observar as imagens, quais foram os elementos visuais que associou aos websites seguros?</td><td>a. Considerando o mapa de calor neste website, poderia descrever as razões que o/a levaram a olhar para estas áreas mais escuras?</td></tr>
</table>

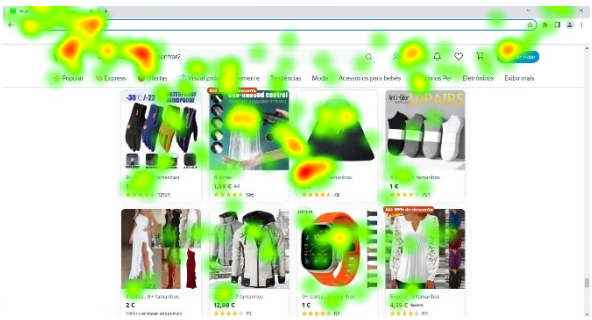
| | | | |
|---|---|---|---|
| **II. Perceções e Significados atribuídos aos *Websites* Visualizados** | Segurança<br>Legitimidade<br>Confiança | | b. O que o/a levaria a fornecer os seus dados pessoais ou bancários nos *websites*? |
| | | 4. O que é que o/a levou a confiar nos *websites*? | a. O que é que o/a deixou desconfiado nos *websites*?<br>b. Quais foram as semelhanças (ou diferenças) que encontrou entre o aspeto visual destes *websites* e outros em que realizou compras?<br>c. O que considerou mais atrativo? |
| **III. Riscos Percebidos e Cibervitimação** | Tipos de Riscos<br>Experiências de Cibervitimação<br>Literacia Digital | 5. Quais são os riscos que associa às compras nos *websites*? | a. De que forma esses riscos afetam a sua intenção de compra nos *websites*?<br>b. Alguma vez foi enganado/a quando fazia compras em *websites*? Se sim, pode-me contar?<br>c. Que comportamentos adota para evitar ser enganado nos *websites* de comércio?<br>d. O que faria se fosse enganado ao realizar compras nos *websites*? |
| **IV. Recomendações** | Mudanças nos *Websites*<br>Conselhos Interpessoais | 6. O que poderia ser alterado nos *websites* de comércio para aumentar a confiança? | a. O que gostaria de aconselhar a quem realiza compras nos websites de comércio? |
| Para concluir, no futuro, o que poderá influenciar as suas compras nos *websites* de comércio?<br><br>Antes de concluirmos a entrevista, gostaria de lhe perguntar se existe mais alguma informação que considere relevante mencionar.<br><br>Muito obrigado pela sua colaboração! Acredito que o seu contributo enriquecerá este estudo. | | | |

## ANEXO I – Mapas de Calor dos *Websites* Legítimos e Fraudulentos

| *Websites* Legítimos |
|---|

L1

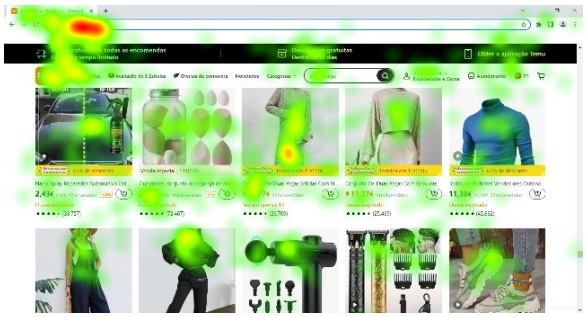


L2

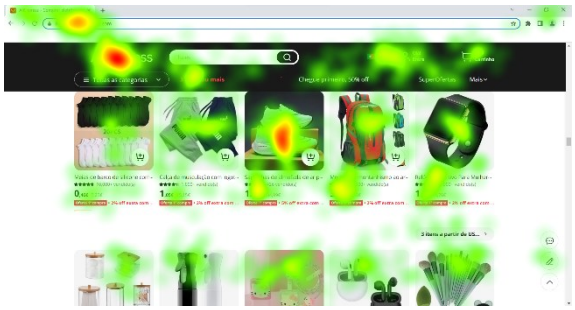
L3

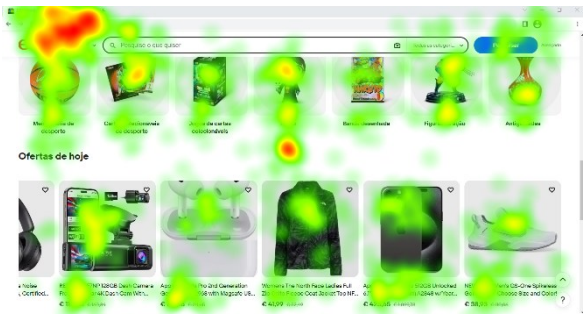


L4

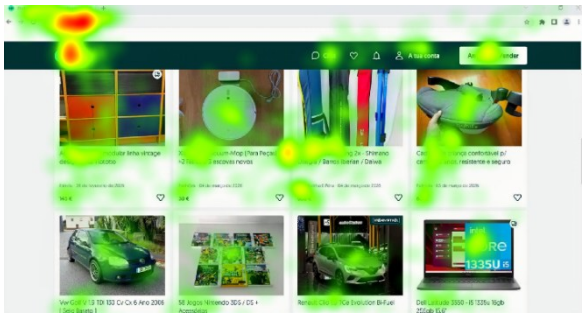
L5





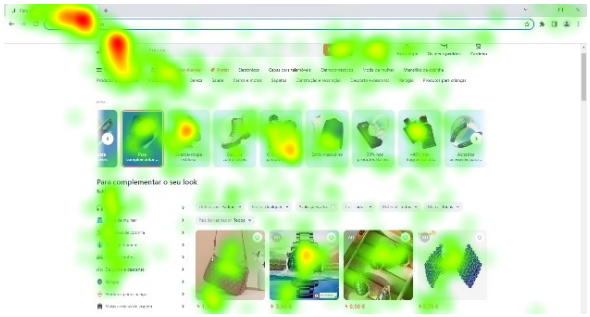

L7

L8

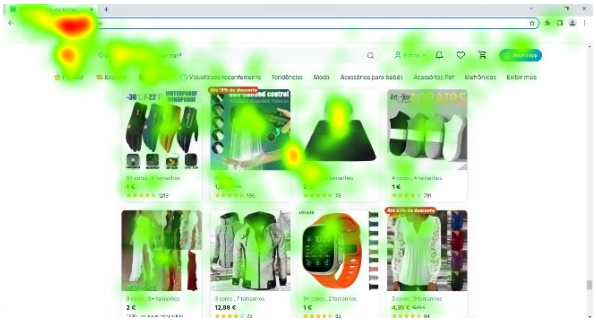


## *Websites* Fraudulentos

F1



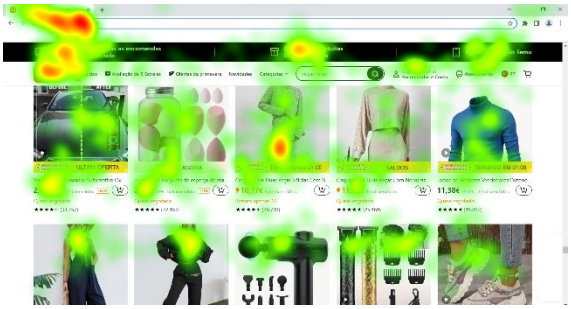

F2



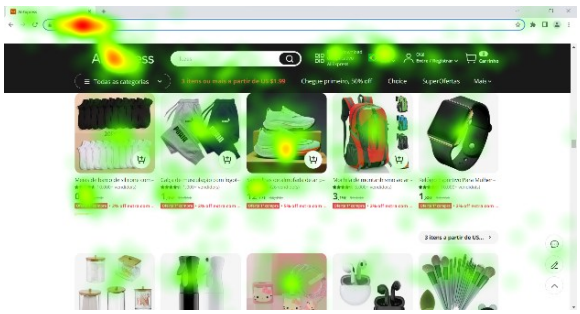
F3



F4



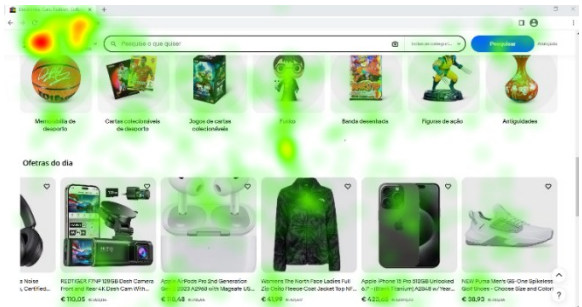
F5



F6




F7



## ANEXO J – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI de cada *Website* Fraudulento

| | Não Suscetíveis | Suscetíveis | p |
|---|---|---|---|
| | M ± SD | M ± SD | |
| Duração Média das Fixações (ms) | | | |
| F1 | | | |
| Área do Utilizador | .30 ± .30 | .26 ± .30 | .619 |
| Produtos Comerciais | .88 ± 1.24 | 1.90 ± 1.38 | **.023** |
| Marca | .30 ± .26 | .28 ± .24 | .953 |
| URL | .58 ± .65 | .14 ± .47 | **.023** |
| Informação Comercial | .00 ± .00 | .01 ± .04 | .736 |
| Pesquisa | 2.85 ± 1.71 | 4.22 ± 1.44 | **.044** |
| Pistas Fraudulentas | .05 ± .10 | .01 ± .04 | .564 |
| F2 | | | |
| Área do Utilizador | .21 ± .20 | .11 ± .17 | .145 |
| Produtos Comerciais | 2.80 ± 1.84 | 5.45 ± 1.63 | **<.001** |
| Marca | .74 ± .51 | .34 ± .43 | **.027** |
| URL | 1.96 ± 1.35 | .16 ± .35 | **<.001** |
| Informação Comercial | .17 ± .24 | .12 ± .20 | .708 |
| Pesquisa | .98 ± .60 | .99 ± .87 | .580 |
| Pistas Fraudulentas | .17 ± .24 | .12 ± .20 | .708 |
| F3 | | | |
| Área do Utilizador | .06 ± .09 | .07 ± .16 | .827 |
| Produtos Comerciais | 1.99 ± 1.42 | 4.86 ± 1.87 | **<.001** |
| Marca | .38 ± .34 | .29 ± .32 | .437 |
| URL | 1.16 ± 1.18 | .06 ± .12 | **.002** |
| Informação Comercial | .09 ± .12 | .15 ± .24 | .827 |
| Pesquisa | 1.13 ± .63 | 1.05 ± .87 | .592 |
| Pistas Fraudulentas | .09 ± .19 | .08 ± .14 | .890 |
| F4 | | | |
| Área do Utilizador | .13 ± .28 | .18 ± .23 | .437 |
| Produtos Comerciais | 2.39 ± 2.10 | 5.47 ± 1.64 | **<.001** |
| Marca | .11 ± .16 | .13 ± .16 | .827 |
| URL | 1.22 ± .99 | .15 ± .29 | **.003** |
| Informação Comercial | 1.09 ± 1.07 | .82 ± .83 | .648 |
| Pesquisa | .27 ± .24 | .44 ± .47 | .414 |
| Pistas Fraudulentas | .04 ± .13 | .13 ± .18 | .222 |
| F5 | | | |
| Área do Utilizador | .31 ± .35 | .16 ± .32 | .178 |
| Produtos Comerciais | 2.88 ± 1.83 | 5.71 ± 1.37 | **<.001** |
| Marca | .57 ± .39 | .53 ± .44 | .682 |
| URL | 1.80 ± 1.52 | .11 ± .18 | **<.001** |
| Informação Comercial | .35 ± .40 | .14 ± .28 | .057 |
| Pesquisa | .76 ± .66 | .44 ± .38 | .202 |
| Pistas Fraudulentas | .50 ± .39 | .17 ± .32 | **.013** |

| | | | |
|---|---|---|---|
| F6 | | | |
| Área do Utilizador | .50 ± .51 | .37 ± .56 | .381 |
| Produtos Comerciais | 1.59 ± 1.26 | 2.82 ± 1.27 | **.007** |
| Marca | .65 ± .54 | .24 ± .21 | **.025** |
| URL | 1.31 ± .94 | .23 ± .63 | **.005** |
| Informação Comercial | .60 ± .61 | .80 ± .64 | .202 |
| Pesquisa | .81 ± .48 | 1.22 ± .76 | .135 |
| Pistas Fraudulentas | .47 ± .56 | .38 ± .38 | .986 |
| F7 | | | |
| Área do Utilizador | .00 ± .00 | .00 ± .00 | 1.000 |
| Produtos Comerciais | 2.04 ± 1.36 | 3.05 ± 1.27 | **.052** |
| Marca | .98 ± .74 | .78 ± 1.19 | .135 |
| URL | 1.40 ± 1.69 | .06 ± .12 | **.002** |
| Pesquisa | 2.71 ± 1.06 | 3.04 ± 1.22 | .421 |
| Pistas Fraudulentas | .01 ± .04 | .02 ± .08 | .986 |
| F8 | | | |
| Área do Utilizador | .42 ± .63 | .15 ± .24 | .538 |
| Produtos Comerciais | 3.20 ± 1.06 | 6.33 ± 1.53 | **<.001** |
| Marca | .43 ± .36 | .25 ± .26 | .222 |
| URL | .39 ± .49 | .11 ± .28 | .094 |
| Pistas Fraudulentas | .39 ± .69 | .09 ± .20 | .179 |

**ANEXO K – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI dos *Websites* Legítimos**

| | Não Suscetíveis | | Suscetíveis | | p |
|---|---|---|---|---|---|
| | M ± SD | MR | M ± SD | MR | |
| Duração Média das Fixações (ms) | | | | | |
| Área do Utilizador | .40 ± .33 | 42.56 | .17 ± .17 | 28.32 | **.004** |
| Produtos Comerciais | 2.71 ± 1.59 | 20.88 | 4.64 ± 1.26 | 40.71 | **<.001** |
| Marca | .36 ± .22 | 34.88 | .35 ± .26 | 32.71 | .660 |
| URL | 1.11 ± .98 | 50.79 | .11 ± .14 | 23.62 | **<.001** |
| Informação Comercial | .50 ± .37 | 38.02 | .35 ± .25 | 30.92 | .148 |
| Pesquisa | 1.42 ± .67 | 29.13 | 1.61 ± .62 | 36.00 | .162 |
| Número Total Médio das Fixações | | | | | |
| Área do Utilizador | 1.70 ± 1.32 | 42.83 | .77 ± .72 | 28.17 | **.003** |
| Produtos Comerciais | 13.46 ± 7.42 | 20.77 | 21.48 ± 5.51 | 40.77 | **<.001** |
| Marca | 1.58 ± .89 | 36.17 | 1.42 ± .91 | 31.98 | .391 |
| URL | 3.76 ± 2.61 | 50.65 | .49 ± .55 | 23.70 | **<.001** |
| Informação Comercial | 2.45 ± 1.64 | 39.04 | 1.67 ± 1.04 | 30.33 | .076 |
| Pesquisa | 7.34 ± 3.06 | 30.25 | 8.14 ± 2.98 | 35.36 | .298 |
| Latência (ms) | | | | | |
| Área do Utilizador | 5.30 ± 1.51 | 32.80 | 4.61 ± 1.70 | 24.80 | .070 |
| Produtos Comerciais | 1.23 ± .84 | 41.71 | .72 ± .47 | 28.81 | **.009** |
| Marca | 2.38 ± 1.65 | 37.84 | 1.77 ± 1.79 | 27.84 | **.024** |
| URL | 2.05 ± 1.08 | 21.41 | 3.79 ± 2.79 | 30.23 | **.038** |
| Informação Comercial | 3.36 ± 2.00 | 35.04 | 2.76 ± 2.06 | 28.55 | .166 |
| Pesquisa | 2.26 ± 1.37 | 41.81 | 1.45 ± 1.25 | 28.75 | **.008** |

**ANEXO L – Diferença de Médias entre Participantes Não Suscetíveis e Suscetíveis nas AOI de cada *Website* Legítimo**

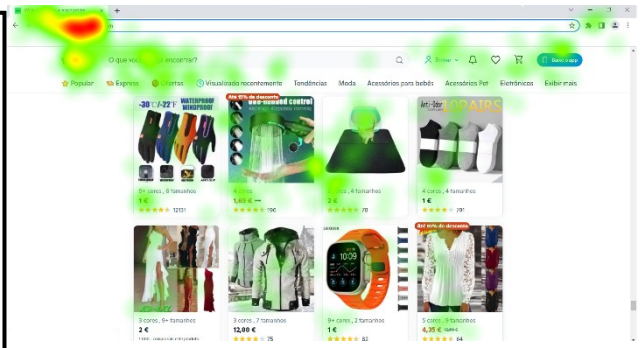
| | Não Suscetíveis | Suscetíveis | p |
|---|---|---|---|
| | M ± SD | M ± SD | |
| Duração Média das Fixações (ms) | | | |
| L1 | | | |
| Área do Utilizador | .44 ± .34 | .23 ± .41 | **.027** |
| Produtos Comerciais | 1.22 ± .99 | 2.07 ± .93 | **.009** |
| Marca | .46 ± .26 | .45 ± .40 | .532 |
| URL | 1.42 ± 1.48 | .11 ± .19 | **<.001** |
| Informação Comercial | .10 ± .16 | .07 ± .13 | .708 |
| Pesquisa | 3.01 ± 1.02 | 3.87 ± 1.06 | **.025** |
| L2 | | | |
| Área do Utilizador | .36 ± .28 | .06 ± .13 | **.004** |
| Produtos Comerciais | 2.61 ± 1.45 | 5.13 ± 1.64 | **<.001** |
| Marca | .44 ± .40 | .40 ± .55 | .486 |
| URL | .58 ± .63 | .09 ± .14 | **.003** |
| Informação Comercial | .32 ± .49 | .24 ± .28 | .953 |
| Pesquisa | 1.28 ± .90 | .98 ± .72 | .437 |
| L3 | | | |
| Área do Utilizador | .13 ± .21 | .12 ± .19 | .901 |
| Produtos Comerciais | 3.00 ± 2.33 | 5.04 ± 1.72 | **.018** |
| Marca | .39 ± .35 | .29 ± .34 | .307 |
| URL | 1.32 ± 1.18 | .09 ± .19 | **<.001** |
| Informação Comercial | .74 ± .79 | .43 ± .45 | .361 |
| Pesquisa | .90 ± .67 | .92 ± .87 | .817 |
| L4 | | | |
| Área do Utilizador | .37 ± .50 | .06 ± .11 | .057 |
| Produtos Comerciais | 3.64 ± 2.36 | 5.90 ± 1.25 | **.005** |
| Marca | .13 ± .16 | .24 ± .21 | .155 |
| URL | 1.37 ± 1.49 | .07 ± .12 | **<.001** |
| Informação Comercial | .92 ± .99 | .45 ± .42 | .290 |
| Pesquisa | .56 ± .67 | .32 ± .31 | .361 |
| L5 | | | |
| Área do Utilizador | .28 ± .34 | .26 ± .40 | .736 |
| Produtos Comerciais | 2.93 ± 1.76 | 5.85 ± 1.71 | **<.001** |
| Marca | .65 ± .52 | .38 ± .33 | .154 |
| URL | .92 ± 1.14 | .11 ± .29 | .065 |
| Informação Comercial | .16 ± .16 | .13 ± .22 | .462 |
| Pesquisa | .68 ± .57 | .54 ± .61 | .414 |
| L6 | | | |
| Área do Utilizador | .66 ± .81 | .31 ± .31 | .437 |
| Produtos Comerciais | 1.23 ± .83 | 3.67 ± 2.15 | **<.001** |
| Marca | .17 ± .32 | .31 ± .39 | .193 |
| URL | .80 ± .75 | .15 ± .28 | **.036** |

| | | | |
|---|---|---|---|
| Informação Comercial | .96 ± .59 | 1.08 ± .88 | .796 |
| Pesquisa | 1.16 ± .84 | 1.25 ± .91 | .953 |
| L7 | | | |
| Área do Utilizador | .05 ± .11 | .00 ± .00 | .349 |
| Produtos Comerciais | 2.18 ± 1.80 | 3.26 ± 1.71 | .121 |
| Marca | .21 ± .27 | .35 ± .32 | .254 |
| URL | .65 ± .91 | .16 ± .25 | .166 |
| Informação Comercial | .05 ± .08 | .02 ± .09 | .328 |
| Pesquisa | 2.13 ± 1.07 | 3.40 ± 1.63 | **.040** |
| L8 | | | |
| Área do Utilizador | .77 ± .96 | .34 ± .45 | .290 |
| Produtos Comerciais | 4.16 ± 2.01 | 6.40 ± .93 | **<.001** |
| Marca | .42 ± .41 | .40 ± .24 | .957 |
| URL | 1.25 ± .99 | .05 ± .11 | **<.001** |

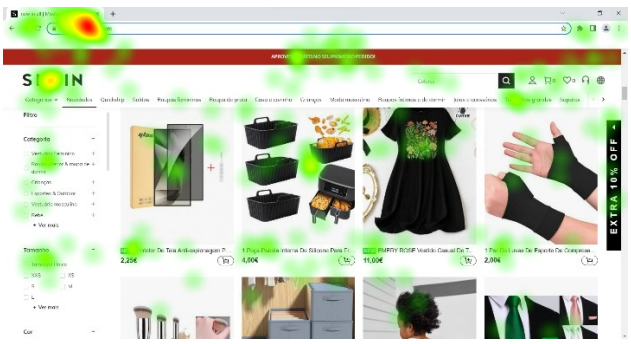
## ANEXO M – Mapas de Calor dos Participantes Não Suscetíveis e Suscetíveis

### Participantes Não Suscetíveis

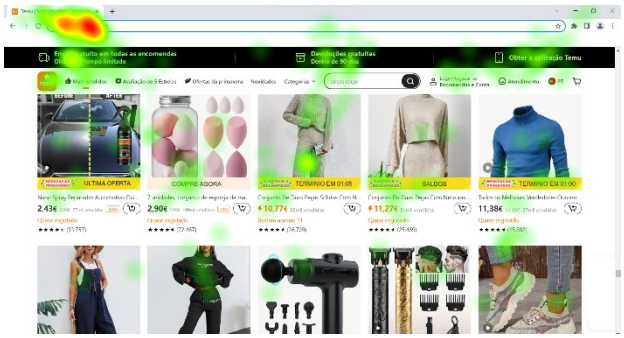
F2



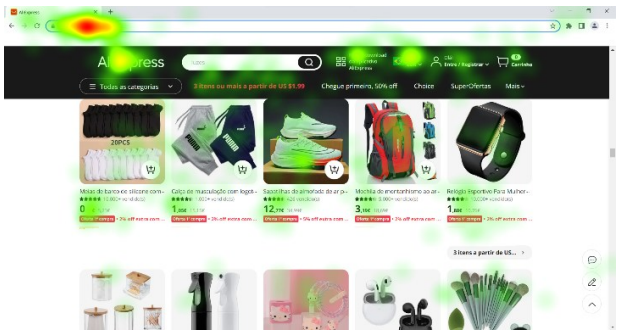
F3



F4



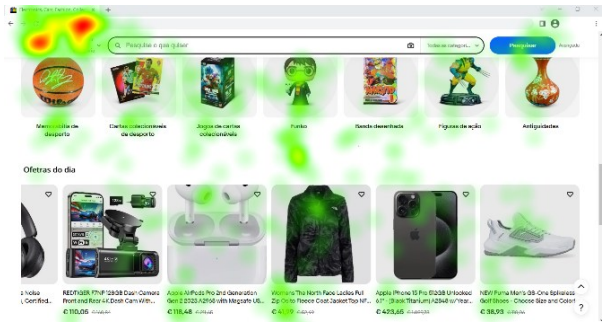
F5



F6

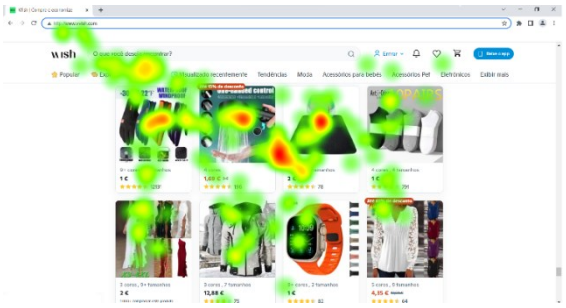



F7

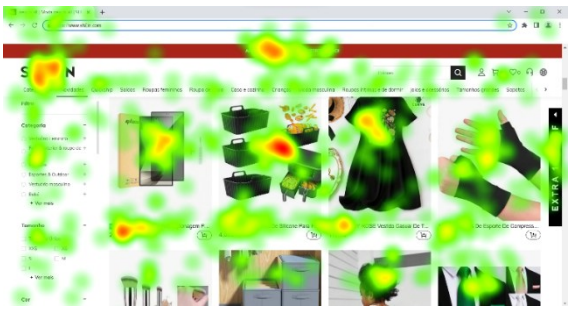


## Participantes Suscetíveis

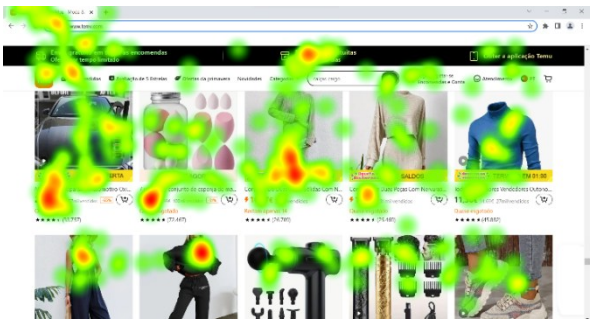
F2



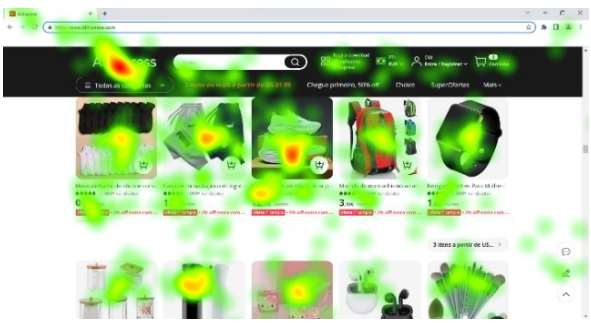
F3



F4



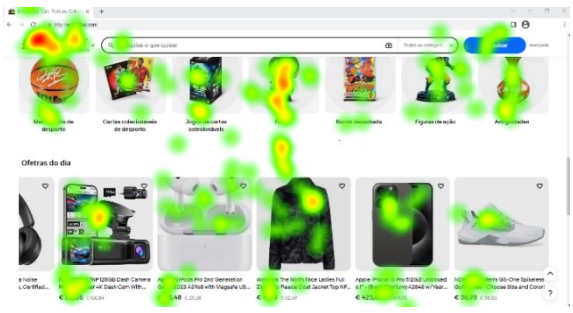
F5



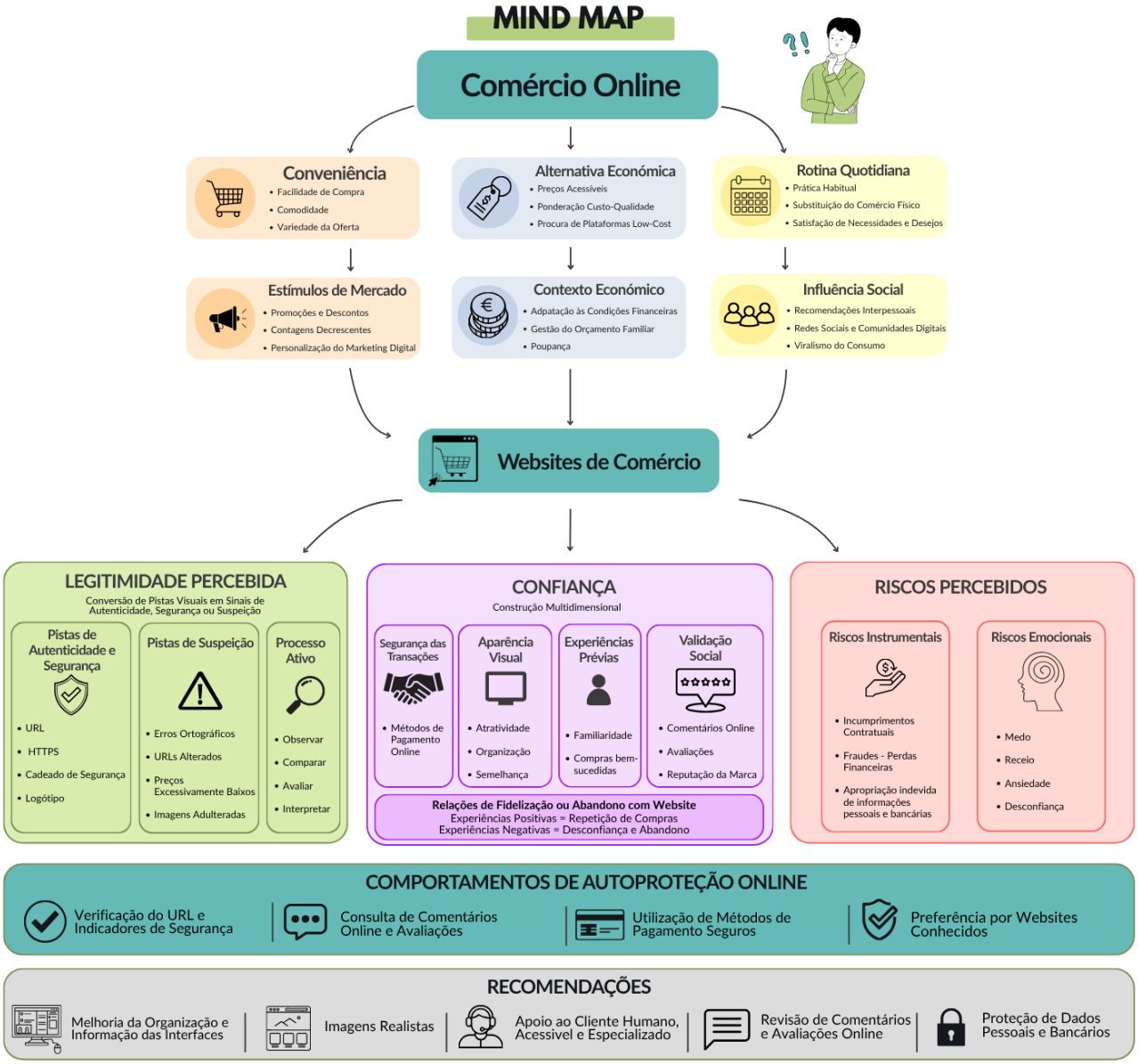
F6




F7

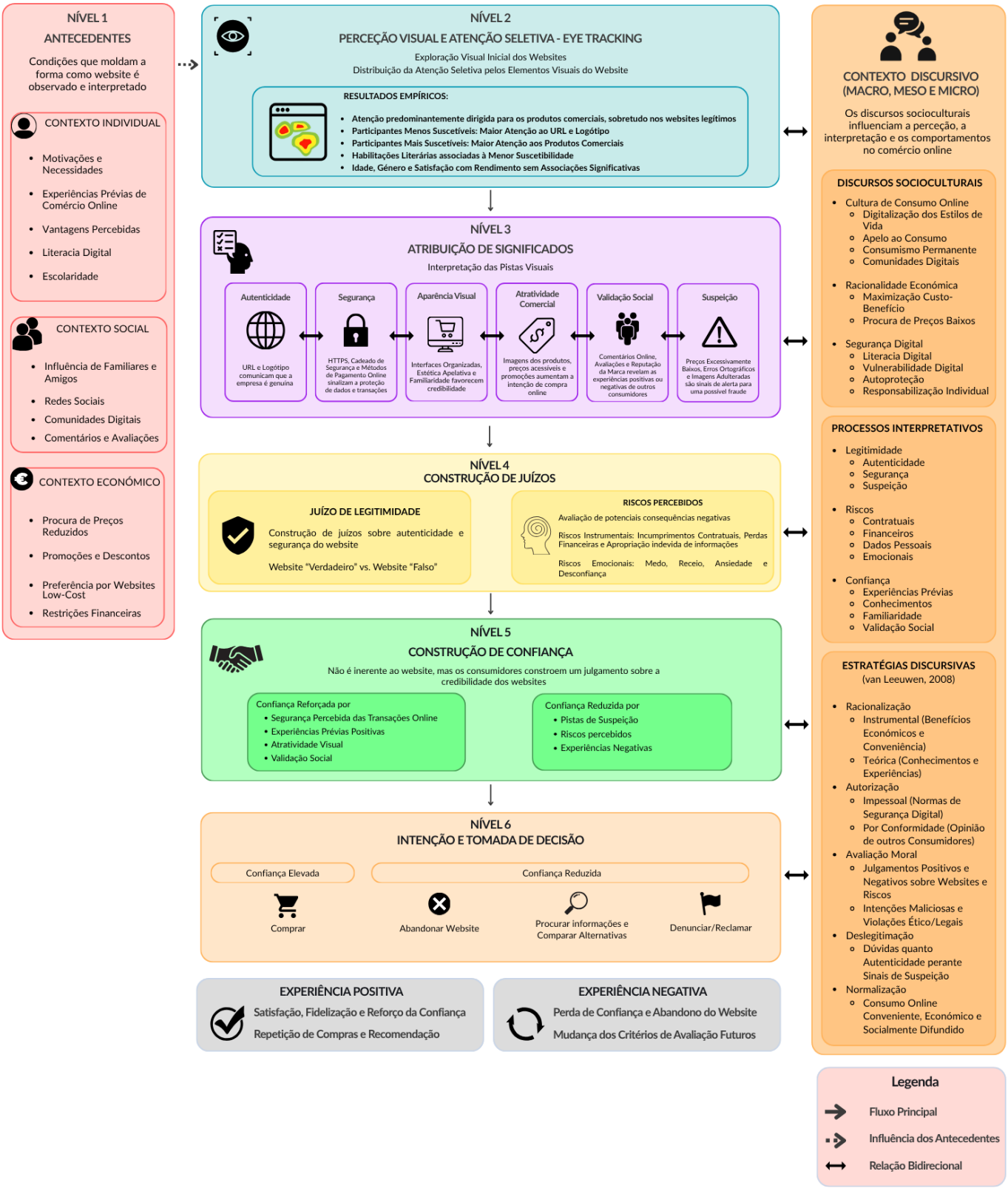


## ANEXO N – *Mind Map* das Entrevistas




Fonte: Elaborado pelo Próprio no *Canva*

## ANEXO O – Modelo Sequencial de Construção da Confiança




Fonte: Elaborado pelo Próprio no *Canva*

FACULDADE DE **DIREITO**