U.PORTO

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

BURLA E *ROMANCE SCAM*: PERCEÇÃO PÚBLICA SOBRE A NATUREZA, GRAVIDADE DA ILICITUDE E COMPORTAMENTOS DE EVITAMENTO

Ângelo Carvalho Ribeiro

M

2026

Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade do Porto para obtenção do grau de Mestre em Criminologia elaborada sob orientação do Professor Doutor Pedro Sousa

Agradecimentos

A presente dissertação de mestrado provém do culminar de um percurso académico desenvolvido ao longo destes últimos anos, mas representa igualmente o resultado do apoio, incentivo e contributo de várias pessoas que, de diferentes formas, estiveram presentes ao longo deste caminho. Neste sentido, deixo aqui o registo de um sincero agradecimento a todos aqueles que, direta ou indiretamente, contribuíram para a concretização deste trabalho.

À Universidade do Porto, enquanto instituição de ensino à qual pertenço atualmente, manifesto o meu reconhecimento. Aos docentes da área da Criminologia com quem tive a oportunidade de me cruzar ao longo deste percurso académico, agradeço não apenas a transmissão de conhecimentos científicos, mas também o desenvolvimento do pensamento crítico, elementos determinantes na construção do meu percurso académico.

Ao meu orientador, Professor Doutor Pedro Sousa, expresso a minha profunda gratidão pela orientação, disponibilidade, paciência e apoio constantes ao longo do desenvolvimento desta investigação, bem como pelo acompanhamento esclarecedor nos momentos de dúvida e indecisão.

Aos colegas de curso, com quem partilhei aprendizagens, desafios e momentos marcantes, deixo igualmente uma palavra de apreço pelas amizades construídas ao longo deste trajeto.

Aos meus pais, irmãos e à minha família, pelo apoio constante, pela confiança, pelos conselhos e pelo afeto demonstrados ao longo de todo este percurso, fundamentais para a superação dos desafios enfrentados.

Por último, mas certamente não menos importante, dedico um agradecimento muito especial à Mariana Monteiro, minha companheira de vida ao longo destes últimos anos, pelo amor incondicional, paciência e compreensão. A sua presença, carinho e incentivo foram um verdadeiro porto seguro nos desafios mais exigentes desta caminhada académica, tornando cada conquista ainda mais significativa. Sem ela, este percurso não teria sido vivido da mesma forma.

A todos, expresso o meu mais profundo reconhecimento, pelo contributo prestado, não apenas ao meu percurso académico, mas também ao meu crescimento pessoal.

Resumo

O presente trabalho de investigação analisa o fenómeno do *romance scam*, uma forma de criminalidade digital caracterizada pela exploração de vulnerabilidades psicológicas das vítimas através da manipulação emocional e de técnicas digitais, de modo a obter vantagens económicas. A investigação teve como objetivo analisar a relação entre a perceção pública sobre o *romance scam* e os comportamentos de evitamento adotados pelos utilizadores em contexto online. Para o efeito, foi desenvolvido um estudo quantitativo, transversal e descritivo, recorrendo à aplicação de um questionário online a uma amostra de 100 participantes (≥18 anos). Os resultados evidenciaram que, apesar do conhecimento específico sobre o *romance scam* ser reduzido, a maioria dos participantes considera-o um crime grave e reconhece que qualquer pessoa pode ser vítima. Verificou-se ainda a adoção de diversos comportamentos preventivos, nomeadamente a rejeição de contactos de desconhecidos online e a limitação da partilha de informações pessoais. Os participantes demonstraram níveis elevados de preocupação relativamente às burlas online, reconhecendo a sua crescente sofisticação e o potencial impacto financeiro e emocional associado à vitimação. Posto isto, os resultados reforçam a importância da promoção da literacia digital e da implementação de estratégias de sensibilização e prevenção.

Palavras-Chave

Burla romântica online; Fraude digital; Vitimação online; Comportamentos de evitamento do crime; Prevenção situacional do crime.

Abstract

This research examines the phenomenon of romance scams, a form of cyber-enabled crime characterized by the exploitation of victims' psychological vulnerabilities through emotional manipulation and digital techniques to obtain financial gain. The study aimed to analyze the relationship between public perceptions of romance scams and the avoidance behaviors adopted by individuals in online environments. To this end, a quantitative, cross-sectional, and descriptive study was conducted using an online questionnaire administered to a sample of 100 participants aged 18 years or older. The findings revealed that, despite limited specific knowledge of romance scams, most participants perceived this type of fraud as a serious crime and recognized that anyone can become a victim. Participants also reported adopting several preventive behaviors, particularly rejecting contact requests from unknown individuals online and limiting the sharing of personal information. Furthermore, participants expressed high levels of concern regarding online fraud, acknowledging its increasing sophistication and the potential financial and emotional impact associated with victimization. Overall, the findings highlight the importance of promoting digital literacy and implementing awareness-raising and prevention strategies.

Keywords

Romance scam; Online fraud; Online victimization; Fraud avoidance behaviors; Situational crime prevention.

Índice Geral

Introdução 1

Parte A – Enquadramento Teórico

1) Perspetiva criminológica do *romance scam* 5

1.1) Relevância social e académica do *romance scam* 8

1.2) Conceitos fundamentais 9

1.3) *Scammer* 13

1.3.1) *Modus operandi* e técnicas de manipulação 16

2) Perspetiva jurídico-criminal do *romance scam* 18

2.1) Enquadramento jurídico-criminal no ordenamento português 18

2.2) Enquadramento jurídico-criminal internacional 20

3) Teorias explicativas do *romance scam* 22

4) Vitimação e comportamentos de autoproteção em contexto digital 27

4.1) Perfil da vítima 28

4.2) Processo de vitimação 29

4.3) Impacto da vitimação 30

4.4) Fatores de risco e fatores de proteção 31

4.5) Comportamentos individuais de prevenção e evitamento do crime 33

5) Perceção pública sobre a criminalidade digital 34

5.1) Subvalorização do *romance scam* e representações sociais da ilicitude 34

5.2) Os mídia e as plataformas digitais na construção da perceção pública 36

6) Cibersegurança e prevenção do *romance scam* 36

6.1) Estratégias institucionais e políticas de prevenção 37

6.2) Literacia digital e perceção do risco 38

6.2.1) Campanhas de sensibilização e educação pública 39

Síntese do Enquadramento Teórico 41

Parte B – Estudo Empírico

1) Objetivos da investigação 43

2) Método 43

2.1) Desenho de investigação 44

2.2) Procedimentos 44

2.3) Descrição da amostra 45

2.4) Instrumento 48

3) Resultados 50

4) Discussão dos resultados 69

Considerações Finais 79

Limitações 83

Referências Bibliográficas 85

Anexos 95

A) Parecer da Comissão de Ética 97

B) Parecer da Unidade de Proteção de Dados 99

C) Inquérito por Questionário 101

Índice de Tabelas

Tabela 1. Características sociodemográficas da amostra (*n*=100) 47

Tabela 2. Utilização da Internet (*n*=100) 52

Tabela 3. Interação com desconhecidos em função da utilização de *apps* de encontros (*n*=100) 53

Tabela 4. Conhecimento acerca das diferentes formas de burla online (*n*=100) 53

Tabela 5.Grau de conhecimento sobre as burlas online e o *romance scam* (*n*=100) 54

Tabela 6. Atribuição de responsabilidade à vítima pela perda financeira (*n*=91) 55

Tabela 7. Sanções consideradas adequadas pelos participantes para os *scammers* (*n*=100) 56

Tabela 8. Preferência pelas sanções segundo o género dos participantes (*n*=99) 56

Tabela 9. Preferência pelas sanções segundo o grupo etário dos participantes (*n*=100) 56

Tabela 10. Características da interação com desconhecidos (*n*=100) 58

Tabela 11. Práticas adotadas como proteção ou evitamento do crime (*n*=100) 59

Tabela 12. Comportamentos de evitamento 61

Tabela 13. Perceção de insegurança 63

Tabela 14. Correlações de *Spearman* entre a gravidade atribuída ao *romance scam* e outras variáveis (*n*=100) 65

Tabela 15. Teste de *Mann-Whitney* segundo o género (*n*=100) 67

Tabela 16. Testes do *Qui-quadrado de Pearson* 68

Lista de Abreviaturas / Siglas

APAV – Associação Portuguesa de Apoio à Vítima

CC – Código Civil

CNCS – Centro Nacional de Cibersegurança

CPP – Código Penal Português

CPT – *Crime Pattern Theory*

CRP – Constituição da República Portuguesa

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

FTC – *Federal Trade Commission*

GCI – Gabinete de Comunicação e Imagem

IA – Inteligência Artificial

IC3 – *Internet Crime Complaint Center*

JASP – *Jeffrey's Amazing Statistics Program*

LIS – Linha Internet Segura

MP – Ministério Público

PJ – Polícia Judiciária

RASI – Relatório Anual de Segurança Interna

RAT – *Routine Activity Theory*

RCT – *Rational Choice Theory*

SCP – *Situational Crime Prevention*

TIC – Tecnologias de Informação e Comunicação

VPN – *Virtual Private Network*

Introdução

O aumento exponencial do uso das tecnologias de comunicação nas últimas décadas tem vindo a transformar significativamente as interações sociais, abrindo novas oportunidades, mas também novos riscos de vitimação online. Entre estes, destacam-se as burlas e os *romance scams* (também designados por burlas românticas em contextos lusófonos) que exploram a vulnerabilidade emocional e financeira de inúmeros indivíduos (APAV, 2025; Europol, 2025). Em Portugal, a título de exemplo, o *romance scam* destacou-se como um dos métodos mais frequentes de cibercrime reportados na Linha Internet Segura (LIS) da Associação Portuguesa de Apoio à Vítima (APAV) em 2023, integrando o crime de burla que ocupou o primeiro lugar com 332 denúncias, tendo registado um aumento significativo face a anos anteriores (APAV, 2024). Este aumento levou à criação da plataforma "Última Palavra", dedicada exclusivamente a apoiar vítimas deste tipo de fraude (APAV, 2025).

O *romance scam* caracteriza-se pela criação de relações afetivas fictícias, mediadas por plataformas digitais, redes sociais e aplicações de encontros, com o objetivo de obter vantagens económicas, dados pessoais ou outros benefícios (Buil-Gil & Zeng, 2022; Cross et al., 2018; Whitty & Buchanan, 2014). De acordo com Cross (2020, p.937) e Guerreiro et al. (2024), o *romance scam* consiste num método através do qual os indivíduos utilizam a perceção de uma relação legítima para manipular e explorar a vítima. Os ofensores abusam da vulnerabilidade das vítimas, criando uma relação temporária aparente, ludibriando-as através de manipulação emocional e afetiva, com o objetivo principal de ganho financeiro (Buil-Gil & Zeng, 2022; Cross et al., 2018; Whitty & Buchanan, 2016). Muitas vezes, estas fraudes incluem o denominado *double whammy*[1], combinando perda financeira com trauma emocional resultante da "perda" da relação (Boccardi et al., 2020; Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2016).

Estudos recentes indicam que os *romance scams* não são casos isolados, mas podem envolver também redes transnacionais organizadas, com registos crescentes em países africanos, como a Nigéria e Moçambique, bem como esquemas locais em Portugal e no

[1] Sem tradução direta para português. Refere-se à situação em que uma vítima sofre simultaneamente um prejuízo financeiro e um impacto psicológico profundo, sendo duplamente afetada pelo mesmo crime.

Brasil (Europol, 2025; FTC, 2025; Rege & Lavorgna, 2023). Em termos estatísticos, a subnotificação continua a ser elevada devido à vergonha e estigmatização das vítimas (APAV, 2025; Whitty, 2018). Em Portugal, apenas em 2022, 48 mulheres reportaram perdas de aproximadamente um milhão de euros (APAV, 2025), e globalmente, dados do *Federal Bureau of Investigation* (FBI) e da *Federal Trade Commission* (FTC) indicam que os prejuízos anuais ultrapassam os 500 a 1000 milhões de dólares (FTC, 2025).

A análise de processos-crime e decisões judiciais tem sido fundamental para compreender a dimensão legal destes esquemas. Estudos em países como os Estados Unidos e o Reino Unido revelam que, apesar do aumento do número de casos reportados, poucos resultam em condenações, muito devido à complexidade das investigações e à dificuldade de rastrear os autores (Whitty, 2018). Em Portugal, a jurisprudência é ainda limitada, mas a aplicação do artigo 217.º do Código Penal Português (CPP), crime de burla, com agravantes nos casos que envolvem meios informáticos (art.º 221 do CPP), tem sido registada em alguns casos judiciais (Código Penal - Edição Académica, 2023), demonstrando a relevância de enquadramentos legais adaptados às especificidades da criminalidade digital.

O perfil da vítima de *romance scam* é multifacetado e não pode ser reduzido a características individuais isoladas (Cross et al., 2018; Whitty & Buchanan, 2016). A vitimação emerge da interação complexa entre fatores emocionais, cognitivos, sociais e tecnológicos, explorados por ofensores que recorrem a técnicas de manipulação sofisticadas (Bilz et al., 2023; Rege & Lavorgna, 2023). O impacto desta vitimação é profundo, abrangendo dimensões emocionais, sociais e económicas, o que evidencia a necessidade de abordagens multidisciplinares na análise do fenómeno (Cross et al., 2018; Whitty & Buchanan, 2016). A compreensão do *modus operandi* dos *scammers*, que combina estratégias de manipulação emocional com técnicas digitais e organização estruturada, é essencial para o desenvolvimento de políticas de prevenção, campanhas de sensibilização e mecanismos de apoio às vítimas (Bilz et al., 2023; FTC, 2025; Rege & Lavorgna, 2023).

Neste contexto, a presente investigação propõe-se a analisar a perceção pública sobre a gravidade do *romance scam* e os comportamentos de evitamento adotados pelos utilizadores perante o risco de vitimação online. Para concretizar este propósito, a investigação orienta-se por um conjunto de objetivos específicos, nomeadamente os de caracterizar a perceção pública sobre a gravidade do *romance scams*, identificar os

comportamentos de evitamento adotados pelos utilizadores, analisar a associação entre fatores de ordem individual e a perceção da gravidade do fenómeno, bem como examinar a relação entre essa perceção e os comportamentos preventivos adotados

Esta dissertação encontra-se estruturada em duas grandes partes – Parte A e Parte B. Na Parte A, dedicada ao enquadramento teórico, procura-se estabelecer uma compreensão abrangente do tema, contextualizando o fenómeno do *romance scam* e clarificando conceitos fundamentais para a análise que se segue, com o objetivo de explorar o impacto devastador que tais incidentes têm sobre as vítimas. Além disso, são abordadas diversas teorias da criminologia relevantes para a compreensão dos fatores motivacionais e padrões de atuação dos ofensores, bem como dos fatores favoráveis à vitimação e perceção pública destes crimes. A Parte B, por sua vez, é dedicada à apresentação do estudo empírico e dos seus resultados. De forma a investigar a perceção da gravidade do *romance scam*, os comportamentos de evitamento e a perceção de insegurança e vulnerabilidade perante o fenómeno, recorreu-se a uma abordagem quantitativa, de carácter transversal e descritivo. A amostra selecionada abrange 100 participantes adultos (≥18 anos), recrutados de forma voluntária, com acesso à Internet e com competências digitais básicas. Os dados foram recolhidos através de um inquérito por questionário digital composto por 47 questões, abrangendo características sociodemográficas, experiências pessoais, perceção da gravidade do *romance scam*, bem como comportamentos de autoproteção, evitamento e perceção de insegurança e vulnerabilidade perante o fenómeno.

Após apresentação do estudo empírico realizado, entra-se na discussão dos resultados, onde será empreendida uma análise crítica interpretativa dos dados explorando as implicações e contribuições para o campo de estudo em questão e relevância para políticas de prevenção e literacia digital assim como nas limitações identificadas ao longo do presente trabalho.

Por sua vez, a conclusão final refletirá as principais ideias e aprendizagens extraídas desta investigação, relevando o conhecimento produzido sobre o fenómeno do *romance scam*, os seus impactos e estratégias de mitigação, e relevando as limitações da presente investigação.

Parte A – Enquadramento Teórico

1) Perspetiva criminológica do *romance scam*

Embora o termo *romance scam*[2] não tenha uma tradução específica no contexto português, pode-se referir a ele como burla romântica (Guerreiro et al., 2024) ou fraude no namoro. Trata-se de um tipo de delito em que o agente utiliza plataformas digitais para estabelecer relações emocionais fictícias, de modo a manipular a vítima e, assim, obter ganhos financeiros, inserindo-se assim no contexto mais amplo dos crimes cibernéticos (Cross et al., 2018; Whitty & Buchanan, 2014). Encontra-se tipificado no artigo 217.º-A do CPP, onde são abordados os crimes que envolvem o uso da Internet (Código Penal - Edição Académica, 2023). A compreensão deste fenómeno implica, contudo, considerar a sua evolução histórica, profundamente ligada ao desenvolvimento das tecnologias digitais.

Nas décadas iniciais da Internet (entre os anos 1990-2000), prevaleceram formas rudimentares de fraude online, tais como o *phishing* por correio eletrónico ou e-mail e os esquemas do tipo *Nigerian Prince*[3] (Verizon, 2025). Após 2010, a explosão das redes sociais acelerou a evolução dos crimes digitais, com os criminosos a explorar as interações pessoais em plataformas como o Facebook e, posteriormente, o Instagram, bem como as *apps* de encontros para a prática do crime de *romance scam* (Europol, 2025). Esta migração reflete uma transição de ataques impessoais para manipulações dirigidas, nas quais o agente criminoso se serve de dados pessoais disponíveis online para construir relações de confiança fictícias com as vítimas (Europol, 2025).

A consolidação dos smartphones e das *apps* de encontros, como o Tinder ou o Bumble, veio facilitar ainda mais a prática de *romance scams*, permitindo contactos contínuos e em larga escala (Boccardi et al., 2020). Mais recentemente, a integração de Inteligências

[2] Em português "burla romântica". Na presente dissertação, opta-se pela utilização do termo em língua inglesa, por se tratar da designação mais comummente utilizada e reconhecida e nível internacional para caracterizar este fenómeno.

[3] Em português "príncipe nigeriano". Esquema fraudulento disseminado por correio eletrónico, no qual o remetente se faz passar frequentemente por uma personalidade da realeza ou da elite nigeriana a solicitar ajuda para transferir uma grande quantia de dinheiro, prometendo uma recompensa financeira em troca. Na prática, o objetivo é obter dados bancários da vítima.

Artificiais (IA) gerou *deepfakes*[4] e *chatbots*[5] capazes de simular conversas humanas autênticas, aumentando consideravelmente as taxas de sucesso destes esquemas fraudulentos (Europol, 2025). Estudos recentes estimam perdas globais superiores a mil milhões de dólares anuais associadas ao *romance scam* (FTC, 2025).

A massificação da Internet impulsionou a transição das fraudes tradicionais para o ambiente digital, ampliando o seu alcance geográfico e a sua sofisticação técnica (Europol, 2025). Neste contexto, relatórios recentes da Europol e do FBI destacam o aumento significativo das ocorrências de *romance scam* em Portugal e na União Europeia, bem como das perdas financeiras associadas ao fenómeno, agravado pela utilização de criptomoedas como instrumento de lavagem de dinheiro (Europol, 2025; Interpol, 2022). Este crescimento está intimamente associado à expansão das plataformas digitais e das redes sociais, que facilitam o contacto entre desconhecidos, ao mesmo tempo que oferecem oportunidades para a manipulação psicológica sofisticada dos potenciais alvos (Bilz et al., 2023; Wang & Topalli, 2024). Estudos sistemáticos recentes demonstram que a literatura sobre o *romance scam* tem vindo a ampliar-se, evidenciando tanto padrões de vitimação como estratégias de mitigação, no entanto, persistem lacuna em termos de investigações empíricas de maior escala e de carácter multidisciplinar (Bilz et al., 2023). Face a esta realidade, revela-se necessário desenvolver respostas multidimensionais, que incluam a promoção da literacia digital junto da população, a cooperação internacional entre autoridades judiciárias, a criação ou melhoria de mecanismos de denúncia acessíveis às vítimas e o estabelecimento de protocolos de partilha de informação entre as plataformas digitais e as forças de segurança.

De acordo com a literatura científica e com relatórios de organismos institucionais, este tipo de fraude apresenta um impacto significativo e crescente, com prejuízos financeiros avultados e uma sofisticação criminal progressiva (Soares & Lazarus, 2024; Europol, 2025). Investigadores estimam que, em 2022, perdas financeiras associadas a estas burlas ultrapassaram os 1,3 mil milhões de dólares, num contexto norte-americano e global, sendo que as vítimas relatam frequentemente impactos psicológicos que superam o próprio dano económico imediato (FTC, 2025; Lazarus, 2024). Contudo, a subnotificação

[4] Em português "falsificações profundas". Conteúdos audiovisuais gerados ou manipulados por IA de forma a simular, de modo convincente, a aparência ou a voz de uma pessoa real.

[5] Sem tradução direta para português. Programas informáticos que simulam conversas humanas através de respostas automatizada.

mantém-se elevada, comprometendo a obtenção de estimativas realistas e o desenvolvimento de políticas de prevenção eficazes (Grant & Buil-Gil, 2025).

No contexto português, a relevância crescente do *romance scam* é evidenciada pelos dados da APAV, segundo os quais, em 2023, foram contabilizados 731 processos de atendimento e apoio relativos a situações de cibercrime, com um aumento expressivo face ao ano anterior (APAV, 2024). Este crescimento é, em parte, atribuível à transformação digital acelerada pelo contexto pandémico de 2020, que intensificou a dependência tecnológica e alargou o espaço das interações sociais ao ambiente online (Guerreiro et al., 2024). Já em 2024, os dados da LIS registaram 681 processos de atendimento e apoio relativos a situações de cibercrime, refletindo um ligeiro decrescimento face ao ano anterior. Ainda assim, o crime de burla online manteve-se como o mais reportado, com 247 denúncias, sendo o *romance scam* o método fraudulento mais utilizado (APAV, 2025).

Além dos prejuízos financeiros, a investigação académia recente indica que a manipulação emocional conduz a consequências psicológicas profundas, nomeadamente ansiedade, depressão, vergonha e isolamento social, efeitos documentados por diversas análises qualitativas sobre vitimação neste contexto (Boccardi et al., 2020; Cole, 2024; Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2016). Estas consequências evidenciam a necessidade de integrar perspetivas psicológicas e comportamentais no estudo do fenómeno, para além da esfera patrimonial tradicional (Alam et al., 2021; Yosiandra & Sakariah, 2024), dimensão que, por questões metodológicas, não foi contemplada na investigação realizada no âmbito desta dissertação.

À escala social, a resposta ao *romance scam* é também condicionada pela perceção pública e pelos estigmas associados às vítimas (Whitty & Buchanan, 2016). A literatura evidencia que muitos indivíduos afetados não denunciam a fraude por vergonha ou por falta de reconhecimento de que foram efetivamente vitimados, o que vem reforçar a importância das campanhas de sensibilização e da literacia digital como componentes fundamentais da prevenção e da proteção dos cidadãos no espaço virtual (Lazarus, 2024; Malwarebytes, 2024).

Em síntese, o *romance scam* representa um fenómeno criminal multifacetado que combina dimensões tecnológicas, psicológicas e sociais, exigindo abordagens integradas que articulem investigação científica, educação pública e políticas de cibersegurança

(Europol, 2025; Holt et al., 2022), cuja crescente prevalência tem sido documentada por organismos internacionais como a Interpol (2022).

1.1) Relevância social e académica do *romance scam*

Nas últimas décadas, a expansão das plataformas digitais e o aumento das interações sociais mediadas pelas novas tecnologias criaram condições propícias ao surgimento e crescimento do *romance scam* enquanto fenómeno criminal de visibilidade e impacto social crescentes (Bilz et al., 2023; Europol, 2025; Rege & Lavorgna, 2023). A intensificação do uso da Internet e das redes sociais, se por um lado alargou as possibilidades de contacto interpessoal, por outro favoreceu o desenvolvimento de formas cada vez mais sofisticadas de fraudes online, assentes na manipulação emocional e na exploração da confiança das potenciais vítimas (Bilz et al., 2023). Este tipo de burlas distinguem-se, conforme evidenciado por estudos recentes, pela conjugação de estratégias de manipulação psicológica e aproveitamento de vulnerabilidades afetivas, características que contribuem para a gravidade dos danos causados e para a dificuldade em reconhecer a natureza criminosa da relação, quer por parte das vítimas, quer pela sociedade em geral (Whitty & Buchanan, 2016; Yosiandra & Sakariah, 2024).

Do ponto de vista social, o *romance scam* representa um problema de particular relevância, na medida em que afeta indivíduos de diferentes faixas etárias, níveis socioeconómicos e contextos culturais (Cross et al., 2018; Europol, 2025), contrariando a perceção de que se trata de um fenómeno circunscrito a grupos específicos. Tal como referido anteriormente, as consequências deste crime ultrapassam largamente o prejuízo económico, sendo a vitimação caracterizada pela literatura recente como emocionalmente devastadora, com efeitos comparáveis aos de experiências de trauma relacional grave (Bilz et al., 2023; Whitty & Buchanan, 2016). Neste contexto, a compreensão da perceção pública do *romance scam* assume particular importância para o desenvolvimento de estratégias eficazes de prevenção, apoio às vítimas e políticas públicas de cibersegurança.

Do ponto de vista académico, o *romance scam* assume uma natureza multidisciplinar, constituindo um objeto de estudo relevante, na medida em que se situa na interseção de várias áreas do conhecimento, designadamente a criminologia, pelo enquadramento dos padrões de vitimação e comportamentos criminais; a psicologia, pela compreensão dos mecanismos de manipulação emocional e do impacto nas vítimas; a sociologia, pela

análise das dinâmicas sociais e culturais que favorecem a ocorrência do crime; e o direito penal, pelo enquadramento jurídico e resposta institucional ao fenómeno (Bilz et al., 2023; Whitty & Buchanan, 2014). Apesar do crescimento da produção científica sobre o tema, persistem lacunas relevantes na literatura, sobretudo no que respeita à perceção pública da ilicitude, à avaliação da gravidade do crime e aos comportamentos de evitamento adotados pelos utilizadores de plataformas digitais (Bilz et al., 2023; Cross et al., 2018). Diversos autores sublinham ainda a necessidade de analisar os fatores socioculturais que moldam a interpretação social deste fenómeno e influenciam tanto a prevenção como a resposta institucional (Cross et al., 2018; Rege & Lavorgna, 2023), bem como de aprofundar a compreensão dos mecanismos de vitimação, identificar fatores de risco e contribuir para o desenvolvimento de políticas preventivas mais eficazes (Cross et al., 2018).

A relevância académica do estudo do *romance scam* justifica-se ainda pela necessidade de repensar e atualizar os quadros teóricos tradicionais da criminologia e do direito penal, originalmente concebidos para crimes presenciais e não para práticas ilícitas mediadas pela tecnologia digital. Este fenómeno criminal desafia as categorias jurídicas clássicas e coloca questões probatórias complexas, frequentemente associadas à transnacionalidade do crime e à natureza intangível das interações online, exigindo novas abordagens conceptuais e metodológicas. Neste sentido, a investigação académica desempenha um papel fundamental na adaptação dos enquadramentos teóricos e legais existentes, contribuindo para a formulação de políticas públicas mais eficazes e para o desenvolvimento de estratégias de prevenção baseadas em evidência científica (Bilz et al., 2023).

Em síntese, o presente estudo do *romance scam* procura contribuir para uma compreensão mais aprofundada do fenómeno, assim como para o desenvolvimento de respostas mais eficazes em matérias de prevenção, investigação criminal e apoio às vítimas.

1.2) Conceitos fundamentais

O *romance scam* tem vindo a assumir crescente relevância na criminologia contemporânea, sobretudo devido à expansão das interações mediadas por tecnologias digitais (Europol, 2025; Rege & Lavorgna, 2023). A compreensão deste fenómeno exige, antes de mais, a clarificação dos conceitos que lhe são subjacentes, nomeadamente os de

cibercrime, burla, *romance scam* e *scammer*, cuja delimitação se revela essencial para a análise da perceção pública sobre este tipo de criminalidade, e para o desenvolvimento de estratégias de prevenção eficazes.

Os cibercrimes, também designados por crimes informáticos, caracterizam-se pelo conjunto de atos ilícitos praticados através do ciberespaço (Guerreiro et al., 2024). No que respeita à sua classificação, a Europol (2018) distingue duas categorias fundamentais: os crimes ciberdependentes, cuja prática depende integralmente de sistemas informáticos, e os crimes ciberassistidos, que correspondem a infrações comuns facilitadas pelo recurso à Internet, mas que poderiam ser cometidas sem intervenção das Tecnologias de Informação e Comunicação (TIC). De forma complementar, Albuquerque (2006) propõe uma distinção entre crimes informáticos puros, em que o meio informático constitui condição especial essencial para a prática do ilícito, e crimes informáticos impuros, que correspondem a factos já tipificados na lei penal mas praticados com recurso a meios digitais. A cibercriminalidade caracteriza-se ainda por três elementos estruturantes que a distinguem da criminalidade tradicional (Dias, 2012). O elemento da transnacionalidade (Dias, 2012), que se refere à capacidade das redes informáticas de transferir dados a nível global de forma praticamente imediata, o que dificulta significativamente o controlo e a interceção por parte das autoridades competentes, permitindo ao agente atuar a partir de qualquer localização geográfica (Guerreiro et al., 2024). O elemento da deslocalização (Dias, 2012), que reflete a transposição dos métodos tradicionais de práticas criminosas para o ambiente digital, com recurso a ferramentas proporcionadas pela evolução tecnológica (Guerreiro et al., 2024). E, o último elemento, o anonimato (Dias, 2012), que possibilita a ocultação da identidade do agente e da informação circulante, nomeadamente através de técnicas de encriptação, o que dificulta de forma expressiva a identificação e localização do criminoso (Guerreiro et al., 2024). Os dados estatísticos disponíveis confirmam a crescente expansão do cibercrime a nível nacional e internacional.

De acordo com o *Internet Crime Complaint Center* (IC3), entidade gerida pelo FBI, em 2025, foram registadas mais de um milhão de denúncias relacionadas com crimes praticados pela Internet, apresentando-se como o número mais elevado desde a criação do IC3, representado um aumento de 17% face a 2024, com perdas totais a atingirem os 20,9 mil milhões de dólares, um aumento de 26% face ao ano anterior (FBI, 2026). Os indivíduos com 60 anos ou mais foram o grupo etário mais afetado, com 201 266 denúncias registas e perdas totais de 7,7 mil milhões de dólares, um aumento de 59% face

a 2024 (FBI, 2026). No que respeita especificamente ao *romance scam*, as perdas totalizaram 929 milhões de dólares (FBI, 2026). O *phishing*[6] e a falsificação de identidade mantiveram-se como os tipos de cibercrime mais frequentemente reportados, com 192 000 denúncias (FBI, 2026). Por fim, o estado com maior número de denúncias foi a Califórnia, com cerca de 20 000 participações (FBI, 2026). Em Portugal, os dados do Relatório Anual de Segurança Interna (RASI) referentes a 2024, evidenciam uma ligeira diminuição das participações de crime informático, de 2 515 em 2023 para 2 492 em 2024, correspondendo a uma variação de -0,8% (Sistema de Segurança Interna, 2025). No que respeita especificamente à burla informática e nas comunicações, os dados indicam igualmente uma descida, de 20 159 participações em 2023 para 18 624 em 2024 (Sistema de Segurança Interna, 2025), tendência que poderá estar associada, em parte, à reorganização das tipologias criminais adotadas pelo relatório neste período.

A burla, por sua vez, configura um delito patrimonial, caracterizado pela indução em erro de terceiros através de informações falsas ou meios fraudulentos, com o objetivo de obter um benefício ilegítimo (Guerreiro et al., 2024). Este crime distingue-se dos demais por assentar no dolo deliberado, em oposição à ameaça ou à violência física, com recurso à exploração da boa-fé das vítimas (Martins et al., 2023). No âmbito digital, este tipo de delito assumiu modalidades cada vez mais complexas, das quais se destacam as fraudes cibernéticas (Europol, 2025; Rege & Lavorgna, 2023). Quando perpetrada em contexto digital, a burla assume contornos particulares, assentes na construção de uma identidade fictícia adaptada às características e necessidade da vítima, favorecida pela exposição pessoal nas redes sociais e pela falsa sensação de segurança decorrente do distanciamento físico entre vítima e ofensor (Guerreiro et al., 2024).

Por fim, o *romance scam*, emerge como uma variante específica da burla, na qual o agente criminoso estabelece uma ligação afetiva fictícia através de plataformas digitais, como as redes sociais ou as aplicações de encontros, com o objetivo de extrair recursos financeiros ou materiais da vítima (Cross et al., 2018; Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2014). Distingue-se da burla convencional pela dimensão da manipulação emocional persistente, na qual as fragilidades psicológicas da vítima, como a solidão ou o anseio por afetividade, são deliberadamente exploradas (Boccardi et al., 2020; Cole,

[6] Em português "pesca de dados". Técnica de fraude digital na qual o agente criminoso de faz passar por uma entidade legítima através do envio de correio eletrónico ou outros meios de comunicação com o objetivo de induzir a vítima a revelar dados pessoais, credenciais de acesso ou informações financeiras.

2024). Em termos de dinâmica criminal, trata-se de um processo deliberado e cuidadosamente planeado (Europol, 2025; Rege & Lavorgna, 2023), no qual os ofensores, atuando de forma isolada ou integrados em redes criminosas, recorrem à construção de identidades falsas, à elaboração de narrativas convincentes e à análise comportamental da vítima, com vista ao reforço progressivo do controlo sobre esta (Europol, 2025; Interpol, 2022). A criação gradual de um vínculo emocional intenso constitui uma estratégia central na medida em que reduz a resistência da vítima e aumenta a sua sustentabilidade a pedidos de natureza financeira (Whitty & Buchanan, 2016).

A literatura distingue várias tipologias de *romance scam*, baseadas no grau de organização dos ofensores, nos métodos de abordagem e nas técnicas de manipulação utilizadas (Bilz et al., 2023; Rege & Lavorgna, 2023). Embora existam diversas variações terminológicas entre os estudos disponíveis, é possível agrupar as principais modalidades em quatro categorias principais:

a) *Romance scam* tradicional: Operado de forma individual ou em pequenos grupos, envolve a criação de um perfil falso em aplicações de encontros ou redes sociais, com vista ao desenvolvimento de uma relação afetiva simulada com a potencial vítima (Cross et al., 2018; Whitty & Buchanan, 2016; Whitty & Buchanan, 2014). O objetivo é consolidar um determinado nível de confiança e, posteriormente, solicitar transferências monetárias com base em falsos pretextos (Cross et al., 2018; Whitty & Buchanan, 2016; Whitty & Buchanan, 2014).
b) *Romance scam* organizado: Gerido por redes criminosas estruturadas, comuns em regiões como a África Ocidental ou o Sudeste Asiático, caracteriza-se pela divisão de tarefas em larga escala, com recurso a *scripts*[7] profissionais, engenharia social avançada e ferramentas tecnológicas sofisticadas (Bilz et al., 2023; Europol, 2025; Rege & Lavorgna, 2023).
c) *Pig-butchering*[8] *romance scam*: Fraude híbrida altamente sofisticada que combina a manipulação emocional com esquemas fraudulentos de investimento, em particular com criptomoedas (FTC, 2025; Malwarebytes, 2024; Wang, 2026; Wang & Topalli, 2024). Após o estabelecimento de uma relação afetiva ou de

[7] Sem tradução direta para português. Refere-se a guiões ou roteiros pré-definidos utilizados pelos *scammers* para conduzir as interações com as vítimas.

[8] Em português "abate de porco". Refere-se a uma modalidade de *romance scam* em que a vítima é "engordada" emocionalmente antes de ser "abatida" financeiramente.

proximidade emocional, o *scammer* apresenta oportunidades de investimento fictícias, o que resulta em perdas financeiras muito elevadas (FTC, 2025; Malwarebytes, 2024; Wang & Topalli, 2024).

d) *Sextortion* romântica: Combina a sedução afetiva com a chantagem emocional e sexual. O *scammer* conduz o contacto de forma a obter conteúdos íntimos da vítima (Monteiro, 2024), seguindo-se a extorsão de dinheiro através da ameaça de divulgação desses conteúdos (Interpol, 2022). Embora nem sempre tenha sido classificada como uma forma de *romance scam*, a literatura recente reconhece a sua proximidade conceptual, dada a forte componente de manipulação emocional envolvida (Interpol, 2022).

Para além destas categorias principais, a literatura identifica subtipos operacionais que se inserem no *romance scam* tradicional e nas variantes híbridas. Entre estes desatam-se o *military romance*, caracterizado por utilização de narrativas associadas a missões militares ou viagens internacionais (Cross et al., 2018; Whitty & Buchanan, 2016), o *pro-dater*, no qual o ofensor promove encontros presenciais com o objetivo de extrair benefícios económicos indiretos (Malwarebytes, 2024), o *cripto-romance*, frequentemente associado a esquemas fraudulentos de investimento (FTC, 2025; Malwarebytes, 2024; Wang & Topalli, 2024), e o *widower scam*, onde é explorado o luto recente ou prolongado de uma pessoa viúva (Cross et al., 2018; Whitty & Buchanan, 2016). Estas variantes não configuram tipologias autónomas, mas antes adaptações narrativas e contextuais de modelos já consolidados, o que reflete a capacidade de adaptação dos ofensores às oportunidades situacionais e socioculturais.

1.3) *Scammer*

O agente criminoso, no contexto do *romance scam*, designa-se por *scammer*. O perfil deste ofensor é heterogéneo, variando entre indivíduos isolados e redes criminosas organizadas, com domínio de competências tecnológicas, capacidades de manipulação psicológica e estratégias de engenharia social sofisticadas (Cross et al., 2018; Whitty & Buchanan, 2016; Wang, 2026; Wang & Topalli, 2024). Este assume uma identidade fictícia em plataformas digitais, com recurso a técnicas estratégicas orientadas para o estabelecimento de uma relação de confiança com potenciais vítimas (Anesa, 2020; Carter, 2021; Wang, 2026; Whitty & Buchanan, 2012). Para o efeito, investe tempo

considerável na recolha de informação sobre a vítima, adaptando o seu discurso e comportamento às vulnerabilidades e necessidades afetivas identificadas, com vista à neutralização das resistências emocionais e à criação de vínculos românticos altamente manipuláveis (Schokkenbroek & Snaphaan, 2025; Yosiandra & Sakariah, 2024). O objetivo final é a obtenção de vantagens económicas, alcançado através da exploração das vulnerabilidades afetivas e psicológicas da vítima (Carter, 2021).

Tal como brevemente referenciado no parágrafo anterior, os *scammers* podem atuar de forma autónoma ou integrados em redes criminosas organizadas. Os ofensores individuais atuam de forma autónoma, procedendo à criação de perfis falsos em plataformas digitais e desenvolvem narrativas afetivas convincentes para conquistar a confiança da vítima (Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2016). Tendem a possuir competências básicas a intermédias em tecnologias digitais, como gestão de Redes Privadas Virtuais (VPNs), roubo de imagens ou uso de contas descartáveis, destacando-se sobretudo pela capacidade de personalizar abordagens emocionais adaptadas às vulnerabilidades específicas de cada vítima, com motivações predominantemente financeiras (Boccardi et al., 2020; Wang & Topalli, 2024). As redes criminosas organizadas, por sua vez, são sediadas em regiões com fiscalização digital limitada, como a África Ocidental ou a Ásia (Europol, 2025; Rege & Lavorgna, 2023), e operam de forma transnacional, estruturada, com divisão de tarefas, formação interna, supervisão hierárquica e utilização de *scripts* padronizados (Europol, 2025; Rege & Lavorgna, 2023; Wang & Topalli, 2024). De acordo com Levi (2012), estas organizações utilizam os lucros obtidos através do *romance scam* para financiar outras atividades ilícitas, incluindo o tráfico de droga, branqueamento de capitais e cibercrime organizado. A sua atuação transnacional permite-lhes explorar assimetrias legais, lacunas na cooperação internacional e limitações dos sistemas judiciais, dificultando a investigação e a responsabilização criminal (Europol, 2025; Levi, 2012; Rege & Lavorgna, 2023).

Do ponto de vista técnico, os *scammers* dividem-se em um domínio relevante de ferramentas digitais, incluindo a criação e gestão simultânea de múltiplos perfis falsos, a utilização de identidades fabricadas, a manipulação de geolocalização através de VPNs e, em contextos mais organizados, a automatização de mensagens em larga escala (Europol, 2025; Wang & Topalli, 2024). A par destas competências tecnológicas, estes ofensores demonstram também capacidades psicológicas avançadas, nomeadamente a leitura emocional das vítimas, a adaptação estratégica do discurso às suas

vulnerabilidades e o recurso sistemático a técnicas de *emotional grooming*[9] (Boccardi et al., 2020; Schokkenbroek & Snaphaan, 2025). A articulação entre competências tecnológicas e manipulação emocional constitui um elemento central para a eficácia da fraude, na medida em que reduz a perceção de risco e prolonga a relação enganosa ao longo do tempo (Wang & Topalli, 2024). Esta combinação tecnológica-emocional é central para o sucesso da fraude.

No que respeita à motivação, embora o objetivo principal seja, na maioria dos casos, a obtenção de ganhos económicos, a literatura indica que muitos ofensores recorrem a mecanismos de racionalização moral da sua conduta (Bilz et al., 2023; Lazarus et al., 2023). Estas racionalizações incluem narrativas de necessidade económica, desigualdade social ou a perceção de que as vítimas pertencem a contextos socioeconómicos mais favorecidos, contribuindo para a neutralização da culpa e para a legitimação subjetiva da fraude (Lazarus et al., 2023). Em contextos de criminalidade organizada, o *romance scam* tende ainda a assumir contornos de atividade profissionalizada, com estruturas internas definidas, metas financeiras e sistemas de recompensa, sendo encarado pelos ofensores como uma ocupação regular e não como um comportamento desviante esporádico (Bilz et al., 2023; Europol, 2025; Wang & Topalli, 2024).

De acordo com Schokkenbroek e Snaphaan (2025), a atuação do *scammer* assenta num conjunto de estratégias padronizadas e meticulosamente planeadas, incluindo: a criação de identidades falsas através de perfis fictícios em redes sociais e/ou aplicações de encontros, apresentando-se como um indivíduo atrativo e financeiramente estável (Boccardi et al., 2020); o desenvolvimento progressivo de laços afetivos fictícios, onde o *scammer* explora as fragilidades emocionais da vítima (Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2016); a solicitação de assistência financeira com recurso a emergências fabricadas, tais como crises de saúde ou imprevistos, para justificar os pedidos monetários (Cole, 2024); e o controlo psicológico alimentado por um falso sentido de urgência e pela indução do medo, com vista a assegurar o envolvimento contínuo da vítima (Boccardi et al., 2020; Yosiandra & Sakariah, 2024). Estes esquemas são frequentemente desenvolvidos por redes criminosas organizadas de carácter transnacional, que recorrem a ferramentas tecnológicas avançadas para dificultar a sua

[9] Em português "aliciamento emocional". Refere-se ao processo pelo qual o scammer constrói deliberadamente uma relação de confiança e proximidade emocional com a vítima, com o objetivo de reduzir as suas resistências e aumentar a sua suscetibilidade à manipulação.

rastreabilidade e preservar o anonimato dos agentes criminosos (Whitty & Buchanan, 2016).

No que respeita às características sociodemográficas dos ofensores, a evidência disponível sugere que os homens tendem a ser os principais perpetradores, embora diversos estudos apontem igualmente para um papel ativo e central das mulheres no *romance scam* (Guerreiro et al., 2024). Uma investigação conduzida no Gana revelou que as mulheres que assumem o papel de ofensoras estão sujeitas a um estigma social mais acentuado do que os homens, em resultado da transgressão das expectativas de género socialmente atribuídas ao sexo feminino (Guerreiro et al., 2024). No que respeita às estratégias de abordagem, a literatura aponta para diferenças em função do género, as ofensoras tendem a privilegiar a sedução como forma de captação de vítimas, ao passo que os ofensores do sexo masculino recorrem com maior frequência à construção de perfis associados a estatutos sociais elevados ou de prosperidade financeira (Guerreiro et al., 2024).

1.3.1) *Modus operandi* e técnicas de manipulação

O processo de execução do *romance scam* segue um padrão estruturado e consciente, quer se trate de ofensores individuais ou de grupos organizados, assente na combinação de engenharia social, manipulação afetiva e ferramentas digitais (Bilz et al., 2023; Wang & Topalli, 2024).

A construção de credibilidade inicial é determinante para o sucesso da fraude. Os perfis falsos recorrem a fotografias roubadas, biografias detalhadas e elementos que apelam à empatia ou admiração da vítima, com profissões de prestígio (militares, engenheiros ou médicos) ou histórias de vida emocionalmente marcantes (Bilz et al., 2023; Whitty & Buchanan, 2016). Após o contato inicial, dá-se início a um processo de *emotional grooming*, caracterizado por mensagens frequentes, demonstrações de afeto, validação emocional e criação de uma sensação de exclusividade (Whitty, 2018; Whitty & Buchanan, 2016). O discurso é adaptado às necessidades emocionais da vítima, identificadas através da observação cuidadosa e perguntas estratégicas (Bilz et al., 2023; Cross et al., 2018; Whitty & Buchanan, 2016).

Consolidada a relação emocional, surgem narrativas de emergência fabricadas, como doenças, problemas legais, dificuldades profissionais ou oportunidades de investimento, que justificam os pedidos de apoio monetário (Whitty & Buchanan, 2016). Estes pedidos são apresentados de forma gradual, com valores inicialmente reduzidos que aumentam progressivamente, explorando a empatia, a lealdade e o medo de perder a relação (FTC, 2025; Wang & Topalli, 2024). Em redes organizadas, como foi dito anteriormente, estas narrativas seguem *scripts* padronizados e testados (Wang & Topalli, 2024).

Em paralelo, são utilizadas diversas técnicas de controlo psicológico com vista a manter a vítima envolvida na dinâmica da fraude. Entre estas destacam-se o reforço intermitente, através da alternância entre afeto intenso e períodos de afastamento, o *gaslighting*[10], que consiste na negação de contradições ou inconsciências acompanhadas da culpabilização da vítima, estratégias de isolamento social, com o desincentivo à partilha da relação com familiares ou amigos (Cross et al., 2018; Whitty & Buchanan, 2016). Os apelos emocionais diretos, como a afirmação de que apenas a vítima pode salvar o ofensor, reforçam o vínculo e a sensação de responsabilidade afetiva (Cross et al., 2018).

No plano operacional, os *scammers* recorrem a mecanismos de ocultação e anonimato, como o uso de VPNs, números de telefone virtuais, contas bancárias temporárias ou intermediários financeiros (Boccardi et al., 2020; Europol, 2025; Wang & Topalli, 2024). Em contextos organizados, verifica-se uma clara divisão de funções, com equipas responsáveis pelo primeiro contato, pela manutenção da relação emocional e pela receção e movimentação dos fundos, o que permite uma atuação em larga escala e dificulta a identificação dos responsáveis (Rege & Lavorgna, 2023; Soares & Lazarus, 2024).

Na fase final, quando os recursos financeiros da vítima se encontram esgotados ou surgem suspeitas mais consistentes, o ofensor tende a desaparecer abruptamente (Bilz et al., 2023; Cross, 2020; Whitty & Buchanan, 2016). Em muitos casos ocorre ainda a revitimação, através da abordagem por novas entidades falsas que prometem recuperar o dinheiro perdido mediante o pagamento de novas quantias, perpetuando o ciclo de exploração económica emocional (Whitty & Buchanan, 2016).

[10] Sem tradução direta pra português. É uma forma de manipulação psicológica na qual o agressor nega sistematicamente a realidade percebida pela vítima, através da distorção de factos, da negação de acontecimentos ou da culpabilização da vítima pelas inconsistências da relação, com o objetivo de a fazer duvidar da sua própria perceção e discernimento.

2) Perspetiva jurídico-criminal do *romance scam*

A análise jurídico-criminal do *romance scam* implica uma abordagem que vá além da aplicação automática dos tipos legais tradicionais, atendendo às especificidades decorrentes da sua prática em ambientes digitais e da centralidade da manipulação emocional no processo criminoso (Cross et al., 2018; Whitty & Buchanan, 2014). Embora este fenómeno seja, em muitos ordenamentos jurídicos, enquadrado no crime de burla, a sua concretização através de plataformas digitais e de relações afetivas simuladas levanta desafios relevantes ao nível da subsunção jurídico-penal, da prova e da resposta sancionatória, colocando em causa a adequação de categorias dogmáticas concebidas para contextos presenciais (Cross et al., 2018; Whitty & Buchanan, 2014).

Acresce que o *romance scam* assume frequentemente uma dimensão transnacional, envolvendo agentes criminosos, vítimas e infraestruturas tecnológicas localizadas em diferentes jurisdições, o que dificulta a investigação criminal e exige mecanismos eficazes de cooperação internacional (Europol, 2025; Interpol, 2022). Neste sentido, nos subcapítulos seguintes procede-se, por um lado, à análise do enquadramento jurídico-criminal do *romance scam* no ordenamento jurídico português, identificando os tipos legais aplicáveis e as principais dificuldades dogmáticas e probatórias e, por outro lado, à apreciação do contexto jurídico-criminal internacional, marcado por instrumentos de cooperação, esforços de harmonização normativa e limitações práticas associadas à natureza global do cibercrime (Europol, 2025; Interpol, 2022).

2.1) Enquadramento jurídico-criminal no ordenamento português

No ordenamento jurídico português, as condutas associadas ao *romance scam* encontram em regra enquadramento na figura típica da burla prevista no artigo 217.º do CPP, e no artigo 218.º, quando qualificada, integrada nos crimes contra o património (Código Penal - Edição Académica, 2023). A previsão legal deste crime pressupõe a utilização de meios enganosos, como artifícios, manipulações ou falsas representações, com vista à indução da vítima em erro, levando-a à prática de atos que resultam num prejuízo patrimonial (Código Penal - Edição Académica, 2023). A estrutura típica exige, além do nexo causal entre o engano e o prejuízo, a verificação de uma intenção de enriquecimento ilegítimo à custa do património alheio (Albuquerque, 2024; Costa, 2020), sendo o bem jurídico tutelado o património, constitucionalmente protegido pelo artigo 62.º da Constituição da

República Portuguesa (CRP) (Guerreiro et al., 2024). Trata-se, na generalidade dos casos, de um crime semipúblico, dependente de queixa, punível com pena de prisão até três anos ou pena de multa (Guerreiro et al., 2024). O artigo 218.º do CPP aplica-se quando esteja em causa um prejuízo patrimonial de valor elevado, quando o agente criminoso faça da burla um modo de vida, quando a vítima se encontre em situação de especial vulnerabilidade em razão de idade, deficiência ou doença, ou quando a vítima fique em difícil situação económica na sequência do crime (Código Penal - Edição Académica, 2023; Guerreiro et al., 2024). Neste caso, o crime é punível com pena de prisão até cinco anos ou pena de multa até 600 dias (Código Penal - Edição Académica, 2023).

Para além do enquadramento no artigo 217.º, o ordenamento jurídico português prevê ainda a figura da burla informática e nas comunicações, consagrada no artigo 221.º do CPP, cuja aplicação se revela pertinente nas situações em que o engano é perpetrado exclusivamente através de meios tecnológicos (Código Penal - Edição Académica, 2023). No *romance scam*, o meio fraudulento utilizado é inteiramente digital, com recurso a perfis falsos, sistemas de comunicação eletrónica e outras ferramentas digitais (Lazarus et al., 2023), o que torna esta norma particularmente relevante. A evolução da jurisprudência tem vindo a reconhecer a necessidade de uma interpretação funcional destas normas, capaz de responder às especificidades da criminalidade digital e às novas formas de execução da burla em ambientes online (Albuquerque, 2024; Costa, 2020).

No contexto específico do *romance scam*, a verificação dos elementos construtivos do crime de burla (o engano, o prejuízo patrimonial e a intenção de enriquecimento) assume contornos particulares. A atuação do *scammer* desenvolve-se, em regra, ao longo do tempo, através da construção gradual de uma relação afetiva fictícia assente na manipulação emocional e na exploração da confiança da vítima (Cross et al., 2018; Whitty & Buchanan, 2016). O carácter fraudulento da interação nem sempre é imediatamente percetível, quer para a vítima, quer para terceiros, o que dificulta a identificação precoce do engano e, consequentemente, a intervenção atempada das autoridades (Cross et al., 2018; Whitty & Buchanan, 2016).

O *romance scam* pode ainda entrecruzar-se com outras formas de criminalidade (Guerreiro et al., 2024). A conduta do agente pode gerar responsabilidade civil pelos danos patrimoniais e morais causados à vítima, nos termos dos artigos 483.º e seguintes do Código Civil (CC) (Portugal, 1966). Em função das circunstâncias concretas, poderão ainda ser convocados outros tipos legais, nomeadamente os crimes informáticos previstos

na Lei n.º 109/2009, de 15 de setembro (Assembleia da República, 2009), a fraude sexual prevista no artigo 167.º do CPP (Código Penal - Edição Académica, 2023) ou, em contextos de maior gravidade, o crime de violência doméstica nos termos do artigo 152.º do CPP (Código Penal - Edição Académica, 2023). Não obstante a abrangência deste enquadramento, o *romance scam* é frequentemente tratado como crime exclusivamente patrimonial, o que tende a desconsiderar a dimensão emocional e relacional da vitimação, revelando lacunas na resposta institucional a este tipo de criminalidade.

Acresce que o *romance scam* apresenta frequentemente uma dimensão transnacional, decorrente da utilização de plataformas digitais e redes sociais que permitem ao agente atuar a partir de jurisdições distintas daquela em que se encontra a vítima (Cross et al., 2018; Soares & Lazarus, 2024). Esta circunstância coloca desafios significativos à investigação criminal, designadamente no que respeita à identificação dos agentes criminosos, à recolha e preservação da prova digital, e à efetivação da cooperação judiciária internacional (Cross et al., 2018; Soares & Lazarus, 2024).

2.2) Enquadramento jurídico-criminal internacional

No plano internacional, o *romance scam* é amplamente reconhecido como uma modalidade específica de fraude cibernética, integrada no fenómeno mais amplo da cibercriminalidade (Europol, 2025; Interpol, 2022). A crescente dependência das plataformas digitais enquanto meios de interação interpessoal tem proporcionado um ambiente particularmente favorável à prática deste tipo de crimes, ao permitir aos agentes criminais o contacto com vítimas localizadas em diferentes jurisdições (Europol, 2025; Interpol, 2022; Holt et al., 2022). Organizações internacionais de cooperação policial, como a Interpol e Europol e o FBI, têm vindo a assinalar o impacto global do *romance scam*, destacando que estas práticas são frequentemente desenvolvidas por redes criminosas transnacionais estruturadas, o que agrava a complexidade da sua investigação e repressão penal (Europol, 2025; Interpol, 2022).

Em vários ordenamentos jurídicos, o *romance scam* enquadra-se no âmbito dos crimes de fraude praticados por meios eletrónicos. A título de exemplo, nos Estados Unidos da

América (EUA), estas condutas são, em regra, integradas no crime *wire fraud*[11], previsto no 18 U.S.C § 1343, que criminaliza o uso de comunicações eletrónicas com intenção de defraudar terceiros (Wang, 2025). Os dados divulgados anualmente pelo IC3, evidenciam um crescimento consistente deste tipo de criminalidade ao longo dos anos, bem como a crescente sofisticação das estratégias utilizadas pelos agentes criminosos (Wang, 2025).

A Convenção sobre o Cibercrime de 2001, conhecida como Convenção de Budapeste, constitui o principal instrumento jurídico internacional no combate à criminalidade digital, firmada no âmbito do Conselho da Europa e ratificado por Portugal em 2010 (Council of Europe, 2022). Este tratado desempenhou um papel central na harmonização legislativa entre os Estados signatários e no reforço dos mecanismos de cooperação internacional em matérias como a recolha e preservação da prova digital, a investigação criminal e a extradição (Council of Europe, 2022; Tropina, 2024). Estas dimensões assumem particular relevância no combate ao *romance scam*, dado o seu carácter frequentemente transfronteiriço. Não obstante, a literatura especializada sublinha que persistem disparidades significativas entre o sistema jurídicos nacionais, bem como assimetria nos recursos técnicos e institucionais disponíveis, o que continua a representar um obstáculo significativo à construção de um sistema penal uniforme e eficaz (Tropina, 2024).

Diversos estudos indicam que, muitas das vítimas deste crime enfrentam barreiras emocionais e sociais à denúncia, nomeadamente sentimentos de vergonha, estigmatização social e dificuldade em reconhecer a manipulação sofrida (Cole, 2024; Cross et al., 2018; Whitty & Buchanan, 2016). Estes fatores contribuem para a subnotificação dos casos e para a persistência de elevadas cifras negras associadas a este fenómeno criminal (Boccardi et al., 2020; Schokkenbroek & Snaphaan, 2025). Uma resposta jurídico-criminal eficaz exige, assim, não apenas instrumentos legais adequados e cooperação internacional reforçada, mas também estratégias que atendam às especificidades da vitimação associada ao *romance scam* (Cole, 2024; Europol, 2025; Tropina, 2024).

[11] Em português "fraude eletrónica". Consiste na utilização de meios de comunicação eletrónica com o objetivo de executar esquemas fraudulentos para obtenção de dinheiro ou bens de terceiros.

3) Teorias explicativas do *romance scam*

O *romance scam* tem sido analisado à luz de diversas perspetivas teóricas no âmbito da criminologia. Todavia, a literatura empírica disponível sugere que tais abordagens tendem a explicar dimensões específicas e distintas entre si, em vez de fornecerem uma explicação única e abrangente (Bilz et al., 2023; Schokkenbroek & Snaphaan, 2025). De forma consistente, os estudos demonstram que determinadas teorias são particularmente úteis para compreender os fatores que aumentam a exposição e a oportunidade de vitimação, enquanto outras se focam na análise dos processos de decisão e da adaptação estratégica dos ofensores (Abubakari & Oseh-Ovarah, 2025; Dickinson et al., 2023; Offei et al., 2022). Paralelamente, algumas teorias destacam os mecanismos que sustentam o envolvimento continuado da vítima, designadamente através de estratégias de manipulação emocional e de controlo relacional (Carter, 2021; Coluccia et al., 2020; Whitty, 2013). Neste contexto, assumem particular relevância a teoria dos estilos de vida, a teoria das atividades rotineiras, a prevenção situacional do crime, a teoria dos padrões criminais, a teoria da escolha racional, a teoria da racionalidade limitada e a teoria do controlo social, uma vez que, de forma complementar, permitem analisar os fatores que influenciam a seleção do alvo, a execução do esquema fraudulento e a continuidade do processo de vitimação (Dickinson et al., 2023; Feng, 2025; Schokkenbroek & Snaphaan, 2025). Cada uma destas abordagens será analisada em seguida, procurando evidenciar o seu contributo para a compreensão do fenómeno.

A teoria dos estilos de vida foi proposta por Hindelang, Gottfredson e Garofalo, em 1978, e sustenta que a probabilidade de vitimação está relacionada com os diferentes estilos de vida adotados por cada indivíduo (Costa, 2021), resultando de fatores sociais e externos, e não de características pessoais, biológicas ou psicológicas (Monteiro, 2024). Neste contexto, a maior ou menor predisposição de um indivíduo para se tornar numa potencial vítima é determinada pelo estilo de vida que adota e pelo consequente grau de exposição ao risco (Costa, 2021). No ambiente digital, este enquadramento revela-se útil ao considerar que hábitos online, como o tempo despendido em redes sociais, podem ampliar a exposição a fraudes. Estudos recentes sugerem que a permanência prolongada em plataformas digitais está associada a uma maior suscetibilidade a riscos cibernéticos, incluindo esquemas de *romance scam* (Tintori et al., 2023). Contudo, um dos limites desta teoria reside no pressuposto de que a vitimação é sempre influenciada pelos hábitos dos indivíduos, o que tende a subestimar a aleatoriedade e a ação deliberada do *scammer*

(Costa, 2021). Whitty & Buchanan (2012), analisaram fatores clássicos desta teoria, como procura ativa de parceiros online, a exposição em *apps* de encontros e os comportamentos de risco em ambiente digital, concluindo que a utilização frequente destas plataformas constitui uma rotina digital que aumenta a exposição a ofensores motivados. Vakhitova et al. (2019), demonstraram, por sua vez, que estilos de vida digitais e a exposição frequente a interações sociais online estão associados a um maior risco de vitimação. Guerra & Ingram (2022), reforçam esta perspetiva, destacando a exposição digital e a vulnerabilidade online como fatores determinantes na suscetibilidade à vitimação por *romance scam*.

A teoria das atividades rotineiras (RAT) formulada por Lawrence Cohen e Marcus Felson, em 1979, explica o aumento das taxas de criminalidade após a Segunda Guerra Mundial através das transformações sociais e das alterações nas rotinas quotidianas dos indivíduos (Cohen & Felson, 1979). Embora originalmente desenvolvida para explicar a vitimação em contextos presenciais, a RAT é igualmente aplicável ao ciberespaço, onde o uso recorrente de tecnologias cria oportunidades para a ação criminosa (Monteiro, 2024). De acordo com Martins et al. (2023), no ciberespaço, a maioria das fraudes envolve conteúdos informativos digitais e atividades rotineiras realizadas online, que aumentam o risco e a atratividade para um potencial *scammer*. A RAT evidencia ainda como a crescente dependência de meios digitais amplia a exposição dos indivíduos a situações de risco, na medida em que a intensificação das interações online cria novas oportunidades para ofensores motivados explorarem vítimas em ambientes onde os mecanismos de proteção são frequentemente insuficientes (Cohen & Felson, 1979; Holt et al., 2022). De acordo com Saraiva (2021), esta teoria assenta na verificação simultânea de três condições, sendo que, na ausência de qualquer uma destas, o crime não ocorre: i) a presença de um alvo apropriado e atrativo, que pode ser um objeto, uma pessoa, ou outro alvo de conduta criminal; ii) a ausência de vigilância ou de um guardião adequado; iii) a existência de um transgressor motivado. Um dos pontos críticos desta teoria é a suposição de que o infrator está sempre motivado, o que nem sempre se verifica na prática (Saraiva, 2021). Vakhitova et al. (2019), demonstraram que rotinas online, padrões de utilização da Internet e exposição frequente a interações sociais digitais estão associados a um maior risco de vitimação. Guerra & Ingram (2022), reforçam esta perspetiva, destacando as atividades de risco em ambientes digitais como fator determinante na suscetibilidade à vitimação.

A teoria da prevenção situacional do crime (SCP), desenvolvida por Ronald Clarke em 1980, parte do princípio de que o crime ocorre na presença de uma oportunidade e, de que, por isso, as estratégias de prevenção devem centrar-se na redução dessas oportunidades (Clarke, 1995). A principal crítica a esta abordagem é a ideia de que a eliminação da oportunidade seria suficiente para impedir a ocorrência do crime, independentemente da motivação do ofensor (Saraiva, 2021). No ambiente digital, contudo, as oportunidades são abundantes, dado o elevado número de utilizadores vulneráveis e a facilidade do contacto entre desconhecidos. Neste sentido, Leukfeldt (2014), demonstrou que o design tecnológico, a ausência de barreiras e as vulnerabilidades situacionais facilitam a prática de crimes online. Do mesmo modo, as plataformas digitais encontram-se frequentemente estruturadas de forma pouco eficaz, com ausência de verificação robusta de identidades e possibilidade de contacto instantâneo entre desconhecidos (Abu-Salma et al., 2025). Cross, et al. (2016), complementam esta perspetiva destacando a ausência de controlo institucional e de mecanismos de confiança como fatores que ampliam as oportunidades criminais. Face a este diagnóstico, a literatura aponta para a necessidade de reduzir as oportunidades criminais, aumentar o risco percebido pelo ofensor e reforçar a vigilância nas plataformas digitais (Cross, et al., 2016), bem como de identificar e mitigar as vulnerabilidades situacionais através de estratégias de prevenção baseadas no ambiente digital (Schokkenbroek & Snaphaan, 2025).

A teoria dos padrões criminais (CPT), proposta por Paul e Patricia Brantingham, em 1980, analisa o crime como resultado da convergência simultânea de vários elementos, como o alvo, o ofensor e a localização (Saraiva, 2021). Ao contrário de outras teorias, a CPT enfatiza a importância do contexto e do espaço onde o crime ocorre, argumentando que a ocorrência criminal não é aleatória, mas antes resultado de processos planejados ou oportunistas (Saraiva, 2021). No *romance scam*, a localização pode ser entendida como o ambiente digital global onde o ofensor e a vítima se encontram através de plataformas online, sendo as oportunidades determinadas por fatores como a vulnerabilidade da vítima, o nível de segurança cibernética e os comportamentos de risco dos utilizadores de Internet (Monteiro, 2024). Whitty (2018), demonstrou que os ofensores tendem a concentrar a sua atuação em determinados ambientes digitais, com seleção criteriosa das vítimas em plataformas específicas. Schokkenbroek & Snaphaan (2025), complementam esta perspetiva, identificando padrões de deslocação digital entre plataformas e a

utilização de múltiplos canais de contato como estratégias recorrentes dos agentes criminosos. De acordo com Leukfeldt & Yar (2016), os ambientes digitais estruturam e condicionam as oportunidades criminais, determinando em larga medida os contextos em que a vitimação ocorre.

A teoria da escolha racional (RCT), desenvolvida em 1995, sustenta que os potenciais ofensores agem de forma deliberada, avaliando custos e benefícios antes de praticar o crime (Saraiva, 2021). O crime tende a ocorrer quando o ofensor avalia que as vantagens obtidas superam os riscos envolvidos (Saraiva, 2021), podendo a criminalidade ser reduzida através de estratégias que aumentem esses riscos. Clarke (1995) propôs um conjunto de 25 estratégias preventivas, agrupadas em cinco categorias: 1) reduzir as recompensas e benefícios associados à prática do crime; 2) aumentar os riscos associados à prática do crime; 3) aumentar o esforço tornando mais difícil para os criminosos cometerem os crimes; 4) remover as "desculpas", eliminando as justificativas que os criminosos possam utilizar para justificar os seus atos; 5) reduzir as provocações que incentivam a ocorrência de crimes. De acordo com Kopp et al. (2015), o ofensor seleciona alvos vulneráveis com o objetivo de os explorar de forma eficiente e maximizar o lucro obtido. Cross, et al. (2016), acrescenta que os ofensores avaliam igualmente a probabilidade de denúncia por parte da vítima, explorando a sua reduzida propensão para reportar o crime como forma de minimizar o risco percebido e otimizar a relação custo-benefício da fraude.

A teoria da racionalidade limitada, baseada em Simon (1997), e aprofundada por Kahneman (2011), explica como fatores emocionais e cognitivos podem conduzir a decisões que parecem irracionais. Em situações de elevada carga emocional, como as relações afetivas online, a capacidade de processamento de informação tende a ser reduzida, tornando a vítima mais suscetível à manipulação (Grant & Buil-Gil, 2025). De acordo com Whitty (2013), o *scammer* constrói gradualmente uma relação de confiança com a vítima, através da manipulação das suas emoções e do seu isolamento cognitivo, conduzindo-a à tomada de decisões não totalmente racionais, sob forte influência afetiva e com consequente redução da capacidade crítica. A vítima passa a interpretar os sinais de confiança de forma enviesada, a ignorar alertas e inconsistências (Kopp et al., 2015), manifestando dependência emocional, suscetibilidade à manipulação relacional e coerção psicológica (Cross et al., 2018), bem como impulsividade, idealização romântica e necessidade de afeto (Lazarus et al., 2023).

A teoria do controlo social, formulada por Hirschi em 1969, defende que, indivíduos com laços sociais enfraquecidos, pela ausência de vínculos familiares, comunitários ou institucionais, tendem a ser mais suscetíveis à manipulação, tornando-se alvos mais vulneráveis a esquemas como o *romance scam*, onde a exploração emocional assenta precisamente nessas fragilidades relacionais (Holt et al., 2022). Whitty & Buchanan (2012), demonstraram que muitas vítimas experienciavam sentimentos de solidão e procuravam uma ligação emocional, o que vem evidenciar que laços sociais frágeis aumentam a vulnerabilidade à manipulação. Esta vulnerabilidade é agravada quando o ofensor promove ativamente o isolamento da vítima, desincentiva o contato com terceiros e cria dependência emocional, sendo que, quanto maior for a fragilidade dos vínculos sociais maior será o risco de manipulação (Cross et al., 2018). Lazarus et al. (2023), reforça esta perspetiva, identificando a solidão, a necessidade de pertença e a procura intensa de intimidade como fatores que, articulados com o enfraquecimento dos vínculos sociais, potenciam a vitimação por *romance scam*.

Em síntese, tanto as perspetivas teóricas como a evidência empírica disponível, não sustentam a existência de uma única teoria explicativa do fenómeno do *romance scam*. Em vez disso, a literatura aponta para a necessidade de uma abordagem integradora, que articule diferentes quadros concetuais na compreensão deste tipo de fraude (Cross, 2020; Feng, 2025; Wang, 2026). Neste sentido, as teorias centradas na exposição ao risco e nas oportunidades de vitimação permitem compreender os fatores que aumentam a probabilidade do contacto entre vítimas e ofensores, enquanto que, as teorias da decisão contribuem para explicar a forma como os ofensores ajustam estrategicamente as suas condutas em função do risco e da potencial recompensa (Abubakari & Oseh-Ovarah, 2025; Dickinson et al., 2023). Por sua vez, as abordagens psicológicas e relacionais esclarecem os mecanismos que favorecem a manutenção do envolvimento da vítima, mesmo perante indícios de fraude (Cross, 2020; Whitty, 2013). Nesta perspetiva, o *romance scam* é melhor compreendido como um fenómeno multidimensional, resultante da articulação entre oportunidades digitais, estratégias criminosas adaptativas, processos de neutralização e racionalização do comportamento por parte do ofensor e vulnerabilidades emocionais e relacionais da vítima (Holt et al., 2022; Rege & Lavorgna, 2023; Schokkenbroek & Snaphaan, 2025). Consequentemente, um dos principais avanços da investigação tem consistido na transição de explicações unidimensionais para modelos analíticos integradores (Cross, 2020; Feng, 2025; Wang, 2026). Apesar deste progresso,

permanece por esclarecer-se, com maior robustez empírica, de que forma estas diferentes dimensões interagem ao longo das várias fases do esquema fraudulento e em distintos subtipos de *romance scam* (Schokkenbroek & Snaphaan, 2025; Wang, 2026).

4) Vitimação e comportamentos de autoproteção em contexto digital

A criminologia tem vindo a contribuir para a análise do *romance scam*, ao fornecer perspetivas sobre a vitimação, analisar as motivações criminais e os contextos ambientais digitas (Boccardi et al., 2020; Cole, 2024; Schokkenbroek & Snaphaan, 2025), complementando as teorias abordadas anteriormente.

A vitimologia identifica padrões de vulnerabilidade explorados pelos *scammers*, como a solidão e a baixa literacia digital, verificando-se uma maior incidência em vítimas do sexo feminino e de meia-idade (Souza, 2022). Os estudos criminológicos destacam o duplo impacto financeiro e emocional deste tipo de crime, distinguindo o *romance scam* de outras fraudes pela manipulação prolongada da confiança (Whitty, 2018). A criminologia ambiental, por sua vez, examina as plataformas digitais como espaços de elevada concentração criminal, onde o anonimato e os algoritmos de correspondência aumenta a exposição e a vulnerabilidade das vítimas (Felson & Eckert, 2021; Rege & Lavorgna, 2023).

No plano individual, a adoção de uma postura analítica e a recusa em partilhar informações pessoais ou realizar transferências financeiras para desconhecidos revelam-se fundamentais para a mitigação do risco (Europol, 2025; FTC, 2025; Schokkenbroek & Snaphaan, 2025). Do mesmo modo, a identificação de indicadores de risco, como solicitações monetárias, narrativas excessivamente dramáticas ou pressões emocionais, constitui um elemento essencial na prevenção da vitimação (Boccardi et al., 2020; Cole, 2024; Yosiandra & Sakariah, 2024).

Face a estas vulnerabilidades, a literatura aponta para a necessidade de estratégias preventivas que incluam campanhas de sensibilização, legislação direcionada para plataformas negligentes e o desenvolvimento de uma perceção pública mais clara sobre a gravidade e a ilicitude deste tipo de crime (Europol, 2025; Schokkenbroek & Snaphaan, 2025; Souza, 2022).

4.1) Perfil da vítima

As vítimas de *romance scam* têm sido alvo de estudo devido à conjugação de fatores emocionais, sociais e patrimoniais que aumentam a sua vulnerabilidade (Cole, 2024; Cross et al., 2018; Whitty & Buchanan, 2016). Embora determinados fatores individuais possam contribuir para o aumento dessa vulnerabilidade, a vitimação resulta sobretudo da combinação entre características pessoais, circunstâncias emocionais estratégias sofisticadas de manipulação utilizadas pelos ofensores (Cross et al., 2018; Whitty & Buchanan, 2016). A literatura identifica, contudo, padrões recorrentes que permitem delinear características típicas das vítimas, não obstante a inexistência de um perfil único e universal.

No que respeita aos fatores demográficos, os estudos internacionais indicam que as vítimas se situam maioritariamente em faixas etárias adultas ou de meia-idade, com particular incidência entre os 40 e os 65 anos, embora os casos envolvendo jovens adultos estejam em crescimento devido à expansão das plataformas digitais (FTC, 2025; Wang & Topalli, 2024). O género não constitui um fator determinante, ainda que algumas investigações apontem para uma ligeira predominância de vítimas do sexo feminino em determinados contextos culturais (Cross et al., 2018; Lazarus, 2024).

No que concerne às vulnerabilidades emocionais situacionais, a literatura destaca que estados emocionais específicos, como a solidão, o isolamento social e as carências efetivas, podem aumentar a suscetibilidade à manipulação (Boccardi et al., 2020; Cross et al., 2018). Estas vulnerabilidades não são de natureza patológica, mas refletem momentos de maior necessidade de conexão social, que os ofensores exploram através de estratégias de *emotional grooming* (Cross et al., 2018; Schokkenbroek & Snaphaan, 2025).

Relativamente aos fatores psicológicos e cognitivos, alguns estudos sugerem que as vítimas de *romance scam* tendem a apresentar níveis elevados de confiança interpessoal, empatia e desejo de intimidade, características que, embora positivas, podem ser instrumentalizadas pelos ofensores (Whitty & Buchanan, 2016). A heurística da reciprocidade, a tendência para acreditar em narrativas coerentes e a dificuldade em reconhecer sinais de fraude na presença de envolvimento emocional são elementos frequentemente observados neste tipo de vitimação (Kahneman, 2011).

No plano socioeconómico e cultural, a pressão social para a formação de relações afetivas, a estigmatização da solidão e a normalização das interações digitais contribuem para a exposição a este tipo de fraude (Lazarus, 2024; Whitty & Buchanan, 2014). Embora todas as classes sociais possam ser alvo, indivíduos com recursos financeiros disponíveis tendem a ser explorados com maior frequência, dada a possibilidade de um maior ganho monetário por parte do ofensor (Europol, 2025). A vergonha associada à vitimação, frequentemente reforçada por discursos públicos culpabilizadores agrava o impacto psicológico e dificulta a denúncia (Cole, 2024; Cross et al., 2018).

Por fim, no que respeita à literacia digital e à perceção de risco, a baixa literacia digital, aliada ao desconhecimento de práticas de engenharia social, constitui um fator de risco relevante (Cross et al., 2018; Tintori et al., 2023). Muitas vítimas não identificam sinais de alerta como perfis inconsistentes, pedidos de dinheiro ou padrões comunicacionais típicos de esquemas fraudulentos (Europol, 2025; Malwarebytes, 2024). A perceção de risco tende a diminuir à medida que a relação emocional se intensifica, com consequente redução da capacidade crítica e aumento da dependência afetiva.

4.2) Processo de vitimação

O processo de vitimação no *romance scam* caracteriza-se por ser gradual, estruturado e emocionalmente intenso, distinguindo-se de outras fraudes patrimoniais pela profundidade da manipulação psicológica envolvida. Este crime não se limita a causar prejuízo económico, também desencadeia um conjunto de dinâmicas emocionais e cognitivas que moldam a experiência da vítima e dificultam a perceção do engano (Cross et al., 2018; Whitty & Buchanan, 2016). A literatura atual destaca os seguintes processos de vitimação:

a) Ilusão da intimidade: A vitimação tem início com a criação de uma relação afetiva simulada, construída de forma gradual através de plataformas digitais (Whitty & Buchanan, 2016). A vítima desenvolve sentimentos de confiança e ligação emocional com o ofensor, acreditando estar perante uma relação autêntica (Bilz et al., 2023; Whitty & Buchanan, 2016). Esta fase corresponde ao *emotional grooming*, no qual o ofensor reduz a perceção de risco e aumenta a dependência emocional da vítima.

b) Dependência emocional: À medida que a relação se aprofunda, a vítima passa a depender emocionalmente do ofensor, valorizando a atenção, o apoio e a sensação de intimidade criada artificialmente (Cross et al., 2018; Schokkenbroek & Snaphaan, 2025). Esta dependência dificulta a interrupção do contato ou o reconhecimento de sinais de fraude, mesmo perante inconsistências evidentes (Cross et al., 2018; Schokkenbroek & Snaphaan, 2025). O envolvimento afetivo funciona como um mecanismo de controlo, com consequente diminuição da capacidade crítica e reforço da vulnerabilidade (Boccardi et al., 2020; Cole, 2024).
c) Vergonha e estigmatização: Após o surgimento de pedidos financeiros ou a descoberta da fraude, muitas vítimas tendem a experienciar sentimentos intensos de culpa, vergonha e humilhação (Cole, 2024; Cross et al., 2018; Whitty & Buchanan, 2016). Estes sentimentos são amplificados pelo estigma social associado à vitimação em *romance scam*, frequentemente percecionadas como resultados de ingenuidade ou falta de cautela (Boccardi et al., 2020; Cross et al., 2018). A vergonha contribui para o isolamento social e constitui um dos principais fatores que explicam a elevada subnotificação deste crime (Cross et al., 2018; Europol, 2025; Schokkenbroek & Snaphaan, 2025).
d) Impacto psicológico: Para além do prejuízo económico, as consequências emocionais do *romance scam* podem incluir ansiedade, depressão, baixa autoestima, perda de confiança interpessoal e, em alguns casos, sintomas compatíveis com trauma emocional (Cross et al., 2018; Whitty & Buchanan, 2014). Ao contrário do impacto financeiro, o impacto psicológico tende a prolongar-se no tempo, sobretudo quando a vítima enfrenta dificuldades em aceitar a manipulação sofrida ou quando ocorre revitimação.

Estes processos demonstram que o *romance scam* é um fenómeno multidimensional, no qual a exploração emocional e psicológica se combina com a obtenção de ganhos patrimoniais, exigindo abordagens de prevenção, intervenção e apoio que transcendam o âmbito estritamente económico.

4.3) Impacto da vitimação

O impacto da vitimação no *romance scam* manifesta-se de forma profunda e multidimensional, ultrapassando largamente o prejuízo económico inicial. A literatura

especializada destaca consequências psicológicas, sociais e económicas duradouras, com efeitos significativos no bem-estar e na qualidade de vida das vítimas (Cross et al., 2018; Whitty & Buchanan, 2014).

Do ponto de vista psicológico, as vítimas de *romance scam* apresentam frequentemente sintomas de ansiedade, depressão, stress pós-traumático, baixa autoestima e sentimentos persistentes de desvalorização pessoal (Cole, 2024; Cross et al., 2018). A descoberta da fraude tende a provocar um colapso emocional associado à perceção de traição, à perda de confiança e à rotura da ilusão afetiva construída ao longo do tempo (Whitty & Buchanan, 2014). Em casos mais graves, são identificados sintomas de trauma psicológico, sobretudo quando a relação fraudulenta se prolonga ou envolve perdas financeiras significativas (Cross et al., 2018; Schokkenbroek & Snaphaan, 2025).

No plano social, o impacto do *romance scam* traduz-se frequentemente em isolamento, retraimento social e dificuldades em estabelecer ou retomar relações interpessoais (Boccardi et al., 2020; Whitty & Buchanan, 2016). O estigma associado e a tendência para culpabilizar a vítima fomentam sentimentos de vergonha e silêncio, limitando o acesso a redes de apoio formal e informal e contribuindo para a subnotificação dos casos (Cole, 2024; Cross et al., 2018; Europol, 2025).

No plano económico, as consequências financeiras podem gerar efeitos secundário relevantes, como endividamento, a perda de poupanças, a instabilidade financeira e o comprometimento da autonomia pessoal, com particular incidência em vítimas em idade avançada ou em situação de vulnerabilidade prévia (Europol, 2025; FTC, 2025). Estas consequências tendem a intensificar os efeitos psicológicos, criando um ciclo de fragilização emocional e social.

Por fim, a literatura sublinha o risco de revitimação, na medida em que vítima emocionalmente fragilizadas ficam mais expostas a novas situações de exploração (Bilz et al., 2023). Este fenómeno reforça a necessidade de respostas integradas que articulem prevenção, apoio psicológico especializado e intervenção institucional.

4.4) Fatores de risco e fatores de proteção

A vitimação em *romance scam* está associada a múltiplos fatores de risco interligados, que incluem características psicológicas, emocionais, situacionais e digitais, bem como

fatores de proteção que podem mitigar a probabilidade de ser alvo desta forma de crime (Cross et al., 2018; Lazarus et al., 2023; Whitty & Buchanan, 2016). Estudos empíricos revelam que indivíduos com experiência reduzida no uso de plataformas digitais ou literacia digital limitada, tendem a apresentar maior exposição e sustentabilidade a perfis e interações fraudulentas, dada a dificuldade em reconhecer sinais de alerta, padrões comunicacionais suspeitos ou técnicas de engenharia social utilizadas pelos ofensores (Saad et al., 2018). Estudos de revisão sistemática recentes indicam que variáveis psicológicas e de personalidade, como a impulsividade, a tendência à idealização romântica, a elevada confiança interpessoal e a procura ativa de parceiro em plataformas online, estão associadas a um maior risco a risco de vitimação em *romance scam* (Lazarus et al., 2023; Schokkenbroek & Snaphaan, 2025; Whitty, 2018).

Do ponto de vista demográfico, estudos sistemáticos indicam que, determinados grupos populacionais, como mulheres com níveis educacionais mais elevados, adultos de meia-idade e utilizadores que frequentam ativamente *apps* de encontros, podem apresentar um maior risco de vitimação, possivelmente em função de uma maior exposição à interação online de níveis variáveis de literacia digital (Lazarus et al., 2023; Thumboo & Mukherjee, 2024; Whitty, 2018). Além disso, fatores situacionais como o *design* da plataforma, os contactos instantâneos e a ausência de verificação rigorosa de identidades facilitam o surgimento de relações aparentemente legítimas que evoluem para esquemas fraudulentos (Abu-Salma et al., 2025; Schokkenbroek & Snaphaan, 2025; Thumboo & Mukherjee, 2024).

No que respeita aos fatores de proteção, a literacia digital, definida como a capacidade de compreender, interpretar e agir de forma crítica em ambientes digitais, é amplamente reconhecida como um elemento que melhora a perceção do risco, facilita a identificação de perfis suspeitos e reduz comportamentos de exposição a *scammers* (DECO PROTeste, 2024). A consciência das próprias vulnerabilidades e dos mecanismos de engenharia social está igualmente associada a uma maior cautela, com adoção de práticas como a verificação de identidade, o recurso a videochamadas em detrimento de comunicação exclusivamente textual e a consulta de terceiros antes do envio de dinheiro ou dados sensíveis (ACI Worldwide, 2024).

O suporte social e familiar constitui também um fator de proteção relevante, na medida em que oferece uma rede de verificação e orientação capaz de atenuar o isolamento e a pressão emocional, reduzindo a suscetibilidade à manipulação afetiva pelos ofensores

(RSRC, 2025). A conjugação destes fatores de proteção contribui para a diminuição, tanto da exposição a situações de risco, como do impacto após a vitimação ocorrer, reforçando a resiliência dos utilizadores face a esquemas fraudulentos em ambientes online.

4.5) Comportamentos individuais de prevenção e evitamento do crime

Os comportamentos de proteção e evitamento do crime constituem elementos centrais na mitigação da vitimação associada ao *romance scam*. A implementação de práticas preventivas de cibersegurança, como a utilização de ferramentas tecnológicas de proteção (e.g., autenticação de dois fatores, bloqueadores de *spam* e antivírus atualizados), tem vindo a ser associada a uma diminuição da vulnerabilidade e ao reforço das estratégias de autoproteção entre os utilizadores digitais (DECO PROTeste, 2024). Tais práticas incluem condutas preventivas concretas, reconhecidas como boas práticas de segurança online, tais como evitar clicar em *links* suspeitos, não divulgar informações pessoais e adotar políticas de *passwords* robustas (University of California, 2025).

A investigação sobre vitimação digital evidencia ainda que, indivíduos com maior perceção de risco tendem a apresentar comportamentos de proteção mais consistentes, como a verificação crítica de mensagens, o recurso a sistemas de verificação de identidade e a adoção de medidas de segurança adicionais após experiências de vitimação (e.g., alteração de *passwords*, ativação de autenticação de dois fatores, entre outros) (Tsunoda & Sato, 2025). Ainda assim, a literatura sublinha que a adesão a estas medidas permanece desigual em relação aos casos conhecidos de *romance scam*, revelando limitações ao nível da autoeficácia percebida em segurança digital (Hameed et al., 2023).

Por outro lado, estratégias de evitamento, tais como a redução voluntária do uso de *apps* de encontros ou a limitação de interações com desconhecidos em plataformas digitais, surgem frequentemente como respostas defensivas após a perceção do risco (Tsunoda & Sato, 2025). Contudo, a literatura sobre vitimação digital, alerta que um evitamento exacerbado pode gerar efeitos contraproducentes, tais como o aumento de ansiedade em interações online, a redução de oportunidades legítimas de relacionamento e a diminuição da confiança geral no uso da Internet, o que, por sua vez, pode inibir a participação plena e saudável no meio digital (Tsunoda & Sato, 2025). Assim, uma abordagem equilibrada centrada na vigilância crítica e não na exclusão do ambiente digital, revela-se mais eficaz na prevenção da vitimação.

5) Perceção pública sobre a criminalidade digital

A perceção pública da criminalidade digital constitui um elemento central para a compreensão da resposta social, institucional e jurídica a fenómenos como o *romance scam*. Para além da dimensão objetiva do ilícito, a forma como estes crimes são socialmente interpretados influencia a visibilidade do problema, a disposição das vítimas para denunciar, a priorização policial e a formulação de políticas públicas. Neste sentido, a criminalidade digital desafia as categorias tradicionais de compreensão do crime, na medida em que ocorre em ambientes virtuais, frequentemente sem contato físico direto e com fronteiras espaciais difusas.

No caso específico do *romance scam*, a perceção pública é moldada por representações sociais sobre a tecnologia, a intimidade online e a responsabilidade individual, fatores que tendem a influenciar a avaliação da gravidade do crime e a legitimidade do estatuto de vítima (Cole, 2024; Cross et al., 2018; Whitty & Buchanan, 2016). A análise desta perceção permite compreender não apenas as atitudes sociais face a este tipo de fraude, mas também os mecanismos simbólicos que contribuem para a sua normalização, invisibilidade ou desvalorização enquanto forma de criminalidade.

5.1) Subvalorização do *romance scam* e representações sociais da ilicitude

A perceção pública do *romance scam* é frequentemente marcada pela subvalorização da sua gravidade em comparação com outras formas de criminalidade patrimonial, não obstante as evidências empíricas que demonstram prejuízos financeiros e impactos emocionais significativos nas vítimas (Bleiman et al., 2025). Estudos recentes indicam que esta desvalorização está associada a narrativas de culpabilização da vítima, frequentemente expressas como ingenuidade ou falta de cautela, que contribuem de forma persistente para o estigma social associado a estes crimes dificultando a denúncia e o reconhecimento Público da sua gravidade (Bleiman et al., 2025).

Este estigma contribui de forma significativa para a subnotificação do *romance scam*, na medida em que gera sentimentos de vergonha, humilhação e medo de julgamento social, o que leva muitas vítimas a ocultar experiência ou a evitar o contato com as autoridades (Cole, 2024; Cross et al., 2018; Schokkenbroek & Snaphaan, 2025; Whitty & Buchanan, 2016). Ausência de contato físico e de violência direta favorece ainda a perceção de que

os crimes digitais representam uma ameaça menor do que os crimes tradicionais, reforçando a ideia de que o *romance scam* constitui um ilícito de baixo risco ou de reduzida relevância penal, apesar do seu impacto real (Cross et al., 2018; Europol, 2025; Lazarus et al., 2023).

A perceção pública é igualmente moldada por representações sociais sobre a tecnologia, a intimidade online e a responsabilidade individual, fatores que influenciam a avaliação da gravidade do crime e a legitimidade do estatuto de vítima (Cole, 2024; Cross et al., 2018; Thumboo & Mukherjee, 2024). Estudos recentes sublinham que o próprio design das plataformas digitais contribui para estas representações, na medida em que interfaces visualmente credíveis e mecanismos de validação simbólica tendem a reforçar perceções erróneas de segurança e autenticidade nas interações afetivas online, reduzindo a perceção de risco (Thumboo & Mukherjee, 2024; Schokkenbroek & Snaphaan, 2025). Importa ainda assinalar que a perceção pública varia em função da literacia digital, do género e das experiências anteriores, persistindo estereótipos como a ideia de que este tipo de fraude apenas afeta quem procura relações online (Lazarus et al., 2023; Thumboo & Mukherjee, 2024).

A perceção da gravidade destes crimes depende igualmente de variáveis individuais, como as competências digitais e as experiências prévias de cada indivíduo, as quais moldam condutas preventivas como autenticação de perfis ou a denúncia atempada (Cole, 2024; Martins et al., 2023; Tintori et al., 2023). A tendência para minimizar a ilicitude deste tipo de crime contribui ainda para a revitimação, reforçando a importância das iniciativas de sensibilização pública (Boccardi et al., 2020; Schokkenbroek & Snaphaan, 2025), numa perspetiva interdisciplinar, que conjugue contributos da criminologia da psicologia.

No espaço público, o *romance scam* tende a ser representado mais como um desvio moral ou uma falha individual do que como um crime organizado e estruturado, o que contribui para a sua desvalorização simbólica face a formas tradicionais de criminalidade patrimonial (Whitty & Buchanan, 2016). Esta construção social da ilicitude, fortemente influenciada pela mediação tecnológica, promove uma dissociação entre o ato criminoso e as suas consequências económicas, psicológicas e institucionais, afastando o *romance scam* para uma posição inferior na hierarquia informal da criminalidade (Cole, 2024; Cross et al., 2018; Levi, 2012).

5.2) Os media e as plataformas digitais na construção da perceção pública

Os media desempenham um papel determinante na forma como o *romance scam* é percebido no debate público, moldando a perceção sobre a sua gravidade e relevância social. Estas fraudes são maioritariamente cobertas de forma episódica e sensacionalista, com enfoque em casos extremos e na dimensão emocional das vítimas, em detrimento da análise estrutural do fenómeno criminoso (Spiller et al., 2025). Esta abordagem tende a reforçar interpretações individualistas do crime, ocultando o seu carácter organizado, transnacional e sistemático (Cross et al., 2018; Europol, 2025; Levi, 2012).

As plataformas digitais moldam igualmente a perceção pública, tanto através dos seus modelos de interação como das políticas de moderação e alerta de riscos (Abu-Salma et al., 2025; Schokkenbroek & Snaphaan, 2025). Estudos recentes demonstram que as redes sociais e as aplicações de encontros tendem a enquadrar o *romance scam* como um problema de segurança individual ou de uso indevido, atribuindo a responsabilidade da prevenção aos utilizadores (Abu-Salma et al., 2025; Thumboo & Mukherjee, 2024). Esta perspetiva reforça a ideia de que a vitimação resulta sobretudo de falhas pessoais de vigilância ou de literacia digital, em vez de refletir vulnerabilidades estruturais exploradas por redes criminosas organizadas, o que acaba por contribuir para uma diminuição da perceção pública da dimensão criminal do fenómeno (Rege & Lavorgna, 2023; Wang & Topalli, 2024).

6) Cibersegurança e prevenção do *romance scam*

A abordagem teórica da cibersegurança no contexto do *romance scam* fundamenta-se na interseção entre vulnerabilidades individuais, riscos digitais e estratégias de mitigação, tendo em consideração que a manipulação emocional e a exploração de fragilidades psicológicas constituem fatores centrais na vitimação. A prevenção não se limita à aplicação de tecnologias de proteção, mas integra igualmente competências de literacia digital, perceção de risco, comportamentos de evitamento e educação pública. A compreensão da forma como fatores cognitivos, emocionais e sociais interagem com o ambiente online revela-se, neste contexto, essencial. Esta perspetiva permite enquadrar a análise das medidas preventivas, destacando o papel complementar das ações individuais, institucionais e educativas na redução da exposição ao crime e na proteção das vítimas.

6.1) Estratégias institucionais e políticas de prevenção

No contexto português, a prevenção do *romance scam* tem vindo a ser progressivamente enquadrada no âmbito mais amplo das políticas de combate à criminalidade digital, reconhecendo-se que a resposta a este fenómeno exige uma atuação articulada entre instituições do sistema de justiça, entidades reguladoras, o setor financeiro e as plataformas digitais (Europol, 2025). Esta abordagem reflete a compreensão de que os fatores de risco individuais, analisados anteriormente, são amplificados por contextos estruturais e tecnológicos que ultrapassam a esfera de controlo das vítimas (Europol, 2025).

Na investigação criminal, a Polícia Judiciária (PJ) assume um papel central por intermédio das suas unidades especializadas em cibercrime, responsáveis pela receção de denúncias, pela investigação de esquemas fraudulentos online e pela cooperação com entidades internacionais (Levi, 2025; Rege & Lavorgna, 2023). Contudo, a dimensão transfronteiriça do *romance scam*, combinada com infraestruturas digitais fragmentadas, continua a gerar obstáculos significativos à identificação e localização dos ofensores e à aplicação efetiva da lei, exigindo um maior reforço contínuo da cooperação judiciária, europeia e internacional (Levi, 2025; Rege & Lavorgna, 2023).

As instituições financeiras desempenham igualmente uma função preventiva relevante, nomeadamente através da monitorização de transferências suspeitas, da implementação de alertas comportamentais e da interrupção de operações financeiras potencialmente fraudulentas (Lazarus et al., 2023). Estudos recentes sublinham que a articulação entre bancos, autoridades policiais e o Ministério Público (MP) pode reduzir significativamente o impacto económico da fraude quando identificada em fases iniciais, embora a eficácia dependa, em larga medida, da celeridade da denúncia por parte das vítimas (Lazarus et al., 2023).

No âmbito da cibersegurança e da prevenção estrutural, o Centro Nacional de Cibersegurança (CNCS), tem vindo a desempenhar um papel estratégico na sensibilização para os riscos digitais, na elaboração de materiais informativos e na difusão de boas práticas de segurança online (Tech for Good Institute, 2025). Todavia, a literatura crítica alerta para a persistência de lacunas ao nível da literacia digital e da avaliação do risco, particularmente nas interações afetivas online, onde o fator emocional tende a sobrepor-se ao discernimento racional face ao perigo (Coluccia et al., 2020).

As plataformas digitais e as *apps* de encontros disponíveis em Portugal, constituem igualmente um eixo fundamental nas estratégias preventivas, sendo estas obrigadas a adotar mecanismos de deteção de perfis fraudulentos, sistemas de denúncia acessíveis e respostas eficazes a comportamentos suspeitos (Europol, 2025). A investigação recente demonstra que medidas de moderação eficazes e intervenções ao nível do *design* das plataformas podem reduzir as oportunidades de vitimação, embora a sua eficácia dependa do grau de compromisso regulatório e da responsabilização das empresas tecnológicas (Europol, 2025).

Em síntese, as estratégias institucionais de combate ao *romance scam* em Portugal evidenciam progressos relevantes, mas permanecem condicionadas por desafios estruturais associados à dimensão transnacional do crime, à velocidade das interações digitais e à dependência da denúncia precoce. Esta realidade reforça a necessidade de complementar a resposta repressiva com medidas preventivas orientadas para a capacitação dos utilizadores, em particular, ao nível da literacia digital e da perceção do risco.

6.2) Literacia digital e perceção do risco

A literacia digital assume um papel central na prevenção do *romance scam*, ao influenciar diretamente a forma como os indivíduos percecionam, interpretam e avaliam o risco em interações afetivas mediadas por plataformas digitais. A capacidade de reconhecer padrões fraudulentos não depende exclusivamente de competências técnicas, mas da articulação entre conhecimento digital, interpretação social e avaliação emocional das interações online (Lazarus et al., 2023; Martins et al., 2023; Thumboo & Mukherjee, 2024).

No contexto específico do *romance scam*, a perceção do risco tende a ser significativamente reduzida pela manipulação emocional, o que explica que indivíduos com nível adequados de literacia digital possam, ainda assim, tornar-se vítimas deste tipo de crime (Cross et al., 2018). Esta dissociação entre conhecimento e comportamento evidencia que a literacia digital, por si só, é insuficiente na ausência de estratégias educativas que integrem as dimensões emocionais e relacionais da vitimação. Tal constatação justifica a relevância das campanhas de sensibilização e educação pública

enquanto instrumentos complementares de reforço da perceção do risco e da prevenção primária.

6.2.1) Campanhas de sensibilização e educação pública

As campanhas de sensibilização e educação pública constituem um dos pilares fundamentais na prevenção do *romance scam*, sobretudo num contexto de elevada exposição a interações digitais (Europol, 2025; FTC, 2025). A literatura recente evidencia que estas campanhas são mais eficazes quando combinam informação factual com abordagens narrativas que exploram os mecanismos psicológicos da manipulação emocional, de forma a promover o reconhecimento de sinais de alerta e a redução do estigma associado à vitimação (Europol, 2025; FTC, 2025).

No contexto português, estas iniciativas têm sido desenvolvidas sobretudo através de entidades públicas como a PJ, o CNCS e o Banco de Portugal, frequentemente em articulação com campanhas europeias de prevenção da criminalidade digital (Europol, 2025). O objetivo central destas campanhas é o reforço da literacia digital da população, através da explicação do modo de atuação dos ofensores, dos mecanismos psicológicos envolvidos e dos comportamentos que potenciam o risco d vitimação, assumindo uma função preventiva essencial num cenário marcado por elevados níveis de estigmatização das vítimas (Europol, 2025).

Para além da informação preventiva, estas ações desempenham uma função estrutural ao nível do reforço da literacia digital, da normalização da denúncia e da corresponsabilização entre utilizadores, instituições financeiras e plataformas digitais (Rege & Lavorgna, 2023).

Síntese do Enquadramento Teórico

A literatura científica contemporânea evidencia que o fenómeno do *romance scam* constitui uma realidade complexa, cuja compreensão integral exige a superação de perspetivas teóricas isoladas (Wang, 2026). Embora a RAT e a Teoria dos Estilos de Vida se destaquem pela sua capacidade explicativa da exposição diferencial ao risco em ambientes digitais, estas abordagens revelam limitações quando aplicadas de forma estrita à totalidade do processo de vitimação (Bilz et al., 2023). A evidência empírica demonstra que a análise do *romance scam* beneficia da articulação destas teorias com a RCT, no que respeita à análise das decisões estratégicas dos ofensores (Abubakari & Oseh-Ovarah, 2025). Simultaneamente, o recurso a perspetivas psicológicas e relacionais torna-se indispensável para compreender os mecanismos de manipulação emocional e o fenómeno do envolvimento da vítima no esquema fraudulento (Schokkenbroek & Snaphaan, 2025).

A investigação não identifica a existência de um perfil sociodemográfico único ou de características determinísticas que permitam prever com exatidão o alvo da vitimação (Bilz et al., 2023). Pelo contrário, os estudos convergem na identificação de um conjunto de fatores de vulnerabilidade individuais que, ao interagirem com as oportunidades proporcionadas pelo ambiente digital e com estratégias de *grooming* altamente adaptativas, potenciam o risco de *romance scam* (Schokkenbroek & Snaphaan, 2025). Do mesmo modo, o ofensor não apresenta um perfil delimitado, operando frequentemente através de redes organizadas que ajustam o seu perfil às carências da vítima (Cross, 2020). Neste sentido, o *romance scam* deve ser interpretado como o resultado da interação entre fatores individuais, relacionais, situacionais e tecnológicos, e não como uma atuação isolada de qualquer um dos intervenientes (Schokkenbroek & Snaphaan, 2025).

Consequentemente, o principal contributo académico recente reside na evolução das explicações centradas em fatores isolados para modelos analíticos integradores capazes de explicar o fenómeno de forma mais abrangente (Wang, 2026). Não obstante os progressos alcançados através da análise de *scripts* criminais, permanecem lacunas relevantes quanto à forma como os diferentes fatores interagem ao longo das várias fases do *romance scam* (Schokkenbroek & Snaphaan, 2025). Torna-se, portanto, necessário aprofundar o estudo sobre as variações dessa interação em distintos contextos culturais e

perfis de vitimação, visando o desenvolvimento de estratégias de prevenção mais robustas (Schokkenbroek & Snaphaan, 2025; Wang, 2026).

Posto isto, da revisão da literatura realizada emerge um conjunto de conclusões que fundamentam a presente investigação empírica. A literatura evidencia que a perceção pública sobre o *romance scam* tende a subestimar a sua gravidade e ilicitude, sendo influenciada por fatores como a literacia digital, as experiências prévias e as representações sociais sobre a responsabilidade individual na vitimação. Paralelamente, os comportamentos de evitamento adotados pelos utilizadores em contexto online revelam-se insuficientemente estudados numa perspetiva integrada que contemple simultaneamente as dimensões cognitivas, emocionais e sociodemográficas. Destas lacunas decorrem as seguintes questões de investigação:

1. Estarão os comportamentos de evitamento adotados pelos utilizadores associados à perceção da gravidade do *romance scam*?
2. Em que medida a perceção da gravidade associada ao *romance scam* e os comportamentos de evitamento variam em função de fatores de ordem individual?
3. Existem diferenças sociodemográficas significativas nos comportamentos de evitamento adotados pelos utilizadores face ao *romance scam*?

Com base nestas questões, formulam-se as hipóteses a testar no estudo empírico, nomeadamente que uma maior literacia digital está associada a uma perceção mais elevada do risco e a comportamentos de evitamento mais eficazes, e que a perceção da gravidade do *romance scam* se relaciona positivamente com a adoção de práticas de autoproteção online.

Parte B – Estudo Empírico

1) Objetivos da investigação

A presente investigação centra-se na seguinte questão orientadora: "De que forma a perceção pública sobre a natureza, gravidade e ilicitude das burlas e *romance scams* se relaciona com os comportamentos de evitamento adotados pelos utilizadores em contexto online?". Esta questão permite integrar, de forma articulada, os diferentes elementos que compõem o fenómeno em análise, nomeadamente as perceções sociais acerca destes crimes e as práticas de autoproteção adotadas pelos utilizadores.

Tendo por base esta questão central, o objetivo geral da investigação consiste em analisar a perceção pública sobre a natureza, gravidade e ilicitude das burlas e *romance scams*, bem como compreender de que modo essas perceções influenciam os comportamentos de evitamento adotados pelos utilizadores online.

Para operacionalizar este objetivo geral, definem-se os seguintes objetivos específicos:

a) Caracterizar a perceção pública sobre a gravidade das burlas e, em particular, do *romance scam*.
b) Identificar os comportamentos de evitamento adotados pelos utilizadores de modo a reduzir o risco de vitimação online.
c) Analisar a associação entre os fatores de ordem individual na perceção da gravidade associada ao *romance scam*, bem como os comportamentos de evitamento adotados pelos utilizadores.
d) Examinar a relação entre a perceção da gravidade do *romance scam* e os comportamentos de evitamento adotados pelos utilizadores.
e) Explorar possíveis diferenças sociodemográficas na perceção da gravidade do *romance scam* e nos comportamentos de evitamento adotados pelos utilizadores.

2) Método

A investigação desenvolvida adota uma abordagem metodológica quantitativa, orientada para a recolha e o tratamento de dados através de técnicas estatísticas (Coutinho, 2023). Isto, partindo do pressuposto de que os fenómenos sociais podem ser analisados de forma

objetiva e sistemática através da aplicação de métodos científicos, permitindo a verificação e validação estatística dos resultados obtidos (Coutinho, 2023). O estudo assume um desempenho transversal, uma vez que a recolha de dados ocorre num intervalo temporal limitado, e apresenta um carácter descritivo, com o objetivo de analisar e compreender o fenómeno em estudo (Coutinho, 2023).

2.1) Desenho de investigação

A presente investigação adotou uma abordagem metodológica quantitativa, orientada para a recolha e o tratamento de dados através de técnicas estatísticas (Coutinho, 2023). O estudo assume um carácter descritivo, na medida em que, por um lado, visa caracterizar e compreender as perceções públicas sobre o *romance scam* e os comportamentos de evitamento adotados pelos utilizadores e, por outro, procura analisar a relação entre essas perceções e esses comportamentos. O desenho é transversal, uma vez que a recolha de dados ocorreu num único momento temporal, não havendo seguimento longitudinal dos participantes (Coutinho, 2023).

2.2) Procedimentos

A implementação deste estudo teve início com a submissão do projeto de investigação à Comissão de Ética da Universidade do Porto, tendo sido obtido parecer favorável a 14 de março de 2025 (cf. Anexo A). O mesmo se aplicou à obtenção do parecer favorável da Unidade de Proteção de Dados da Universidade do Porto, a qual aprovou o estudo a 30 de julho de 2025 (cf. Anexo B). Em simultâneo, procedeu-se ao desenvolvimento e aperfeiçoamento do questionário, de forma a assegurar a sua adequação aos objetivos e questões de investigação.

Prévio à recolha dos dados, o questionário foi submetido a um pré-teste, junto de uma pequena amostra de participantes com características semelhantes às da população-alvo, o que possibilitou a identificação e correção de ambiguidades e/ou dificuldades de compreensão (Coutinho, 2023).

Foram definidos critérios de inclusão que abrangem indivíduos com idade igual ou superior a 18 anos, independentemente do género, fluentes em língua portuguesa, com acesso à Internet e com competências digitais básicas, atendendo ao facto de a recolha de

dados decorrer em formato digital. Consequentemente, foram excluídos todos os participantes que não cumprissem os critérios de inclusão supramencionados.

A recolha de dados foi realizada através de um inquérito por questionário em formato digital, disponibilizado na plataforma online *LimeSurvey*. Esta opção permitiu garantir o anonimato dos participantes, facilitar a divulgação do estudo e ampliar o alcance da amostra. O questionário permaneceu disponível entre março de 2025 e julho de 2026, de forma a assegurar a participação do número mínimo de indivíduos necessários. A divulgação do questionário foi efetuada através da rede de contactos do investigador, bem como através do Gabinete de Comunicação e Imagem (GCI) da Universidade do Porto, de modo a maximizar o alcance da amostra. Importa ainda salientar que todos e quaisquer dados recolhidos são anónimos e armazenados de forma segura em pasta protegida por palavra-passe, garantindo a confidencialidade da informação.

De modo a garantir a proteção e a privacidade dos participantes, foram adotadas todas as diretrizes éticas e legais aplicáveis. Antes de aceder ao questionário, os participantes deparam-se com uma breve apresentação do investigador. Posteriormente, foi apresentado um consentimento informado, no qual constavam os objetivos do estudo, a natureza da participação, o tipo de dados recolhidos, os procedimentos de armazenamento e proteção da informação, bem como o carácter voluntário e confidencial da participação. Foi igualmente disponibilizado o contacto do investigador para o esclarecimento de quaisquer dúvidas. Em nenhum momento foram solicitados dados pessoais identificáveis, sendo recolhida apenas informação sociodemográfica de carácter não comprometedor. O avanço para o preenchimento do questionário só foi possível após aceitação do consentimento informado, garantindo uma participação plenamente esclarecida.

Concluída a recolha, os dados coletados foram exportados para formato *Excel* e posteriormente analisados com recurso ao programa informático *Jeffrey's Amazing Statistics Program* (JASP), com recurso a procedimentos estatísticos descritivos e inferenciais adequados aos objetivos da investigação (Coutinho, 2023).

2.3) Descrição da amostra

No que respeita aos procedimentos de amostragem, recorreu-se a diferentes métodos amostrais. Destaca-se a amostragem não probabilística acidental ou de conveniência, uma

vez que a seleção dos participantes não obedece a critérios de aleatoriedade, ou seja, é composta por indivíduos que, de forma voluntária, aceitam participar no estudo, através do acesso ao link disponibilizado e do preenchimento do inquérito (Coutinho, 2023). Este método é justificado pela natureza exploratória da investigação e pela facilidade de acesso aos participantes dentro do contexto definido (Coutinho, 2023).

No presente estudo, foram recolhidas um número total de 128 respostas ao questionário. No entanto, após uma breve verificação do cumprimento dos critérios de inclusão previamente definidos e da qualidade dos dados recolhidos, foram excluídas 28 respostas. Destas, uma foi excluída por corresponder a um participante menor de idade, não cumprindo os critérios de inclusão estabelecidos, e, as restantes 27 por se tratarem de questionários incompletos, sem informação suficiente para responder aos objetivos do estudo. Consequentemente, a amostra final considerada para a análise estatística é constituída por 100 participantes (cf. Tabela 1).

Relativamente à idade, a amostra é constituída por participantes com idades compreendidas entre os 18 e os 68 anos (cf. Tabela 1). A classe de idade mais frequentemente observada na amostra corresponde aos 18 a 28 anos (66%; *n*=66) (cf. Tabela 1), sendo os 26 anos o mais mencionado (14%; *n*=14). A idade menos frequente situa-se entre os 59 e os 68 anos (4%; *n*=4) (cf. Tabela 1). Estes resultados evidenciam uma predominância de jovens adultos, embora a amplitude das idades observadas indique uma distribuição etária relativamente diversificada (cf. Tabela 1).

Já no que diz respeito ao género, verificou-se uma distribuição relativamente equilibrada da amostra, sendo que 52 (52%) dos participantes são do sexo feminino, 47 (47%) do sexo masculino e 1 (1%) optou por não revelar o seu género (cf. Tabela 1).

Relativamente ao grau de escolaridade, observou-se um 52 (52%) participantes com o ensino secundário, seguido de 29 (29%) que possuem licenciatura e 14 (14%) com mestrado (cf. Tabela 1). Apenas 3 (3%) dos participantes tinham o ensino básico como habilitação literária e 2 (2%) tinham o grau de doutoramento (cf. Tabela 1).

Na situação profissional, a amostra é predominantemente constituída por trabalhadores por conta de outrem (49%; *n*=49), seguindo-se os estudantes (19%; *n*=19), os trabalhadores por conta própria (16%; *n*=16) e os desempregados (15%; *n*=15) (cf. Tabela 1). Verificou-se ainda que apenas 1 (1%) participante se encontra aposentado (cf. Tabela 1).

Por sua vez, relativamente ao estado civil, verificou-se um predomínio de participantes solteiros com 66 respostas (66%), seguindo-se os casados ou em união de facto (28%; *n*=28) (cf. Tabela 1). Os participantes divorciados e viúvos representam, cada um, 3% (*n*=3) da amostra (cf. Tabela 1).

Tabela 1. Características sociodemográficas da amostra (*n*=100)

Categoria	***Subcategorias***	***n***	***%***
Faixa etária	18-28	66	66,0
	29-38	17	17,0
M=30,15	39-48	5	5,0
DP=11,14	49-58	8	8,0
	59-68	4	4,0
Sexo	Feminino	52	52,0
	Masculino	47	47,0
	Não revelado	1	1,0
Habilitações literárias	Ensino básico	3	3,0
	Ensino secundário	52	52,0
	Licenciatura	29	29,0
	Mestrado	14	14,0
	Doutoramento	2	2,0
Situação profissional	Aposentado/a	1	1,0
	Desempregado/a	15	15,0
	Estudante	19	19,0
	Trabalhador/a por conta de outrem	49	49,0
	Trabalhador/a por conta própria	16	16,0
Estado civil	Casado/a ou em união de facto	28	28,0
	Divorciado/a ou separado/a	3	3,0
	Solteiro/a	66	66,0
	Viúvo/a	3	3,0

No que respeita ao distrito de residência, observou-se uma predominância de participantes em Vila Real (62%; *n*=62), abrangendo ainda outros distritos, por ordem de predominância de respostas: o Porto (15%; *n*=15), Braga (7%), Aveiro (5%; *n*=5) e Lisboa (4%; *n*=4). Os restantes distritos (Viseu, Bragança, Faro, Castelo Branco, Região

Autónoma da Madeira) apresentam uma representatividade residual, totalizado apenas 7% (*n*=7) participantes.

Por último, quanto ao contexto da residência, a maioria da amostra encontra-se localizada em meios rurais ou pouco urbanizados (62%; *n*=62), enquanto que, os restantes 38 (38%) participantes residem em meios urbanos ou muito urbanizados.

2.4) Instrumento

O instrumento selecionado para a recolha dos dados, em consonância com a questão central de investigação, foi o inquérito por questionário, aplicado em formato digital através da plataforma *LimeSurvey*. A opção por este formato visa facilitar o acesso ao instrumento, de forma a possibilitar a participação de um número mais alargado de indivíduos, bem como a recolha sistemática e organizada das respostas.

O questionário, composto por 47 questões de natureza mista (cf. Anexo C), incluindo itens de resposta obrigatória e não obrigatória, e é precedido por um consentimento informado, que assegura aos participantes compreender os objetivos do estudo e a natureza voluntária da sua participação. O preenchimento do questionário tem início apenas após a confirmação e aceitação das condições apresentadas. O instrumento encontra-se estruturado em sete secções distintas, cada uma dedicada a um domínio específico considerado relevante para os propósitos da investigação, conforme descrito em seguida.

A primeira secção incide sobre os dados sociodemográficos, sendo composta por sete questões relativas à idade, género, grau de escolaridade, situação profissional estado civil, local de residência e contexto urbano ou rural do participante. A recolha destas variáveis justifica-se pela necessidade de caracterizar a amostra e de analisar possíveis diferenças na perceção da gravidade do *romance scam* e nos comportamentos de evitamento em função das características sociodemográficas dos participantes. Esta secção encontra-se em consonância com o objetivo e) da investigação.

Segue-se uma secção dedicada ao uso da Internet e das redes sociais, sendo composta por seis questões que abordam a frequência de utilização das redes sociais, o tipo de interações estabelecidas com desconhecidos, os dispositivos utilizados para o acesso à Internet, as plataformas mais frequentemente utilizadas e o tempo despendido online

diariamente. Esta secção justifica-se pela necessidade de compreender os padrões de utilização digital dos participantes, uma vez que as características da exposição ao ambiente online constituem um fator de risco relevante para a vitimação por *romance scam*.

A terceira secção aborda as burlas digitais e os *romances scams*, com seis questões que exploram o conhecimento prévio dos participantes sobre estes fenómenos, bem como a familiaridade com casos reais. A inclusão desta secção prende-se com a necessidade de avaliar o nível de literacia digital e de consciencialização dos participantes face a este tipo de criminalidade, na medida em que o conhecimento prévio poderá influenciar tanto as perceções como os comportamentos de evitamento adotados.

Por sua vez, a quarta secção centra-se na perceção da gravidade do *romance scam* e é composta por quatro questões relativas à responsabilidade atribuída à vítima, às consequências da vitimação, à gravidade percebida do *romance scam* e à sanção considerada adequada. Esta secção responde diretamente aos objetivos a) e c) da investigação, permitindo analisar a forma como os participantes percecionam a gravidade deste fenómeno, atribuem responsabilidade à vítima e avaliam as repostas sancionatórias consideradas adequadas.

As duas seções seguintes, as mais extensas do questionário, focam-se nos comportamentos de evitamento e de proteção e nos sentimentos de insegurança, reunindo vinte e duas questões no total. Estas secções exploram experiências pessoais, práticas de autoproteção, níveis de desconfiança, definições individuais de privacidade, bem como perceções de vulnerabilidade, de risco, de vitimação e de impacto emocional. Dada a centralidade destas dimensões para a investigação, estas secções assumem particular relevância, correspondendo diretamente aos objetivos b) e d), ao permitirem identificar os comportamentos de evitamento adotados pelos participantes e analisar a sua relação com a perceção da gravidade do *romance scam*.

Por fim, a última secção integra duas questões de resposta aberta, através das quais os participantes podem expressar sugestões sobre formas de reduzir o número de vítimas de *romance scam*, bem como partilhar experiências pessoais ou reflexões adicionais sobre o tema, enriquecendo assim a análise quantitativa com perspetivas individuais dos participantes, possibilitando a recolha de informação não antecipada pelo investigador.

No que respeita aos formatos de resposta, o questionário apresenta uma diversidade de formatos, nomeadamente itens de resposta fechada em questões de escolha múltipla, questões de resposta única e itens baseados na escala de *Likert*, contemplando igualmente a possibilidade de resposta aberta em determinadas secções.

3) Resultados

A análise dos dados descritivos relevou que, dos 100 participantes, 76% (*n*=76) utiliza a Internet mais do que três vezes ao dia, sendo que apenas 1% (*n*=1) afirmou utilizar a Internet apenas uma vez por dia (cf. Tabela 2).

Já no que diz respeito aos dispositivos utilizados para aceder às redes sociais, observou-se um claro predomínio do telemóvel, referido por 99 (99%) participantes. Apenas 4 (4%) participantes indicaram recorrer a outros dispositivos, nomeadamente à televisão (cf. Tabela 2).

Relativamente às redes sociais utilizadas, o Instagram foi a plataforma mais frequentemente referida com 89% (*n*=89) das respostas, seguindo-se o Facebook com 71% (*n*=71) e o TikTok com 70% (*n*=70), o Twitter/X, por sua vez, é utilizado por 49% (*n*=49) dos participantes, enquanto as aplicações de encontros como o Tinder e o Bumble foram referidas por 39% (*n*=39) e por 22% (*n*=22) respetivamente (cf. Tabela 2). Apenas 6 (6%) participantes referiram não utilizar qualquer rede social (cf. Tabela 2). Com o objetivo de caraterizar o padrão de utilização de plataformas digitais pelos participantes, foi criada uma variável derivada a partir das respostas relativas à utilização de redes sociais e *apps* de encontros. Esta variável permitiu agrupar os participantes de acordo com o tipo de plataformas utilizadas, de forma a distinguir entre aqueles que utilizam exclusivamente redes sociais (55%; *n*=55), aqueles que utilizam simultaneamente redes sociais e *apps* de encontros (39%; *n*=39), aqueles que utilizam apenas *apps* de encontros (0%; *n*=0) e aqueles que não utilizam qualquer uma destas plataformas (6%; *n*=6) (cf. Tabela 2).

No que respeita ao tempo médio diário despendido nas redes sociais, verificou-se que a categoria mais frequente correspondeu a entre uma e duas horas por dia (30%; *n*=30), seguiram-se os participantes que referiram utilizar as redes sociais entre trinta minutos e uma hora (25%; *n*=25) e entre duas e três horas (23%; *n*=23) (cf. Tabela 2). Por sua vez,

12 participantes (12%) indicaram utilizar as redes sociais mais de três horas diárias, enquanto que apenas 7% (*n*=7) referiram uma utilização inferior a trinta minutos por dia (cf. Tabela 2).

Quando questionados sobre a sua interação com desconhecidos através das redes sociais ou de outras plataformas digitais, verificou-se que a maioria dos participantes (82%; n=82) referiu já ter interagido online com pessoas que não conhecia previamente, enquanto 18 (18%) participantes indicaram nunca ter tido esse tipo de interação (cf. Tabela 2). Num mesmo enquadramento, quando abordados relativamente a encontros presenciais com pessoas conhecidas exclusivamente através da Internet, 52 (52%) participantes referiram já se ter encontrado presencialmente com alguém com quem mantinham apenas contacto online, 34 (34%) indicaram nunca o ter feito e, 14 (14%) optaram por não responder a esta questão (cf. Tabela 2). Posto isto, verificou-se que, todos os participantes que referiram utilizar *apps* de encontros (100%; *n*=39) indicaram já ter interagido online com pessoas desconhecidas (cf. Tabela 3). Adicionalmente, a maioria destes participantes (89,7%; *n*=89) referiu já se ter encontrado presencialmente com pessoas conhecidas exclusivamente através da Internet (cf. Tabela 3). Em contraste, entre os participantes que referiram não utilizar *apps* de encontros, 70,5% (*n*=43) também já tiveram algum tipo de interação com desconhecidos online e, 27,9% (*n*=17) afirmaram já se ter encontrado presencialmente com alguém conhecido exclusivamente online (cf. Tabela 3). O que evidencia que não só as *apps* de encontros servem como foco de utilização para o *romance scam*, mas também as várias redes sociais às quais estamos expostos diariamente.

Tabela 2. Exposição à Internet (*n*=100)

Categoria	***Subcategorias***	***n***	***%***
Frequência	Mais do que três vezes ao dia	76	76,0
	Duas ou três vezes ao dia	23	23,0
	Uma vez ao dia	1	1,0
Dispositivo utilizado*	Telemóvel	99	99,0
	Tablet	25	25,0
	Computador	55	55,0
	Outro (TV)	4	4,0
Redes sociais*	Instagram	89	89,0
	Facebook	71	71,0
	TikTok	70	70,0
	Twitter/X	49	49,0
	Tinder	39	39,0
	Bumble	22	22,0
	Outro	2	2,0
	Não utiliza	6	6,0
Perfil de utilização das plataformas digitais	Apenas redes sociais	55	55,0
	Redes sociais e *apps* de encontros	39	39,0
	Apenas *apps* de encontros	0	0,0
	Não utiliza nenhuma plataforma	6	6,0
Tempo médio despendido em redes sociais diariamente	Menos de 30 minutos	7	7,0
	Entre 30 minutos e 1 hora	25	25,0
	Entre 1 e 2 horas	30	30,0
	Entre 2 e 3 horas	23	23,0
	Mais de 3 horas	12	12,0
	Não aplicável	3	3,0
Interação online com pessoas desconhecidas	Sim	82	82,0
	Não	18	18,0
Encontro presencial com pessoas conhecidos exclusivamente através da Internet	Sim	52	52,0
	Não	34	34,0
	Preferiu não responder	14	14,0

*As percentagens não são mutuamente exclusivas.

Tabela 3. Interação com desconhecidos em função da utilização de *apps* de encontros (*n*=100)

Utilização de apps de encontros	***Interação online***	***Não interagiu***	***Encontro presencial***	***Não se encontrou***	***Não respondeu***
Sim (*n*=39)	39 (100,0%)	0 (0,0%)	35 (89,7%)	3 (7,7%)	1 (2,6%)
Não (*n*=61)	43% (70,5%)	18 (18,0%)	17 (27,9%)	31 (50,8%)	13 (21,3%)

A questão seguinte remetia ao seu conhecimento acerca dos variados tipos de burla online. Verificou-se que, as burlas através do WhatsApp ou de chamadas automáticas constituíram a tipologia mais conhecida pelos participantes, sendo identificada por 71% (*n*=71), seguiram-se as burlas bancárias com 61% (*n*=61) e as burlas em lojas online com 52% (*n*=52), já o phishing foi reconhecido por 29 (29%) dos participantes, enquanto que o vishing foi identificado por apenas 15 (15%) (cf. Tabela 4). Apenas 1 (1%) participante referiu conhecer outro tipo de burla online e 20 (20%) participantes indicaram não conhecer nenhum dos tipos de burla apresentados (cf. Tabela 4).

Tabela 4. Conhecimento acerca das diferentes formas de burla online (*n*=100)

Categoria	***Subcategoria***	***n***	***%***
Conhecimento dos tipos de burla online*	Phishing	29	29,0
	Vishing	15	15,0
	Burlas do WhatsApp ou chamadas automáticas	71	71,0
	Burlas em lojas online	52	52,0
	Burlas bancárias	61	61,0
	Outra	1	1,0
	Nenhum	20	20,0

*As percentagens não são mutuamente exclusivas.

Com o objetivo de caracterizar o grau de conhecimento dos participantes relativamente às burlas online e, em particular, ao fenómeno do *romance scam*, foi analisado o

conhecimento autoavaliado sobre este tipo de fraude, bem como a familiaridade prévia com o conceito e o contacto direto com situações de vitimação.

No que respeita ao conhecimento autoavaliado sobre as burlas online, verificou-se que a maioria dos participantes percecionou o seu nível de conhecimento como baixo (30%; *n*=30) ou moderado (30%; *n*=30) (cf. Tabela 5). Por sua vez, 9 (9%) e 6 (6%) consideraram possuir um nível de conhecimento alto e muito alto, respetivamente (cf. Tabela 5). Apenas 3 (3%) participantes referiram possuir um conhecimento nulo sobre este tipo de fraude (cf. Tabela 5).

Relativamente ao fenómeno específico do *romance scam* verificou-se que apenas 38 (38%) participantes referiram já ter conhecimento prévio deste tipo de fraude, enquanto que 62% (*n*=62) indicaram nunca ter ouvido falar acerca deste tipo de burla (cf. Tabela 5).

Quanto ao contacto direto com casos de vitimação, 32 (32%) participantes afirmam conhecer alguém que já foi vítima deste tipo de burla, enquanto que 68 (68%) referiram não conhecer qualquer vítima (cf. Tabela 5).

Tabela 5.Grau de conhecimento sobre as burlas online e o *romance scam* (*n*=100)

Variável	***Categoria***	***n***	***%***
Conhecimento autoavaliado sobre as burlas online	Nulo	3	3,0
	Muito baixo	22	22,0
	Baixo	30	30,0
	Moderado	30	30,0
	Alto	9	9,0
	Muito alto	6	6,0
Conhecimento do termo *romance scam*	Sim	38	38,0
	Não	62	62,0
Contacto com casos de vitimação	Sim	32	32,0
	Não	68	68,0

No que respeita à atribuição de responsabilidade pela perda financeira decorrente do *romance scam*, verificou-se que, entre os participantes que responderam à questão (91%; n=91), 55% (*n*=50) consideram que a vítima é responsável pelo prejuízo sofrido, enquanto

que 25,3% (*n*=23) entendem que esta responsabilidade depende das circunstâncias e, 19,8% (*n*=18) consideram que a vítima não é, de todo, responsável (cf. Tabela 6). É de ter em atenção que foram registadas 9 respostas omissas.

Para além das consequências financeiras os participantes identificam diversos impactos psicológicos e sociais associados à vitimação por *romance scam*. Entre as consequências mais frequentemente referidas destacam-se os problemas psicológicos nomeadamente "depressão", "ansiedade", "baixa autoestima", bem como dificuldades a nível de confiança interpessoal. Foram igualmente mencionados o "isolamento social", o medo de estabelecer novas relações efetivas e ainda uma referência ao risco de suicídio

Tabela 6. Atribuição de responsabilidade à vítima pela perda financeira (*n*=91*)

Variável	***Categoria***	***n***	***%***
Responsabilidade da vítima pela perda financeira	Responsável	50	55,0
	Não responsável	18	19,8
	Depende da situação	23	25,3

*Percentagens calculadas com base nas respostas válidas (*n*=91), tendo em conta que se verificaram 9 respostas omissas.

Relativamente às sanções que, na opinião dos participantes, deveriam ser aplicadas aos autores deste tipo de crime, a medida mais frequentemente apontada foi a proibição de acesso à Internet (60%; *n*=60), seguida da pena de prisão (53%; *n*=53) e da aplicação de multa (39%; *n*=39) (cf. Tabela 7).

Quando analisadas estas preferências em função do sexo dos participantes, observou-se que as mulheres tendem a selecionar com maior frequência a pena de prisão (59,6% *Vs*. 44,7%) e a aplicação de multa (46,2% *Vs*. 31,9%) comparativamente aos homens (cf. Tabela 8). Relativamente à proibição de acesso à Internet, verificaram-se percentagens semelhantes entre ambos os géneros (63,5%; *n*=33 e 57,4%; *n*=27) (cf. Tabela 8). Estas diferenças não são, porém, estatisticamente significativas.

No que respeita aos grupos etários, a proibição de acesso à Internet foi a sanção mais frequentemente assinalada em todos os grupos (cf. Tabela 9). A pena de prisão apresentou maior expressão entre os participantes com 35 a 44 anos (83,3%; *n*=5), embora este grupo

fosse constituído por um reduzido número de participantes, enquanto que a aplicação de pena de multa foi mais frequentemente referida pelos participantes dos grupos etários mais jovens (cf. Tabela 9). Apesar do carácter meramente descritivo destes resultados, as tendências observadas reforçam o interesse em explorar a eventual relação entre a idade dos participantes e a preferência pelas diferentes sanções, contribuindo para uma compreensão mais aprofundada das perceções sobre a resposta penal ao *romance scam*.

Tabela 7. Sanções consideradas adequadas pelos participantes para os *scammers* (*n*=100)

Categoria	***Subcategoria***	***n***	***%***
Sanções que deveriam ser impostas a quem pratica este tipo de crime*	Pena de prisão	53	53,0
	Multa	39	39,0
	Proibição de acesso à Internet	60	60,0
	Outro	1	1,0

*As percentagens não são mutuamente exclusivas.

Tabela 8. Preferência pelas sanções segundo o género dos participantes (*n*=99)*

Sanção	***Género feminino (n=52)***	***Género masculino (n=47)***	***χ^2 (p)***
Pena de prisão	31 (59,6%)	21 (44,7%)	2,208 (0,137)
Pena de multa	24 (46,2%)	15 (31,9%)	2,096 (0,148)
Proibição de acesso à Internet	33 (63,5%)	27 (57,4%)	0,374 (0,541)

*Foi excluído um participante que preferiu não responder

Tabela 9. Preferência pelas sanções segundo o grupo etário dos participantes (*n*=100)

Sanção	***18-24 (n=35)***	***25-34 (n=46)***	***35-44 (n=6)***	***≥45 (n=13)***
Pena de prisão	18 (51,4%)	22 (47,8%)	5 (83,3%)	8 (61,5%)
Pena de multa	16 (45,7%)	16 (34,8%)	3 (50,0%)	4 (30,8%)
Proibição de acesso à Internet	21 (60,0%)	28 (60,9%)	3 (50,0%)	8 (61,5%)

Quando questionados sobre se consideram o *romance scam* um problema grave para a sociedade, a grande maioria dos participantes (96%; n=96) respondeu afirmativamente, enquanto que apenas 4% (n=4) consideraram que este fenómeno não constitui um problema grave.

Posteriormente, após a apresentação de uma breve descrição do fenómeno do *romance scam*, os participantes foram questionados acerca da gravidade que, na sua perspetiva, atribuíam a este tipo de crime. Numa escala de *Likert* de 1 a 5 pontos (1=nada grave; 5=muito grave), obteve-se uma média de 4,01 (DP=1,01), o que vem evidenciar uma perceção globalmente elevada da gravidade deste tipo de crime (cf. Tabela 12). Em termos da distribuição das respostas, verificou-se que 47% (*n*=47) classificaram o *romance scam* como grave e 34% (*n*=34) considerou como muito grave. Em contrapartida, 8 (8%) participantes atribuíram uma classificação de gravidade moderada, outros 8 (8%) consideram-no como pouco grave e, apenas 3 (3%) como nada grave.

Com o objetivo de caracterizar os comportamentos de evitamento adotados pelos participantes para reduzir o risco de vitimação online, analisaram-se diversas estratégias preventivas relacionadas com a gestão da privacidade, a interação com desconhecidos e a resposta perante situações potencialmente fraudulentas.

Relativamente à reação perante mensagens recebidas de pessoas desconhecidas nas redes sociais ou outras plataformas digitais, verificou-se que a resposta mais frequente consistiu em verificar o perfil do remetente antes de responder, opção assinalada por 47 (47%) participantes (cf. Tabela 10). Em seguida 28 (28%) participantes referiram que ignorariam a mensagem, enquanto que 19 (19%) indicaram que bloqueariam ou denunciariam o utilizador (cf. Tabela 10). Apenas 6% (*n*=6) afirmaram que responderiam normalmente a este tipo de contacto (cf. Tabela 10). Estes resultados sugerem uma tendência para a adoção de comportamentos de precaução perante interações iniciadas por pessoas desconhecidas em contexto digital.

Tendo-se questionado se o participante já teria suspeitado estar perante uma tentativa de burla online, 14 (14%) optaram por não responder. De entre os restantes, verificou-se que 70,9% (*n*=61) dos participantes referiram já ter suspeitado, em algum momento, estar perante uma tentativa de burla online, e 29,1% (*n*=25) indicaram nunca ter tido essa suspeita.

Perante uma eventual situação de burla online, a maioria dos participantes (63%; *n*=63) referiu que denunciaria o caso às autoridades competentes (cf. Tabela 10). Além disso, 48 (48%) indicaram que deixariam de responder ao utilizador suspeito, enquanto que 26 (26%) afirmaram que tentariam recuperar o dinheiro ou quaisquer bem eventualmente subtraído (cf. Tabela 10).

Tabela 10. Características da interação com desconhecidos (*n*=100)

Categoria	***Subcategoria***	***n***	***%***
Reação ao receber mensagens de desconhecidos	Respondo normalmente	6	6,0
	Verifico o perfil antes de responder	47	47,0
	Ignoro a mensagem	28	28,0
	Bloqueio ou denuncio o utilizador	19	19,0
Em caso de burla online*	Denunciaria às autoridades	63	63,0
	Deixaria de responder	48	48,0
	Tentaria recuperar o dinheiro e/ou a propriedade de eventuais bens subtraídos	26	26,0

*As percentagens não são mutuamente exclusivas.

Relativamente às medidas de prevenção adotadas para reduzir o risco de vitimação por burlas online, verificou-se que a estratégia mais frequentemente referida consistiu em não partilhar informações pessoais com desconhecidos, opção assinalada por 67 (67%) participantes, seguida da verificação de perfis suspeitos antes de qualquer interação por 54 (54%) participantes, enquanto que 32 (32%) referiram utilizar a autenticação de dois fatores como medida de segurança (cf. Tabela 11). Além disso, 30 (30%) participantes afirmam evitar sites de encontro ou websites desconhecidos (cf. Tabela 11). Apenas 3 (3%) participantes indicaram não adotar qualquer uma das medidas apresentadas (cf. Tabela 11).

Tabela 11. Práticas adotadas como proteção ou evitamento do crime (*n*=100)*

Categoria	***n***	***%***
Não partilha informações pessoais com desconhecidos	67	67,0
Verifica perfis suspeitos antes de qualquer interação	54	54,0
Usa autentificação de dois fatores	32	32,0
Evita sites de encontros ou sites desconhecidos	30	30,0
Nenhum	3	3,0

*As percentagens não são mutuamente exclusivas.

A análise revelou que 74 (74%) participantes já alteraram as definições de privacidade das suas contas online com o objetivo de evitar serem contactados por pessoas desconhecidas. Em contraste, 10 (10%) participantes referiram nunca o ter feito e 16 (16%) preferiram não responder.

Com o objetivo de compreender os comportamentos de evitamento adotados pelos participantes perante o fenómeno do *romance scam*, procedeu-se à análise de diversos indicadores associados às diferentes práticas de segurança online, tais como o estabelecimento de relações online, a verificação de identidades antes de interações online, a partilha de fotografias ou informações pessoais online e a aceitação ou rejeição de pedidos de amizade de desconhecidos em contexto online.

Relativamente à frequência com que o participante refere evitar estabelecer relações online por receio de ser enganado, é possível observar-se uma média de 3,43 (DP=1,19), numa escala de *Likert* de 1 a 5 pontos (1=nunca; 5=sempre), indicando uma tendência de moderada para evitar este tipo de interação (cf. Tabela 12). Em termos de distribuição de respostas, a categoria mais frequentemente referida foi a 4 (38%; *n*=38), seguida pela categoria 5 (19%; *n*=19), o que vem demonstrar que mais de metade dos participantes (57%; *n*=57) evita frequentemente ou totalmente o estabelecimento de novas relações em contexto online por receio de serem enganados. Em contrapartida, apenas 6 (6%) participantes indicam não evitar este tipo de relações.

Em relação à verificação da identidade de pessoas desconhecidas antes de iniciar uma interação online, observou-se uma média de 3,79 (DP=1,16), numa escala de *Likert* de 1 a 5 pontos (1=nunca; 5=sempre), indicando uma tendência global para a adoção deste comportamento preventivo (cf. Tabela 12). Em termos de distribuição das respostas, 30%

(*n*=30) dos participantes referiram fazê-lo sempre. Por sua vez, 41% (*n*=41) afirmam verificar frequentemente, 10% (*n*=10) apenas às vezes, 13% (*n*=13) raramente, e, 5% (*n*=5) nunca adotam este comportamento. Registou-se ainda uma resposta omissa a esta questão.

Relativamente à partilha fotografias e de informações pessoais na Internet verificou-se uma média de 3,39 (D=1,15) numa escala de *Likert* de 1 a 5 (1=não evita; 5=não estabelece nenhum relação online), sugerindo uma tendência moderada para a adoção deste comportamento preventivo (cf. Tabela 12). Em termos da distribuição das respostas, 42 (42%) participantes referiram evitar bastante este tipo de partilha por receio de que a informação possa ser utilizada contra si, enquanto 15 (15%) afirmaram evitá-la totalmente. Por outro lado, 16 (16%) participantes indicaram um nível moderado de evitamento, 21 (21%) um evitamento reduzido e, apenas 6 (6%) referiram não evitar este comportamento.

Uma tendência semelhante foi observada relativamente à aceitação de pedidos de amizade ou de mensagens provenientes de desconhecidos. Obteve-se uma média de 3,49 (DP=1,12) numa escala de *Likert* de 1 a 5 (1=nunca rejeita; 5=rejeita sempre) (cf. Tabela 12). A maioria dos participantes revelou rejeitar estes contactos frequentemente (45%; *n*=45) ou sempre (16%; *n*=16), enquanto 17 (17%) participantes indicaram fazê-lo apenas algumas vezes. Em menor proporção, 16 (16%) participantes referiram rejeitar raramente estes pedidos e apenas 6 (6%) afirmaram nunca os rejeitar.

Esta perceção parece refletir-se também na avaliação que os próprios participantes fazem dos seus comportamentos de prevenção, uma vez que 70 (70%) participantes consideram adotar mais comportamentos de evitamento do que as restantes pessoas do seu círculo social. Em contrapartida, 13 (13%) não partilham dessa opinião e, 17 (17%) afirmam não saber.

Por fim, perante um cenário hipotético em que suspeitassem estar a ser alvo de uma burla online, a estratégia mais frequentemente apontada consistiu em bloquear ou denunciar a conta do suspeito (59%; *n*=59). A denúncia às autoridades foi referida por 19 (19%) participantes, enquanto 12 (12%) optariam por confrontar diretamente a pessoa. Por sua vez, 8 (8%) participantes procurariam aconselhamento junto de familiares ou amigos, e apenas 2 (2%) participantes indicaram que não adotariam qualquer comportamento por não terem a certeza de que se trataria efetivamente de uma burla online.

Tabela 12. Comportamentos de evitamento*

Variáveis	*M*	*MD*	*DP*	*Mín.*	*Máx.*
Frequência com que evita estabelecer novas relações online por receio de ser enganado/a	3,43	4	1,19	1	5
Frequência de verificação da identidade de desconhecidos antes de interagir online	3,79	4	1,16	1	5
Frequência com que evita partilhar fotografias/informação pessoais por receio de uso indevido	3,39	4	1,15	1	5
Frequêmncia da rejeição de pedidos de amizade/mensagens de desconhecidos por receio de burla	3,49	4	1,12	1	5

*M=Média; MD=Mediana; DP=Desvio-Padrão.

No que respeita à escala de comportamentos de evitamento (cf. Tabela 12), as médias variaram entre 3,39 e 3,79, evidenciando uma tendência global para a adoção de estratégias preventivas durante as interações em ambiente digital. A média mais elevada foi observada na variável relativa à verificação da identidade de pessoas desconhecidas antes de iniciar uma interação online (M=3,79; DP=1,16), seguida da rejeição de pedidos de amizade de desconhecidos (M=3,49; DP=1,12), da evitação de novas relações online (M=3,43; DP=1,19) e da evitação da partilha de fotografias e informação pessoal (M=3,39; DP=1,15). Estes resultados sugerem que, de um modo geral, os participantes adotam comportamentos preventivos com uma frequência moderada a elevada.

Por outro lado, com o objetivo de compreender a perceção de insegurança e vulnerabilidade dos participantes perante as burlas online e, em particular, perante o fenómeno do *romance scam*, foram analisados diversos indicadores relacionados com a vulnerabilidade percebida, o risco de vitimação, o sentimento de insegurança e o impacto emocional associado a este tipo de crime

No que respeita ao sentimento de vulnerabilidade perante diferentes tipos de burlas online, obteve-se uma média de 2,78 (DP=1,33), numa escala de *Likert* de 1 a 5 (1=nada vulnerável; 5=totalmente vulnerável), evidenciando uma perceção global moderada de

vulnerabilidade (cf. Tabela 13). Em termos de distribuição de respostas, 24 (24%) participantes consideraram-se nada vulneráveis e 22 (22%) pouco vulneráveis, 34 (34%) participantes classificaram-se como muito vulneráveis e 7 (7%) como totalmente vulneráveis. Os restantes 13 (13%) consideraram apresentar um nível moderado de vulnerabilidade.

Relativamente ao risco percebido de vir a ser vítima de uma burla online, verificou-se uma média de 2,84 (DP=1,24), numa escala de *Likert* de 1 a 5 (1=nenhum risco; 5=risco máximo), sugerindo igualmente uma perceção moderada do risco de vitimação (cf. Tabela 13). A categoria mais frequente correspondeu a pouco risco (28%; *n*=28), seguida de muito risco (26%; *n*=26) e risco moderado (21%; *n*=21). Em menor proporção, 16 (16%) participantes consideram não correr qualquer risco e 9 (9%) avaliaram o seu risco como máximo.

Apesar desta distribuição, 68 (68%) participantes consideram que o medo de serem vítimas de uma burla condiciona a sua liberdade de atuação no meio digital. Apenas 29% (*n*=29) dos participantes responderam negativamente e 3% (*n*=3) afirmam não saber.

A maioria dos participantes (77%; *n*=77) considerou ainda que qualquer pessoa pode ser vítima de uma burla online, independentemente do seu nível de conhecimento sobre novas tecnologias. Apenas 17 (17%) participantes discordam desta afirmação, enquanto 3 (3%) responderam "não sei", e outros 3 (3%) não responderam.

Quanto ao sentimento de insegurança durante a interação com pessoas desconhecidas em ambiente digital, obteve-se uma média de 3,35 (DP=1,28) numa escala de *Likert* de 1 a 5 (1=nada inseguro; 5=muito inseguro), indicando uma tendência par níveis relativamente elevados de insegurança (cf. Tabela 13). Em termos da distribuição das respostas, 33 (33%) participantes se consideram bastante inseguros e 19 (19%) muito inseguros. Em contraste, 20% (*n*=20) dos participantes referiram sentir-se pouco inseguros e 9% (*n*=9) nada inseguros. Os restantes 13 (13%) participantes classificaram o seu nível de insegurança como moderado e registaram-se 6 (6%) respostas omissas.

Relativamente à preocupação com a partilha de dados pessoais, obteve-se uma média de 3,64 (DP=1,17) numa escala de *Likert* de 1 a 5 (1=nada preocupado; 5=muitíssimo preocupado), evidenciando um nível elevado de preocupação (cf. Tabela 13). Em consonância com este resultado, 63 (63%) participantes afirmam estar bastante ou muitíssimo preocupados com a possibilidade de partilhar informações com alguém que

não seja quem afirma ser, ao passo que, apenas 20 (20%) revelam níveis reduzidos de preocupação.

A influência de relatos de vitimação mostrou-se igualmente expressiva. 72 (72%) participantes referiram que o conhecimento de casos de *romance scam* aumentou o seu sentimento de insegurança e, entre estes, 61 (61%) afirmam ter alterado algum comportamento em consequência dessa informação.

De forma praticamente consensual, 97 (97%) participantes consideram que as burlas online se têm tornado progressivamente mais sofisticadas e difíceis de detetar.

Quando confrontados com a hipótese de serem vítimas de *romance scam*, a variável relativa ao impacto emocional esperado apresentou uma média de 3,80 (DP=1,03) numa escala de *Likert* de 1 a 5 (1=nenhum impacto; 5=muito impacto), indicando que oss participantes antecipam consequências emocionais significativas caso viessem a ser vítimas deste tipo de fraude (cf. Tabela 13). Em termos da distribuição de respostas, (67%) participantes anteciparam que a experiência teria um impacto emocional bastante ou muito elevado, enquanto que, apenas 13% (*n*=13) consideram que esse impacto seria inexistente ou reduzido.

Por fim, 86 (86%) participantes consideraram que os órgãos de comunicação social contribuem para o aumento do sentimento de insegurança relativamente às burlas online.

Tabela 13. Perceção de insegurança*

Variáveis	***M***	***MD***	***DP***	***Mín.***	***Máx.***
Vulnerabilidade percebida	2,78	3	1,33	1	5
Risco percebido de ser vítima	2,84	3	1,24	1	5
Insegurança ao interagir online	3,35	4	1,28	1	5
Preocupação com a partilha de dados pessoais	3,64	4	1,17	1	5
Impacto emocional esperado caso fosse vítima	3,80	4	1,03	1	5

*M=Média; MD=Mediana; DP=Desvio-Padrão.

No que diz respeito à perceção de insegurança mediante as variáveis apresentadas (cf. Tabela 13), as médias oscilaram entre 2,78 e 3,80. A gravidade atribuída ao *romance scam* apresentou a média mais elevada (M=4,01; DP=1,01), evidenciando que os participantes percecionam este fenómeno como um crime grave. Verificaram-se igualmente valores elevados no impacto emocional esperado caso viessem a ser vítimas (M=3,80; DP=1,03) e na preocupação com a partilha de dados pessoais (M=3,64; DP=1,17). Em contrapartida, as médias mais baixas observaram-se na vulnerabilidade percebida (M=2,78; DP=1,33) e na perceção do risco de vitimação (M=2,84; DP=1,24), sugerindo que, apesar de reconhecerem a gravidade do *romance scam*, os participantes tendem a percecionar uma probabilidade relativamente reduzida de virem a ser vítimas deste tipo de burla.

Em relação às questões de resposta aberta, os participantes foram convidados a apresentar sugestões para reduzir o número de vítimas de *romance scam*. As respostas evidenciaram consenso em torno das ações de consciencialização (e.g. "campanhas de sensibilização", "medidas de prevenção" e "reforço da literacia digital"). Foram igualmente referidas medidas relacionadas com o reforço dos mecanismos de segurança por parte das plataformas digitais (e.g. "verificação de identidades" e "identificação e remoção de perfis falsos"). Outras sugestões incluíram a disponibilização de mais informações acerca do tema, a criação de canais de atendimento e gestão de denúncias disponíveis nas próprias plataformas e o agravamento das penas aplicadas aos autores deste tipo de crime. Na última questão, destinada à partilha de experiências pessoais ou de opiniões adicionais sobre o tema, alguns participantes relataram situações de burla online vivenciadas por si ou por pessoas do seu círculo de relações, ilustrando diferentes formas de burla online. Em contrapartida, vários participantes referiram não possuir experiência pessoal relacionada com este fenómeno ou indicaram não ter informações adicionais a acrescentar. Entre as restantes respostas, destaca-se ainda a opinião de um participante que salientou a importância da aplicação de penas de prisão aos autores deste tipo de crime.

Com o intuito de analisar a relação entre a perceção da gravidade do *romance scam* e os comportamentos de evitamento, foram calculadas as correlações de *Spearman* (cf. Tabela 14). Através dos resultados foi possível observar-se correlações positivas e significativas entre a perceção da gravidade dos *romance scams* e a verificação da identidade de indivíduos desconhecidos antes da interação online (ρ=0,418; p<0,001), a rejeição dos pedidos de pedidos de amizade de desconhecidos (ρ=0,305; p=0,002), o evitamento de

novas relações online (ρ=0,312; p=0,002), a insegurança na interação online (ρ=0,285; p=0,005) e a preocupação relativa à partilha de dados pessoais (ρ=0,423; p<0,001) (cf. Tabela 14). Assim, através dos resultados obtidos é possível observar que os indivíduos que atribuem maior gravidade às burlas românticas tendem, com maior frequência, a adotar mais comportamentos de evitamento e de prevenção. Em contraste, não foram encontradas correlações estatisticamente significativas entre a perceção da gravidade e a vulnerabilidade percebida (ρ=0,097; p=0,339), o risco percebido de vitimação (ρ=0,044; p=0,666) e a preocupação com a partilha de dados pessoais (ρ=0,178; p=0,076) (cf. Tabela 14). Estes resultados indicam que, embora exista um reconhecimento da gravidade dos *romance scams*, essa perceção não está intrinsecamente associada a uma maior vulnerabilidade ou risco de vitimação.

Tabela 14. Correlações de *Spearman* entre a gravidade atribuída ao *romance scam* e outras variáveis (*n*=100)*

Variáveis	***ρ de Spearman***	***p***	***Interpretação***
Gravidade × Verificação da identidade antes de interagir	0,418	<0,001	Correlação positiva moderada
Gravidade × Evita partilhar fotografias/informação pessoal	0,178	0,076	Não significativa
Gravidade × Rejeita pedidos de amizade de desconhecidos	0,305	0,002	Correlação positiva moderada
Gravidade × Vulnerabilidade percebida	-0,097	0,339	Não significativa
Gravidade × Risco percebido	0,044	0,666	Não significativa
Gravidade × Insegurança ao interagir online	0,285	0,005	Correlação positiva fraca
Gravidade × Evita estabelecer novas relações online	0,312	0,002	Correlação positiva moderada
Gravidade × Preocupação com a partilha de dados pessoais	0,423	<0,001	Correlação positiva moderada

*ρ=Coeficiente de correlação de *Spearman*; *p*=Nível de significância estatística; Nível de significância considerado: p<0,05.

Com o intuito de analisar a existência de diferenças entre o género masculino e o género feminino relativamente às variáveis em estudo, foi usado o teste não paramétrico de *Mann-Whitney* (cf. Tabela 15). Nesta tabela, o valor U corresponde à estatística do teste de *Mann-Whitney* e, o p, representa o *p-value*. Foi adotado neste estudo um nível de significância de 5% ($p<0,05$), considerando-se a existência de diferenças significativas sempre que p for inferior a 0,05. É possível verificar diferenças significativas a nível estatístico entre os géneros, no que respeita à perceção da gravidade ($U=924,0$; $p=0,024$), sendo que as mulheres, em média, apresentam uma perceção de gravidade maior relativamente aos homens (cf. Tabela 15). Também se encontraram significativas diferenças na frequência em que os indivíduos verificam a identidade de desconhecidos antes de interagir ($U=838,5$; $p=0,007$), no evitamento de partilha de fotografias ou informações pessoais ($U=868,0$; $p=0,009$), em rejeitar pedidos de amizade ou mensagens de desconhecidos ($U=823,5$; $p=0,004$), em evitar estabelecer novas relações online ($U=735,5$; $p<0,001$) e em manifestar preocupação com a partilha de dados pessoais ($U=823,5$; $p=0,004$) (cf. Tabela 15). Foi ainda notória uma discrepância quanto à insegurança sentida na interação com desconhecidos online ($U=588,0$; $p<0,001$), bem como no que diz respeito ao impacto emocional esperado perante uma vitimação ($U=906,5$; $p=0,021$) (cf. Tabela 15). Em contrapartida não se encontraram diferenças significativas entre homens e mulheres no risco percebido de vitimação ($U=1256,5$; $p=0,807$) e na vulnerabilidade face aos *romance scams* ($U=1184,5$; $p=0,789$) (cf. Tabela 15). Assim sendo, os resultados evidenciam uma tendência, por parte das mulheres, em atribuir uma maior gravidade ao *romance scam* e na adoção de comportamento preventivos e de evitamento, comparado com os homens. Foi ainda possível observar que ambos apresentam níveis semelhantes no que diz respeito à vulnerabilidade e perceção do risco de vitimação.

Tabela 15. Teste de *Mann-Whitney* segundo o género (*n*=100)*

Variável	***U***	***p***	***Diferença significativa***
Gravidade atribuída ao *romance scam*	924,0	0,024	Sim
Verificação da identidade antes da interação	838,5	0,007	Sim
Evita partilhar fotografias/informação pessoal	868,0	0,009	Sim
Rejeita pedidos de amizade de desconhecidos	834,5	0,004	Sim
Vulnerabilidade percebida	1184,5	0,789	Não
Risco percebido de vitimação	1256,5	0,807	Não
Insegurança ao interagir com desconhecidos online	588,0	<0,001	Sim
Evita estabelecer novas relações online	735,5	<0,001	Sim
Preocupação com a partilha de dados pessoais	823,5	0,004	Sim
Impacto emocional esperado caso fosse vítima	906,5	0,021	Sim

*Nível de significância: $p<0,05$.

Por fim, com o intuito de analisar a associação entre diferentes varáveis categóricas relacionadas com o conhecimento dos *romance scams*, experiência prévia de vitimação (direta ou indireta), adoção de comportamentos de proteção e algumas características sociodemográficas, utilizou-se o teste do *Qui-quadrado de Pearson* (cf. Tabela 16). Os resultados evidenciam uma associação estatística significativa apenas entre o grau de escolaridade e o conhecimento prévio do fenómeno (χ^2=17,590; GL=4; P=0,001), indicando que o conhecimento sobre o *romance scam* varia em função do nível de escolaridade, sendo que, de acordo com o valor de *V de Cramer*, indicia uma associação moderada (cf. Tabela 16). Mais concretamente, verificou-se que 11 dos 14 participantes com mestrado (78,6%) e os 2 participantes detentores de doutoramento (100%), revelaram um maior conhecimento prévio do fenómeno. Em contrapartida, 14 dos 52 participantes com ensino secundário (26,9%) apresentam níveis de conhecimento substancialmente inferiores.

Por outro lado, não foram encontradas associações estatísticas significativas entre género e o conhecimento do *romance scam*, entre género e conhecimento de experiências de vitimação, entre grau de escolaridade e o conhecimento do fenómeno, entre a vitimação e a alteração de definições de privacidade e, entre o conhecimento prévio do *romance scam* e a perceção da gravidade do fenómeno na sociedade. Contudo, importa referir a necessidade de cautela na interpretação dos resultados das análises que envolvem o grau de escolaridade, uma vez que algumas categorias apresentam um número reduzido de participantes, o que leva a frequências inferiores ao recomendado pelo teste, que por sua vez pode vir a afetar os dados estatísticos. Adicionalmente, nas análises referentes ao género, excluiu-se o participante que optou por "prefiro não dizer" por representar apenas um elemento na sua categoria.

Tabela 16. Testes do *Qui-quadrado de Pearson**

Variáveis	***χ²***	***GL***	***P***	***V de Cramer***	***Associação significativa***
Género × Conhecimento do *Romance Scam*	0,657	1	0,417	0,082	Não
Género × Conhece alguém que foi vítima de *Romance Scam*	1,460	1	0,227	0,121	Não
Escolaridade × Conhecimento do *Romance Scam*	17,590	4	0,001	0,419	Sim
Escolaridade × Conhece alguém que foi vítima de *Romance Scam*	5,799	4	0,215	0,241	Não
Conhece alguém que foi vítima × Alterou as definições de privacidade	3,521	2	0,172	0,202	Não

*χ^2=Estatística do teste do *Qui-quadrado de Pearson*; GL=Grau de liberdade; *P*=Nível de significância estatística; *V de Cramer*=Medida da força da associação.

*Considerou-se um nível de significância de 5% ($p<0,05$).

4) Discussão dos resultados

A presente investigação teve como principal objetivo o de analisar a perceção pública sobre a natureza, gravidade e ilicitude das burlas online, com especial atenção no fenómeno do *romance scam*, procurando também perceber como os participantes se comportam para se protegerem do risco de ser vítimas, e de qual é a perceção de insegurança e de vulnerabilidade a que estão sujeitos. De um modo geral, os resultados obtidos evidenciam uma perceção amplamente generalizada da gravidade deste tipo de criminalidade, bem como níveis elevados de preocupação relativamente aos riscos associados, às interações online e uma tendência para a adoção de comportamentos de autoproteção. A discussão que se segue procura interpretar estes resultados à luz da literatura científica, relacionando-os com os objetivos definidos para a presente investigação e com o conhecimento existente sobre o *romance scam*.

No que respeita à perceção pública sobre a natureza do *romance scam*, os resultados evidenciaram um conhecimento específico relativamente reduzido desta tipologia de fraude, uma vez que apenas 38 (38%) participantes referiram já ter ouvido falar deste fenómeno, enquanto 62 (62%) afirmaram nunca ter tido contacto prévio com esta designação. Contudo, apesar deste conhecimento limitado, 96 (96%) participantes consideraram o *romance scam* um crime grave para a sociedade e, após a apresentação de uma breve definição do fenómeno, 81 (81%) participantes classificaram-no como grave ou muito grave para si próprios. Estes resultados sugerem que o desconhecimento parece incidir sobretudo na designação atribuída a este fenómeno criminal e, não necessariamente, sobre as suas características, gravidade ou consequências. Esta interpretação é consistente com a literatura, que tem demonstrado que as potenciais vítimas desconhecem a terminologia associada ao *romance scam*, apesar de reconhecerem os comportamentos fraudulentos que caracterizam este tipo de crime. Whitty e Buchanan (2016), referem que a identificação deste fenómeno ocorre frequentemente apenas após a vitimação ou através da divulgação de casos pelos meios de comunicação social, contribuindo para um conhecimento limitado da sua designação específica. Paralelamente Rege e Lavorgna (2023) salientam que a evolução constante da criminalidade digital e a crescente sofisticação da estratégia utilizadas pelos ofensores dificultam a identificação das diferentes tipologias de fraude por parte da população, reforçando assim a necessidade de promover a literacia digital. Assim, é fulcral a difusão destes termos junto da população, permitindo a identificação, de uma forma facilitada, deste tipo de

criminalidade e uma maior rapidez no reconhecimento dos fatores de risco. Também aqui se pode referenciar brevemente a teoria das atividades rotineiras, segundo a qual a adoção de medidas capazes de reduzir a exposição a potenciais ofensores e aumentar a proteção das potenciais vítimas contribui para diminuir as oportunidades de vitimação (Cohen & Felson, 1979). De igual modo, os princípios da perspetiva situacional do crime permitem interpretar estes comportamentos como estratégias destinadas a dificultar a atuação dos ofensores, através da limitação do acesso à informação pessoal e do reforço das medidas de segurança nas interações online (Clarke, 1995).

Paralelamente, os participantes identificaram um conjunto diversificado de consequências associadas à vitimação, onde se destacam não apenas as perdas financeiras, mas também impactos psicológicos e sociais, como é o caso da ansiedade, depressão, perda de confiança, isolamento social, diminuição da autoestima e, em casos mais extremos, ideação suicida. Estes resultados corroboram a literatura, que descreve o *romance scam* como uma das formas de fraude online com maior impacto multidimensional, uma vez que as perdas económicas são frequentemente acompanhadas por consequências emocionais profundas e duradouras (Bilz et al., 2023; Cross et al., 2018; Whitty, 2018). Estudos desenvolvidos por Bilz et al. (2023), Cross et al. (2018) e Whitty (2018) demonstram que este tipo de fraude pode comprometer significativamente o bem-estar das vítimas, conduzindo a sentimentos de vergonha, isolamento, ansiedade, depressão e perda de confiança interpessoal. Uma possível explicação para esta elevada perceção da gravidade poderá residir na crescente divulgação deste fenómeno pelos meios de comunicação social e por campanhas de sensibilização, que têm contribuído para aumentar a consciencialização pública acerca das consequências das burlas online (Europol, 2025; FTC, 2025).

Um outro aspeto relevante prende-se com a responsabilidade atribuída à vítima pela perda financeira decorrente do *romance scam*. Os resultados demonstraram uma distribuição relativamente heterogênea das opiniões, verificando-se que 50 (50%) participantes consideraram a vítima responsável pela perda financeira, 23 (23%) entenderam que essa responsabilidade depende das circunstâncias do caso concreto e, apenas 18 (18%) defenderam que a vítima não deve ser responsabilizada. Estes resultados sugerem que continua a existir uma tendência para atribuir, pelo menos parcialmente, responsabilidade às vítimas deste tipo de fraude, o que poderá refletir a persistência de estereótipos associados à vitimação e a perceção de que determinados comportamentos individuais

poderiam ter evitado o crime. Esta tendência tem sido amplamente discutida na literatura, sendo frequentemente apontada como um dos fatores que contribuem para a estigmatização das vítimas e para a subnotificação destes crimes (Cross et al., 2018). De igual modo, Bleiman et al. (2025), referem que a perceção pública tende a subestimar a complexidade dos mecanismos de manipulação emocional utilizados pelos ofensores, conduzindo frequentemente à culpabilização da vítima e desvalorização do impacto psicológico inerente ao processo de vitimação. Importa, contudo, salientar que o *romance scam* assenta em estratégias de engenharia social e manipulação afetiva cuidadosamente planeadas, capazes de explorar vulnerabilidades emocionais independentemente da idade, gênero ou nível de escolaridade das vítimas (Bilz et al., 2023; Whitty, 2018). Assim, a atribuição de responsabilidade às vítimas poderá constituir um obstáculo ao reconhecimento deste fenómeno enquanto problema social e criminal, podendo desencorajar a denúncia dos casos e dificultar o acesso das vítimas ao apoio institucional e psicossocial de que necessitam (Cross et al., 2018).

Nas sanções que os participantes consideraram adequadas para os autores deste tipo de crime, a proibição de acesso à Internet foi a medida mais frequentemente apontada (60%; *n*=60), seguida da pena de prisão (53%; *n*=53), e da aplicação de multas (39%; *n*=39). Estes resultados evidenciam que os participantes reconhecem o *romance scam* como uma forma de criminalidade que justifica uma resposta penal e preventiva firme. Esta perceção é consistente com a literatura, que tem vindo a destacar o impacto significativo deste tipo de fraude nas vítimas e a crescente necessidade de desenvolver resposta jurídico-criminais eficazes, atendendo à sua complexidade e ao seu carácter frequentemente transnacional (Rege & Lavorgna, 2023; Europol, 2025). Paralelamente, as respostas obtidas nas questões abertas reforçam esta interpretação, uma vez que vários participantes defenderam o agravamento das penas aplicadas aos ofensores, bem como um maior controlo das plataformas digitais, a identificação de perfis falsos, a verificação da identidade dos utilizadores e o reforço das campanhas de sensibilização e da literatura digital. Em conjunto, estes resultados demonstraram que os participantes não atribuem a prevenção deste fenómeno exclusivamente aos utilizadores, reconhecendo igualmente a importância da intervenção das plataformas digitais, das autoridades competentes e do sistema de justiça na redução da vitimação por *romance scam*.

No que respeita aos comportamentos de evitamento adotados pelos participantes, verificou-se uma elevada preocupação com a proteção da privacidade e com a redução da

exposição a potenciais situações de risco em contexto online. A maioria dos inquiridos (74%; *n*=74) afirmou ter alterado as definições de privacidade das suas contas para evitar ser contactada por desconhecidos. Além disso, também a maioria, 57 (57%) participantes referiram evitar bastante ou totalmente a partilha de fotografias e informações pessoais por receio de uma utilização indevida desses dados. Enquanto 61 (61%) participantes indicaram rejeitar frequentemente ou sempre pedidos de amizade ou mensagens provenientes de pessoas desconhecidas. Estes dados evidenciam uma atitude predominantemente preventiva perante os riscos associados às interações digitais, refletindo uma preocupação crescente com a segurança online. Esta tendência encontra respaldo na literatura, que descreve a adoção de estratégias de autoproteção como uma resposta ao aumento de complexidade e sofisticação dos *romance scmas*, bem como à maior consciencialização dos utilizadores relativamente aos riscos inerentes ao ambiente digital (Europol, 2025; Rege & Lavorgna, 2023). Esta interpretação pode também ser enquadrada na teoria das atividades rotineiras, segundo a qual a diminuição das oportunidades para a prática do crime depende, entre outros fatores, da adoção de comportamentos que reduzam a vulnerabilidade dos potenciais alvos (Cohen & Felson, 1979). Simultaneamente, estes comportamentos encontram igualmente suporte nos princípios da perspetiva situacional do crime, ao evidenciarem a implementação de medidas que dificultam a atuação dos ofensores e reforçam a proteção dos utilizadores no ambiente online (Clarke, 1995).

A adoção de comportamentos preventivos tornou-se igualmente evidente na forma como os participantes referiram reagir perante potenciais situações de risco. Quando confrontados com a possibilidade de receber mensagens enviadas por desconhecidos, 47 (47%) participantes afirmaram verificar previamente o perfil do remetente antes de responder. Já perante um cenário de suspeita de burla, a maioria indicou que bloquearia ou denunciaria a conta (59%; *n*=59). Estes resultados revelam uma postura marcadamente cautelosa perante contactos estabelecidos em ambientes digitais, privilegiando estratégias de verificação e interrupção da interação sempre que exista suspeita de fraude. Esta tendência encontra-se em consonância com a literatura, que identifica a desconfiança perante contactos não solicitados, a verificação de identidade dos interlocutores e a denúncia de comportamentos suspeitos como medidas fundamentais na prevenção da vitimação por *romance scam* (Bilz et al., 2023; Rege & Lavorgna, 2023; Whitty & Buchanan, 2016).

A relevância atribuída à prevenção refletiu-se igualmente nas estratégias que os participantes identificaram como mais eficazes para reduzir o risco de vitimação. Entre as medidas de autoproteção mais frequentemente referidas destacam-se a não partilha de informações pessoais com desconhecidos (67%; *n*=67), a verificação de perfis suspeitos antes de qualquer interação (54%; *n*=54), a utilização da autenticação de dois fatores (32%; *n*=32) e o facto de evitar sites de encontros ou de páginas desconhecidas (30%; *n*=30). Paralelamente, nas questões de resposta aberta, os participantes defenderam, de forma recorrente, a necessidade de reforçar as campanhas de sensibilização e prevenção, promover a literacia digital da população, aumentar o controlo exercido pelas plataformas digitais, melhorar os mecanismos de verificação da identidade dos utilizadores e facilitar a denúncia de perfis falsos na própria página. Estas respostas parecem inferir que a prevenção do *romance scam* é percecionada como uma responsabilidade partilhada entre os próprios utilizadores, as plataformas digitais e as entidades competentes. Esta perspetiva encontra-se alinhada com a literatura, que defende que a redução da vitimação depende de uma abordagem integrada, assente na sensibilização dos utilizadores, no reforço das medidas de segurança das plataformas e na cooperação entre as diferentes entidades envolvidas na prevenção e combate à criminalidade digital (Europol, 2025; FTC, 2025; Rege & Lavorgna, 2023).

Os resultados relativos ao padrão de utilização das plataformas digitais permitem igualmente contextualizar estes comportamentos preventivos. Verificou-se que todos os participantes que utilizavam aplicações de encontros referiram já ter interagido online com pessoas desconhecidas e que, a grande maioria, também se encontrou presencialmente com alguém conhecido exclusivamente através da Internet. Contudo, verificou-se igualmente que uma proporção considerável dos participantes que não utilizavam aplicações de encontros também referiu estabelecer este tipo de interações através de outras plataformas digitais. Estes resultados sugerem que a exposição ao risco de *romance scam* não se restringe às *apps* de encontro, estendendo-se igualmente às redes sociais generalizadas, o que vem reforçar a necessidade de desenvolver estratégias preventivas dirigidas a todos os utilizadores de plataformas digitais, e não apenas aos utilizadores de aplicações especificamente destinadas ao estabelecimento de relações afetivas.

Os resultados mostraram também que os participantes reconhecem a crescente complexidade deste fenómeno e a sua capacidade para afetar qualquer utilizador,

independentemente do nível de conhecimento tecnológico. Com efeito, 97 (97%) participantes consideraram que as burlas online têm-se tornado cada vez mais sofisticadas e de difícil deteção, enquanto que 77 (77%) participantes afirmam que qualquer pessoa pode ser vítima deste tipo de fraude, independentemente do seu conhecimento sobre as novas tecnologias. Estes resultados sugerem que a perceção de ilicitude não assenta apenas no reconhecimento da natureza criminosa destes comportamentos, mas também na consciência de que os ofensores recorrem a estratégias de manipulação cada vez mais elaboradas e difíceis de identificar. Esta interpretação encontra suporte na literatura, que caracteriza o *romance scam* como uma forma de criminalidade digital assente em técnicas de engenharia social, manipulação emocional e exploração das vulnerabilidades das potenciais vítimas (Bilz et al., 2023; Rege & Lavorgna, 2023; Whitty, 2013). O reconhecimento desta evolução poderá contribuir para uma maior consciencialização dos utilizadores relativamente à gravidade do fenómeno e à necessidade de adotar comportamentos preventivos durante as interações estabelecidas em ambiente digital.

No que refere à exposição a experiências de vitimação, verificou-se que 72 (72%) participantes referiram que o conhecimento de relatos de vítimas de *romance scam* contribuiu para o aumento do seu sentimento de insegurança e, entre estes, 61 (61%) afirmam ter alterado os seus comportamentos após tomarem conhecimento dessas situações. Paralelamente 86 (86%) participantes consideraram que os órgãos de comunicação social contribuem para o aumento do sentimento de insegurança relativamente às burlas online. Estes resultados sugerem que a perceção da ilicitude é influenciada não apenas pelo conhecimento do fenómeno, mas também pela exposição a experiências de vitimação e pela forma como a informação é transmitida pela cobertura mediática. Esta interpretação encontra respaldo na literatura, que evidencia que a divulgação de casos de *romance scam* contribui para aumentar a consciencialização pública acerca das estratégias utilizadas pelos ofensores e das consequências associadas à vitimação, favorecendo uma maior perceção da gravidade deste tipo de criminalidade (Cross et al., 2016; Lazarus et al., 2023; Tech for Good Institute, 2025). Simultaneamente, a crescente visibilidade das burlas online poderá potenciar uma maior sensibilização dos utilizadores para os riscos existentes no ambiente digital, promovendo uma atitude mais vigilante perante potenciais tentativas de fraude.

Verificou-se ainda que 41 (41%) participantes se consideraram muito ou totalmente vulneráveis aos diferentes tipos de burla online, enquanto 35 (35%) percecionaram

apresentar um nível de risco muito elevado ou máximo de virem a ser vítimas de fraudes online. Paralelamente, 52 (52%) participantes afirmaram sentir-se bastante ou muito inseguros ao interagir com desconhecidos na Internet e, 63 (63%) participantes referiram preocupar-se bastante ou muitíssimo com a possibilidade de partilhar dados pessoais com alguém que não seja quem afirma ser. Embora estes resultados não permitam estabelecer uma relação estatisticamente comprovada entre a perceção do risco e os comportamentos de evitamento, evidenciam uma tendência para que níveis mais elevados de preocupação coexistam como uma maior consciência dos potenciais perigos associados às interações em ambientes digitais. Esta interpretação encontra-se em consonância com a literatura, que descreve a perceção do risco como um fator relevante na adoção de estratégias de autoproteção, particularmente perante formas de criminalidade assentes na manipulação emocional e na engenharia social, como acontece no *romance scam* (Bilz et al., 2023; Rege & Lavorgna, 2023; Whitty, 2018).

A análise descritiva sugere também que a consciência dos riscos associados ao *romance scam* poderá tender a uma utilização mais cautelosa das plataformas digitais. Esta tendência reforça a importância da promoção da literacia digital enquanto estratégia preventiva, não apenas através da transmissão de informação sobre as diferentes modalidades de fraude, mas também pelo desenvolvimento de competências que permitam aos utilizadores identificar sinais de manipulação, avaliar criticamente as interações estabelecidas em ambientes digitais e adotar práticas de utilização mais seguras. Neste contexto, a prevenção do *romance scam* não deverá assentar exclusivamente em resposta jurídico-criminais, mas também em intervenções de consciencialização e de sensibilização que promovam a segurança digital conforme defendido por Bilz et al. (2023), Europol (2025) e Rege e Lavorgna (2023).

De um modo geral, os resultados obtidos sugerem que os participantes reconhecem o *romance scam* como uma forma de criminalidade digital particularmente grave, embora persistam algumas lacunas ao nível do conhecimento específico sobre este fenómeno. Simultaneamente, verificou-se uma tendência para a adoção de comportamentos de autoproteção e de evitamento em contexto online, refletindo uma crescente preocupação com os riscos associados às interações digitais. Neste sentido, os resultados reforçam a importância de investir na promoção da literacia digital e no desenvolvimento de campanhas de sensibilização dirigidas à população, não apenas sobre as burlas online em geral, mas também sobre as suas diferentes modalidades, de forma a aumentar o

conhecimento acerca dos mecanismos utilizados pelos ofensores e das estratégias preventivas que poderão contribuir para reduzir o risco de vitimação.

Para além da análise descritiva acima apresentada, optou-se ainda pela realização de análises inferenciais com o intuito de aprofundar e melhorar a compreensão das relações existentes ou não entre as variáveis e a resposta às questões de investigação.

No que diz respeito à relação da perceção da gravidade e comportamentos preventivos do fenómeno, verifica-se que as correlações de *Spearman* demonstram que, indivíduos que atribuem uma maior gravidade a este fenómeno tendem a adotar estratégias de proteção e evitamento com maior frequência. Existem ainda associações estatisticamente positivas entre a gravidade atribuída e a verificação da identidade de desconhecidos antes de uma interação no mundo digital, a rejeição de pedidos de amizade de desconhecidos, o evitamento de estabelecimento de novas relações online, o sentimento de insegurança perante interações com desconhecidos e sentimento de preocupação com a partilha de dados pessoais. Os resultados sugerem que a existência de uma maior perceção do risco constitui um fator de relevo na adoção de comportamentos preventivos, o que vai ao encontro da literatura, uma vez que refere que, quanto maior os níveis de consciencialização do risco, maior a adoção de diferentes estratégias e evitamento e proteção no mundo digital (Bilz et al., 2023; Rege e Lavorgna, 2023; Whitty, 2018).

Em contrapartida, não foram identificadas associações significativas entre a gravidade atribuída ao fenómeno e a vulnerabilidade percebida, o risco subjetivo de vitimação ou o evitamento de partilha de dados pessoais. Poderão, assim, estes dados indicar que algumas perceções individuais não dependem exclusivamente da gravidade do *romance scam*, podendo ser influenciadas por características individuais, experiências pessoais ou níveis de literacia digital diferentes.

No que respeita às diferenças grupais realizadas pelos testes de *Mann-Whitney*, foi possível observar uma reduzida influência do género em grande parte das variáveis analisadas, sugerindo perceções e comportamentos preventivos semelhantes por parte dos homens e das mulheres. Estes resultados podem assim refletir o aumento da disseminação deste fenómeno pelos meios de comunicação social e/ou campanhas de sensibilização, o que contribui para uma distribuição relativamente homogénea de práticas preventivas e conhecimento sobre o fenómeno entre homens e mulheres.

Relativamente ao grau de escolaridade, as análises realizadas através do teste do *Qui-quadrado* identificaram uma associação estatisticamente significativa entre o conhecimento prévio do *romance scam* e o grau de escolaridade. Isto sugere que os indivíduos com um grau de escolaridade mais elevado tendencionalmente possuem uma maior familiarização com os *romances scams*, podendo refletir maiores níveis de literacia digital, mais e melhor exposição a qualidade de informação e/ou um maior contacto com conteúdos ligados à cibercriminalidade. Estes resultados vão ao encontro aos pensamentos de Rege e Lavorgna (2023), uma vez que a literacia digital se demonstra um fator relevante para a familiaridade com os *romance scams*. Também Bilz et al. (2023), refere que a informação e educação dos utilizadores desempenha um papel determinante na prevenção de vitimação no mundo digital. Contudo, este resultado deve ser interpretado com prudência, uma vez que duas categorias de escolaridade apresentam um número reduzido de participantes, o que poderá limitar a robustez da análise, uma vez que essas categorias apresentam frequências inferiores às recomendadas à aplicação do teste.

As restantes analises realizadas através do teste *Qui*-quadrado não evidenciam associações significativas, sugerindo que, apesar da existência de diferenças no conhecimento específico da terminologia em função da escolaridade, a perceção da gravidade do fenómeno parece, de certo modo, estar relativamente disseminada entre os participantes, independentemente das características sociodemográficas analisadas. Estas evidencias corroboram as observações de Whitty (2018), uma vez que a crescente difusão de informação relativamente a este tipo de fraude, por exemplo através dos meios de comunicação social, tem contribuído para um aumento da consciencialização pública no que diz respeito aos riscos associado às relações online.

Os resultados obtidos, de uma forma geral, permitem concluir que a perceção da gravidade dos *romance scams* é um elemento mais relevante para adoção de comportamentos preventivos do que as características sociodemográficas. Por sua vez, as correlações observadas demonstram que, quanto maior a perceção da gravidade a este fenómeno, maior a probabilidade de adoção de comportamentos de autoproteção de uma forma frequente, como é o caso da verificação de identidade, rejeição de pedidos de amizade de desconhecidos e preocupação com os seus dados pessoais. É assim evidenciada a importância da promoção da literacia digital e da sensibilização da sociedade enquanto elemento fulcral na redução da exposição ao fenómeno. Isto

enquadra-se na teoria das atividades rotineiras de Cohen e Felson (1979) e na teoria da prevenção situacional do crime (Clarke 1997), pois ambas evidenciam que as adoções de comportamentos de autoproteção reduzem as oportunidades dos ofensores, diminuindo consequentemente a probabilidade de vitimação.

C**onsiderações Finais**

A presente dissertação de mestrado explorou o fenómeno do *romance scam*, enquanto forma específica de criminalidade digital, com especial atenção à perceção da gravidade deste fenómeno, aos comportamentos de evitamento adotados pelos utilizadores em contexto online e às relações existentes entre estas dimensões. O estudo teve início com uma análise sistematizada da literatura científica sobre *romance scam*, abrangendo os principais conceitos, os padrões de vitimação e o impacto emocional, social e económico associado a este tipo de fraude. Ao longo da investigação, foi evidenciada a relevância crescente do fenómeno, com particular atenção aos enquadramentos legais e jurídico-criminais aplicáveis, bem como às teorias criminológicas e abordagens da criminalidade digital que permitem compreender os mecanismos de atuação dos ofensores e as vulnerabilidades das vítimas. A gravidade do *romance scam* foi igualmente destacada, não apenas através da análise do modus operandi e das técnicas de manipulação emocional utilizadas pelos ofensores, mas também pelo reconhecimento do impacto profundo e duradouro da vitimação, frequentemente marcado por perdas financeiras significativas e consequências psicológicas persistentes.

Conforme evidenciado ao longo da presente dissertação, as burlas e os *romance scams* destacam-se, na perspetiva jurídico-criminal, pela conjugação de fatores emocionais e patrimoniais, o que representa um desafio significativo para os sistemas de justiça penal no que respeita à sua identificação, investigação e repressão. No contexto português, a legislação vigente oferece um enquadramento sólido, nomeadamente através dos artigos 217.º e 221.º do CPP, embora enfrente limitações na abordagem do carácter transnacional destes crimes, reflexo da complexidade inerente à criminalidade digital. A nível internacional, a crescente sofisticação das redes criminosas e o recurso a tecnologias avançadas reforçam a necessidade de uma cooperação eficaz entre Estados e organizações internacionais, bem como de estratégias integradas de prevenção e monitorização.

A compreensão plena do fenómeno exige uma abordagem interdisciplinar, que articule as dimensões jurídica, criminológica e tecnológica, de modo a identificar padrões de atuação dos ofensores, vulnerabilidades das vítimas e práticas de autoproteção. Só assim será possível desenvolver estratégias preventivas e repressivas mais eficazes face a esta forma de criminalidade. A literatura demonstra que, apesar dos progressos na compreensão dos

ofensores, das vítimas e dos esquemas utilizados, persistem lacunas significativas, nomeadamente ao nível da perceção pública sobre a gravidade destes crimes, da subnotificação e da efetividade das respostas judiciais e preventivas.

Em síntese, o *romance scam* ultrapassa as categorias tradicionais de burla, integrando dimensões patrimoniais, emocionais e sociais que exigem uma abordagem criminológica multidisciplinar. A sua crescente prevalência evidencia a necessidade de reforçar a literacia digital, aperfeiçoar os enquadramentos legais e desenvolver sistemas de apoio adequados às vítimas, de modo a mitigar o impacto deste crime na sociedade contemporânea.

Por sua vez, o estudo empírico teve como principais objetivos caracterizar a perceção pública sobre a gravidade do *romance scam*, identificar os comportamentos de evitamento adotados pelos utilizadores para reduzir o risco de vitimação online, analisar a associação entre fatores de ordem individual e a perceção da gravidade do fenómeno, examinar a relação entre essa perceção e os comportamentos preventivos adotados e explorar possíveis diferenças sociodemográficas na perceção da gravidade e nos comportamentos de evitamento. Para esse efeito, foi adotada uma metodologia quantitativa, de carácter transversal e descritivo, recorrendo à aplicação de um inquérito por questionário em formato digital.

A presente investigação estabelece, assim, uma base teórica e metodológica sólida para a exploração da perceção pública sobre o *romance scam* e os comportamentos de evitamento adotados pelos utilizadores em contexto online.

Os resultados principais deste estudo evidenciaram que a maioria dos participantes reconhece a gravidade do *romance scam* considerando-o um crime sério e potencialmente gerador de consequências financeiras e emocionais significativas para as vítimas. Apesar de se verificar um conhecimento limitado acerca do conceito específico de *romance scam* e de algumas das suas modalidades, os participantes demonstraram um elevado grau de preocupação relativamente às burlas online, reconhecendo a crescente sofisticação destes esquemas e admitindo qualquer pessoa pode vir a tornar-se vítima, independentemente do seu nível de conhecimento tecnológico. Paralelamente observou-se uma elevada adoção de comportamentos preventivos e de evitamento, nomeadamente através da alteração das definições de privacidade, da rejeição de pedidos de contacto provenientes de desconhecidos, da limitação da partilha de informação pessoal e da verificação de

identidade de potenciais interlocutores antes de estabelecer interações online. Os participantes revelaram ainda níveis elevados de insegurança relativamente às interações com desconhecidos em contexto digital e reconheceram que o receio de serem vítimas de burla online condiciona, em muitos casos, os seus comportamentos digitais. As respostas às questões abertas reforçam igualmente a importância atribuída à literacia digital, às campanhas de sensibilização, ao reforço dos mecanismos de segurança das plataformas digitais e ao agravamento das respostas dirigidas aos autores deste tipo de criminalidade.

Para além da caracterização descritiva da amostra, as análises inferenciais permitiram aprofundar a compreensão das relações entre as variáveis em estudo. Os resultados evidenciaram associações estatisticamente significativas entre a perceção da gravidade do *romance scam* e diversos comportamentos de evitamento, verificando-se que os participantes que atribuem maior gravidade a este fenómeno tendem a adotar, com maior frequência, estratégias preventivas, como a verificação da identidade de pessoas desconhecidas, a rejeição de pedidos de amizade, o evitamento do estabelecimento de novas relações online e uma maior preocupação com a proteção dos dados pessoais. Por outro lado, as análises revelaram diferenças sociodemográficas reduzidas, identificando-se apenas uma associação estatisticamente significativa entre o grau de escolaridade e o conhecimento prévio do romance scam, o que sugere que a perceção da gravidade e os comportamentos preventivos se encontram relativamente disseminados entre os participantes, independentemente das características sociodemográficas analisadas.

Contudo, o estudo apresentou algumas limitações, nomeadamente a ausência de contacto direto entre o investigador e os participantes, inerente à aplicação do questionário em formato digital, bem como a natureza transversal da investigação, que não possibilitou uma análise aprofundada da evolução das perceções e dos comportamentos de evitamento ao longo do tempo. Adicionalmente, a amostra revelou limitações ao nível da representatividade geográfica e sociocultural, o que condiciona a generalização dos resultados para a totalidade da população.

Em síntese, as análises realizadas evidenciam que existe uma associação estatisticamente significativa entre a perceção da gravidade do *romance scam* e diversos comportamentos preventivos como uma maior preocupação com a segurança online e pela adoção de estratégias de autoproteção. Simultaneamente, evidenciam a persistência de lacunas ao nível do conhecimento específico sobre esta tipologia criminal, reforçando a necessidade

de desenvolver iniciativas de educação e sensibilização que permitam melhorar a capacidade dos utilizadores para reconhecer sinais de fraude e atuar preventivamente.

Um dos principais contributos desta investigação consistiu na demonstração empírica da existência de associações entre a perceção da gravidade do *romance scam* e a adoção de comportamentos preventivos, evidenciando que uma maior consciencialização sobre este fenómeno tende a estar associada a uma maior adoção de estratégias de autoproteção. Deste modo, o estudo reforça a importância da promoção da literacia digital e da sensibilização da população enquanto instrumentos fundamentais para a prevenção da vitimação em contexto digital.

Assim, a presente investigação contribui para o alargamento do conhecimento científico sobre esta forma de criminalidade e para a identificação de fatores relevantes na promoção da segurança online. Espera-se que as conclusões apresentadas possam servir de ponto de partida para futuras investigações mais abrangentes, preferencialmente com amostras mais diversificadas e metodologias complementares, bem como apoiar o desenvolvimento de estratégias de prevenção, políticas públicas e práticas institucionais mais eficazes.

Em suma, os resultados obtidos permitiram responder aos objetivos e às questões de investigação inicialmente formuladas, demonstrando que a perceção da gravidade do romance scam está associada à adoção de comportamentos de evitamento, enquanto as características sociodemográficas assumem um papel mais limitado na explicação destes comportamentos. Estes resultados reforçam a importância da promoção da literacia digital e da sensibilização da população como instrumentos fundamentais de prevenção da vitimação online.

Limitações

Durante a elaboração da presente dissertação de mestrado, emergiram várias limitações que influenciaram tanto o desenvolvimento do trabalho como a interpretação dos resultados obtidos. Uma das principais dificuldades identificadas foi a escassez de estatísticas atualizadas e detalhadas sobre a criminalidade digital, em particular no que respeita ao *romance scam*. A reduzida disponibilidade de dados oficiais poderá estar associada à especificidade deste tipo de crime, o que limita a compreensão global da sua prevalência e impacto.

Outra limitação relevante prendeu-se com a baixa adesão ao questionário, apesar do esforço de divulgação realizado. Verificou-se ainda uma distribuição desigual de respostas entre os diferentes distritos de Portugal, com alguns sem qualquer participação registada. Esta assimetria compromete a representatividade geográfica e sociodemográfica da amostra, condicionando a generalização dos resultados.

Apesar destas limitações, espera-se que a presente investigação venha a ter um contributo relevante para a compreensão das perceções públicas e dos comportamentos de evitamento associados ao *romance scam*, servindo de base para o desenvolvimento de futuras investigações e o aprofundamento do conhecimento científico neste domínio.

Referências Bibliográficas

Abu-Salma, R., Murdoch, S., & Zytko, D. (2025). Online Dating Platform Safeguards and Self-Protection: How Dating Platforms Characterise, Respond to, and Safeguard Against Harms. *Proceedings of the CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3706599.3719825

Abubakari, Y., & Oseh-Ovarah, V. (2025). The gamification of online romance fraud through offenders' cards. *Digital Threats: Research and Practice*, *6*(4), Article 34. https://doi.org/10.1145/3773289

ACI Worldwide. (2024). 2024 *Scamscope Report: The battle for trust*. https://www.aciworldwide.com/wp-content/uploads/2024/11/2024-Scamscope-Report-The-Battle-for-Trust.pdf

Alam, N., Dhillon, G., & Oliveira, T. (2021). Psychological antecedents and consequences of online romance scam victimization fear. In *Proceedings of the 27th Americas Conference on Information Systems* (AMCIS 2021). Association for Information Systems. https://aisel.aisnet.org/amcis2021/social_computing/social_computing/11/

Albuquerque, P. P. (2024). *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos* (6ª ed.). UCP Editora.

Albuquerque, R. (2006). Os objetos intangíveis na era da criminalidade informática. *Espaço Jurídico*, *7*(2), 165-177. https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/8794/4832

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, 35 https://doi.org/10.1016/j.dcm.2020.100398

Assembleia da República. (2009, 15 de setembro). *Lei n.º 109/2009: Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa*. Diário da República: Série I (179).

Associação Portuguesa de Apoio à Vítima (APAV). (2024, 6 de fevereiro). *Estatísticas Linha Internet Segura: 2023*. https://www.internetsegura.pt/noticias/estatisticas-linha-internet-segura-2023

Associação Portuguesa de Apoio à Vítima (APAV). (2025, 11 de fevereiro). *Estatísticas APAV - Linha Internet Segura 2024*. https://apav.pt/estatisticas-apav-linha-internet-seura-2024

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers*, 35(6), 773–788. https://doi.org/10.1093/iwc/iwad048

Bleiman, R., Park, H., & Rege, A. (2025). Educating students on the behavioral and psychological aspects of romance scam victimization via a social engineering competition. *Journal of Cybersecurity Education, Research and Practice*, 2025(1), Article 3. https://digitalcommons.kennesaw.edu/jcerp/vol2025/iss1/3

Boccardi, V., Paoloni, C., Cossu, G., & Mecocci, P. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice & Epidemiology in Mental Health*, 16(Suppl-1), 1–12. https://doi.org/10.2174/1745017902016010001

Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: Investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*, 29(2), 460–475. https://doi.org/10.1108/JFC-02-2021-0042

Carter, E. (2021). Distort, exort, deceive and exploit: Exploring the inner workings of romance fraud. *The British Journal of Criminology*, 61(2), 283-302. https://doi.org/10.1093/bjc/azaa072

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91-150. https://www.jstor.org/stable/1147596

Código Penal - Edição Académica. (2023). (12.ªed.). Porto Editora.

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

Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2024.100060

Coluccia, A., Pozza, A., Fagiano, A., Gualtieri, G., Incalza, M. A., & Ferretti, F. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice & Epidemiology in Mental Health*, 16(Suppl-1), 24–35. https://doi.org/10.2174/1745017902016010024

Costa, A. M. A. (2020). *A burla no Código Penal Português* (1.ª ed.). Edições Almedina.

Costa, D. (2021). Vitimologia positivista e radical. In L. M. Nunes & A. Sani (Eds.), *Manual de criminologia e vitimologia* (pp. 27-38). Pactor.

Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

Coutinho, C. P. (2023). *Metodologia de investigação em ciências sociais e humanas: Teoria e prática* (2.ªed.). Edições Almedina.

Cross, C. (2020). Romance fraud. In T. J. Holt & A. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 935–954). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-90307-1

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, 58(6), 1303–1322. https://doi.org/10.1093/bjc/azy014

Cross, C., Richards, K., & Smith, R. G. (2016). *Improving responses to online fraud victims: An examination of reporting and support* (Final report for Criminology Research Grant 29/13-14). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/29-1314-FinalReport.pdf

DECO PROTeste. (2024, 29 de outubro). *Ciberameaças: Portugueses dizem conhecer riscos online*. https://www.deco.proteste.pt/tecnologia/computadores/noticias/ciberameacas-portugueses-dizem-conhecer-riscos-online

Dickinson, T., Wang, F., & Maimon, D. (2023). What money can do: Examining the effects of rewards on online romance fraudsters' deceptive strategies. *Deviant Behavior*, *44*(9), 1386–1400. https://doi.org/10.1080/01639625.2023.2197547

Dias, V. (2012). A problemática da investigação do cibercrime. *Data Venia*, *1*(1), 64-87. https://datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf

Europol. (2018). *Internet Organised Crime Threat Assessment 2018*. Europol. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

Europol. (2025). *Steal, deal and repeat: How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment* (IOCTA) 2025 (10th ed.). Publications Office of the European Union. https://doi.org/10.2813/4926508

Federal Bureau of Investigation (FBI) . (2026). *Internet crime report 2025*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Federal Trade Commission (FTC). (2025). *Consumer sentinel network data book 2024*. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024

Felson, M., & Eckert, M. (2021).*Crime and everyday life* (7th ed.). SAGE Publications.

Feng, M. (2025). Online romance fraud as a form of emotional and economic partner violence: A social-ecological framework of enabling factors. *Nordic Journal of Studies in Policing*, *12*(2), 1–22. https://doi.org/10.18261/njsp.12.2.4

Grant, S., & Buil-Gil, D. (2025). The effect of true crime docuseries on romance fraud reporting to the police. *Crime Science*, 14(1). https://doi.org/10.1186/s40163-025-00244-y

Guerra, C., & Ingram, J. R. (2022). Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, 43(1), 44–60. https://doi.org/10.1080/01639625.2020.1774707

Guerreiro, A., Costa, L., Carneiro, A. T., & Cruz, O. S. (2024). Burla romântica: Em torno de um conceito de vitimização. *Cadernos do Arquivo Municipal*, 22, 1–16. https://doi.org/10.48751/CAM-2024-22380

Hameed, M. A., Arachchilage, N. A. G., & Haddad, H. M. (2023). Thwarting instant messaging phishing attacks: The role of self-efficacy and the mediating effect of attitude

towards online sharing of personal information. *International Journal of Environmental Research and Public Health*, 20(4), Article 3514. https://doi.org/10.3390/ijerph20043514

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge. https://doi.org/10.4324/9780429343223

Interpol. (2022). *2022 INTERPOL Global Crime Trend Summary Report*. https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, 9(2), 205–217. https://www.cybercrimejournal.com/pdf/Koppetal2015vol9issue2.pdf

Lazarus, S. (2024). *How online fraudsters are romancing away people's savings*. London School of Economics. https://www.lse.ac.uk

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, 2, 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

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

Levi, M. (2012). The organization of serious crimes for gain. In *The Oxford handbook of organized crime* (pp. 70–94). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.013.0004

Levi, M. (2025). Human, institutional, political and technological factors involved in a public health approach to frauds against individuals. *European Journal of Criminology*, 22(4), 646–670. https://doi.org/10.1177/14773708251341076

Malwarebytes. (2024). *Romance scam costlier than ever: Survey finding*. https://www.malwarebytes.com

Martins, J. P., Guedes, I. S., Sani, A., & Moreira, S. (2023). Effects of individual and contextual dimensions on an aggregate measure of cybervictimization. *Victims & Offenders*, 1-17. https://doi.org/10.1080/15564886.2023.2248483

Monteiro, M. S. (2024). *Crimes sexuais contra menores*: *Uma análise da consciencialização parental sobre os riscos de abuso sexual nos jogos online* (Dissertação de mestrado, Universidade Fernando Pessoa). http://hdl.handle.net/10284/13450

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2022). How do individuals justify and rationalize their criminal behaviors in online romance fraud? *Information Systems Frontiers*, *24*(2), 475–491. https://doi.org/10.1007/s10796-020-10051-2

Portugal. (1966). Código Civil (Com as alterações e atualizações subsequentes). *Diário da República*, I Série, 256 (25 de novembro de 1966).

Rege, A., & Lavorgna, A. (2023). Cyber-enabled fraud and the role of online platforms. *Crime, Law and Social Change*, 79(2), 165–184. https://doi.org/10.1007/s10611-022-10053-4

Romance Scam Research Center (RSRC). (2025). *The trajectory of romance scams in the U.S.* https://romancescamresearch.org/library/59

Saad, M. E., Norul, S., & Zamri, M. (2018). Cyber romance scam victimization analysis using routine activity theory versus Apriori algorithm. *International Journal of Advanced Computer Science and Applications*, 9(12), 479–485. https://doi.org/10.14569/IJACSA.2018.091267

Saraiva, M. (2021). Perspetiva ecológica/ambiental da criminologia. In L. M. Nunes & A. Sani (Eds.), *Manual de criminologia e vitimologia* (pp. 98-106). Pactor.

Schokkenbroek, J. M., & Snaphaan, T. (2025). Love as bait: A scoping review and crime script analysis of online romance scams. *Trauma, Violence, & Abuse*. Advance online publication. https://doi.org/10.1177/15248380251361046

Simon, H. A. (1997). *Administrative behavior* (4th ed.). Free Press.

Sistema de Segurança Interna. (2025). *Relatório Anual de Segurança Interna 2024*. Gabinete do Secretário-Geral do Sistema de Segurança Interna. https://www.ssi.gov.pt/en/publicacoes/rasi/RASI%202024.pdf

Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies*, 37(4), 328–351. https://doi.org/10.1080/1478601X.2024.2429088

Souza, F. M. (2022). *Sextorsão e romance scam no estado do Pará* [Dissertação de mestrado, Universidade Federal do Pará]. Repositório Institucional da UFPA. https://www.ppgsp.propesp.ufpa.br/ARQUIVOS/teses_e_dissertacoes/dissertacoes/2020/202005%20-%20FERNANDA%20MAUES%20DE%20SOUZA.pdf

Spiller, K., Bull, S., Hanoch, Y., & Flint, O. (2025). Fraud on TV: The Reith principles and watching British public service broadcasting. *Crime Media Culture*. https://doi.org/10.1177/17416590251384590

Tech for Good Institute. (2025). *Building resilience against digitally-enabled scams and fraud in Southeast Asia: A whole-of-society approach*. https://techforgoodinstitute.org/wp-content/uploads/2025/08/External-Scams-and-Fraud-SEA-6-1.pdf

Thumboo, J., & Mukherjee, S. (2024). Digital romance fraud targeting unmarried women. *Discover Global Society*, 2(1), Article 132. https://doi.org/10.1007/s44282-024-00132-x

Tintori, A., Ciancimino, G., Bombelli, I., Rocchi, D., & Cerbara, L. (2023). Children's online safety: Predictive factors of cyberbullying and online grooming involvement. *Societies*, 13(2), 47. https://doi.org/10.3390/soc13020047

Tropina, T. (2024). 'This is not a human rights convention!': The perils of overlooking human rights in the UN cybercrime treaty. *Information & Communications Technology Law*, 33(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517

Tsunoda, M., & Sato, H. (2025). Patterns and predictors of cyber fraud victimization: Testing routine activity theory and general theory of crime in Japan. *Journal of Economic Criminology*, 9, Article 100186. https://doi.org/10.1016/j.jeconc.2025.100186

University of California. (2025). *Cybersecurity Awareness Month 2025: Stop. Spot. Report Scams*. https://security.ucop.edu/resources/security-awareness/cyber-security-month-2025.html

Vakhitova, Z. I., Reyns, B. W., & Simpson, R. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior*, 101, 420–430. https://doi.org/10.1016/j.chb.2019.07.012

Verizon. (2025). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Wang, F. (2025). A quantitative analysis on the sentencing disparity in online romance scam cases in United States: A focal concern theory perspective. *Crime & Delinquency*, 71(1), 59–87. https://doi.org/10.1177/00111287241266561

Wang, F. (2026). A scoping review of online romance scams: Conceptual construction and comparative analysis. *International Review of Victimology*. Advance online publication. https://doi.org/10.1177/02697580251414141

Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. Computers in Human Behavior, 154, Article 108133. https://doi.org/10.1016/j.chb.2023.108133

Whitty, M. T. (2013). The scammers persuasive technique model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, 53(4), 665–684. https://doi.org/10.1093/bjc/azt00

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105-109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. Cyberpsychology, *Behavior, and Social Networking*, 15(3), 181-183. https://doi.org/10.1089/cyber.2011.0352

Whitty, M. T., & Buchanan, T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – Both financial/non-financial. *Criminology & Criminal Justice*, 16(2), 176–194. https://doi.org/10.1177/1748895815603773

Yosiandra, S. Y., & Sakariah, D. S. (2024). Unveiling the romance scam scheme: Psychological manipulation and its impact on victims. *Humanika*, 31(2), 185–199. https://doi.org/10.14710/humanika.v31i2.67604

Anexos

Anexo A) Parecer da Comissão de Ética

Comissão de Ética
Faculdade de Direito
Universidade do Porto

Porto, 14 de março de 2025

Parecer n.º 86/2025

1. Solicitou **Ângelo Carvalho Ribeiro** a emissão de Parecer relativo ao projeto de investigação intitulado «**Burla e Romance Scam: Perceção Pública Sobre a Natureza, Gravidade da Ilicitude e Comportamentos de Evitamento**», realizado sob a orientação de: Prof. Doutor Pedro Sousa.

2. Enquadrando-se o objeto da investigação na área científica de **Criminologia**, foi distribuída à Prof.ª Doutora Inês Guedes, Vogal da Comissão de Ética, a responsabilidade de elaborar um Projeto de Parecer.

3. No confronto com os elementos com que o pedido foi instruído, foi apresentado o seguinte Projeto de Parecer:

> «Relativamente ao pedido P86/2025, de Ângelo Carvalho Ribeiro (Burla e Romance Scam: Perceção Pública Sobre a Natureza, Gravidade da Ilicitude e Comportamentos de Evitamento), o projeto pretende pretende analisar a perceção pública sobre a natureza e gravidade tanto das burlas como dos esquemas de romance. Para tal, visa obter uma amostra de adultos para responderem a um questionário online, através da plataforma EU Survey. O estudo não visa a recolha de dados sensíveis. Pela descrição do documento pode concluir-se que os princípios éticos parecem estar assegurados, nomeadamente: i) os participantes irão ter acesso ao consentimento informado e só irão preencher o questionário caso concordem com os termos; ii) os dados serão anonimizados e os participantes não colocarão o seu nome em nenhum local do questionário; iii) haverá a garantia da confidencialidade dos dados; iv) os dados obtidos serão armazenados num local seguro, acessível com password, apenas à qual apenas os investigadores terão acesso. Neste sentido, não se identifica nenhum obstáculo de natureza ética à realização do projeto.»

4. A apreciação das implicações éticas do projeto de investigação foi realizada pelo plenário da Comissão de Ética, tendo sido votada a emissão de Parecer favorável, por adesão aos fundamentos avançados.

Comissão de Ética
Faculdade de Direito
Universidade do Porto

Diante dos fundamentos expostos, **a Comissão de Ética da Faculdade de Direito da Universidade dá, por unanimidade, parecer favorável** à realização do projeto de investigação acima identificado (n.º 1), por, a partir dos elementos instruídos, concluir pela não desconformidade com os padrões éticos e deontológicos aplicáveis.



Prof. Doutor Manuel Carneiro da Frada
(Presidente da Comissão de Ética)

Aprovaram o Parecer, além do Presidente, os seguintes Vogais: Prof. Doutor António Manuel de Almeida Costa, Prof. Doutora Inês Guedes, Prof. Doutor Tiago Azevedo Ramalho e Prof.ª Doutora Ana Margarida Amorim dos Santos.

Anexo B) Parecer da Unidade de Proteção de Dados

U.PORTO	Unidade de Proteção de Dados	DATA: 30/07/2025

PARECER A-133/2025

Nome	Ângelo Carvalho Ribeiro
Nº. Mecanográfico	202303332
Entidade Constitutiva	FDUP
Título	Tese de Mestrado : Burla e Romance Scam - Perceção Pública Sobre a Natureza, Gravidade da Ilicitude e Comportamentos de Evitamento

Sumário do Pedido

Foi solicitado à Unidade de Proteção de Dados da Universidade do Porto que se pronunciasse sobre o estudo a ser conduzido pelo Requerente no âmbito da sua dissertação de Mestrado em Criminologia da Faculdade de Direito da Universidade do Porto (FDUP) intitulada «*Burla e Romance Scam: Perceção Pública Sobre a Natureza, Gravidade da Ilicitude e Comportamentos de Evitamento*».

De acordo com a informação recolhida, o objeto da investigação consiste na análise da perceção pública quanto à natureza e gravidade das burlas, com especial enfoque nos denominados *romance scams*, bem como na identificação de comportamentos de evitamento e na aferição da aceitação social dessas práticas ilícitas. O estudo pretende avaliar, através de um instrumento de inquérito, o grau de compreensão dos participantes relativamente à ilicitude das condutas em análise e às suas repercussões sociais, económicas e psicológicas.

Conclusões

Da análise efetuada pela UPD, o estudo dirige-se a indivíduos com idade igual ou superior a 18 anos e recorre a um inquérito por questionário anónimo, disponibilizado na plataforma institucional LimeSurvey, mantida e alojada nos servidores da Universidade do Porto. Apurou-se que a participação é voluntária, confidencial e anónima, sendo assegurada a possibilidade de desistência em qualquer fase do preenchimento.

A recolha dos dados será efetuada mediante:

- Divulgação através do Serviço de Comunicação e Imagem (SCI);
- Divulgação direta pelo Requerente, junto da sua rede de contactos pessoais.

Conforme a definição constante do artigo 4.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados (RGPD) – Regulamento (UE) 2016/679 –, dados pessoais são "informações relativas a uma pessoa singular identificada ou identificável". Ora, sendo o inquérito concebido de forma estritamente anónima, sem recolha de quaisquer elementos identificativos (nome, email, IP, etc.), inexiste tratamento de dados pessoais na aceção legal.

Neste contexto, conforme doutrina pacífica (v. Maria da Glória Garcia, *Direito da Proteção de Dados Pessoais*, Almedina, 2020, p. 47), "a anonimização completa e irreversível de dados afasta a aplicação do RGPD, pois deixa de haver qualquer risco de reidentificação dos titulares dos dados".

Além disso, de acordo com pareceres emitidos por autoridades nacionais e europeias de proteção de dados (v. Comité Europeu para a Proteção de Dados, *Guidelines 05/2020 on consent under Regulation 2016/679*), os dados anonimizados de forma eficaz, que não permitam a reidentificação dos participantes por meios razoáveis, não se encontram sujeitos à disciplina do RGPD.

A plataforma LimeSurvey, utilizada na presente investigação, é mantida internamente pela Universidade do Porto, estando os dados recolhidos alojados nos seus próprios servidores, o que assegura a conformidade com as normas de segurança, integridade e confidencialidade previstas no artigo 32.º do RGPD — ainda que o mesmo, como vimos, não se aplique ao caso concreto.

O projeto de investigação foi previamente aprovado pela Comissão de Ética da Faculdade de Direito da

Universidade do Porto, o que garante a conformidade da metodologia e dos instrumentos de recolha com os padrões éticos exigíveis na investigação científica, nos termos do disposto no *Código de Ética e Boas Práticas Científicas* da U.Porto.

Com base no exposto, e tendo em consideração os princípios jurídicos aplicáveis à investigação científica e à proteção de dados pessoais, conclui-se que o inquérito em causa, por se tratar de um instrumento anónimo que não recolhe nem permite a identificação dos participantes, não configura tratamento de dados pessoais, não sendo, por conseguinte, aplicável o disposto no Regulamento (UE) 2016/679 (RGPD). Adicionalmente, verifica-se que não ocorre qualquer transferência de dados para entidades terceiras, sendo todo o processamento efetuado através de infraestrutura tecnológica interna da Universidade do Porto, assegurando-se, assim, a segurança e a confidencialidade da informação recolhida.

A metodologia adotada cumpre os requisitos legais e éticos inerentes à proteção dos participantes, nomeadamente no que respeita à voluntariedade, anonimato, confidencialidade e integridade dos dados.

Por fim, constata-se que a informação prestada aos participantes no início do inquérito é clara, completa e juridicamente adequada, respeitando os princípios da transparência e da autodeterminação informacional, pelo que o estudo delineado pelo Requerente se encontra aprovado em matéria de proteção de dados.

A Encarregada da Proteção de Dados
da Universidade do Porto

Raquel Mendes da Rocha

Digitally signed by Raquel Mendes da Rocha
Date: 2025.07.30 16:06:50 +01'00'

Dra. Raquel Mendes da Rocha

Anexo C) Inquérito por Questionário

Burla e Romance Scam - Perceção Pública Sobre a Natureza, Gravidade da Ilicitude e Comportamentos de Evitamento

O questionário que se segue é proveniente de um estudo académico de investigação científica conduzido por Ângelo Carvalho Ribeiro, estudante do 2º ciclo de estudos em Criminologia da Faculdade de Direito da Universidade do Porto, sob orientação do Prof. Doutor Pedro Sousa.

Este questionário é destinado a indivíduos com idade igual ou superior a 18 anos e tem como objetivos compreender a perceção pública sobre as burlas online dando um especial relevo aos *"romance scam"*, bem como avaliar a perceção da sua gravidade e os comportamentos de evitamento adotados pelos indivíduos.

O questionário foi implementado numa plataforma interna disponibilizada pela U.Porto, a LimeSurvey, sendo esta entidade responsável pela recolha e pelo armazenamento seguro de dados. Durante o inquérito, não será solicitada qualquer informação que permita a sua identificação, garantindo-se que as suas respostas serrão tratadas de forma estritamente confidencial. Os dados recolhidos destinam-se exclusivamente a tratamento coletivo e estatístico, sendo utilizados apenas no âmbito deste estudo e para fins de investigação académica

.

A participação no estudo é individual, confidencial e voluntária. Os dados obtidos serão de uso unicamente académico, sendo totalmente assegurado o anonimato dos participantes. A todo e qualquer momento o participante por optar por desistir do preenchimento do questionário.

O presente estudo foi aprovado pela Comissão de Ética da Faculdade de Direito da Universidade do Porto.

No caso de surgir qualquer duvida que deseje ser esclarecida, pode contactar o investigador através do seguinte email: up202303332@up.pt

De notar que carregando em "Seguinte" encontra-se a concordar com a sua participação no estudo através da resposta do questionário

Existem 47 perguntas neste questionário.

Dados demográficos

Qual é a sua idade? *

Por favor, escreva aqui a sua resposta:

Género: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Masculino
- ◯ Feminino
- ◯ Outro
- ◯ Prefiro não dizer

Grau de escolaridade: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sem escolaridade
- ◯ Ensino básico
- ◯ Ensino secundário
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento

Situação Profissional: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Estudante
- ◯ Desempregado/a
- ◯ Trabalhador/a por conta de outrem
- ◯ Trabalhador/a por conta própria
- ◯ Aposentado/a

Estado civil: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Solteiro/a
- ◯ Casado/a ou união de facto
- ◯ Divorciado/a
- ◯ Viúvo/a

Distrito de residência: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Aveiro
- ◯ Beja
- ◯ Braga
- ◯ Bragança
- ◯ Castelo Branco
- ◯ Coimbra
- ◯ Évora
- ◯ Faro
- ◯ Guarda
- ◯ Leiria
- ◯ Lisboa
- ◯ Portalegre
- ◯ Porto
- ◯ Região Autónoma dos Açores
- ◯ Região Autónoma da Madeira
- ◯ Santarém
- ◯ Setúbal
- ◯ Viana do Castelo
- ◯ Vila Real
- ◯ Viseu
- ◯ Outro

Caracterização da localidade em que reside: *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Meio rural ou pouco urbanizado
- ◯ Meio urbanizado ou muito urbanizado

Uso da Internet e Redes Sociais

Com que frequência utiliza a Internet? *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Várias vezes por dia
- ◯ Duas a três vezes por dia
- ◯ Uma vez por dia
- ◯ Algumas vezes por semana
- ◯ Uma vez por semana
- ◯ Algumas vezes por mês
- ◯ Nunca

Alguma vez interagiu online (na internet) com pessoas que não conhecia? *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não

Que dispositivo normalmente usa para aceder à Internet (Pode selecionar mais do que uma opção)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- [ ] Telemóvel
- [ ] Tablet
- [ ] Computador
- [ ] Não responde por não utilizar internet
- [ ] Outro: _____

Utiliza ou já utilizou redes sociais ou aplicações de encontros? (Pode selecionar mais do que uma opção)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- [ ] Facebook
- [ ] Instagram
- [ ] Twitter/X
- [ ] TikTok
- [ ] Tinder
- [ ] Bumble
- [ ] Não utilizo nem nunca utilizei redes sociais ou aplicações de encontros
- [ ] Outro: _____

Qual é o tempo médio despendido diariamente nestas aplicações?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Menos de 30 minutos
- ◯ Entre 30 minutos e 1 hora
- ◯ Entre 1 e 2 horas
- ◯ Entre 2 e 3 horas
- ◯ Mais de 3 horas
- ◯ Não utilizo nenhuma aplicação

Se já utilizou algumas redes sociais ou aplicações de encontros, chegou a encontrar-se presencialmente com pessoas que apenas tinha contactado online (na internet)?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não

Burla e romance scam

Já ouviu falar de algum dos seguintes tipos de burlas (pode escolher mais que uma opção)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- [ ] Phishing
- [ ] Vishing
- [ ] Burlas do WhatsAap ou chamadas automaticas
- [ ] Burlas em lojas online
- [ ] Burlas bancárias ou de criptomoedas
- [ ] Nenhuma
- [ ] Outro:

Como classifica o seu conhecimento sobre este tipo de fraude?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Nulo
- ◯ Muito baixo
- ◯ Baixo
- ◯ Moderado
- ◯ Alto
- ◯ Muito alto

Já ouviu falar Romance Scam, também denominado de burlas românticas?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não

Se sim, o que é?

Por favor, escreva aqui a sua resposta:

Já foi ou tem conhecimento de alguém que já foi vítima de burla romântica? *

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não

Considera que estas burlas são um problema grave para a sociedade?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não

Perceção da Gravidade da Ilicitude

Acredita que as vítimas dessas burlas são responsáveis pelas suas perdas financeiras?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não
◯ Depende da situação

Para além de consequências financeiras que outro impactos acha que estes atos tem nas vitimas?

Por favor, escreva aqui a sua resposta:

Sendo os romance scam um aproveitamento da vulnerabilidade da vítima, onde o delinquente manipula e ilude a vítima afetiva e emocionalmente com o objetivo de extrair riqueza ou favorecimentos pessoais, quão grave considera ser este tipo de burlas? (Sendo 1 nada grave e 5 muito grave)

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Na sua opinião, que sanções legais deveriam ser impostas a quem pratica este tipo de crimes? (Pode selecionar mais que uma opção)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- ☐ Pena de prisão
- ☐ Multa
- ☐ Proibição de acesso à internet
- ☐ Outro: _____

Comportamentos de Evitamento e de proteção

Com que frequência verifica a identidade de pessoas desconhecidas antes de interagir online, utilizando a seguinte escala de 5 pontos, em que 1 significa **nunca** e 5 significa **sempre**?

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Quando recebe mensagens de desconhecidos em redes sociais ou plataformas, qual é a sua reação mais comum?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Respondo normalmente
- ◯ Antes de responder, verifico o perfil
- ◯ Ignoro a mensagem
- ◯ Bloqueio ou denuncio o utilizador
- ◯ Outro [ ]

Alguma vez desconfiou que estivesse a ser alvo de uma burla online?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não

Caso descobrisse que estava a ser enganado por um burlão online, o que faria? (pode escolher mais do que uma alternativa)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- [ ] Denunciaria às autoridades
- [ ] Deixaria de responder
- [ ] Tentaria recuperar o dinheiro e a propriedade de eventuais bens subtraídos
- [ ] Outro: _____

Que práticas adota para se proteger de burlas online? (pode selecionar mais que uma opção)

*

Assinale todas as que se aplicam
Please choose **all** that apply:

- [ ] Não partilho informações pessoais com desconhecidos
- [ ] Verifico perfis suspeitos antes de qualquer interação
- [ ] Uso autentificação de dois fatores
- [ ] Evito sites de encontros ou sites desconhecidos
- [ ] Nenhum
- [ ] Outro: _____

Alguma vez alterou as suas definições de privacidade para evitar ser contactado/a por desconhecidos?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não
- ◯ Prefiro não dizer

Com que frequência **evita** partilhar fotografias ou informações pessoais online por receio de serem usadas contra si, utilizando a escala de 5 pontos, onde 1 ponto corresponde **a não evita - está sempre aberto a novas ligações** e 5 pontos a **não estabelece nenhuma relação online**?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Com que frequência rejeita pedidos de amizade ou mensagens de desconhecidos por receio de poder ser vítima de burla, utilizando a escala de 5 pontos, em que 1 ponto refere-se a **nunca rejeita** e 5 pontos a **rejeita sempre**?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Considera que adota mais comportamentos de evitamento do que as outras pessoas do seu círculo social?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não
- ◯ Não sei

Imagine que desconfia que alguém pode estar a enganá-lo/a, como iria reagir?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Confrontaria a pessoa diretamente
- ◯ Bloquearia ou denunciaria a conta
- ◯ Pediria conselhos a amigos ou familiares
- ◯ Participar (denunciar) às autoridades
- ◯ Nada, pois não teria certeza se era ou não uma burla
- ◯ Outro [ ]

Sentimento de insegurança

Em que medida considera ser vulnerável aos diferentes tipos de burla online como é o caso do romance scam, utilizando a escala de 1 a 5 pontos onde 1 corresponde a **nada vulnerável** e 5 a **totalmente vulnerável**?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Com uma escala de 1 a 5 pontos, onde 1 representa **nenhum risco** e 5 representa **risco máximo**, como considera ser o seu nível de risco de ser vítima de uma fraude online?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Acredita que o medo de ser vítima de uma burla limita a sua liberdade, no que diz respeito a conhecer novas pessoas?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não
- ◯ Não sabe

Acredita que qualquer pessoa pode ser vítima de uma burla, independente do seu conhecimento das novas tecnologias?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não
- ◯ Não sabe
- ◯ Outro

Sente-se inseguro/a ao interagir com desconhecidos online, utilizando uma escala de 5 pontos, em que a 1 corresponde a **nada inseguro** e 5 corresponde **muito inseguro**?

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Com que frequência **evita** estabelecer novas relações online por receio de ser engando/a, utilizando a escala de 1 ponto (**não evita novas relações**) a 5 pontos (**evita totalmente novas relações**)?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Em que medida se preocupa com a possibilidade de partilhar dados pessoais com alguém que pode não ser quem afirma ser, utilizando uma escala de 5 pontos em que 1 corresponde a **nada preocupado** e 5 **muitíssimo preocupado**?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Já ouviu relatos de vítimas de burlas online que o/a fizeram sentir mais inseguro/a?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não
◯ Prefiro não responder

Se sim, após ter conhecimento de casos de burla online, mudou algum comportamento para evitar ser vítima?

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não
◯ Prefiro não responder

Considera que as burlas online estão a tornar-se cada vez mais sofisticadas e de difícil deteção?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

◯ Sim
◯ Não
◯ Não sabe

Caso fosse vítima de um romance scam, quanto acharia que seria o nível de impacto emocional deste tipo de burla, sendo 1 correspondente a **nenhum impacto** e 5 **muito impacto**?

*

Please choose **only one** of the following:

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

Considera que os órgãos de comunicação social contribuem para o aumento de sentimento de insegurança em relação às burlas?

*

Escolha uma das seguintes respostas
Please choose **only one** of the following:

- ◯ Sim
- ◯ Não
- ◯ Não sei

Questões de opinião pessoal

No seu ponto de vista o que poderia ser feito para reduzir o número de vítimas de romance scam/burlas românticas online? (Relembro que esta é uma questão de resposta aberta, neste sentido solicito que tenha em atenção o facto de não incluir informações e/ou dados que permitam a sua identificação)

Por favor, escreva aqui a sua resposta:

Gostaria de partilhar alguma experiência pessoal ou opinião adicional sobre o tema? (Relembro que esta é uma questão de resposta aberta, neste sentido solicito que tenha em atenção o facto de não incluir informações e/ou dados que permitam a sua identificação)

Por favor, escreva aqui a sua resposta:

Obrigado pela sua participação!
22/07/2026 – 19:04
Submeta o seu inquérito.
Obrigado por ter concluído este inquérito.

FACULDADE DE DIREITO

