U.PORTO

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

Vitimação e Sentimento de Insegurança de Furto de Identidade Online: um estudo empírico antes e depois do COVID-19

Joana Filipa da Silva Martins

M

2022

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para obtenção do grau de Mestre em Criminologia sob orientação da Professora Doutora Inês Sousa Guedes e Professora Doutora Carla Cardoso

RESUMO

O desenvolvimento da *Internet* levou a que não apenas novos crimes surgissem, mas também, que outros se estendessem para o mundo *online*, como é o caso do furto de identidade *online*. Para além disso, a pandemia de Covid-19 aumentou a dependência do ciberespaço para a realização de diversas atividades diárias. O deslocamento destas atividades para o ciberespaço tem feito com que os infratores procurem oportunidades criminais com consequências nefastas para as suas vítimas. Por estas razões, o cibercrime em geral e o furto de identidade *online* em particular merecem, indubitavelmente, atenção científica. Nesta senda, a presente investigação pretende, por um lado, comparar os níveis de vitimação e de medo de furto de identidade *online*, antes e depois da pandemia de Covid-19. Por outro, com recurso à Teoria das Atividades de Rotina (TAR), pretende-se perceber quais os fatores relacionados com a vitimação e com o medo de furto de identidade. Por fim, procura-se perceber qual é a influência de variáveis sociodemográficas (e.g., género, idade, estatuto socioeconómico e educação), do medo geral do crime e do nível de conhecimento informático, nas referidas variáveis dependentes. Os dados foram recolhidos através de um questionário *online*, sendo a amostra constituída por 730 estudantes universitários e staff (feminino= 71.4%, média de idades= 27.13). Os resultados demonstram que a vitimação por furto de identidade *online* nos últimos 12 meses aumentou relativamente ao período prévio à pandemia, registando-se 8.5% de vítimas na amostra pós-Covid (amostra pré-Covid= 5.8%). Quanto à vitimação, as variáveis sociodemográficas não se relacionam com o furto de identidade. O mesmo sucede com a exposição *online*. Relativamente ao alvo adequado, a abertura de links duvidosos está positivamente relacionada a vitimação. Por fim, o guardião eficaz e o conhecimento informático não se relacionam com a vitimação. Em relação ao medo de furto de identidade *online*, as mulheres, as pessoas que adotam mais rotinas de lazer, quem adota mais comportamentos de evitamento e os que procuram mais informação sobre o cibercrime, reportam mais medo de furto de identidade. Contrariamente, os que comunicam mais com estranhos e fornecem informações pessoais *online* reportam menos medo. Também se pode concluir que, aqueles que relatam mais medo do crime, reportam mais medo de furto de identidade e a vitimação prévia por furto de identidade é preditora da perceção do risco de furto de identidade, mas não do medo de furto de identidade *online*. Estes resultados serão discutidos posteriormente e realçaremos a importância da prevenção.

Palavras-chave: cibercrime, furto de identidade *online*, medo de furto de identidade *online*, Covid-19 e Teoria das Atividades de Rotina

ABSTRACT

The development of Internet led, not only to the emergence of new crimes, but also to the practice of old crimes on the web, being an example of that *online identity theft*. Moreover, due to the Covid-19 global pandemic, individuals became even more dependent of the cyberspace to carry out their daily activities. The displacement to the Internet of such activities has led offenders to look for criminal opportunities, with hazardous consequences to the victims, in the cyberspace. Thus, online crime, and especially online identity theft, deserve, without a doubt, scientific attention. For that reason, this research intends, on one hand, to compare the levels of victimization and fear of online identity theft before and after the Covid-19 pandemic, and, on the other hand, by resorting to the routine activities' theory, this study will also try to understand which factors are related to victimization by online identity theft and fear of said offense. Lastly, we try to uncover the influence of sociodemographic variables (e.g., gender, age, social-economic status, and educational levels), general fear of crime and computer skills, on the mentioned dependent variable. The data was collected from a self-reported online survey administered to a sample of 730 university students and staff (female= 71.4%, M age= 27.13). The results show that victimization of online identity theft – in the last 12 months – increased when compared to the pre-pandemic sample, with 8.5% of the individuals reporting victimization (pre-Covid sample=5.8%). We concluded that the sociodemographic variables and the online exposure are not related to online identity theft e. One item of the online target suitability – open dubious links – was positively related to online identity theft. However, capable guardianship and computer skills were not related to victimization. Regarding the fear of online identity theft, women, those who adopted more leisure routines and avoiding behaviours and those who looked up for more information about cybercrime, reported more fear of identity theft. In contrast, individuals that communicate with strangers and provide personal information online, reported less fear of online identity theft. We could also conclude that those who reported more fear of crime also reported more fear of identity theft, and previous victimization by identity theft is a predictor of risk perception, but not of fear of online identity theft. These results will be further discussed, and the importance of prevention will also be highlighted.

Keywords: cybercrime, online identity theft, fear of online identity theft, Covid-19, Routine Activity Theory

Agradecimentos

Primeiramente, gostaria de expressar o meu agradecimento à minha Orientadora, Professora Doutora Inês Sousa Guedes. É um verdadeiro exemplo e, acima de tudo, uma inspiração. Agradeço-lhe por todos os ensinamentos transmitidos ao longo destes anos, pela dedicação a esta investigação e por toda a confiança que depositou em mim. Agradeço-lhe, também, pela exigência e pelo desafio, foram fatores determinantes para a realização deste trabalho. Por fim, obrigada pelo esforço que fez, mesmo perante todas as adversidades, para nos acompanhar até ao último minuto. A si, o meu sincero e sentido agradecimento. Só posso desejar que os nossos caminhos se continuem a cruzar.

Em segundo lugar, agradeço à minha Coorientadora, Professora Doutora Carla Cardoso. Para além de toda a sabedoria científica e metodológica transmitida, quero agradece-lhe por todas as sugestões, críticas construtivas e por toda a motivação. Agradeço-lhe, também, pela disponibilidade que sempre teve perante as minhas dúvidas e incertezas.

Paralelamente, agradeço a todos os Docentes da Escola de Criminologia que, ao longo destes anos, contribuíram para a minha formação enquanto Criminóloga e, não menos importante, que me mostraram o quão magnifica é a Criminologia.

Agradeço, agora, a um conjunto de pessoas sem as quais a realização desta dissertação não teria sido possível. Agradeço profundamente aos meus pais, ao meu irmão e ao Miguel, por serem o meu porto seguro, por toda a paciência e pelo alento nos momentos de desânimo. Obrigada, também, aos meus amigos, aos de sempre e aos que esta Casa me deu que tornaram o caminho mais bonito e a despedida mais difícil. Agradeço, em particular, às que comigo passaram horas a fio no CJS, por acalmarem os meus anseios e por todas as gargalhadas que demos juntas. Por fim, aos meus meninos, um agradecimento especial por semana após semana, serem luz e alegria.

Findo com um especial agradecimento à Casa amarela da Rua dos Bragas: "*saudades e memórias nunca me vão faltar*."

Como não poderia deixar de ser, dedico este trabalho à minha Avó.

Lista de abreviaturas

AF: Action Fraud

CERP: Equipa de Resposta a Incidentes de Segurança Informática Nacional

CNCS: Centro Nacional de Cibersegurança

CP: Código Penal

IOCTA: Internet Organized Crime Threat Assessment

LC: Lei do Cibercrime

RASI: Relatório Anual de Segurança Interna

TAR: Teoria das Atividades de Rotina

TIC: Tecnologias da Informação e Comunicação

UNC3T: Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

ÍNDICE

Índice de tabelas

Introdução

O exponencial crescimento da *Internet* permitiu o desenvolvimento da Sociedade Digital e desempenha um papel fulcral ao nível governamental, militar, económico e, ainda, ao nível das telecomunicações, transportes, educação e saúde. Por estar presente em todos os ramos da vida quotidiana, e fazendo parte dela, tem permitido a multiplicação de "*condutas lesivas e ilícitas, praticáveis e praticadas na Internet, ou por intermédio desta*" (Dias, 2012, p. 65) que foram agravadas pela chegada da pandemia de Covid-19 (Naidoo, 2020). Por este motivo, há investigadores que entendem que, atualmente, se vive na "*sociedade virtual do risco*" (Capeller, 2001, p. 231) e, como tal, afigura-se necessário que a Criminologia investigue os fenómenos criminais que ocorrem no ciberespaço de forma a ser capaz de responder eficazmente aos mesmos. Assim sendo, têm-se desenvolvido estudos sobre a vitimação *online* e, por norma, estes têm como base teórica de explicação a TAR (e.g., Reyns, 2013) e/ou a Teoria Geral do Crime (e.g., Ngo & Paternoster, 2011). Por sua vez, embora no domínio *offline* o Sentimento de Insegurança seja um objeto de estudo já largamente aprofundado, no âmbito do ciberespaço, verifica-se que são escassas as investigações até então realizadas (e.g., Roberts *et al.*, 2013).

Quanto à investigação da cibercriminalidade, por um lado, há estudos que utilizam uma medida agregada de vários tipos de cibercrime (e.g., Virtanen, 2017) e, por outro, há estudos que se focam somente num cibercrime (e.g., Reyns, 2013). Como é expectável, as medidas agregadas, quer seja ao nível do medo, quer seja ao nível da vitimação, perdem algum rigor porque não permitem a associação de fatores individualizados à tipologia específica de crime. Por esse motivo, esta investigação foca-se no estudo do furto de identidade *online*, explorando um conjunto de fatores individuais (e.g., género) e contextuais (e.g., variáveis derivadas da TAR) na relação com as duas variáveis dependentes, a vitimação e o medo, estabelecendo uma comparação entre o momento pré e pós-pandemia de Covid-19. Desta forma, pretende-se contribuir para o crescente corpo de investigações científicas sobre o furto de identidade *online* e, ao mesmo tempo, colmatar a falta de estudos sobre este fenómeno em Portugal.

Para o efeito, a presente dissertação encontra-se dividida em quatro capítulos. No capítulo I, do enquadramento teórico, encontra-se a delimitação do conceito de cibercrime e de furto de identidade o*nline*. Ainda neste capítulo é abordada a TAR, a sua aplicabilidade ao ciberespaço e o sentimento de insegurança e seus componentes. Em relação ao estudo empírico, que se encontra no capítulo II, serão abordados os objetivos e hipóteses da presente investigação, assim como a caracterização do estudo e constituição da amostra. Ainda neste capítulo, é descrito o

instrumento utilizado e os procedimentos de análise estatística aplicados. Já no capítulo III são apresentados os resultados obtidos tanto ao nível da vitimação como do sentimento de insegurança. Por fim, no capítulo IV, é apresentada a discussão dos resultados, as limitações da investigação e é feita uma abordagem à importância da prevenção deste fenómeno criminal.

Capítulo I: Enquadramento Teórico

1. Cibercrime: definição e tipologias

Apesar da evolução tecnológica e da *Internet* apresentarem múltiplas vantagens, também é verdade que, associado a esta evolução, surgiram novas ameaças, perigos e oportunidades criminais (Antunes & Rodrigues, 2018), tendo-se criado um verdadeiro campo criminal virtual, no qual qualquer utilizador pode ser uma potencial vítima (Dias, 2012). Assim sendo, é possível afirmar que, atualmente, se vive em dois mundos paralelos, sendo estes, o mundo físico e o mundo cibernético (Choi *et al.,* 2019). Neste mundo cibernético, a *Internet* afigura-se como um veículo rápido, barato, global, pautado pelo anonimato, contudo, "*as fantásticas e inegáveis vantagens da Internet*" (Dias, 2012, p. 84) acarretam consequências negativas e as ameaças de prática do que muitos autores denominam como *cibercrime* (Guedes *et al*., 2021) que, hoje, já não se trata de um facto negável (Correia, 2021).

A grande problemática relacionada com o cibercrime diz respeito à sua conceptualização pois, apesar de os autores concordarem que este é um dos grandes desafios criminais da atualidade, não há uma definição que seja universalmente aceite por todos os investigadores e académicos (Yar, 2006). Esta dificuldade deve-se ao rápido desenvolvimento tecnológico, às divergências nas legislações, à existência de múltiplos atores, públicos e privados, envolvidos na regulação e controlo do cibercrime (William & Wall, 2013) e à sobreposição de entidades de diferentes setores, nomeadamente das disposições legais, das agências de aplicação da lei, das empresas de segurança cibernética e dos académicos (Tsakalidis *et al.,* 2019). Apesar de existirem variadas expressões para designar a prática de ofensas cibernéticas (e.g., crime informático, crime digital e crime relacionado com computadores), nesta investigação será adotado o termo cibercrime, abarcando o conjunto de ofensas que partilham uma característica, que é o facto de serem cometidas através de um computador e de tecnologia, como a *Internet*.

Primeiramente importará perceber o que é, afinal, o ciberespaço. Para Antunes e Rodrigues (2018) o ciberespaço é um espaço virtual criado através das comunicações e dos meios tecnológicos disponíveis, sem haver necessidade de intervenção humana. Neste contexto das Tecnologias da Informação e Comunicação (TIC), define-se o ciberespaço como a

infraestrutura que potencia a comunicação global entre todos utilizadores e equipamentos digitais (Antunes & Rodrigues, 2018). Inevitavelmente, aqui se incluí a *Internet*, assim como, os seus serviços e protocolos, mas também, outras infraestruturas de comunicação, como por exemplo, as redes de telefones e telemóveis. Dada a diversidade de meios tecnológicos disponíveis no ciberespaço, são múltiplos os crimes que podem ser perpetrados neste meio, o qual, os estudiosos designam de cibercrime (*idem*). Sendo o ciberespaço marcado por características como a transnacionalidade, atemporalidade e deslocalização e, sobretudo, pelo anonimato (Dias, 2012), torna-se complexo o conhecimento e a medição rigorosa deste fenómeno que é a cibercriminalidade. Assim, a função dos criminólogos passa por definir este fenómeno, entender que comportamentos são abrangidos pelo conceito de cibercrime, estudar de forma aprofundada os fatores que levam ao cometimento de crimes *online* e à vitimação para que possam ser desenvolvidas estratégias de prevenção adequadas (Mikkola *et al*., 2021).

Por este motivo, alguns autores continuam a dedicar-se à definição deste conceito. Segundo Wall (2007), é possível identificar diferentes tipos de cibercrimes de acordo com a mediação tecnológica. Primeiramente, podem identificar-se os crimes tradicionais que utilizam os computadores como mera assistência, como acontece, por exemplo, com as fraudes bancárias e com o furto de identidade *online*. Estas ofensas têm um elevado impacto, uma vez que, mesmo que a *Internet* seja removida continuarão a persistir, dado que os ofensores vão apenas mudar a forma como os cometem. Por outro lado, identificam-se os crimes convencionais para os quais o aparecimento da *Internet* criou oportunidades globais, isto é, permitiu que o crime praticado tenha um impacto mais vasto e até mesmo global. Neste caso, o computador não é o instrumento principal da atividade, mas o meio de realização de prova assume a forma digital (e.g., tráfico de droga; Grabosky, 2004). Por último, identificam-se os verdadeiros cibercrimes, ou seja, aqueles que são fruto da própria *Internet* e não existiriam sem ela (e.g., *hacking*[1]). Para além disto, Wall (2007) acrescenta que se podem definir os cibercrimes de acordo com as ofensas cometidas e, neste sentido, podem distinguir-se três tipos, nomeadamente, i) crimes contra a integridade dos computadores, como o *hacking* e os vírus; ii) crimes assistidos por computadores, como as fraudes; e iii) crimes relacionados com o conteúdo dos computadores, como a distribuição de pornografia. Outra distinção, muito acolhida na literatura científica, é a de Furnell (2002) e que tem como critério principal o papel desempenhado pela tecnologia. O autor distingue as ofensas focadas no computador e as ofensas assistidas pelo computador. As

[1] O *hacking* refere-se à realização de atividades ilícitas de invasão e acesso ilegítimo a sistemas informáticos de instituições/ empresas/ particulares, com objetivo de obter informações importantes (Antunes & Rodrigues, 2018).

primeiras englobam os crimes que têm como alvo a própria infraestrutura eletrónica. Já as segundas, as ofensas assistidas pelo computador abarcam os crimes que já existiam antes da *Internet*, mas que agora encontram uma nova via para serem cometidos.

A nível nacional, Venâncio (2011, p. 17) apresenta uma definição de cibercrime segundo uma perspetiva jurídica, categorizando os cibercrimes em sentido amplo e sentido estrito:

> "*em sentido amplo* (…) *a criminalidade informática englobará toda a panóplia de atividade cibercriminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios. Em sentido estrito, entendemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integradora do tipo legal ou mesmo como o seu objeto de proteção*."

Para além da definição do conceito de cibercrime, os investigadores têm-se debruçado sobre a descrição de tipologias de atos ilegais que decorrem no ciberespaço de forma a simplificar a sua compreensão. Wall (2001), cria uma das tipologias mais debatidas e apresentadas na literatura científica. Segundo o autor, o cibercrime pode ser dividido em quatro diferentes áreas, dependendo do alvo ou objeto da ofensa.

Com efeito, o *cybertrespass* engloba os comportamentos em que os ofensores ultrapassam as fronteiras do sistema informático de outrem, sem o seu consentimento. O ofensor pode fazê-lo de diferentes formas, nomeadamente, através de vírus informáticos e *hacking*, por exemplo. Já nas *cyberdeceptions* and *thefts* incluem-se as burlas e os furtos *online*, nomeadamente atividades cujos danos aquisitivos podem ter lugar no ciberespaço. Nesta área abrangem-se comportamentos que, apesar de existirem fora do ciberespaço são, também, praticados em contexto digital. Alguns exemplos, enumerados pelo autor, são a fraude de cartão de crédito e o acesso à conta bancária *online*. Ainda dentro destas inclui-se a *cyberpiracy* que consiste na apropriação da propriedade intelectual que ocorre no ciberespaço. Esta categoria pode ser dividida em contrafação de produtos, onde a *Internet* é utilizada como rede de distribuição e a violação de propriedade intelectual como imagens, música ou textos. De seguida, na classificação do autor, surge a *cyberpornography* que se refere às publicações ou a negócios que estejam relacionados com conteúdos sexuais no ciberespaço. Por fim, encontra-se a *cyberviolence*, que engloba os comportamentos que produzem um impacto negativo nos sujeitos, grupos sociais ou políticos e, aqui, os danos referidos são essencialmente os de natureza emocional e psicológica que, na maior parte das vezes, são irreparáveis. Dentro desta

tipologia corre-se o risco de haver incitamento a comportamentos físicos violentos contra indivíduos, nomeadamente através do *cyberstalking* e do *cyberhate* (Wall, 2001).

1.1. Enquadramento legal

Embora exista uma tentativa de harmonização legal em relação ao cibercrime, sobretudo ao nível europeu, ainda não existe um acordo em função das especificidades de cada sistema jurídico (Yar, 2006). Para além disso, tanto as polícias como os tribunais são instituições consideradas conservadoras que baseiam a sua atuação em princípios tradicionais nos quais as barreiras geográficas estão fortemente estabelecidas (Wall, 2007), o que colide com o cibercrime, na medida em que, este é um fenómeno que ocorre ao nível transnacional e que não conhece barreiras geográficas (Dias, 2012). Em Portugal, a intervenção ao nível o cibercrime, é feita através do Código Penal (CP) e, no que toca à proteção dos sistemas informáticos e dos dados informáticos, através da Lei n.º 109/2009 – Lei do Cibercrime (LC).

É precisamente na LC que está consagrada uma definição que diz respeito à criminalidade informática e cuja definição alude a todos os atos em que "*o computador serve como meio para atingir um objetivo criminoso ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto do crime*". Para além disso, esta lei é igualmente aplicável às situações em que os crimes são cometidos por meio de um sistema informático ou em relação aos quais se verifique a necessidade de recolher prova em suporte eletrónico (art. n.º 11). Já ao nível do direito penal português, há uma intervenção nesta matéria ao nível do CP para proteção do fim criminoso e dos bens jurídicos visados. Ademais, o cibercrime não se reduz ao CP, estende-se à Lei nº 46/2018, de 13 de agosto, que transpõe uma diretiva do Parlamento e Conselho europeu, e que visa estabelecer o regime jurídico da segurança no ciberespaço.

Pese embora o marco legal da cibercriminalidade em Portugal seja a LC, a regulamentação deste fenómeno não se esgota nesta lei. Ao nível do sistema judiciário português, mais concretamente na competência da Polícia Judiciária, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) é a unidade operacional especializada que dá resposta à cibercriminalidade, tendo como principais funções a prevenção, detenção e investigação deste fenómeno (Decreto-Lei n.º 81/2016, de 28 de novembro). Quanto ao Ministério Público, foi criado o Gabinete do Cibercrime[2] que tem como missão a coordenação, a formação de magistrados, a interação com o setor privado e com os órgãos de política criminal e, eventualmente, o acompanhamento de determinados processos. Já o Centro Nacional de

[2] Criado por um Despacho do Procurador-Geral da República, a 7 de dezembro de 2011.

Cibersegurança (CNCS)[3], funciona no âmbito do Gabinete Nacional de Segurança, e tem como principais linhas de ação a sensibilização para comportamentos mais seguros e responsáveis no ciberespaço; a disseminação de alertas, orientações e boas práticas; a produção de conhecimento sobre o estado da cibersegurança em Portugal; e, por fim, exerce competências de regulação e supervisão dos setores de atividade económica[4]. Através do serviço CERT.PT[5] (Equipa de Resposta a Incidentes de Segurança Informática Nacional), o CNCS, realiza uma efetiva coordenação nas respostas aos variados incidentes que afetam o ciberespaço, coordenando a resposta com as entidades da Administração Pública, operadores de infraestruturas críticas, operadores dos serviços essenciais e prestadores de serviços digitais.

1.2. Impacto da Covid-19 na cibercriminalidade

Em janeiro de 2020, a Organização Mundial de Saúde declarou a doença do novo coronavírus como uma emergência de saúde pública internacional. Consequentemente, a pandemia de Covid-19 causou mudanças drásticas a vários níveis, mas essencialmente a nível social e económico (Horgan *et al*., 2020), levando à construção de um "novo normal" (Collier *et al*., 2020). Perante a adoção de medidas de confinamento, ao nível mundial, foram várias as organizações que alertaram para a possibilidade do aumento da prática de cibercrimes.

A Europol (2020a), por exemplo, advertiu para o facto dos cibercriminosos estarem à procura de novas formas de obter benefício próprio com as medidas de confinamento, tendo mesmo advertido para o facto da "*pandemia global de Covid-19 ser não apenas um grave problema de saúde, mas também, um risco ao nível da segurança cibernética*" (Europol, 2020a, p. 4). Posteriormente, a *Internet Organized Crime Threat Assessment* (IOCTA) constatou que a pandemia ampliou os problemas já existentes ao nível do cibercrime (Europol, 2020b). Na mesma linha, há investigações que indicam que a Covid-19 teve a capacidade de expor as vulnerabilidades tanto tecnológicas, como do próprio utilizador da *Internet*, vulnerabilidades essas que são exploradas pelos cibercriminosos (Naidoo, 2020). Em 2021, no IOCTA, constata-se que o efeito da Covid-19 é notável. Durante a pandemia, o *ransomware* foi utilizado para comprometer o desempenho das redes das corporações e instituições públicas; verificou-se um

[3] Lei Orgânica do Gabinete Nacional de Segurança, Decreto-Lei nº3/2012, de 16 de janeiro.
[4] Decreto-Lei n.º 136/2017, de 6 de novembro.
[5] https://www.cncs.gov.pt/pt/certpt/, acedido em maio de 2022.

aumento no *grooming*[6]; e, por fim, a engenharia social e o *phishing* continuaram a ser os métodos privilegiados no cometimento de fraudes (Europol, 2021a).

No que concerne à evolução do cibercrime durante a pandemia em Portugal, o Gabinete do Cibercrime da Procuradoria-Geral da República, registou um aumento progressivo e persistentes de queixas recebidas. Considerando apenas o período compreendido entre janeiro e maio de 2020 foram reportadas mais queixas do em todo o ano de 2019 (aumento de 139%). Outro dado apresentado por esta instituição governamental são as situações mais reportadas pelas vítimas, nomeadamente a fraude por Mbway, fraude através do e-mail ou mensagens que contêm *malware*, *phishing* e extorsão por e-mail (Gabinete do Cibercrime, 2020). Já no ano de 2021, as situações mais reportadas pelas vítimas foram os ataques de *phishing*, fraude *online* e fraudes relacionadas com criptoativos[7]. Para além disso, os relatórios demonstram que, independentemente do maior número de denúncias se registar durante os períodos de confinamento, verifica-se uma ampliação consistente e progressiva do cibercrime nos últimos anos. Exemplo disso, é o incremento de 288% de denúncias registado de 2019 para 2020 e o aumento de 213% registado de 2020 para 2021 (Gabinete do Cibercrime, 2021).

Outra fonte importante de informação é o Relatório de Riscos e Conflitos de 2021, desenvolvido pelo Observatório de Cibersegurança. Neste relatório, observa-se que os ataques de *phishing*/ *smishing* foram as ameaças mais prevalentes durante o ano de 2020, registando-se mais 160% do que no ano de 2019, seguido da infeção por *malware* que aumentou 37% comparando com o ano de 2019. Por fim, as fraudes cometidas através do Mbway foram as mais prevalentes (Observatório de Cibersegurança, 2021). Não obstante, o Relatório de Segurança Interna (RASI) de 2021 através dos dados do CERT.PT constatou que os fenómenos mais reportados foram a fraude, código malicioso, recolha de informação e intrusão[8] (RASI, 2021). Já no Relatório de Riscos e Conflitos de 2022 verifica-se que se mantém a tendência de aumento do volume de incidentes no ciberespaço, tanto no ano de 2021 como no ano de 2022, sendo que em 2021 as ameaças mais dominantes foram o *phishing*, *smishing*, *vishing*[9],

[6] Expressão utilizada para definir genericamente a atividade dos predadores sexuais na *Internet*, desde o contacto inicial até à exploração sexual de crianças e jovens (Antunes & Rodrigues, 2018).
[7] Segundo o Banco de Portugal, os criptoativos são representações digitais de valores ou de direitos que podem ser transferidos e armazenados eletronicamente. Estes não podem ser utilizados para realizar pagamentos, contudo podem ser utilizados como ativos de investimento, sendo um dos mais conhecidos a *bitcoin* (https://www.bportugal.pt/page/criptoativos-stablecoins-e-euro-digital-descubra-diferencas-1 consultado em maio de 2022).
[8] A designação dos incidentes pode ser consultada na Taxonomia em Comum da Rede Nacional de CSIRT em vigor: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf
[9] Perpetuação do *phishing* através de chamadas telefónicas (Holt & Bossler, 2020).

ransomware e comprometimento de contas (Observatório de Cibersegurança, 2022). Em suma, os relatórios acima apresentados mostram uma tendência de aumento geral do cibercrime durante a pandemia de Covid-19 em Portugal.

Para além dos relatórios nacionais e internacionais, que procuram perceber qual é o efeito da pandemia nas tendências do cibercrime, também começam a surgir investigações empíricas que procuram estudar estas tendências. No Reino Unido, realizou-se uma investigação na qual estudaram o efeito da pandemia na deslocação das oportunidades criminais do mundo terrestre para o mundo digital através dos casos reportados ao *Action Fraud* (AF). Os investigadores concluíram que, as fraudes relacionadas com as compras *online e* leilão – que em maio de 2019 registou 5619 situações e em maio de 2020 registou 8482 – e o *hacking* de redes sociais e do e-mail – que no mês de maio de 2019 registou 939 denúncias e em maio de 2020 receberam 1449 – foram os tipos de cibercrime mais prevalentes durante a pandemia de Covid-19 (Buil-Gil *et al*., 2021). Já nos Estados Unidos, Payne (2020) encontrou resultados semelhantes, pois aumentaram as denúncias por fraude nos primeiros três meses de 2020, quando comparado com o mesmo período de 2019. Consistentemente, Lallie e colaboradores (2021) observaram que, globalmente, os ciberataques se tornaram mais prevalentes durante a pandemia. Já a investigação de Collier e colaboradores (2020), sugere que os ataques de negação de serviço aumentaram substancialmente depois do anúncio das medidas de confinamento, tendo os autores apontado como possível explicação o facto dos cibercriminosos tentarem explorar os efeitos psicológicos da pandemia, de forma a causarem medo e ansiedade.

Por sua vez, noutra investigação, foi feita uma análise temporal a dados relativos a fraudes denunciados à AF no Reino Unido, por forma a avaliar se se registava algum aumento na prática de cibercrimes desde a chegada da Covid-19. Os investigadores concluíram, por um lado, que os cibercrimes efetivamente aumentaram depois da adoção de medidas de confinamento, superando as previsões, contudo as mudanças nas taxas de vitimação não foram homogéneas para todos os tipos de fraude analisados nesta investigação. Se, por um lado, se verificou um aumento nas fraudes relacionadas com as compras *online*, fraude romântica e crimes cibernéticos (e.g., *hacking* de redes sociais e do e-mail), por outro, observou-se uma diminuição significativa da fraude relacionada com a compra de bilhetes, visto que todos os eventos foram cancelados (Kemp *et al*., 2021). Contrariamente, noutra investigação, realizada nos Estados Unidos, verificou-se que as ordens implementadas para a contenção dos contágios não alteraram radicalmente as rotinas *online* e não foram suficientes para alterar as taxas de cibervitimação. Assim, os investigadores concluem que os níveis globais de cibervitimação

depois da pandemia são idênticos aos níveis globais registados antes da pandemia. Por fim, o uso da *dark web*[10], o tempo despendido *online* a ler notícias/ artigos e, ainda, o uso das redes sociais, aumentou significativamente a probabilidade de um indivíduo ser vítima de cibercrime. Por outro lado, comportamentos de proteção como cobrir a câmara do computador, ter a identidade protegida e ter antivírus estavam inversamente relacionados com a probabilidade de vitimação *online* (Hawdon *et al*., 2020).

Um estudo mais recente, realizado por Buil-Gil e Zeng (2022) no Reino Unido, procurou perceber até que ponto a fraude romântica aumentou durante a pandemia e, mais especificamente, quais os grupos populacionais mais afetados e, para tal, recorreu aos dados da AF. Os resultados indicam um aumento daquele tipo de ofensa, especialmente na camada dos jovens adultos, isto é, dos jovens com idades compreendidas entre os 20 e os 29 anos – que em novembro/dezembro registavam 100 casos e em novembro/dezembro de 2020 foram denunciados 177 – e dos jovens adultos com idades compreendidas entre 30 a 39 anos – que em novembro/dezembro de 2019 registavam 138 casos e nos mesmos meses de 2020 registaram 199. Para além disso, os investigadores enfatizaram o facto de que, durante a perpretação deste tipo de fraude, os cibercriminosos adotam uma identidade falsa para se tornarem os parceiros "ideais", explorando os efeitos psicológicos adversos causados pela pandemia, como por exemplo, a solidão. No fundo, perfilham esta identidade falsa com o objetivo de ganhar a confiança da vítima e, a partir daí, iniciam um processo de manipulação para obterem vantagens, como por exemplo, para obtenção de informações que de outra forma não seria possível. A partir daqui, é possível concluir que o furto de identidade *online* é utilizado para a prática de outras ofensas (Buil-Gil & Zeng, 2022).

Em súmula, é irrefutável que a pandemia de Covid-19 teve um forte impacto na prevalência e incidência de alguns tipos de cibercrimes. No entanto, como referem Kemp e colegas (2021), sendo o cibercrime um guarda-chuva que engloba crimes tão diferentes entre si e, além disso, sendo a pandemia capaz de alterar as taxas de vitimação de forma diferencial consoante o tipo de ofensa, urge a realização de estudos que se foquem em cibercrimes específicos (e.g., Hawdon *et al.*, 2020; Kemp *et al*., 2021). Por este motivo, e perante a ausência de informação sobre as tendências específicas do furto de identidade *online*, tanto ao nível de vitimação, como ao nível do medo e perceção do risco, este estudo procura contribuir para o crescimento de

[10] Subespaço constituído por um conjunto de redes privadas. É uma rede fechada e secreta, restrita a um grupo restrito de utilizadores (Antunes & Rodrigues, 2018).

conhecimento científico neste âmbito. Para o efeito, será agora abordada a definição de furto de identidade *online*, bem como o *modus operandi* para a perpretação desta ofensa.

2. Furto de Identidade Online

2.1. Definição

Pese embora o termo mais utilizado a nível internacional seja *identity theft* (roubo de identidade; e.g., Reyns, 2013) e, no âmbito jurídico-legal, a denominação utilizada seja *usurpação de identidade*[11] (e.g., Silva, 2014), na presente dissertação o termo adotado foi *furto de identidade online*, visto que se trata da terminologia adotada pela literatura anglo-saxónica, que é a mais influente, e por ser o termo mais utilizado na área criminológica.

O furto de identidade, uma ofensa eminentemente tradicional, ganhou uma nova vida com a chegada a *Internet,* passando a ser cometido com maior frequência. Com efeito, o desenvolvimento tecnológico e da *Internet* permitiu o acesso a um elevado número de informações de carácter pessoal e financeiro (Smith, 2011), colocando em causa a ciberidentidade dos indivíduos. Esta ciberidentidade tem sido definida como "*o conjunto de elementos físicos, fisiológicos, psíquicos, económicos, culturais e sociais de um utilizador, constantes na Internet, que correspondem à identidade real da pessoa*", ou seja, a aquela pode ser entendida como uma extensão da identidade pessoal na *Internet* e, qualquer ato atentatório do direito à ciberidentidade será, à partida, ilícito (Silva, 2014, pp. 16-17). Por sua vez, Roberts e colaboradores (2013) consideram que o termo identidade *online* representa o conjunto de informações pessoais que deveriam ser intransmissíveis. Já para Hille e colegas (2015) a identidade da pessoa é constituída pela combinação de informações pessoais e financeiras. Perante as definições de identidade *online* supramencionadas, conclui-se que todas atribuem um papel central às informações de natureza pessoal e realça-se o facto de, na última definição, se atribuir igual importância às informações de cariz financeiro que são publicadas *online*. Assim, esta ciberidentidade, vai ser posta em causa pelo furto de identidade.

Posto isto, para Reyns (2013), o furto de identidade é um termo utilizado para categorizar vários crimes que envolvam o uso fraudulento de informações pessoais de um certo indivíduo para fins criminosos e, ainda, sem o seu consentimento. A esta ideia, Solove (2002) acrescenta

[11] Segundo Silva (2014), a terminologia a adotar deve ser *usurpação de identidade* por três razões. Primeiro, porque no art. n.º 38º da Lei 12/91 de 21 de maio – revogada pela Lei 33/99 de 18 de maio – tinha como epígrafe "usurpação de identidade". Para além disso entende que a identidade não pode ser furtada (art. 203º) ou roubada (art. 210º) por não se tratar de coisa móvel suscetível de deslocação espacial Por fim, o conceito de usurpação tem sido compreendido como "*a apresentação como próprio do que é alheio*" (Ascenção, 1993, p.19 cit. in Silva, 2014), o que, no entender de Silva (2014), define com abrangência e rigor conceptual o objeto de estudo.

que o ofensor obtém as informações pessoais e utiliza-as de várias maneiras fraudulentas para se fazer passar pela vítima ou para gerar informações falsas sobre a mesma. Esta aquisição da identidade pode ocorrer com recurso a diferentes meios e o uso da informação obtida pode ser utilizada para diferentes fins, nomeadamente, para o cometimento de outros crimes (Newman & McNally, 2005) conforme será visto adiante. Já para Harrell (2015, p. 2), o furto de identidade consiste no "*uso não autorizado, ou tentativa de uso, de uma conta existente (e.g., cartão de crédito ou débito) ou de dados pessoais que permitam a criação de uma nova conta ou uso indevido dessas informações pessoais para fins fraudulentos*". Por fim, para Saunders e Zucker (1999), o furto de identidade *online* consiste no uso, de forma ilícita, dos dados identitários de outra pessoa (e.g., nome, data de nascimento, número do cartão de crédito) para perpetrar fraudes económicas ou para se fazer passar pela vítima na *Internet*. Assim, tendo por base as diferentes definições apresentadas, é possível observar que há elementos que são consensuais em todas, desde logo, i) o facto das informações pessoais e financeiras serem utilizadas de forma fraudulenta e, ainda, ii) a utilização dessas mesmas informações para outros fins sem conhecimento e consentimento prévio da vítima. Dado que na presente dissertação o objeto de estudo é o furto de identidade *online* com objetivos financeiros, e não em geral, a definição adotada foi criada a partir das definições de Reyns (2013), Harrell (2015) e de Saunders e Zucker (1999): ato de obter dados pessoais e financeiros de outrem, via *Internet*, sem a autorização desta com o objetivo de obter ganhos financeiros.

Em Portugal, o furto de identidade teve, outrora, qualificação penal pela Lei n.º 12/91, de 21 de maio, Lei da Identificação Civil e Criminal, especificamente no artigo 38º, postulava que:

> "*Quem induzir alguém em erro, atribuindo, falsamente, a si ou a terceiro, nome, estado ou qualidade que por lei produza efeitos jurídicos, para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem será punido com prisão até 2 anos ou multa até 100 dias, se o facto não constituir crime mais grave*."

Anos mais tarde, esta lei foi revogada[12], fazendo com que o mencionado artigo 38º deixasse de existir. Segundo Silva (2014), nos tempos que correm, perante a ausência de uma norma que regule este fenómeno, o uso da identidade alheia tem relevância em termos penais quando da mesma se procura obter algum benefício ilegítimo ou prejudicar a pessoa cuja identidade foi furtada. Assim, as situações em que a utilização da identidade de outrem parece ter relevância ocorrem (1) quando há cometimento do crime de uso de documento de identificação alheio (art.

[12] A Lei n.º 12/91, de 21 de maio, foi revogada pela Lei n.º 33/99, de 18 de maio.

n.º 261, CP), (2) perante o crime de falsificação de documentos (art. n.º 256, CP), (3) quando se comete o crime de falsificação de estado civil (art. n.º 248, CP), (4) na prática do crime de falsas declarações (art. n.º 348-A, CP) e (5) quando através da usurpação é causado um prejuízo económico a outra pessoa (e.g., crime de burla, n.º 217º e seguintes do CP).

Na perpetração do furto de identidade, têm sido identificadas três etapas fundamentais e, num caso concreto, o furto pode incluir uma dessas fases ou as três. Em primeiro lugar, há a aquisição através do furto que pode ser materializado através do *hacking*, fraude, interceção de correspondência, burla ou por vias legais. Nesta primeira etapa, aquisição da informação, importa mencionar que há diferentes tipos de informações que podem ser alvo de ataque, nomeadamente informações sobre a história de vida (e.g., nome), contas financeiras (e.g., senha da conta bancária), contas não financeiras (e.g., senha de redes sociais) e, por fim, as informações biométricas (e.g., impressões biométricas) (Gercke, 2011; Smith, 2011). Já a segunda etapa diz respeito ao uso da identidade para ganhos financeiros (motivação mais comum) ou para evitar a detenção por parte de instâncias formais de controlo. Por fim, a última etapa é a da descoberta e, o período até à descoberta, pode ser mais ou menos longo dependente de um conjunto de circunstâncias (e.g., perda registada pela vítima; Newman & McNally, 2005). No que toca aos fins pelas quais estas informações são furtadas, a literatura tem encontrado três grandes finalidades: a aquisição de informação para se fazer passar pela vítima (Solove, 2002), a criação de informações falsas sobre a mesma (Solove, 2002; Reyns & Henson, 2016) e, por fim, a obtenção de ganhos financeiros (Newman & McNally, 2005).

Em suma, verifica-se que têm sido feitos esforços para a uniformização da definição de furto de identidade *online* e para a sua delimitação conceptual, assim como se têm identificado as etapas e finalidades do mesmo. Para além disso, a comunidade científica tem procurado identificar o *modus operandi* através dos quais esta ofensa é perpetrada e, de seguida, serão abordadas algumas das técnicas utilizadas pelos ciberofensores.

2.2. Modus Operandi

Com o rápido desenvolvimento da *Internet*, existem técnicas cada vez mais complexas, que se vão aprimorando e facilitam a concretização do furto de identidade *online*, sendo evidente que, estas técnicas utilizadas na perpretação do furto de identidade se vão alterando à medida que a tecnologia evoluí (Wang & Huang, 2011). Assim sendo, os ciberofensores utilizam de forma combinada as TIC e a engenharia social (Guedes *et al*., 2022), perpetrando o furto de identidade, por exemplo, através do *hacking* (e.g., Newman & McNally, 2005), do envio de

software malicioso (e.g., Reyns, 2015), *phishing*, *pharming* (e.g., Brody *et al*., 2007) e *smishing* (e.g., Williams, 2016), entre outros. Como forma de simplificar a compreensão destas estratégias, definem-se, conceptualmente, cada uma delas.

Quanto ao *hacking*, Antunes e Rodrigues (2018, p.105) definem-no como a "*realização de atividades ilícitas de invasão e acesso ilegítimo a sistemas informáticos de instituições, empresas ou particulares, com vista à recolha de informações sobre o seu funcionamento*". No ordenamento jurídico português, o *hacking* é punido como crime de "Acesso ilegítimo" na Lei do Cibercrime no seu artigo 6º. No fundo, o *hacking* traduz-se pelo acesso não autorizado a um dado sistema informático e pelo uso da manipulação, sabotagem ou espionagem (Singh, 2007), sendo que esta é uma técnica utilizada com sucesso por parte dos cibercriminosos na perpretação do furto de identidade *online* (Roberts *et al*., 2013).

Este furto de informação digital pode, também, ser consumado com recurso a *softwares* maliciosos que são programas introduzidos nos sistemas informáticos de forma encoberta, tendo como objetivo comprometer a confidencialidade, integridade ou a disponibilidade dos dados da pessoa, das aplicações ou do sistema operativo. Tendo em conta esta definição, conclui-se que este é um conceito geral que engloba diferentes tipologias e formas de propagação do *software* malicioso, nomeadamente vírus no computador, cavalos de Troia[13] e *spyware*. Uma vez instalado no sistema informático da vítima (individual ou coletiva), pode recorrer-se, por exemplo, ao *pharming* para furtar informações (Reyns, 2015).

Ao nível da engenharia social[14], o *phishing* é assistido pelo computador (Wall, 2007) e o objetivo é confundir os utilizadores da *Internet* para que forneçam informações confidenciais, nomeadamente, credenciais para aceder a determinado serviço (e.g., banco *online*). Note-se que estas tentativas são efetuadas através do envio de e-mails, mensagens instantâneas ou serviços de *chat*, por remetentes aparentemente legítimos, combinadas com o redireccionamento para páginas *web* fraudulentas onde é feito o pedido das informações confidenciais (Antunes & Rodrigues, 2018; Leukfeldt, 2014; Reyns & Henson, 2016). Por sua vez, o *smishing* é uma técnica similar ao *phishing* só que, neste caso, as mensagens são enviadas pelo telemóvel através de mensagens de texto (Williams, 2016). Por norma, as tentativas de *phishing* são autonomizadas e realizadas em massa de forma a atingir o maior número de pessoas possível

[13] Programas maliciosos executáveis, desenvolvidos com o objetivo de entrar no sistema de uma rede ou sistema informático. Reside num sistema como sendo um ficheiro benigno, contudo quando o utilizador o abre é executado e desenvolve uma ação maliciosa (Hoque, Bhuyan, Baishya, Bhattacharyya & Kalita, 2014).
[14] Utilização de técnicas de "contacto social" que visam a obtenção de informação privada (Antunes & Rodrigues, 2018).

(Leukfeldt, 2014). Outra técnica utilizada para o cometimento do furto de identidade *online* é o *pharming* que, apesar de ser similar ao *phishing*, é mais complexa, devido ao facto de utilizar estratégias de *malware* para perpetrar o *phishing*. Na prática, há uma apropriação ou usurpação do nome de domínio ou URL de uma página *web* legítima, redirecionando os utilizadores dessa mesma página para outra fraudulenta na qual é solicitada a informação pessoal (Antunes & Rodrigues, 2018). Num primeiro momento é instalado um vírus ou programa malicioso no dispositivo da vítima e, de seguida, na altura em que a vítima utiliza o *website*, os seus dados podem ser furtados, sendo difícil detetar que tal está a acontecer (Brody *et al.*, 2007).

Finalizando, esta revisão teórica realizada sobre o furto de identidade *online* permite concluir que este é um fenómeno complexo que merece atenção científica. Em traços gerais, este pode ser definido como o uso de informações pessoais e financeiras de determinado indivíduo sem o seu conhecimento e consentimento. Para além disso, esta ofensa pode ser cometida com recurso a diferentes e sofisticadas técnicas que se vão aprimorando à medida que a tecnologia evoluí. Posto isto, importará agora perceber se a vitimação por furto de identidade no ciberespaço pode ser explicada através de uma teoria criminológica que é a TAR.

3. Teoria das Atividades de Rotina

O rápido crescimento tecnológico levantou novas questões, dúvidas e inquietações aos investigadores, especialmente sobre a forma de medir e operacionalizar os crimes cibernéticos. Nos últimos anos, os estudiosos têm procurado perceber se os pressupostos teóricos que se aplicam à criminalidade tradicional podem ser estendidos aos crimes que ocorrem no ciberespaço. A teoria do estilo de vida (*lifestyle theory*) (Hindelang *et al*., 1978), as atividades de rotina (*routine activities theory*) (Cohen & Felson, 1979), assim como a teoria geral do crime (*general theory of crime*) (Gottfredson & Hirschi, 1990) têm sido as teorias mais testadas na explicação da vitimação cibernética de crimes de baixa tecnologia[15] (*low-tech cybercrimes*). Todavia, tendo em conta os objetivos e as hipóteses desta investigação, será apenas abordada e desenvolvida a TAR que se explicará, de seguida.

A escolha da TAR, nesta investigação, deve-se a vários motivos. Primeiramente, por ser uma das principais teorias adotadas pelas investigações que se debruçam sobre a vitimação por furto de identidade *online* (e.g., Reyns, 2013; Reyns & Henson, 2016). Para além disso, esta teoria foi selecionada pelo facto de que, as atividades de rotina *online*, perante guardiões

[15] Estes crimes de baixa tecnologia são os que não exigem conhecimentos especiais de informática e o alvo da conduta é a vítima, no fundo, o uso da tecnologia é um meio para praticar crimes como *cyberstalking*, *sexting* ou *revenge porn*, crimes de ódio, fraude e furto de identidade *online* (van der Wagen & Pieters, 2018).

ineficazes, terem impacto na experiência de vitimação *online* (Williams, 2016). Para além disso, os estudos demonstram que há atividades de rotina *online* (e.g., uso do banco *online*) que são preditoras da vitimação por furto de identidade (Pratt *et al.*, 2010; van Wilsem, 2013; Reyns & Henson, 2016; Williams, 2016). Por fim, outro motivo pela seleção desta teoria, prende-se com o facto de já se ter comprovado que determinados guardiões (e.g., instalação de antivírus) se revelam eficazes na prevenção da vitimação por furto de identidade *online* (Reyns & Henson, 2016). Posto isto, nesta investigação, procurar-se-á perceber se as variáveis contextuais provenientes desta teoria têm ou não poder preditivo quanto à vitimação, medo e perceção do risco de furto de identidade *online*.

3.1. Origem

A TAR, da autoria de Lawrence Cohen e Marcus Felson (1979), foi desenvolvida numa tentativa de explicar as alterações que se verificaram nas taxas de criminalidade na sequência da Segunda Grande Guerra Mundial. Com efeito, os autores concluíram que as mudanças nas rotinas diárias poderiam criar oportunidades situacionais para o cometimento de crimes ou para a vitimação. Segundo esta abordagem criminológica, para que crime ocorra, tem que existir um ofensor motivado que entra em contacto com um alvo adequado, perante a ausência de um guardião eficaz. Contudo, na ausência de um destes três elementos o crime pode não acontecer ou a probabilidade de ser consumado é menor (Cohen & Felson, 1979).

Do ponto de vista do ofensor, esta teoria dá primazia ao cálculo racional, na medida em que, o ofensor calcula os benefícios e desvantagens de cometer determinado crime, assim como, o nível de motivação também pode influenciar o seu comportamento. No que concerne ao alvo, existe uma relação de dependência entre as capacidades que o potencial ofensor tem para realizar aquele ato e as características das vítimas. Ou seja, se por um lado o ofensor avalia o nível de atratividade do alvo, por outro, o alvo pode tornar-se mais atrativo mediante as rotinas que adota, podendo tornar-se mais visível, alcançável e menos resistente. Esta atratividade do alvo é analisada tendo em conta o valor, inércia, visibilidade e acessibilidade (VIVA). Por fim, no que toca ao guardião há uma especial atenção ao nível de proteção que este confere ao alvo, pois com a sua presença pode prevenir a ocorrência do crime e, sempre que está ausente, a probabilidade de vitimação aumenta (Cohen & Felson, 1979).

3.2. Aplicação da Teoria das Atividades de Rotina ao ciberespaço

Capeller (2001, p. 229) chamou a atenção para o facto de que o surgimento do ciberespaço, enquanto realidade virtual, "*exige que a comunidade científica reveja os seus pressupostos*

filosóficos, históricos e sociológicos". Em resposta, Grabosky (2001, p. 243) sugere que a "*criminalidade virtual é basicamente o mesmo que a criminalidade terrestre a que estamos habituados*", considerando que deve existir uma congruência entre o crime terrestre e virtual e as teorias a aplicar ao mesmo. Assim, na perspetiva de Grabosky (2001) os crimes que são praticados em ambiente virtual mais não são do que "*vinho velho em garrafas novas*[16]", ou seja, já são atividades criminosas conhecidas, somente diferem as ferramentas e o *modus operandi*.

No seguimento, Yar (2005) faz uma reflexão teórica acerca da TAR e sobre a capacidade que a mesma tem para ser aplicada ao cibercrime, começando por analisar os elementos da teoria, testando a sua aplicabilidade ao contexto virtual. Quanto aos ofensores motivados, não constata problemas no que toca ao ambiente virtual, na medida em que se podem encontrar *hackers*, piratas, *stalkers* e burlões. Da mesma forma, existem diversos alvos que podem preencher os requisitos de alvos adequados, como por exemplo, os dados pessoais, os serviços de compra e venda e os sistemas dos dispositivos eletrónicos. Também o elemento do guardião eficaz pode assumir uma variedade de formas, incluindo os administradores das redes, os moderadores dos fóruns, os *firewalls* e os antivírus. Até aqui, segundo Yar (2005), não parece haver problema em aplicar a TAR ao ciberespaço, contudo, a proposta do autor é a de ir mais longe e analisar de forma aprofundada. Por exemplo, olhando para o alvo adequado, encontram-se os elementos da sigla VIVA, segundo a qual os alvos possuem valor, inércia, visibilidade e acessibilidade. Considerando a inércia, ou seja, as "*propriedades físicas dos objetos ou pessoas que podem oferecer vários graus de resistência à predação efetiva*", parece difícil transpor de forma direta para o ambiente virtual, pois não possuem propriedades físicas (Yar, 2005, p. 420). No entanto, Yar (2005) admite que o tamanho de um objeto digital (e.g., a quantidade de dados de um arquivo) é capaz de oferecer resistência à predação no que toca à velocidade e tempo que demora a ser baixado. O autor vai mais longe e reflete sobre a ecologia e topologia da TAR, concluindo que esta é uma teoria ecológica no que toca à causa do crime, sendo que a mesma está dependente da localização no tempo e no espaço de ofensores e alvos, pois o evento criminal ocorre quando o ofensor e o alvo se encontram na ausência de um guardião. Para além disso, a ontologia do mundo terrestre é responsável por proporcionar relações de maior ou menor proximidade entre ofensores e alvos, contudo o ambiente virtual parece ter uma configuração diferente, pois no ciberespaço é complexo identificar as relações de proximidade ou distância entre ambos, não havendo um encontro físico entre alvo e ofensor (*idem)*.

[16]A expressão original é "*old wine in new bottles"* (Grabosky, 2001).

Eck e Clarke (2003, p. 34) ao reformularem e ao expandirem a teoria ao ciberespaço, acrescentam que o elemento da localização física é substituído pela "rede". No mundo cibernético, como não existe a convergência do elemento ofensor e alvo, consideram que:

> "(…) a *teoria das atividades de rotina pode ser expandida para acomodar a ação à distância, através de uma modificação. Se o alvo e o infrator fizerem parte da mesma rede geograficamente dispersa, o infrator poderá alcançar o alvo através da rede*."

Embora a vítima e o ofensor não se encontrem num local físico, a sua interação é mantida através de uma rede que permite a convergência de ambos, pois nestas redes desprotegidas criam-se circunstâncias que levam à vitimação. Assim, nesta linha de pensamento, a TAR pode ser aplicada ao furto de identidade *online* (Reyns, 2013). Apesar desta abordagem teórica já ter sido utilizada para explicar diferentes formas de vitimação *online* (e.g., *phishing*, infeção por *malware* ou fraude *online*) (e.g., Choi, 2008; Marcum *et al*., 2010; Reisig *et al*., 2009), são poucas as investigações que examinam empiricamente os cibercrimes cometidos contra a propriedade, como por exemplo, o furto de identidade *online* (e.g., Reyns, 2013). Ademais, quando o fazem não têm operacionalizado os três conceitos centrais desta teoria (exposição, alvo e guardião). Assim, esta investigação tentará colmatar estas lacunas onde, para tal, serão agora revistos os pressupostos teóricos desta teoria aplicados no ciberespaço.

3.3. Pressupostos teóricos

3.3.1. Exposição ao risco no ciberespaço

Na investigação das atividades de rotina, um dos principais elementos é o ofensor motivado que, por norma, é conceptualizado do ponto de vista da vítima (Reyns & Henson, 2016). Quanto à sua operacionalização, este conceito é medido como exposição ao risco que, no fundo, engloba algumas das atividades que influenciam o risco de vitimação, sendo que, quanto maior exposição, maior o risco de vitimação. Aqui, deve ter-se em conta as motivações, as capacidades do indivíduo para realizar a conduta criminal e o cálculo que realiza entre custo e benefício do cometimento daquele ato (Felson & Cohen, 1980).

Inicialmente, a exposição ao risco *online* era operacionalizada através do número de horas que a pessoa passava por dia na *Internet* (e.g., Pratt *et al*., 2010). Contudo, Reyns (2013) alerta para a necessidade de criação de medidas que avaliem a exposição *online* mediante um conjunto de atividades de rotina que realizam *online* e que aumentam a exposição ao risco na ausência de um guardião eficaz. Por exemplo, se se pensar no crime de furto de identidade *online*, há um

conjunto de atividades que, por norma, são utilizadas para medir a exposição ao risco, como por exemplo, uso do banco ou fazer compras *online* (Reyns & Henson, 2016).

Quanto às investigações que se debruçam sobre este pressuposto os resultados são mistos. Por um lado, há estudos que não encontram qualquer associação entre a frequência do uso da *Internet* e a vitimação *online*. Por exemplo, o estudo de Bossler e Holt (2009), não encontrou associações entre fazer compras *online*, ter conversas *online* e utilizar o banco *online* e a perda de informação digital por *malware*. No mesmo sentido, o estudo de Leukfeldt (2014) não observou relações entre as atividades realizadas *online* e a probabilidade de vitimação por *phishing* e infeção por *malware*. No sentido contrário, Marcum e colaboradores (2010) encontraram resultados que indicam que há determinadas atividades *online* que aumentam a probabilidade de o indivíduo receber conteúdos sexualmente explícitos indesejados, ser alvo de assédio sexual e, ainda, ser vítima de solicitações sexuais indesejadas. Já no estudo de Ngo e Paternoster (2011), foram encontradas associações significativas entre a frequência do uso de mensagens instantâneas e o assédio *online*. Por fim, no estudo de van Wilsen (2011), as compras *online* e a participação em fóruns aumentou a probabilidade de vitimação por fraude. Complementarmente, o estudo de Pratt e colaboradores (2010) indica que a exposição a ofensores motivados *online* varia em função de algumas variáveis (e.g., género, idade e raça).

3.3.2. Alvo adequado no ciberespaço

O segundo pressuposto central da teoria, a adequação do alvo, corresponde à atratividade que uma pessoa, lugar ou objeto representa para um determinado ofensor (Cohen *et al*., 1981; McNeeley, 2015), isto é, uma maior adequação do alvo equivale a maiores riscos de vitimação. Originalmente, o alvo adequado foi descrito como possuindo as qualidades da sigla VIVA, ou seja, os alvos adequados são os que têm valor, inércia, visibilidade e acesso (Felson & Clarke, 1998). Clarke (1999) refinou ainda mais o conceito com a sigla CRAVED, ou seja, os alvos atraentes são ocultáveis, removíveis, disponíveis, valiosos, agradáveis e descartáveis. Anos mais tarde, Newman e Clarke (2003) apresentam o acrónimo das características do ambiente digital no que toca ao *hardware* e ao *software* dos sistemas de informação, considerando que os sistemas *online* são caracterizados pelas características do acrónimo SCAREM[17].

No ciberespaço, no que toca ao valor, este vai depender do objetivo do ofensor que tanto pode ter como alvo a informação pessoal e/ou financeira (e.g., dados do cartão de crédito), o

[17] Stealth (furtivo), Challenge (desafiador), Anonymity (anónimo), Reconnaissance (reconhecimento), Escape (evadir) e Multiplicity (multiplicidade).

dispositivo eletrónico (e.g., *software*), o indivíduo (e.g., honra) e, ainda, a propriedade (Holt & Bossler, 2013; Ngo & Paternoster, 2011). Já a inércia, que na literatura tradicional é identificada como as características físicas da pessoa ou do objeto que impedem a prática criminal (e.g., peso, tamanho e forma), no contexto digital passa a corresponder ao volume e/ou tamanho dos ficheiros, velocidade de transferência e capacidade de armazenamento dos mesmos, sendo que, na perspetiva de Yar (2005) é complexo transpor este conceito do contexto tradicional para o virtual. Por outro lado, no que toca à visibilidade, no ciberespaço esta está dependente das atividades que são desenvolvidas *online* (e.g., não ter *software* antivírus instalado e atualizado; clicar em *pop-ups*) (Alshalan, 2006). Estas atividades desenvolvidas *online* podem ser consideradas de risco, por exemplo, caso os indivíduos partilhem informações detalhadas acerca da sua vida pessoal (van Wilsem, 2013). Por último, a acessibilidade, que tradicionalmente está associada às propriedades físicas dos locais, ou seja, ao desenho do espaço e à acessibilidade ao local onde se encontra o objeto e/ou a pessoa, isto é, o alvo (Miró, 2014). Contudo, no ciberespaço, a acessibilidade tem-se relacionado com o uso de determinados navegadores que podem aumentar o risco de vitimação (Leukfeldt, 2014), com o tipo de atividades de rotina realizadas (Reyns, 2013) e com o tipo de informação publicada *online* (Reyns, 2015). Newman e Clarke (2003), os primeiros investigadores a promover a aplicação da TAR ao cibercrime, apontam que a acessibilidade e a visibilidade são características que fazem a distinção entre as vítimas das que não são vítimas de cibercrime.

4.3.3. Guardião eficaz no ciberespaço

A terceira dimensão fundamental da TAR é o guardião eficaz que é normalmente apontado como redutor do risco de vitimação, na medida em que, o guardião pode impedir o cometimento de crimes através de ações voluntárias, ou então, através da sua presença (Miró, 2014).

No ciberespaço, este conceito foi alvo de refinamentos e examinação empírica e, ao longo dos tempos, os investigadores distinguiram os guardiões consoante as suas funções, ou seja, distinguiram a figura do guardião social informal, guardião físico ou tecnológico e guardião pessoal. O guardião social informal pode ser, segundo Yar (2005), o conjunto de administradores de redes internas ou os membros de sistemas de segurança que têm como objetivo vigiar os pagamentos e cobranças feitas eletronicamente. Por sua vez, o guardião físico ou tecnológico, está relacionado com a proteção e segurança dos próprios equipamentos, quer sejam computadores, telemóveis ou tablets e é concretizada através da instalação de *softwares* antivírus, antispyware e *firewall* de *hardware* e *software* (Ngo & Paternoster, 2011; Reyns &

Henson, 2016). A literatura científica identifica, por fim, o guardião pessoal, uma vez que, o guardião físico ou tecnológico tem sido considerado insuficiente face às ameaças cibernéticas. Assim sendo, o guardião pessoal depende de dois fatores, do conhecimento informático individual e dos comportamentos seguros adotados *online*. No que toca ao conhecimento informático de cada pessoa, tem sido estabelecida uma associação negativa com a vitimação, na medida em que, quanto maior for o nível de conhecimento informático, maior é a perceção dos riscos *online* e, como consequência, mais comportamentos de defesa serão adotados, o que reduz ou impede uma possível vitimação (Leukfeldt & Yar, 2016). Por seu turno, os comportamentos seguros adotados *online* englobam os comportamentos capazes de reduzir o risco de vitimação, nomeadamente mudar recorrentemente as palavras-passes, criar palavras-passes consideradas fortes (Vakhitova & Reynald, 2014), evitar comprar *online* e não abrir e-mails de origem desconhecida. Em suma, a junção do guardião físico e do guardião pessoal pode reduzir a probabilidade de vitimação (Williams, 2016).

No que concerne às investigações empíricas, são vários os investigadores que tentam aplicar este conceito ao ciberespaço, tendo-se encontrado resultados mistos. Relativamente ao guardião físico, Holt e Bossler (2008) chegam à conclusão de que o *software* de segurança não reduz o risco de assédio *online*. Contrariamente, Ngo e Paternoster (2011) encontraram uma correlação positiva entre o *software* de proteção e vitimação por *malware* e assédio *online* por parte de estranhos. Já no estudo de Choi (2008), chegou-se à conclusão que os estudantes universitários com um guardião físico capaz apresentam menor risco de vitimação por vírus no computador. Por outro lado, no que ao conhecimento informático diz respeito, tanto Bossler e Holt (2009) como Ngo e Paternoster (2011) não encontraram relações significativas entre a infeção por *malware* e o nível de conhecimento informático. Por fim, ainda sobre o guardião pessoal, Holt e Bossler (2013) encontraram correlações positivas significativas entre o conhecimento informático e a infecção por *malware*.

Em suma, verifica-se que a TAR tem sido uma teoria criminológica amplamente testada em relação à vitimação por diversos cibercrimes e que os resultados encontrados são mistos (e.g., Ngo & Paternoster, 2011; Reyns, 2013; Williams, 2016). Nesta investigação, e mais concretamente na secção seguinte, serão abordados os determinantes do furto de identidade *online* de natureza contextual[18] (e.g., exposição, alvo adequado e guardião), mas também, os determinantes de natureza individual (e.g., género, idade e estatuto socioeconómico).

[18] Na presente investigação, a designação "variáveis contextuais" compreende as variáveis que derivam da TAR.

4. Determinantes do Furto de Identidade Online

Na presente secção, sobre os determinantes do furto de identidade *online*, serão abordados os principais determinantes que a literatura científica tem identificado para a vitimação por esta ofensa em específico. Primeiramente, serão abordados os determinantes de cariz individual e, de seguida, serão abordados os determinantes de natureza contextual.

4.1. Variáveis individuais

A investigação criminológica tem focado a sua atenção nas características individuais que, a par das características contextuais, que serão descritas adiante, podem influenciar a probabilidade de vitimação por furto de identidade *online*. Como será visto nas próximas linhas, a evidência encontrada acerca da importância das variáveis individuais para explicar a vitimação de furto de identidade *online* apresenta resultados mistos.

Quanto ao género, Holt e Turner (2012) e Reyns (2013), chegaram à conclusão que os homens, em comparação com as mulheres, têm uma maior probabilidade de serem vítimas de furto de identidade. Na mesma linha, Alshalan (2006) descobriu que o género tem um efeito na vitimação *online*, sendo os homens os mais vitimados. Na referida investigação, verificou-se que, os homens, despendiam mais tempo *online* do que as mulheres, o que, no ponto de vista deste autor, poderá aumentar o nível de exposição ao risco e, consequentemente, a vitimação por furto de identidade *online*. Por outro lado, e contra o que seria expectável, nas investigações de Martins (2018) e Guedes e colaboradores (2022), os homens apresentavam menos propensão para serem vítimas de furto de identidade *online* (36%) do que as mulheres.

Relativamente à idade, no estudo de Williams (2016) e de Harrell (2015), verificou-se que os mais jovens e os adultos de meia-idade reportava, níveis mais elevados de vitimação por furto de identidade. Contrariamente, na investigação desenvolvida por Reyns (2013) os indivíduos mais velhos apresentavam um maior risco de vitimação pela mesma ofensa. Noutra investigação, desenvolvida por Bunes e colegas (2020), observou-se que os indivíduos com idades compreendidas entre os 39 e os 73 anos apresentavam maior risco para a maioria dos tipos de furto de identidade incluídos no estudo, o que, para os autores, tal resultado poderá ser o reflexo da capacidade económica e dos padrões de consumo dessa geração.

Em termos de estatuto socioeconómico, são várias as investigações (Bunes *et al*., 2020; Reyns, 2013; Reyns & Henson, 2016), que observam que quem tem rendimentos[19] mais altos

[19] [19] O rendimento tem sido uma das formas adotadas pelos investigadores para operacionalizar o estatuto socioeconómico.

apresenta maior risco de se tornar vítima. Segundo Reyns (2013), tal pode dever-se ao facto dos indivíduos com mais rendimentos fazerem mais compras *online* e, consequentemente, exporem mais os seus dados pessoais e financeiros, aumentando o risco de serem furtados. Na mesma linha, para Bunes e colaboradores (2020), indivíduos de estatutos socioeconómicos mais elevados e com níveis de educação mais elevados apresentam maior poder aquisitivo e possuem mais dispositivos com ligação à *Internet* que transferem e armazenam informações, o que pode comprometer os dados de natureza pessoal e financeira. Já no estudo de Williams (2016) o estatuto social estava associado à vitimação, pois indivíduos com estatutos baixos e altos apresentavam níveis de vitimação mais elevados, ao passo que, indivíduos de classe média, apresentavam baixas taxas de vitimação por furto de identidade *online*. Por fim, nas investigações de Leukfeldt e Yar (2005) ou van Wilsem (2013) nenhuma das variáveis individuais explicou a vitimação por furto de identidade *online*.

4.2. Variáveis contextuais

Para além das variáveis individuais previamente explanadas, importa, também, atender às variáveis contextuais que podem ser determinantes do furto de identidade *online*. Assim sendo, nas próximas linhas, serão apresentados alguns dos estudos empíricos que procuram perceber qual é a relação entre a exposição, alvo e guardião e a vitimação num ambiente onde não existe o encontro interpessoal entre vítima e ofensor.

Quanto à exposição *online* e vitimação por furto de identidade *online*, é expectável que quanto maior o nível de exposição, maior o risco de vitimação, logo, é expectável que indivíduos que despendem mais tempo *online* sejam mais vítimas de furto de identidade. Contudo, no estudo de Martins (2018) e Guedes et al. (2022), o tempo passado *online* não tem impacto na vitimação por furto, o que corrobora os resultados de outras investigações previamente realizadas (e.g., Ngo & Paternoster, 2011; Reyns & Henson, 2016). Já na investigação realizada por Reyns (2013) verificou-se que determinadas atividades, como por exemplo, o uso de banco *online* e de mensagens instantâneas fazia com que os indivíduos tivessem 50% mais de probabilidade de serem vítimas de furto de identidade. Para além disso, as atividades relacionadas com downloads e compras *online* apresentavam um risco de 30%. Congruentemente, no estudo de Reyns e Henson (2016), a realização de operações bancárias *online* e a compra de bens e serviços contribuíram de forma positiva e significativa para a vitimação por furto de identidade *online*. Também no estudo de van Wilsem (2013) se verificou que as compras *online* e as visitas a fóruns são responsáveis pelo aumento da probabilidade de

vitimação de furto de identidade *online*. Contrariamente, nas investigações realizadas por Martins (2018) e Guedes e colaboradores (2022) utilizar os serviços bancários e fazer compras *online* não contribuíram para o aumento do risco de vitimação por furto de identidade *online*. Por fim, o estudo de Williams (2016) é uma investigação importante nesta área, na medida em que, recolheu dados em 27 países da Europa, contando com uma amostra de 26593 indivíduos. Começando pelas atividades de rotina *online*, constatou-se que a utilização do e-mail apresentou uma correlação negativa com a vitimação por furto de identidade, enquanto a venda em leilão apresentou uma correlação positiva. Por outro lado, quanto ao local de acesso e frequência de utilização da *Internet*, os indivíduos da amostra que acediam de forma frequente aos computadores de universidades e locais públicos, apresentavam maior taxa de vitimação, quando comparado com os indivíduos que acediam a partir do local de trabalho.

Quanto ao alvo adequado, as investigações empíricas utilizam medidas de valor económico para refletir o conceito de atratividade do alvo (Reyns & Henson, 2016) e, efetivamente, o valor económico pode ser um dos indicadores sobre a atratividade do alvo para quem furta, por exemplo, a identidade. Contudo, há outras dimensões de atratividade a ter em conta. Por exemplo, os indivíduos que visitam sites desprotegidos, fornecem informações pessoais *online* ou têm dados pessoais publicados *online*, podem tornar-se alvos mais fáceis e atraentes para os ofensores (Clarke & Cornish, 1987). Tendo em conta as investigações realizadas sobre o alvo adequado, Leukfeldt e Yar (2016) concluíram que o *targeted browsing* ou a pesquisa de notícias influencia a vitimação por furto de identidade *online*. Já no estudo de Reyns e Henson (2016) a publicação de informações pessoais *online* aumenta a probabilidade de vitimação por furto de identidade *online* e, pelo contrário, a visita de sites arriscados e a publicação de informações pormenorizadas apresenta uma relação negativa. Nas investigações de Martins (2018) e Guedes e colaboradores (2022), uma dimensão do alvo adequado – a visita de conteúdos de risco – teve impacto na probabilidade de vitimação por furto. Nesta medida composta, que englobava a visita de *websites* arriscados e clicar em mensagens *pop-ups*, a probabilidade de vitimação para os indivíduos que adotavam estes comportamentos de risco era 34% maior.

Por fim, apresentam-se os resultados das investigações realizadas sobre o guardião eficaz e o furto de identidade *online*. Na investigação realizada por Williams (2016), foi criada uma tipologia com três formas de tutela, sendo estas, a tutela física passiva (e.g., filtro de *spam* no e-mail, instalação de antivírus e navegação segura), tutela pessoal ativa (e.g., alteração regular das definições de segurança e palavras-passe) e tutela pessoal de evitamento (e.g., evitar a realização de determinadas ações *online*). Verificou-se que, a tutela física passiva é eficaz na

redução do furto de identidade *online* dada a forma automatizada deste tipo de segurança. Para além disso, constatou-se que a instalação de antivírus e a navegação segura foram mais eficazes do que formas pessoais de tutela. No que toca à tutela pessoal de evitamento, verifica-se uma relação curvilínea com a vitimação, na medida em que se encontra associada positivamente até determinado momento, contudo chega a um certo ponto em que a situação se inverte. Por fim, foi encontrada uma correlação positiva entre a vitimação por furto de identidade *online* e a tutela pessoal ativa que é explicada pela reação pós-vitimação, isto é, após serem vítimas de furto de identidade *online* são adotados comportamentos de proteção. Já Reyns e Henson (2016) concluíram que nenhuma medida incluída na operacionalização do guardião eficaz (e.g., instalação de *software* antivírus, eliminação de e-mails desconhecidos e alteração recorrente das *passwords*) teve efeitos estatisticamente significativos na predição do furto de identidade *online*, o que é consistente com a literatura que analisa a relação entre guardião eficaz e vitimação *online* (e.g., Holt & Bossler, 2013; Ngo & Paternoster, 2011).

5. Sentimento de Insegurança

5.1. Definição

Historicamente, a segurança sempre constituiu uma enorme preocupação, uma vez que é fundamental para a sobrevivência humana e é uma forma de satisfazer as necessidades humanas (Beck, 2015). À semelhança do que sucede com a maioria dos conceitos abrangidos pela área das ciências sociais, é um conceito de difícil definição, não havendo uma delimitação conceptual que seja universalmente aceite por todos os investigadores (Duque, 2015). Para Wolfers (1952) a segurança corresponde à ausência de insegurança e, segundo Zedner (2009), o estado de segurança, objetivamente, implica a condição de estar sem qualquer ameaça, contudo, este estado de segurança objetiva é impossível de atingir e, caso chegue a acontecer, é temporário. Apesar de ser difícil a distinção entre segurança objetiva e subjetiva, a autora acrescenta que a segurança representa a proteção contra ameaças, a neutralização, ou não, da exposição a riscos. Esta é, portanto, uma delimitação que engloba uma dimensão subjetiva, visto se tratar da perceção sobre a ausência de ameaças ou riscos e de sentimentos delas recorrentes. No que toca ao quadro normativo, para Valente (2013, p. 108) a segurança é "*uma garantia do cidadão para que exerça segura e tranquilamente os demais direitos fundamentais*". Perante estas perspetivas, conclui-se que a segurança assume um papel central e de relevo para a sociedade, sendo entendida como uma garantia, proteção e direito do cidadão.

A par da segurança, também o sentimento de insegurança[20] (na literatura anglo-saxónica, o *fear of crime*) começou a ser reconhecido como uma área de interesse nos anos 60 e, desde então, têm sido muitas as investigações que se dedicam ao estudo deste fenómeno no que aos crimes tradicionais diz respeito. Para a Criminologia, esta tem sido uma área de especial interesse, nomeadamente, o estudo das componentes da insegurança, o modo de medir e, ainda, o estudo das variáveis individuais e contextuais que estão subjacentes ao medo do crime (Agra, 2007). Dada a vasta investigação que tem vindo a ser desenvolvida, tanto ao nível conceptual, como metodológico, este é um conceito que engloba múltiplas componentes (Guedes *et* al., 2012). Na atualidade, com os avanços tecnológicos e com o aumento do número de utilizadores da *Internet*, o sentimento de insegurança adquire especial relevo no contexto virtual e afigura-se como uma área de investigação de interesse e em crescimento.

Na perspetiva de alguns autores (Agra, 2007; Agra & Kuhn, 2010), o conceito de insegurança é composto por duas dimensões, uma objetiva e outra subjetiva. Relativamente à primeira dimensão, está relacionada com a constatação de problemas de cariz social, como por exemplo, a criminalidade predatória, violência, delinquência juvenil e vandalismo. Por outro lado, a dimensão subjetiva ou o sentimento de insegurança, diz respeito ao que os indivíduos sentem, correspondendo a uma dimensão cognitiva (preocupação com o crime) e outra afetiva (medo de ser vítima). O sentimento de insegurança é considerado um objeto fluído, construído a partir de diversos contextos e atores, o que torna difícil a delimitação empírica do conceito, pois o mesmo faz divergir em seu torno múltiplos elementos da experiência social e da vivência psicológica entre indivíduos (Fernandes & Rêgo, 2011). Dado que o foco deste trabalho incidirá, para além da vitimação, sobre o sentimento de insegurança, e mais especificamente sobre a sua conceptualização, importa, por isso, primeiramente perceber as categorias de conceptualizações que se encontram na literatura científica. Assim, há autores que preferem adotar uma interpretação mais estreita do medo do crime que corresponde à dimensão emocional do sentimento de insegurança (e.g., Ferraro & LaGrange, 1987). Por outro lado, o medo do crime pode ser entendido de uma forma mais larga e que equivale ao sentimento de insegurança, considerando que este é um fenómeno multidimensional que engloba três grandes componentes (emocional, cognitiva e comportamental) (Vandeviver, 2011).

[20] Na presente investigação o termo "sentimento de insegurança" engloba três componentes: medo do crime (componente emocional), perceção do risco (componente cognitiva) e adoção de comportamentos (componente comportamental). Assim sendo, a expressão "medo do crime" corresponde à dimensão emocional.

A comunidade científica tem entendido que o sentimento de insegurança deve ter uma definição tripartida. Assim sendo, Agra (2007), Agra e Kuhn (2010) e Gabriel e Greve (2003), consideram que este conceito se divide em três dimensões: dimensão emocional (corresponde ao medo do crime), dimensão cognitiva (corresponde à perceção do risco de vitimação) dimensão e comportamental (corresponde aos comportamentos adotados em virtude de evitar uma possível vitimação). As dimensões apresentadas remetem para a definição de sentimento de insegurança como representação social, isto é, como forma de dar sentido à realidade (Machado & Agra, 2002).

Para além desta definição tripartida de sentimento de insegurança, que foi apresentada e adotada na presente investigação, importa mencionar outras definições que diferentes autores apresentaram ao longo dos anos e que contribuíram para o crescimento do conhecimento existente acerca deste fenómeno. Nos anos 70, Fustenberg (1971) defendeu que existem duas reações psicológicas fundamentais ao crime, nomeadamente o medo e a preocupação. Quanto ao medo, que Amerio e Roccato (2007) denominaram por medo concreto, corresponde a um estado de ansiedade e agitação relacionadas com a segurança, quer sejam perigos reais ou potenciais. Por outro lado, quanto à preocupação, corresponde a um estado de agitação em relação às ofensas criminais que ocorrem no país em que reside. Conclui-se, com esta divisão, que um indivíduo pode sentir medo por si e, também pelos seus, contudo, o indivíduo pode sentir-se preocupado com o crime como problema social (Guedes *et* al., 2012). Na mesma linha, nos anos 90, Fonseca (1998) distingue preocupação securitária de apreensão vivida. Por um lado, a preocupação securitária corresponde a um julgamento que depende de uma orientação ideológica-normativa. Por outro, a apreensão vivida diz respeito a um sentimento, isto é, constitui-se como uma resposta a sinais percecionados como ameaçadores capazes de provocar alterações de comportamento (Guedes *et al.*, 2012).

Em suma, o sentimento de insegurança, sendo considerado um fenómeno multidimensional, expressa-se em três dimensões distintas: emocional (medo do crime), cognitiva (perceção do risco de vitimação) e comportamental (adoção de comportamentos por razões de segurança) e, apesar de este fenómeno ter surgido inicialmente no mundo *offline*, a sua aplicabilidade não se esgota no que ao crime tradicional diz respeito. Nos últimos tempos, verifica-se que este fenómeno tem assumido cada vez mais importância na investigação que a Criminologia realiza sobre o ciberespaço. Por tudo quanto foi exposto, importará agora explorar, de forma aprofundada, as três dimensões apresentadas e a sua aplicabilidade ao ciberespaço.

5.2. Componentes do Sentimento de Insegurança

5.2.1. Medo do crime

Tal como supramencionado, a investigação criminológica tem adotado uma definição tripartida do sentimento de insegurança que inclui uma dimensão emocional operacionalizada através do medo do crime (Gabriel & Greve, 2003). Apesar de não existir consenso sobre a delimitação concetual de medo do crime, uma das definições mais comumente adotadas é a de Ferraro e LaGrange (1987) segundo a qual o medo do crime é uma resposta emocional de pavor ou ansiedade ao crime ou a símbolos associados a ele. Na mesma linha, o medo do crime é visto como "*uma resposta emocional a possíveis crimes violentos e danos físicos*" (Covington & Taylor, 1991, p. 231). Já Warr (2000) refere que o medo do crime, para a maior parte dos indivíduos, corresponde ao sentimento que é despertado mediante a presença de um perigo imediato. Contudo, alerta para o reducionismo desta definição, pois os seres humanos são capazes de projetar eventos futuros, o que significa que um determinado indivíduo pode sentir medo apenas por antecipar o surgimento de possíveis ameaças. O autor menciona, ainda, que é possível sentir medo pela própria segurança (medo pessoal) e sentir medo por outros indivíduos com que se tenha uma relação de maior proximidade (medo altruísta) (*idem*).

Por sua vez, Garofalo (1981, p. 840), apresenta o medo do crime como a "*reação emocional caracterizada por um sentimento de perigo e ansiedade*" e delimita esta reação à ameaça de dano. Importa distinguir a reação desencadeada pela potencial perda de propriedade - mais cerebral e calculada –, que ele defende que deve ser designada como "preocupação", da reação que ocorre pela possibilidade de dano físico – autonómica e emocional. Por fim, o autor destaca a importância de distinguir o medo real, do medo antecipado, visto que é diferente o indivíduo viver uma situação real de ameaça ou imaginar que poderá vivenciar essa ameaça. A esta ideia, Jackson (2006) acrescenta que o medo do crime é influenciado pela avaliação da ameaça que é feita, avaliação essa que envolve as perceções sobre a probabilidade, capacidade de controlo do ato e as consequências que dele podem resultar (Guedes *et al.*, 2012).

Com o aumento exponencial da cibercriminalidade, o sentimento de insegurança na *Internet* adquire, nos dias de hoje, especial relevo, contudo, poucas são as investigações empíricas que produzem conhecimento sobre esta problemática (e.g., Hille *et al*., 2015; Roberts *et al*., 2013; Virtanen, 2017). Concretamente sobre o medo de furto de identidade *online*, Hille e colaboradores (2015) foram pioneiros, ao desenvolver e validar uma escala que permite medir o medo sentido pelos consumidores que, até então, e como sucede no estudo de Roberts e colaboradores (2013) sobre os preditores deste medo, era medido com recurso a apenas dois

itens[21]. Assim, para Hille e colaboradores (2015, p. 2), o medo de furto de identidade *online* define-se como "*uma emoção negativa que emerge no consumidor e é ativada pela avaliação cognitiva que a pessoa faz sobre a possibilidade de furto de dados pessoais e financeiros de que pode ser vítima, ao realizar transações online e, este medo, pode também ser gerado por estímulos externos (e.g., media), que podem influenciar os seus comportamentos online*". Na prática, o medo de furto de identidade *online* desencadeia a motivação para evitar os resultados que possam eventualmente ser prejudiciais, o que por sua vez, afeta a tomada de decisão e o seu comportamento, como por exemplo, evitar fazer compras *online* (Loewenstein *et al.*, 2001).

Para Hille e colaboradores (2015), o medo de furto de identidade *online* inclui o medo subjetivo da pessoa em relação a experienciar consequências sérias e negativas. A literatura tem avançado que os consumidores têm particularmente medo de perdas financeiras e, ainda, de possíveis danos na sua reputação. Assim sendo, os autores propõem duas dimensões no medo de furto de identidade *online*, a saber i) o medo de perdas financeiras e ii) o medo de danos na reputação. O medo de perdas financeiras corresponde ao medo de apropriação ilegal e não ética de dados pessoais e financeiros e consequente uso da identidade do outro para comprar produtos fraudulentos, para obter crédito ou para aceder à conta bancária da vítima (Acoca, 2007). Por seu turno, a reputação, enquanto conjunto de julgamentos que uma comunidade faz acerca de um dos seus membros (Emler, 1990), representa um conceito central na vida em comunidade. Ora, dada a importância da reputação, é normal que as pessoas percebam o furto de identidade como uma ameaça à mesma. Assim, Hille e colaboradores (2015) definem o medo de danos na reputação como o medo do mau uso ou do uso ilegal dos dados de outrem com o objetivo de se fazer passar pela vítima e causar danos na reputação da mesma. Este uso ilegal da identidade de outra pessoa pode causar danos na reputação ao nível do nome, oportunidades profissionais ou, até mesmo, na acusação de ilícitos que a vítima não cometeu (Miri-Lavassani *et al*., 2009).

5.2.2. Perceção do risco de vitimação

Quanto à dimensão cognitiva do sentimento de insegurança, a perceção do risco de vitimação ou risco percebido, é importante notar que esta difere do medo do crime, visto não ser uma emoção, mas sim uma avaliação cognitiva da segurança ou do perigo de vitimação criminal (Mesch, 2000). Este conceito alude ao modelo de interpretação do risco apresentado por Ferraro (1995) e, segundo o autor, esta perceção corresponde ao reconhecimento de que

[21] No estudo de Roberts e colaboradores (2013), o medo de furto de identidade *online* foi medido com os seguintes itens "*quão preocupado está com a probabilidade disto lhe acontecer*: (1) *ter a sua identidade furtada através da Internet; (2) os dados do seu cartão de crédito serem utilizados ilegalmente na Internet*".

determinados locais ou situações possuem perigo potencial ou vitimação criminal. Adicionalmente, outra diferença entre o medo do crime e a perceção do risco de vitimação é o facto de serem afetadas de forma diferente por variáveis sociais e variáveis demográficas (e.g., género, idade, etnia e estatuto socioeconómico) (Mesch, 2000; Skogan & Maxfield, 1981).

No que concerne à perceção do risco de vitimação *online*, Henson e colaboradores (2013) definem este conceito como a avaliação que o indivíduo faz sobre a probabilidade de vitimação criminal na *Internet* e que pode ser influenciado pela sua vulnerabilidade, ambiente imediato e, ainda, pelo nível de exposição ao risco. No estudo de Henson e colaboradores (2013), o risco percebido destacou-se como um forte preditor do medo do crime *online*, independentemente da relação entre a vítima o ofensor. Já na investigação desenvolvida por Higgins e colegas (2008), focada no estudo da relação entre autocontrolo, risco percebido de vitimação *online* e medo do cibercrime, os autores observaram que o risco percebido estava positiva e significativamente relacionado com o medo de vitimação *online*. Para além disso, verificaram que o risco percebido mediou a relação entre o autocontrolo e o medo de vitimação *online*.

Também a Comissão Europeia tem realizado vários estudos sobre as perceções e atitudes face ao cibercrime. Em outubro de 2019, foi desenvolvido e aplicado o *Special Eurobarometer 499: Europeans' attitudes towards cyber security* (n= 27607 cidadãos de 28 Estados-Membros da União Europeia), com o objetivo de compreender as experiências de vitimação e a perceção dos participantes sobre a cibersegurança. Deste total, 76% acreditam que o risco de se tornarem vítimas de cibercrime está a aumentar e uma proporção de 52% pensa que é capaz de se proteger das ameaças. Os participantes que indicaram estar preocupados com a possibilidade de se tornarem vítimas indicaram maior preocupação com os seguintes tipos de cibercrime: fraude relacionada com a utilização do banco *online* ou uso de cartão bancário (67%), furto de identidade (66%) e a infeção dos dispositivos com *softwares* maliciosos (66%) (Comissão Europeia, 2019). Por sua vez, Yu (2014) observou que a perceção do risco de vitimação foi um preditor significativo do medo de *cyberbullying* e burla *online*. Contudo, esta preocupação com o cibercrime não se verifica com outros tipos de crimes cometidos *online*, ou seja, não é uma preocupação transversal. Por exemplo, quando se trata de *download* ilegal, parece haver uma banalização deste comportamento, isto é, é visto como se fosse um ato legítimo (Yar, 2010).

Em resumo, apesar de as investigações identificarem a vitimação por crime *online* como uma experiência capaz de aumentar o risco percebido e a preocupação com o cibercrime, não é suficiente para explicar os níveis elevados de risco percebido, visto que há uma discrepância entre estes e as efetivas experiências de vitimação. Assim sendo, os estudiosos têm acrescentado

outros fatores que podem explicar os níveis de risco percebido, nomeadamente, o trabalho dos *media*, a vitimação indireta e o anonimato característico das relações sociais da atualidade (Wall, 2008). Note-se que este paradoxo, normalmente designado como "paradoxo medo-vitimação" também se verifica no mundo *offline* (Guedes *et al.,* 2012).

5.2.3. Adoção de comportamentos por razões de segurança

No que concerne aos comportamentos adotados por razões de segurança, a comunidade científica tem entendido que existem duas classes de comportamentos: os de evitamento e os de proteção (e.g., Ferraro, 1995).

Por um lado, quanto aos comportamentos de evitamento, os indivíduos frequentam locais onde se sentem mais seguros e evitam áreas perspetivadas como menos seguras. Contudo, em situações cujos indivíduos não conseguem frequentar áreas mais seguras, em virtude do seu estatuto socioeconómico, por exemplo, tendem a tornar-se prisioneiros das suas habitações e das suas zonas de residência (Liska *et al.,* 1988). Em relação ao ciberespaço, a investigação desenvolvida por Riek e colaboradores (2016) constata que as experiências de vitimação são responsáveis por aumentar o risco percebido que, por sua vez, desencadeia a adoção de comportamentos de evitamento na utilização da *Internet*, designadamente não utilizar o banco *online*, não realizar compras *online* e não comunicar através de redes sociais. Tal como Yar (2010) aponta, as experiências de vitimação no mundo digital e as perceções dos riscos que lhe estão associados são catalisadores dos comportamentos de evitamento, o que faz com que os cidadãos se privem dos benefícios que advêm da *Internet*.

Por outro lado, os comportamentos de proteção referem-se à adoção de instrumentos ou técnicas de segurança (e.g., instalação de alarmes) e à aprendizagem de técnicas para proteção (Garofalo, 1981; Liska *et* al.,1988). Quanto aos comportamentos de proteção adotados no ciberespaço, um dos mais comuns é a instalação de *softwares* de segurança, nomeadamente o antivírus, *antispyware* ou *firewall* (Ngo & Paternoster, 2011). Também há quem identifique como comportamento de proteção o nível de conhecimento tecnológico, pois se os indivíduos tiverem mais conhecimentos serão capazes de prevenir futuras vitimações (Paek & Nalla, 2015). No que toca ao furto de identidade, os principais comportamentos de proteção adotados pelas vítimas são a alteração das palavras-passes com regularidade, ter cautela no tipo de informação partilhada e a alteração dos detalhes bancários (Smith & Hutchings, 2014).

5.3. Variáveis explicativas do Sentimento de Insegurança

São vários os modelos que têm sido avançados na investigação do medo do crime tradicional tendo em vista a sua explicação, como é o caso da tese das vulnerabilidades[22] que realça a importância das características individuais (e.g., Skogan & Maxfield, 1981; Warr, 1984). Contudo, apenas muito recentemente os investigadores iniciaram a investigação sobre a transversalidade das variáveis explicativas do medo do crime, questionando-se se as mesmas seriam aplicáveis ao medo no ciberespaço.

5.3.1. Género

O género é considerado o melhor preditor do medo do crime, sendo que são as mulheres que reportam níveis mais elevados (Hale, 1996; Warr, 2000). Contudo, à exceção dos crimes sexuais, *stalking* e violência doméstica, são os homens os mais vitimados (Rader *et al*., 2007), existindo o que a literatura científica em designado como o paradoxo medo vitimação (Hale, 1996; Rader *et al*., 2007). Este medo sentido pelas mulheres reflete a perceção de vulnerabilidade real (dimensão física) e percebida (percecionam-se como frágeis e incapazes de se defenderem). No fundo, as mulheres entendem que não são capazes de se defender através de meios económicos, físicos e/ou sociais (Guedes *et al*., 2012).

Quanto ao cibercrime, os estudos demonstram que as mulheres reportam níveis mais elevados de medo essencialmente dos cibercrimes que implicam contacto interpessoal e não tanto nos cibercrimes que têm como alvo o dispositivo eletrónico (Virtanen, 2017). Contrariamente, no estudo de Brands e Wilsem (2019), as mulheres reportam níveis mais elevados de medo *online* para a componente financeira. Em termos de cibercrimes específicos, Henson e colaboradores (2013) analisaram crimes de intimidação *online*, solicitações sexuais, perseguição e ameaças de violência e concluíram que as mulheres têm níveis mais elevados de medo do que os homens. Já o estudo de Yu (2014) constatou-se que o único cibercrime em que as mulheres apresentavam níveis mais elevados de medo era no caso do *cyberbullying*. Por fim, Roberts e colaboradores (2013), numa investigação dedicada à identificação dos preditores do medo de furto de identidade *online* e atividades fraudulentas, constataram uma baixa correlação entre o medo e o género feminino. Em relação ao risco percebido, num estudo realizado por Reisig e colaboradores (2009), foi possível concluir que as mulheres não apresentavam um risco percebido significativamente superior ao dos homens.

[22] A vulnerabilidade é a capacidade de lidar com sucesso a situação ou capacidade para recuperar, ou seja, capacidade para repor a sua situação ao nível económico, social, mental e físico que existia antes da vitimação (Hirtenlehner, 2008).

5.3.2. Idade

Quando se pretende estudar o medo geral do crime, na perspetiva da vulnerabilidade, a idade é apontada como uma variável crucial. Segundo esta perspetiva, as pessoas idosas teriam uma vulnerabilidade real e outra percebida. Primeiramente, a vulnerabilidade real é traduzida pela sua fragilidade física e pela menor capacidade de resistir a uma eventual vitimação. Já a vulnerabilidade percebida está relacionada com a dificuldade em lidar com a situação, que poderia levar a uma antecipação do impacto do crime como algo mais gravoso (Machado, 2004). Em termos de investigações empíricas, por um lado, há um conjunto de estudos que sugerem que são os indivíduos mais velhos os que reportam níveis mais elevados de medo (e.g., Reid & Konrad, 2004) e, por outro lado, há estudos que não encontram diferenças entre indivíduos mais velhos e mais novos (e.g., Pain, 1995). Por fim, existem investigações que apontam os mais novos como aqueles que reportam níveis mais elevados de medo do crime, como é o caso da investigação de Ziegler e Mitchell (2003). Esta constatação da existência de resultados mistos também se tem verificado no ciberespaço.

No fundo, há estudos que indicam que os indivíduos mais velhos têm mais medo do cibercrime (Alshalan, 2006), sugerindo que estes atribuem mais valor à propriedade e, portanto, têm medo de a perder. No mundo digital, esta propriedade é assumida pelos sistemas dos computadores e pelos cartões de crédito e/ou débito (*idem*). Na mesma linha, o estudo de Lee e colegas (2019) chegou à conclusão de que os indivíduos mais velhos têm mais medo da vitimação nas redes sociais (e.g., assédio sexual, invasão de privacidade e violência verbal) quando comparados com os mais novos e, no estudo de Brands e Wilsem (2019) os mais velhos reportam mais medo para uma componente financeira. Por sua vez, Fox (2001), numa investigação realizada com jovens norte-americanos, constatou que 60% da amostra (n=2096) tinha medo que o seu cartão de crédito fosse furtado *online*, um resultado inferior ao apresentado pelos elementos mais velhos da amostra, já que os participantes com idades compreendidas entre os 30 a 49 anos apresentaram uma taxa de medo de 72% e os indivíduos com idades compreendidas entre os 50 a 64 anos uma taxa de medo de 73%. Por outro lado, no estudo de Randa (2013) foram encontradas correlações negativas entre a idade e medo, sendo que os indivíduos mais novos reportavam mais medo de *cyberbullying*. Contrariamente, no estudo de Reisig e colaboradores (2009), a idade parece não ter tido influência na perceção do risco de vitimação por furto de cartão de crédito e, quanto ao furto de identidade *online*, no estudo de Roberts e colaboradores (2013) a idade foi um preditor no medo de furto de identidade e das atividades fraudulentas, contudo explicava menos de 1% da variância da variável medo.

Por fim, no estudo de Reisig e colaboradores (2009) a idade não se correlacionava significativamente com a perceção de risco de vitimação de furto na *Internet*. Perante este resultado e o do género – as mulheres não apresentavam maior perceção do risco do que os homens – os autores propõem a hipótese da ausência de vulnerabilidade física no contexto digital como um fator explicativo destes resultados.

5.3.3. Estatuto socioeconómico

Ao contrário do género e idade que são considerados vulnerabilidades físicas, o estatuto socioeconómico e a escolaridade têm sido considerados vulnerabilidades sociais. O baixo estatuto socioeconómico pode aumentar o medo do cibercrime em virtude dos julgamentos que o indivíduo faz da gestão dos custos associados à vitimação por cibercrime. A ligação entre baixo estatuto socioeconómico e o medo do crime é bem estabelecida na literatura sobre crimes tradicionais, mas não sobre o cibercrime, dada a escassez de estudos (e.g., Virtanen, 2017).

Das poucas investigações realizadas, os resultados encontrados são mistos. Alshalan (2006), por exemplo, não encontrou uma associação direta entre o rendimento e o medo do cibercrime. No entanto, na referida investigação, os participantes que não indicaram qual os seus rendimentos relataram níveis mais altos de medo. Outros autores observaram que indivíduos de estatuto socioeconómico mais baixo apresentam mais medo de cibercrime (e.g., Brands & Wilsem, 2019; Guedes *et al*., 2022; Virtanen, 2017). Concretamente, no estudo de Virtanen (2017), chegou-se à conclusão de que a experiência de ser vítima de fraude *online*, aumentou o nível de medo dos indivíduos de estatuto social baixo, sugerindo que estes indivíduos são mais afetados pela vitimação contra a propriedade. Por fim, quanto à perceção do risco, na investigação realizada por Reisig e colegas (2009), os autores concluíram que indivíduos com o estatuto socioeconómico mais baixo apresentavam uma perceção de risco de vitimação maior quanto ao furto de cartão de crédito *online* e, quanto à raça, as minorias apresentavam uma relação com a perceção do risco. Tudo isto, levou a que os autores concluíssem que a perceção do risco está relacionada com a vulnerabilidade social, pois, tal como foi visto anteriormente, são as minorias e as pessoas de estatuto socioeconómico baixo, que registam maior perceção do risco de vitimação por furto de cartão de crédito *online* (Reisig *et al*., 2009).

Apesar dos resultados mencionados anteriormente, Roberts e colaboradores (2013) constataram que o medo de furto de identidade *online* é comum a todos os grupos socioeconómicos, ou seja, não verificaram diferenças ao nível do medo consoante o estatuto socioeconómico. No que toca à perceção do risco de vitimação, o estudo de Reisig e colegas

(2009) encontrou que os indivíduos com maior perceção do risco de vitimação por furto de identidade *online*, pertenciam a um estatuto socioeconómico mais baixo. Para explicar este resultado os autores recorreram à hipótese da vulnerabilidade financeira, isto é, as pessoas com rendimentos mais baixos apresentam maiores dificuldades no momento de repor as perdas que ocorrem na sequência de uma vitimação (Skogan & Maxfield, 1981).

5.3.4. Nível de escolaridade

Ao nível dos crimes tradicionais, tem-se encontrado uma relação negativa entre o medo do crime e a escolaridade, ou seja, os indivíduos com menos escolaridade são os que apresentam mais medo (e.g., Smith & Hill, 1991). Quanto ao medo do cibercrime, o estudo de Roberts e colaboradores (2013), não encontrou relação entre o nível de educação e o medo de furto de identidade e fraude *online*. Contrariamente, o estudo de Brands e Wilsem (2019) concluiu que indivíduos com níveis de educação mais elevados apresentavam níveis mais baixos de medo do cibercrime. Por sua vez, Akdemir (2020) verificou que os indivíduos com maiores níveis de escolaridade tinham mais probabilidade de adotar medidas de segurança *online*, como por exemplo, alteração de palavras-passes com regularidade e eliminação de e-mails suspeitos. Para além disso, constatou que quem tinha níveis mais elevados de escolaridade e, igualmente, um rendimento anual maior, reportava mais medo do cibercrime, quando comparado com indivíduos menos escolarizados e com menores rendimentos.

5.3.5. Nível de conhecimento informático

No que diz respeito às competências técnicas ou nível de conhecimento informático, são poucas as investigações que procuram estudar de que forma esta se pode relacionar com o medo de cibercrime (e.g., Guedes *et al*., 2022; Virtanen, 2017). Segundo Virtanen (2017), a falta de confiança nas habilidades e conhecimento para utilizar a *Internet* pode aumentar o nível de medo de vitimação *online*, já que a não familiarização com a mesma faz com que as pessoas não saibam lidar com as consequências do cibercrime, especialmente no que toca às ofensas focadas no computador, como o *hacking* e os vírus. Esta falta de conhecimento pode, também, aumentar os julgamentos de risco já que um indivíduo pode percecionar-se como mais vulnerável *online* do que as pessoas que possuem esse conhecimento (Virtanen, 2017). Na investigação realizada por Guedes e colaboradores (2022), o nível de conhecimento informático teve uma relação com o medo de furto de identidade *online*, observando-se que, indivíduos que reportam ter menos conhecimento informático, apresentam níveis superiores de medo de furto de identidade *online*. Contrariamente, no estudo pioneiro de Virtanen (2017), estar incluído

num grupo que se perceciona como tendo menos conhecimento informático, não foi um preditor direto de medo de furto de identidade *online*.

5.3.6. Vitimação direta e indireta

No estudo da vitimação direta quanto aos crimes tradicionais, a tese da vitimação tem estabelecido que há uma relação positiva entre experiência de vitimação e o medo, isto é, os indivíduos que já foram vitimados apresentam maior probabilidade de sentirem medo do crime (Skogan & Maxfield, 1981). Contudo, os resultados encontrados nas investigações têm sido mistos (Hale, 1996). No que ao cibercrime diz respeito, tem-se demonstrado que a vitimação tem importância ao nível da insegurança *online*. Alshalan (2006), por exemplo, observou que a experiência prévia de vitimação aumentava o nível de medo de cibercrime, pois as vítimas reportavam uma sensação de insegurança *online*. Depois de analisar esta variável em função do género, o mesmo autor concluiu que as mulheres que tinham sido previamente vitimadas, reportavam níveis mais elevados de medo do cibercrime, em comparação com as mulheres que nunca foram vítimas. Também no estudo de Randa (2013), as experiências anteriores de *cyberbullying* aumentavam o medo de vitimação *online*. Yu (2014), numa investigação focada na burla *online*, *cyberbullying*, vírus informático e pirataria, constatou que apenas o *cyberbullying* e vírus informático eram afetados pela experiência prévia de vitimação *online*. Por fim, Henson e colaboradores (2013), Virtanen (2017), Lee e colaboradores (2019) e Brands e Wilsem (2019) sugerem que a vitimação prévia tem impacto no medo do crime *online*.

No que concerne à vitimação indireta, ou seja, a vitimação vivida por amigos, conhecidos e/ou familiares, é comumente estabelecido que o sentimento de vulnerabilidade pessoal aumenta quando o indivíduo realiza comparações entre si e a vítima (Hale, 1996). Russo e Roccato (2010) consideram que lidar com a vitimação indireta é mais complexo do que ser-se efetivamente vítima de um crime, primeiramente porque é algo que ocorre com mais frequência e, quando o indivíduo se identifica com a vítima, resulta no reforço da vitimação indireta. No contexto cibernético não tem sido encontrada esta relação positiva entre vitimação indireta e medo do cibercrime (Alshalan, 2006; Henson *et al.*, 2013). Segundo Alshalan (2006) a vitimação do outro não afeta a sensação de vulnerabilidade que a pessoa tem sobre si mesma e, ao mesmo tempo, a pessoa pode percecionar-se como capaz de se proteger, logo não se identificam com a vítima. No entanto, importa destacar que Henson e colaboradores (2013) encontraram uma relação significativa, mas negativa, quanto à relação entre vitimação indireta

e o medo do cibercrime, ou seja, os indivíduos que conheciam alguma vítima de crime *online* apresentavam menos medo de vitimação interpessoal *online*.

5.3.7. Medo geral do crime

Nas investigações de Roberts e colaboradores (2013), Martins (2018) e Guedes e colaboradores (2022), o medo geral do crime foi um preditor do medo de furto de identidade *online*. No entendimento dos investigadores, existem uma componente generalizada de medo que inclui tanto o medo tradicional como o medo que é sentido *online*, sugerindo que o medo do crime é um fator disposicional geral (Guedes *et al*., 2022; Martins, 2018; Roberts *et al*., 2013). Os autores acrescentam que este resultado diz mais acerca da pessoa do que propriamente acerca dos reais riscos de vitimação ou sobre contextos situacionais que possam estar relacionados com o furto de identidade *online* (Roberts *et al*., 2013). Também na investigação realizada por Guedes (2018) foi encontrada uma correlação positiva entre o medo disposicional e o medo do crime o que vai de encontro ao que Gabriel e Greve (2003) defendem, isto é, o medo de situações concretas está relacionado com uma tendência geral de sentir medo.

5.3.8. Variáveis contextuais

Um fator explicativo do medo de crime que tem sido alvo de atenção nos últimos anos, no que aos crimes tradicionais diz respeito, é a exposição ao risco. Segundo a TAR, os indivíduos que passam mais tempo fora de casa, terão como resultado a alteração do nível de exposição ao risco de vitimação. Segundo os autores desta teoria, a maior exposição ao risco, com base nas atividades de rotina, aumenta o risco de vitimação (Cohen & Felson, 1979). Embora existam algumas investigações que analisam a influência deste fator na vitimação *online*, o mesmo não se verifica para o medo do cibercrime, talvez pelo facto de existirem poucas investigações.

Dos poucos estudos realizados, a exposição ao risco tem sido operacionalizada através do tempo que o indivíduo passa *online* ou através de um conjunto de atividades desempenhadas *online* (e.g., uso de banco *online*). Por exemplo, Roberts e colaboradores (2013) encontraram uma associação entre a frequência do uso da *Internet* e níveis mais elevados de medo de furto de identidade *online* e atividade fraudulenta. Por outro lado, Alshalan (2006) não encontrou nenhuma correlação significativa. No estudo de Henson e colaboradores (2013), que mediram o tempo despedido *online* e, também, as atividades realizadas, descobriram que nenhuma das atividades teve efeito no medo de vitimação interpessoal *online*, o que pode ser explicado pelo facto da exposição ao risco ter efeitos diferentes nos crimes tradicionais e nos crimes cibernéticos. Por fim, Virtanen (2017) observou que a frequência do uso da *Internet* não está

associada ao medo do cibercrime nos modelos que criou com o género, estatuto social e vitimação. No entanto, o autor sugeriu que os efeitos do uso da *Internet* e o conhecimento dos riscos são mediados pelo já mencionado nível de conhecimento informático. Em suma, os resultados encontrados são mistos.

Capítulo II: Estudo Empírico

Metodologia

Neste capítulo, focado na descrição do estudo empírico, serão expostos os objetivos, tanto gerais como específicos desta e serão apresentadas as hipóteses a testar. Posteriormente, será realizada a caracterização do estudo, da amostra e a construção do instrumento onde se irá descrever a operacionalização das variáveis desta investigação. Por último, serão descritos os procedimentos de recolha de dados e os procedimentos de análise estatística.

Objetivos gerais e específicos

A presente investigação tem **dois objetivos gerais**: i) estabelecer uma comparação da vitimação e de sentimento de insegurança relativo ao furto de identidade *online* num momento pré e pós-pandemia do Covid-19 e ii) explorar a relação entre variáveis individuais (e.g., género, idade, estatuto socioeconómico) e contextuais (e.g., variáveis que derivam da TAR) com as duas variáveis dependentes do presente estudo: vitimação e sentimento de insegurança de furto de identidade *online*.

Destes objetivos gerais decorrem os seguintes **objetivos específicos**:

a) Analisar a relação entre variáveis individuais (género, idade, perceção do estatuto socioeconómico e habilitações literárias), contextuais (exposição *online*, alvo adequado e guardião eficaz) e a experiência de vitimação por furto de identidade *online*;

b) Estudar a relação entre as variáveis do sentimento de insegurança *online* (medo do furto de identidade *online* e perceção do risco) e as variáveis sociodemográficas que têm sido estudadas em investigações anteriores (género, idade e perceção do estatuto socioeconómico);

c) Perceber a relação entre as variáveis constituintes do sentimento de insegurança, acima descritas, e exposição ao risco *online*, atividades de risco *online* e guardiões (variáveis que derivam da TAR);

d) Analisar a relação entre os elementos constituintes do sentimento de insegurança, previamente descritas, e a vitimação direta e indireta *online*;

e) Analisar a relação entre o medo e perceção do risco de furto de identidade *online* e o medo geral do crime.

f) Perceber a evolução em termos de prevalência e incidência do furto de identidade *online* antes e depois da pandemia Covid-19.

g) Estudar a eventual mudança de rotinas *online* durante e após a pandemia de Covid-19.

Hipóteses

Enumerados os objetivos gerais e específicos deste estudo, seguem-se as hipóteses a testar ao nível da vitimação e do sentimento de insegurança por furto de identidade *online*.

Vitimação

H1: Os homens são mais vítimas de furto de identidade *online* do que as mulheres.

H2: A idade influencia a probabilidade de vitimação por furto de identidade *online*.

H3: Os indivíduos com estatuto socioeconómico mais elevado apresentam maior probabilidade de serem vítimas de furto de identidade *online*.

H4: O nível de educação influencia a vitimação por furto de identidade *online*.

H5: Durante e após a pandemia o nível de exposição *online*, a adequação ao alvo e o guardião eficaz aumentaram.

H6: Quanto mais os individuos se expõem *online*, maior a probabilidade de serem vítimas de furto de identidade *online*.

H7: Quanto mais atividades de risco os individuos realizam *online*, maior a probabilidade de vitimação por furto de identidade *online*.

H8: Quanto mais comportamentos de segurança os indivíduos adotam *online*, menor a probabilidade de serem vítimas de furto de identidade *online*.

H9: Quanto maior o conhecimento informático, menor a probabilidade de ser vítima de furto de identidade *online*.

H10: A vitimação de furto de identidade *online*, direta e indireta, aumentou após a pandemia.

H11: O medo geral do crime influencia os níveis de medo e perceção de furto de identidade *online*.

Sentimento de Insegurança

H12: As mulheres reportam mais medo de furto de identidade *online* e perceção do risco do que os homens.

H13: A idade influencia o medo de furto de identidade *online* e a perceção do risco de vitimação por furto de identidade *online*.

H14: O estatuto socioeconómico influencia o medo e a perceção do risco de furto de identidade *online*.

H15: O nível de educação influencia o nível de medo e de perceção do risco de furto de identidade *online*.

H16: A exposição ao risco *online* influencia os níveis de medo de furto de identidade *online* e perceção do risco de vitimação.

H17: Quanto mais atividades de risco desenvolvem *online*, maior o medo de furto de identidade *online* e perceção do risco de vitimação.

H18: Quanto maior a adoção de guardiões eficazes, menor o medo de furto de identidade *online* e a perceção do risco de vitimação.

H19: Quanto maior o conhecimento informático, menor o medo furto de identidade *online* e a perceção do risco de vitimação.

H20: Quanto mais medo geral os indivíduos reportam, maior o medo e perceção do risco de furto de identidade *online*.

H21: Após a pandemia do Covid-19 os indivíduos reportam mais medo e perceção do risco de furto de identidade *online*.

Caracterização do estudo

Para alcançar, tanto os objetivos, como as hipóteses estabelecidas, foi aplicado um questionário *online* que permitiu uma posterior análise de dados através de diversos procedimentos estatísticos e, por esse motivo, este é um estudo de cariz quantitativo (Creswell, 2009). Para além disso, este estudo é considerado correlacional, ou não experimental, na medida em que, não há uma intervenção ou controlo sobre as variáveis, o investigador limita-se a observar as mesmas (Marôco, 2014). Finalmente, caracteriza-se por ser não só um estudo descritivo, já que procura descrever as variáveis e estabelecer relações entre as mesmas, mas também, explicativo, dado que procura explicar a relação entre um conjunto de variáveis (individuais e contextuais) e as referidas variáveis dependentes em análise.

Constituição da amostra

A amostra deste estudo é composta por 730 individuos, sendo essencialmente, na sua maioria, constituída por estudantes, *staff* docentes e não docentes da Universidade do Porto, visto que, o questionário foi enviado por e-mail a toda a comunidade académica, mediante

autorização prévia da Reitoria da Universidade do Porto. Para além disso, também se procedeu à disseminação do questionário nas redes sociais mais usadas em Portugal (e.g., *Facebook*, *LinkedIn*, *WhatsApp* e *Instagram*). Esta forma de divulgação do questionário *online* justifica-se pela maior celeridade no processo de recolha de dados e, ainda, porque é um modo de obter uma amostra mais alargada. Por fim, já que o fenómeno em estudo- furto de identidade *online*- ocorre em contexto digital, pareceu pertinente que o questionário tenha sido aplicado nesse mesmo contexto. Por todos os motivos enunciados, esta é uma amostragem por conveniência, dado que as respostas ao questionário dependem da vontade de cada indivíduo participar no estudo, e, adicionalmente, não probabilística, na medida em que, não se assegura que todos os elementos têm igual probabilidade de serem incluídos no estudo (Marôco, 2014).

Instrumento e variáveis

Tal como supramencionado, de forma a atender aos objetivos e hipóteses da presente investigação, foi utilizado um questionário, já que, este é um instrumento que traduz os objetivos do estudo, através de variáveis mensuráveis, e que permite a recolha de dados de forma rigorosa (Creswell, 2009). Para efeitos de comparabilidade e fiabilidade, o presente questionário foi adaptado da investigação de Martins (2018) e Guedes e colaboradores (2022) onde, às questões originais, foram adicionadas outras que permitissem perceber os hábitos e rotinas *online* antes e após a pandemia. Posto isto, este questionário é composto por cinco grupos de questões que serão agora descritos.

Grupo I: Questões sociodemográficas

O primeiro grupo de questões debruçou-se sobre as características sociodemográficas dos participantes, nomeadamente o género, idade, habilitações literárias, situação profissional, profissão e perceção do estatuto socioeconómico. Com efeito, manteve-se do questionário original este conjunto de variáveis de forma a perceber a sua importância na explicação da vitimação e do sentimento de insegurança por furto de identidade *online*. A codificação das variáveis foi a seguinte: (0= masculino; feminino=1; outro=2), idade (medida em anos), as habilitações literárias (1= até ao 12º ano, 2= licenciatura, 3= pós-graduação, mestrado e doutoramento), a perceção do estatuto socioeconómico (1= baixo; 2=médio; 3=alto) e a situação profissional[23] (1= empregado por conta de outrem, 2= empregado por conta própria, 3= estudante universitário, 4= trabalhador-estudante, 5= reformado/ pensionista, 6= desempregado

[23] Na realização dos testes estatísticos esta variável não foi utilizada.

e 7= outro). Importa mencionar que, aquando da realização da regressão logística para a vitimação por furto de identidade *online*, se procedeu à dicotomização da variável habilitações literárias (0= sem licenciatura, 1= com licenciatura).

Grupo II: Questões contextuais

Na segunda secção do questionário foram colocadas questões relacionadas com a TAR e, mais especificamente, sobre os seus elementos centrais: exposição *online*, alvo adequado e guardião eficaz. Mais uma vez, por questões de fiabilidade, optou-se por manter as mesmas questões do questionário original.

a) Exposição online

A exposição *online* a ofensores motivados foi medida através de duas formas diferentes, mas complementares. Primeiramente, procurou-se saber quanto tempo os indivíduos despendiam por dia na *Internet*, e tendo por base a investigação de Bossler e Holt (2009), foi colocada a seguinte questão aberta "em média, quanto tempo, no total, passa por dia na *Internet*?". Sendo esta uma questão com resposta aberta, as respostas variaram de 1 hora a 24 horas. Nas questões seguintes, pretendia-se saber qual é o número de horas que os indivíduos passavam na *Internet* em quatro locais distintos, nomeadamente, em casa, no local onde estudam/trabalham, em locais públicos e nos estabelecimentos comerciais, sendo que estas questões não têm cariz obrigatório, ou seja, os indivíduos só responderiam caso utilizassem a *Internet* nos locais referidos. Posto isto, as opções de resposta para os quatro locais foram: menos de 1 hora, 1 hora, 2 horas, 3 horas, 4 horas e mais de 4 horas. Para cada um dos locais foi criada uma variável dicotómica (0= não; 1= sim) de forma a indicar se determinado sujeito utilizava, ou não, a *Internet* em casa, no local onde estuda/trabalha, em locais públicos e em estabelecimentos comerciais.

Para além disso, foi colocada a seguinte questão "com que frequência realiza as seguintes atividades na *Internet*?". As atividades incluídas nas opções de resposta foram originalmente baseadas do estudo de Reyns (2013) e os participantes podiam responder numa escala de *Likert* que variava de 1 (Nunca) a 5 (Sempre). Concretamente, as atividades incluídas foram: (1) uso do banco online ou gestão de finanças; (2) uso do e-mail ou mensagens instantâneas; (3) ver televisão ou ouvir rádio; (4) ler jornais ou *websites* de notícias; (5) participar em salas de chat ou outros fóruns; (6) ler ou escrever *blogs*; (7) fazer downloads de músicas, filmes, jogos ou podcasts; (8) utilização de redes sociais (*Facebook*, *LinkedIn*, *Instagram*, *Twitter*, etc.); (9) suporte de trabalho ou estudo; (10) comprar bens ou serviços na *Internet*. De forma a agrupar

as atividades *online* em categorias, foi realizada uma análise fatorial exploratória (anexo 1), tendo-se encontrado três grandes grupos: rotinas financeiras (itens 1 e 10), rotinas de trabalho (itens 2 e 9) e rotinas de lazer (itens 3,5,6 e 7). Por fim, foi pedido aos participantes que indicassem quais a(s) forma(s) de pagamento que utilizavam *online*. As opções de resposta foram as seguintes: Paypal, Cartão de Crédito, Mbnet (criação de cartões virtuais para pagamentos não presenciais), Paysafecard, *homebanking* (transferência bancária), Mbway e "outra opção". Dado o elevado número de pagamentos que são realizados com recurso à aplicação Mbway e, consequentemente, as burlas e fraudes relacionadas com a mesma, foi pertinente, nesta investigação, adicionar esta aplicação como uma das formas de pagamento possíveis *online*. As respostas eram dicotómicas (0= não; 1= sim).

b) Alvo adequado

Para operacionalizar a variável alvo adequado aplicou-se, no questionário original (Martins, 2018), tendo-se mantido no presente estudo, a escala desenvolvida por Ngo e Paternoster (2011). Assim sendo, perguntou-se ao participante se nos últimos 12 meses: (1) comunicou com desconhecidos *online*, (2) forneceu dados pessoais a alguém desconhecido, (3) abriu anexos desconhecidos dos e-mails que recebeu, (4) abriu algum link desconhecido dos e-mails que recebeu, (5) abriu algum ficheiro ou anexo recebido por mensagens instantâneas de alguém desconhecido, (6) clicou em mensagens *pop-up*, ou (7) visitou websites duvidosos. Para esta questão, as opções de resposta eram dicotómicas (0= não; 1= sim). Depois ter sido efetuada a análise fatorial (anexo 2), foram criados três índices: interação com estranhos (itens 1 e 2), abrir links duvidosos (itens 3, 4 e 5) e visitar conteúdos de risco (itens 6 e 7).

c) Guardiões eficazes

Por sua vez, na operacionalização da terceira dimensão da TAR, guardião eficaz, foram analisados 13 comportamentos que, perante a sua presença, podem ter a capacidade de reduzir os riscos de vitimação. Assim, foi questionado à amostra se por razões de segurança: (1) evita utilizar o banco *online*, (2) evita fazer compras *online*, (3) utiliza apenas um computador, (4) utiliza o filtro spam no e-mail, (5) altera as definições de segurança, (6) utiliza diferentes palavras-passe para diferentes sites, (7) evita abrir e-mails de pessoas que não conhece, (8) visita apenas websites fidedignos, (9) tem instalado e atualizado *software* antivírus, (10) tem instalado e atualizado *software antispyware*, (11) tem instalado e atualizado *software* ou *hardware firewall*, (12) participa em workshops destinados à educação pública sobre o cibercrime, ou (13) visita websites destinados à educação pública sobre o cibercrime. As opções

de resposta foram dicotómicas (0= não; 1= sim), mantendo-se o estudo original. Note-se que, os itens 1 a 8 foram adaptados do estudo de Williams (2016), enquanto os itens 9 a 13 foram adaptados da investigação de Ngo e Paternoster (2011). Realizada a análise fatorial exploratória (anexo 3), verificou-se a possibilidade de os comportamentos de segurança serem agregados em quatros grupos: comportamentos de evitamento (itens 1 e 2), proteção do *software*/ *hardware* (itens 9, 10 e 11), comportamentos de proteção (itens 4,5 e 6) e informação/ educação (itens 12 e 13). Por fim, de forma a averiguar qual o nível de conhecimento informático dos participantes manteve-se a adaptação de uma questão da investigação de Holt e Bossler (2013), tendo sido questionado "qual o considera ser o seu nível de conhecimento informático?" à qual os participantes podiam responder com básico (=1), médio (=2) e avançado (=3).

Grupo III: Vitimação online

Neste grupo foram colocadas questões relativamente à vitimação direta e indireta por furto de identidade *online* e, ainda, foi coloca uma questão relacionada com a perceção de vitimação direta por cibercrimes nos últimos 12 meses. Também neste grupo se mantiveram as questões originais do questionário de Martins (2018) e Guedes e colaboradores (2022).

a) Vitimação por furto de identidade online

De modo a analisar a experiência de vitimação direta por furto de identidade *online* foi colocada a seguinte questão "nos últimos 12 meses, quantas vezes alguém se apropriou, via *Internet*, dos seus dados pessoais e financeiros sem o seu consentimento ou conhecimento prévio e utilizou-se de forma indevida?*"*, sendo que as respostas, depois da recodificação, foram dicotomizadas (0= não; 1= sim). Para além disso, de forma a saber se ao longo da vida já tinha sido vítima de furto de identidade *online* colocou-se a seguinte questão "ao longo da sua vida, quantas vezes alguém se apropriou, via *Internet*, dos seus dados pessoais e financeiros sem o seu consentimento ou conhecimento prévio e utilizou-se de forma indevida?". As opções de resposta variavam entre 0 a mais de 5 vezes, contudo, após a recodificação tornaram-se dicotómicas (0= não; 1= sim). Ressalva-se que, na realização dos testes estatísticos, se optou pela utilização da vitimação ao longo dos últimos 12 meses. Quanto à vitimação indireta por furto de identidade *online*, foi colocada a seguinte questão "conhece algum familiar, amigo ou conhecido, em que por via *Internet*, se apropriaram dos seus dados pessoais e financeiros e os utilizaram de forma indevida?" sendo a opção de resposta dicotómica (0= não; 1= sim).

Em relação à perceção de vitimação direta de um qualquer crime cometido *online*, foi questionado ao participante se *"*pensa ter sido vítima de crime *online* nos últimos 12 meses?*"* sendo a opção de resposta dicotómica (0= não; 1=sim).

Grupo IV: Sentimento de Insegurança

a) Sentimento de Insegurança em relação ao furto de identidade online

De forma a analisar o medo de furto de identidade *online*, componente emocional do sentimento de insegurança, manteve-se a questão original dos questionários de Martins (2018) e Guedes e colaboradores (2022) – por questões de fiabilidade – nos quais foi utilizada e adaptada a escala de Hille e colaboradores (2015), utilizando-se apenas três itens da escala que foi utilizada pelos autores na sua investigação. Assim sendo, foi questionado aos participantes: "numa escala de 1 (muito medo) e 4 (nenhum medo), quanto medo tem de as seguintes situações lhe ocorrem? (1) alguém furtar os seus dados pessoais e financeiros via *online*, (2) alguém utilizar os seus dados pessoais e financeiros *online* para obter ganhos financeiros e (3) alguém danificar a sua reputação com base na utilização ilegítima dos seus bens pessoais e financeiros *online*". Depois de recodificada a escala de forma inversa, procedeu-se à criação do índice para o medo de furto de identidade *online*, cuja consistência interna foi de .882 (anexo 4).

No que toca à perceção do risco de vitimação por furto de identidade *online*, a componente cognitiva do sentimento de insegurança, foi questionado aos participantes "numa escala de 1 (nada provável) a 5 (muito provável) quão provável acha de as seguintes situações lhe acontecerem?", para a qual, as opções de resposta foram as seguintes: "alguém utilizar os seus dados pessoais e financeiros *online* para obter ganhos financeiros, nos próximos 12 meses?" e "alguém danificar a sua reputação com base na utilização ilegítima dos seus dados pessoais e financeiros *online* nos próximos 12 meses?". As opções de resposta iam de 1 (nada provável) a 5 (muito provável). Criado o índice da perceção do risco de furto de identidade *online* o valor da consistência interna foi de .822 (anexo 4).

b) Sentimento de Insegurança em contexto virtual e não virtual

Relativamente ao contexto virtual, foram adaptadas medidas globais de medo do crime para medir o nível de insegurança na *Internet*, mantendo-se a questão original da investigação de Martins (2018) e Guedes e colaboradores (2022). Assim sendo, aos participantes, foi pedido que indicassem o seguinte: "numa escala de 1 (muito inseguro) e 5 (muito seguro) quão seguro(a) se sente quando utiliza a *Internet*?". No que toca ao contexto não virtual recorreu-se à componente do medo do crime através da operacionalização de dois itens, nomeadamente:

"como se sente quando caminha sozinho(a) nas suas zonas de residência, depois de escurecer?" e "como é que se sente quando está sozinho(a) na sua casa, depois de escurecer?". Para ambas as questões, as opções de resposta variavam numa escala *Likert* de 5 pontos, indo de 1 (muito inseguro) a 5 (muito seguro). Para o medo geral foi criado um índice cuja consistência interna, ou seja, o valor do alfa de *Cronbach*, apresentava o valor de .389 (anexo 5).

Grupo V: Covid-19 e Cibercrime

Visto que, um dos objetivos deste estudo é estabelecer uma comparação quanto à vitimação e sentimento de insegurança de furto de identidade *online* entre o momento pré e pós pandemia de Covid-19, afigurou-se necessária a criação de uma nova secção de questões direcionadas especificamente ao período da pandemia. Nas próximas linhas será descrita a referida secção.

a) Perceção de vitimação direta de um crime online durante a pandemia

Quanto à perceção de vitimação direta de um crime *online* durante a pandemia, foi apresentado um conjunto de situações, perante as quais os participantes deveriam indiciar se aconteceram, ou não, consigo, tendo sido as respostas dicotomizadas (0= não; 1= sim). Como já foi visto anteriormente, verifica-se uma tendência de aumento do cometimento de cibercrime em Portugal (Gabinete do Cibercrime, 2021; Observatório de Cibersegurança, 2021, 2022) e, por esse motivo, e para perceber quais as situações de vitimação mais prevalentes na amostra, foram incluídos para alem do furto de identidade *online*, situações de *cyberbullying*, *cyberstalking*, extorsão, *hacking*, *phishing*, descoberta de software malicioso, fraude ao consumidor *online* e fraude através do Mbway. A operacionalização foi a seguinte:

a) *Cyberbullying*: recebeu mensagens hostis ou agressivas que lhe causaram dano ou desconforto através da *Internet* ou outros dispositivos eletrónicos (Tokunaga, 2010);
b) *Cyberstalking*: alguém, de forma repetida e intencional, impôs formas indesejadas de comunicação, aproximação ou perseguição, através da *Internet* ou outro dispositivo eletrónico (Pereira & Matos, 2015);
c) Extorsão ou *blackmail*: alguém ameaçou revelar informações a seu respeito *online* caso não realizasse uma determinada ação, como por exemplo, o pagamento de determinada quantia monetária (Cahill, 2014);
d) Furto de identidade o*nline*: alguém se apropriou e usou, sem o seu consentimento, os seus dados pessoais ou financeiros para fins criminosos (Reyns, 2013; Saunders & Zucker, 1999);

e) Criação de perfil falso: alguém criou um perfil falso com os seus dados pessoais utilizando-os ilegalmente sem o seu consentimento (Solove, 2002);
f) *Hacking*: alguém tentou aceder, de forma não autorizada, aos seus dispositivos eletrónicos (Antunes & Rodrigues, 2018);
g) *Phishing*: recebeu e-mails ou mensagens fraudulentas a pedir informação pessoal (e.g., receber mensagens ou e-mails com link de um site falso que pede informações para efetuar um pagamento) (Antunes & Rodrigues, 2018);
h) Descoberta de *software* malicioso: descobriu algum *software* malicioso no seu dispositivo (e.g., vírus, cavalos de Troia, *spyware*) (Comissão Europeia, 2020);
i) Fraude ao consumidor *online*: comprou produtos ou serviços via *Internet* que não chegaram a sua casa, que eram falsificados ou que não eram iguais à forma como lhe foram anunciados (Comissão Europeia, 2020);
j) Fraude através do Mbway: alguma vez, numa compra e/ou venda *online*, foi vítima de burla por Mbway.

b) Exposição a ofensores motivados durante a pandemia de Covid-19[24]

Com o objetivo de perceber se existiu alguma alteração de rotinas *online* durante a pandemia, foram colocadas questões acerca da exposição *online* durante esse mesmo período temporal. Assim sendo, foi questionado aos participantes se a realização de determinadas rotinas *online* aumentou, diminuiu ou se se manteve igual. As rotinas sobre as quais se questionou foram as seguintes: (1) uso do banco *online* ou gestão de finanças; (2) uso do e-mail ou mensagens instantâneas; (3) ver televisão ou ouvir rádio; (4) ler jornais ou websites de notícias; (5) participar em salas de chat ou outros fóruns; (6) ler ou escrever blogs; (7) fazer downloads de músicas, filmes, jogos ou podcasts; (8) utilização de redes sociais (*Facebook*, *LinkedIn*, *Instagram*, *Twitter*, etc.); (9) suporte de trabalho ou estudo; (10) comprar bens ou serviços na *Internet*. Os itens desta questão foram retirados da investigação de Reyns (2013).

c) Alvo adequado durante a pandemia do Covid-19

De seguida, foi operacionalizada a variável do alvo adequado referente ao período da pandemia, sendo que, os itens foram retirados do estudo de Ngo e Paternoster (2011). Assim sendo, foi questionado aos participantes se durante a pandemia a frequência com que realizou um determinado conjunto de atividades aumentou, diminuiu ou manteve-se igual. As atividades

[24] No Grupo V, para a exposição *online*, alvo adequado, guardião eficaz e medo de furto de identidade *online* as respostas foram codificadas da seguinte forma: 1= aumentou; 2= diminuiu; 3= manteve-se.

incluídas foram as seguintes: (1) comunicou com desconhecidos *online*, (2) forneceu dados pessoais a alguém desconhecido, (3) abriu anexos desconhecidos dos e-mails que recebeu, (4) abriu algum link desconhecido dos e-mails que recebeu, (5) abriu algum ficheiro ou anexo recebido por mensagens instantâneas de alguém desconhecido, (6) clicou em mensagens *pop-up*, ou (7) visitou websites duvidosos.

d) Guardiões eficazes durante a pandemia de Covid-19

Ainda no que respeita à TAR, foi medida a variável de guardiões eficazes aplicada ao período da pandemia de Covid-19, tendo-se perguntado se a realização de determinados comportamentos aumentou, diminuiu ou se se manteve igual. As atividades incluídas foram as seguintes: (1) evita utilizar o banco *online*, (2) evita fazer compras *online*, (3) utiliza apenas um computador, (4) utiliza o filtro spam no e-mail, (5) altera as definições de segurança, (6) utiliza diferentes palavras-passe para diferentes sites, (7) evita abrir e-mails de pessoas que não conhece, (8) visita apenas websites fidedignos, (9) tem instalado e atualizado *software* antivírus, (10)) tem instalado e atualizado *software* ou *hardware firewall*, (11) participa em workshops destinados à educação pública sobre o cibercrime, ou (12) visita websites destinados à educação pública sobre o cibercrime. Importa ressalvar que os itens de 1 a 8 foram retirados do estudo de Williams (2016) e os itens de 9 a 13 foram do estudo de Ngo e Paternoster (2011).

e) Medo de furto de identidade online durante a pandemia de Covid-19

Por fim, foi operacionalizado o medo do furto de identidade *online* questionando-se ao participante se "considera que durante a pandemia, o medo que tinha das seguintes situações lhe ocorrerem aumentou, diminuiu ou manteve-se igual" para a qual as opções de resposta eram: (1) alguém furtar os seus dados pessoais e financeiros via *online*, (2) alguém utilizar os seus dados pessoais e financeiros *online* para obter ganhos financeiros e (3) alguém danificar a sua reputação com base na utilização ilegítima dos seus bens pessoais e financeiros *online*. Estas opções de resposta foram baseadas no estudo de Hille e colaboradores (2015).

Procedimento de recolha de dados

O presente questionário foi inserido com recurso à plataforma *Google Forms* e, só após a realização do pré-teste, foi divulgado quer na comunidade académica, quer nas redes sociais. Neste pré-teste, pretendia-se perceber se todas as questões eram percetíveis, se existiam erros e, ainda, qual era o tempo médio de resposta ao questionário, tendo-se o cuidado de selecionar pessoas de diferentes áreas às da Criminologia e, também, de distintas faixas etárias (n=5). Feito

o pré-teste, não houve necessidade de alterações significativas do questionário, somente o alerta para a adição da opção de resposta "outro" na questão relativa ao género e, feita esta alteração, procedeu-se à sua divulgação.

Inicialmente, foi realizado um Pedido de Emissão de Parecer à Comissão de Ética da Faculdade de Direito da Universidade do Porto, de modo a garantir que eram cumpridos e assegurados todos os pressupostos éticos nos quais devem assentar qualquer investigação. Neste pedido foram explanados os objetivos, a descrição do instrumento de recolha de dados, os procedimentos de análise e questões de ordem ética, nomeadamente a voluntariedade, anonimato e confidencialidade. De seguida, foi enviado um pedido à Reitoria da Universidade do Porto para que o questionário fosse enviado por e-mail dinâmico aos estudantes e *staff* desta comunidade académica, tendo ficado disponível durante um mês. Assim, obteve-se uma resposta positiva por parte da Universidade do Porto quanto à divulgação deste questionário visto que o mesmo não envolvia o tratamento de dados pessoais, já que, a partir do conjunto de dados recolhidos, foi garantido que não era possível identificar o respondente[25].

No que concerne aos princípios éticos a ter em conta, a parte inicial do questionário apresentava as informações atinentes aos procedimentos éticos informando-se os participantes sobre a voluntariedade, anonimato e confidencialidade. Com efeito, antes de os indivíduos responderem ao questionário eram apresentados os objetivos do estudo e o tempo de duração previsto de resposta ao questionário (entre 10 a 15 minutos). Ademais, os participantes eram informados de que a sua participação é totalmente voluntária e que os dados seriam utilizados exclusivamente para fins da presente investigação científica. Por último, foi, também, pedido que não colocassem os seus nomes em nenhuma secção do questionário por forma a não se identificarem os sujeitos e, ainda, era garantido que todos os dados fornecidos seriam utilizados exclusivamente para fins científicos (consultar anexo 24).

Procedimentos de análise estatística

Existem vários procedimentos estatísticos, tanto descritivos como inferenciais, que devem ser tidos em conta na análise dos dados. Assim sendo, numa fase inicial, foi criada a base de dados e, de seguida, foi feita a análise preliminar dos dados de forma a avaliar a qualidade da informação recolhida. Seguidamente, tiveram lugar os já referidos procedimentos de análise de

[25] O questionário foi inicialmente criado numa conta *Google* pessoal, teve de ser transferido para uma conta *Google for Education*, para garantir a não utilização dos dados por parte da *Google*, ou seja, estando o questionário numa conta pessoal, os dados dos participantes poderiam ser utlizados pela referida empresa, mesmo que não se conseguisse identificar a pessoa.

estatística descritiva e inferencial, que serão descritos nas próximas linhas. Importa referir que os dados foram analisados com o *software IBM SPSS Statistics* 27.

Procedimentos de análise estatística descritiva

A análise da estatística descritiva passou por recorrer a medidas de tendência central e a medidas de dispersão. No que diz respeito às variáveis quantitativas (e.g., idade), utilizaram-se medidas como a média amostral (M) e o desvio-padrão (SD), de forma a analisar a dispersão em relação ao valor médio (Marôco, 2014). Atendeu-se, ainda, à mediana e à moda para as variáveis qualitativas (e.g., género) e foram calculadas percentagens, visto a natureza destas variáveis não permitir calcular médias. Dado o tamanho amostral (n=730), seguindo o Teorema do Limite Central – segundo o qual à medida que o tamanho da amostra aumenta, a distribuição das médias amostrais tende a seguir distribuição normal – optou-se pela realização de testes paramétricos (Marôco, 2014).

De forma a medir a consistência interna de determinados conjuntos de itens, optou-se pela utilização do coeficiente alfa (α) de *Cronbach* no qual, mediante um α com valor compreendido entre .6 e .7 é considerado fraco, mas aceitável; com um valor entre .7 e .8 é tido como razoável; um valor compreendido entre .8 e .9 é considerado bom; e, por último, um α maior do que .9 é considerado excelente (Hill & Hill, 1998, p. 20). De forma a agrupar os itens em fatores, foram realizadas análises fatoriais, recorrendo-se ao método de rotação *Varimax* com Normalização de Kaiser e, posteriormente, analisou-se o valor do alfa de *Cronbach* para aferir a consistência interna do conjunto de itens que originou a escala (e.g., variáveis contextuais derivadas da TAR). Por fim, foram realizados Testes t para amostras independentes, testes Qui-Quadrado e testes *ANOVA*. Os Testes t foram utilizados com o objetivo de analisar as diferenças de médias entre dois grupos, na presença de uma variável qualitativa e outra quantitativa (e.g., vitimação por furto de identidade *online* e idade). Já o Teste Qui-Quadrado (X^2) foi utilizado para análise de diferenças entre dois ou mais grupos independentes quando se trata de variáveis nominais ou ordinais (e.g., vitimação por furto de identidade *online* e género). Já o teste *ANOVA* é utlizado quando uma das variáveis apresenta três ou mais grupos independentes (e.g., medo de furto de identidade *online* e estatuto socioeconómico), considerando-se que os resultados atingem significância estatística quando o valor do *p. value* < *.05.*

Procedimentos de análise estatística inferencial

Para se proceder à análise correlacional das variáveis recorreu-se ao coeficiente de correlação de Pearson, de forma a avaliar a intensidade e direção da associação entre as

variáveis sendo que esta medida de associação varia entre -1≤ R ≤+1. Segundo Cohen (1988), se a correlação obtiver um valor entre -1 e -0.5 ou entre .05 e 1 é considerada correlação elevada. Já as correlações com um valor entre -0.5 e -0.3 e 0.3 e 0.5 são consideradas moderadas. Por fim, as correlações com um valor situado entre -0.3 e 0 e entre 0 e 0.3 são consideradas fracas. Importa ainda ressalvar que as correlações só obtêm significância estatística se o $p< 0.05$ perante um intervalo de confiança de 95%.

Por fim, foram realizadas regressões lineares (para as variáveis quantitativas medo e risco percebido de furto de identidade online) e regressões logísticas (para a variável qualitativa vitimação por furto de identidade *online*) com o objetivo de saber quais as variáveis independentes que melhor prediziam as variáveis dependentes. Numa fase inicial, realizaram-se modelos parcelares, um com as variáveis individuais (e.g., género, idade, estatuto socioeconómico, habilitações literárias, medo geral do crime, vitimação por furto de identidade *online*) e outro com as variáveis contextuais (e.g., exposição *online*, alvo adequado e guardião eficaz). Por último, foi testado um modelo final no qual foram incluídas as variáveis independentes que obtiveram significância estatística nos modelos parcelares iniciais. Importa ressalvar que, nos modelos de regressão linear, se atendeu aos valores do R, R^2, R^2 ajustado e ao valor de β. Já no modelo de regressão logística teve-se em conta os valores do -2 (Log likelihood) e do pseudo R ao quadrado de Nagelkerke.

Capítulo III: Análise dos resultados

1. Resultados descritivos

1.1. Caracterização sociodemográfica da amostra

Na tabela 1 é possível observar as frequências e respetivas percentagens dos dados sociodemográficos que caracterizam tanto a amostra do estudo realizado em 2018 (n=831), antes da pandemia de Covid-19 (Martins, 2018; Guedes *et al.*, 2022) como da amostra deste estudo realizado após a pandemia (n=730).

Tabela 1: Características sociodemográficas de ambas as amostras (antes e depois do Covid-19)

	COVID			
	Antes		**Depois**	
	N	**%**	**N**	**%**
Género				
Feminino	549	66.1	521	71.4
Masculino	282	33.9	209	28.6
Habilitações literárias				
Até ao 12º ano	329	39.6	321	44

Licenciatura	269	32.4	246	33.7
Pós-graduação, Mestrado ou Doutoramento	232	27.9	161	22.1
Situação profissional				
Empregado(a) por conta de outrem	192	23.1	122	16.7
Empregado(a) por conta própria	15	1.8	19	2.6
Estudante universitário	555	66.7	473	64.8
Trabalhador-estudante	50	6	90	12.3
Reformado(a)	2	0.2	7	1
Desempregado(a)	8	1	15	2.1
Outro	10	1.2	3	0.4
Estatuto socioeconómico				
Baixo	110	13.2	99	13.6
Médio	674	81.1	594	81.4
Alto	47	5.7	37	5
	M±SD	**Min-Max**	**M±SD**	**Min-Max**
Idade	27.13±11.07	17-68	26.29±11.76	18-75

Quanto ao género, verifica-se que a amostra pós-Covid é composta, na sua maioria, por pessoas do género feminino (70.4%). Em termos de habilitações literárias, verifica-se que uma grande percentagem da amostra (44%) estudou até ao 12º ano, licenciatura (33.7%) e pós-graduação, mestrado ou doutoramento (22.1%). No que concerne à situação profissional, como expectável, uma grande parte dos indivíduos da amostra são estudantes universitários (64.8%). Com menor percentagem encontram-se os trabalhadores por conta de outrem (16.7%), os trabalhadores-estudantes (12.3%), os empregados por conta própria (2.6%), os desempregados (2.1%) e os reformados (1%). Relativamente à perceção do estatuto socioeconómico, uma grande percentagem dos indivíduos da amostra, perceciona-se como tendo um estatuto médio (81.4%), registando-se menor frequência no estatuto baixo (13.6%) e no estatuto alto (5%). Por fim, em termos da variável idade, observa-se que o indivíduo mais novo desta amostra tem 18 anos e o mais velho tem 75 anos, sendo que, a média de idades é de M= 26.29 e o desvio-padrão de 11.76. Perante os dados apresentados na tabela 1, constata-se que os dados de ambas as amostras não diferem substancialmente.

1.2. Resultados descritivos das variáveis vitimação, medo e risco percebido de vitimação

A próxima tabela (2) apresenta os resultados descritivos das variáveis vitimação por furto de identidade *online* nos últimos 12 meses, medo geral, medo de furto de identidade *online* e perceção do risco de vitimação por furto de identidade *online*.

Tabela 2: Resultados descritivos das variáveis vitimação, medo e risco percebido de furto de identidade *online*

	COVID				
	Antes		Depois		
	N (%)	M±SD	N (%)	M±SD	*p*
Vitimação					
Vitimação por furto de identidade online (últimos 12 meses)	5.8% (48)		8.5% (62)		**.036**
Vitimação por furto de identidade online (ao longo da vida)	19.5% (162)		24.4% (178)		**.012**
Vitimação indireta	37.7% (347)		47.5% (660)		**.001**
Perceção de vitimação online		.06±.240		.10±.31	**.002**
Medo					
Medo geral do crime		2.34±.85		2.40±.72	.089
Medo de furto de identidade online		3.10±.81		3.13±.75	.447
Risco					
Risco percebido de furto de identidade online		2.10±.77		2.11±.67	.718

Os resultados da tabela 2 indicam que, em termos de vitimação por furto de identidade *online* nos últimos 12 meses, os indivíduos foram mais vítimas na amostra pós-Covid, observando-se que 8.5% reportam ter sido vítimas, enquanto na amostra pré-Covid se registaram 5.8% (p=.036). Na mesma linha, verifica-se que a vitimação por furto de identidade ao longo da vida aumentou na amostra pós-Covid (p=.012). A mesma tendência é observada no que toca à vitimação indireta, visto que, na amostra pós-Covid, as pessoas reportam conhecerem mais amigos e familiares que foram vítimas de furto de identidade *online* do que na amostra pré-Covid (p=.001). Por fim, quanto ao medo, tanto ao nível do medo geral do crime (p=.089), como ao nível do medo de furto de identidade *online* (p=.447), os resultados não atingem significância estatística, sendo que o mesmo sucede com a perceção do risco de vitimação por furto de identidade *online* (p=.718). Logo, comparando os períodos pré e pós pandemia, observa-se a ausência de alterações estatisticamente significativas nestas variáveis.

1.3. Atividades de rotina online antes e após o Covid-19

Nesta investigação pretende-se perceber se as atividades de rotina *online* se alteraram com a pandemia e, se sim, quais foram essas modificações. Considerando os valores apresentados pelas amostras (ver anexo 6), parece existir uma tendência de aumento da exposição *online* na amostra pós-Covid na medida em que, como esperado, os indivíduos passaram mais tempo *online* (*p*=.002) para realizar as suas rotinas financeiras (*p*=.001), de trabalho (*p*=.029) e, também, de lazer (*p*=.001). Ainda no que concerne à exposição, mais especificamente quanto ao método de pagamento utilizado *online*, na amostra pós-Covid os indivíduos indicaram utilizar mais o homebanking (*p*=.001) e o cartão de crédito (*p*=.001) como forma de pagamento e menos o Mbnet (*p*=.001). Adicionalmente, constata-se que na amostra pós-Covid, a forma de pagamento mais utilizada pelos indivíduos é o Mbway (65.1%)[26] seguido, desde logo, pelo cartão de crédito (56.5%) e, na amostra pré-Covid, a forma de pagamento preferencial foi o cartão de crédito (34.5%). No que respeita ao alvo adequado, operacionalizado através de um conjunto de atividades de risco, constata-se que os indivíduos da amostra pós-Covid abriram menos links duvidosos (*p*=.006), não tendo existido mais diferenças estatisticamente significativas quando se comparam as amostras. Por fim, quanto ao guardião eficaz, apesar de as pessoas reportarem que adotam menos comportamentos de evitamento (*p*=.001), de proteção *online* (*p*=.001) e menos proteção do *software/hardware* (*p*=.001), estas investem mais em educação e formação (*p*=.001) sobre cibercrime num momento pós-pandemia. Já relativamente ao nível de conhecimento informático, na amostra pós-Covid, os indivíduos percecionam-se como tendo menos níveis de conhecimento informático (*p*=.011).

1.4. Vitimação online durante a pandemia

Quanto à vitimação *online d*urante a pandemia, os indivíduos da presente amostra foram vítimas de tentativa de *phishing* (61%), seguido de *hacking* (19.8%) e *cyberstalking* (15.4%). Para além da vitimação por estas três ofensas foram, também, vítimas de infeção por *software* malicioso (13.8%), *cyberbullying* (13.2%), fraude *online* (10.6%), extorsão (3.4%) e fraude por Mbway (2.3%). No que concerne ao objeto de estudo desta investigação, o furto de identidade *online*, apenas 3.2% dos indivíduos da amostra foi vítima de furto de identidade *online* com fins criminosos e 2.9% foi vítima de furto de identidade com o objetivo de criar perfis falsos no período pandémico. Por fim, a variabilidade de cibercrimes sofridos é de 1.45, ou seja, em

[26] Na investigação de Martins (2018) e Guedes et al. (2022) o método de pagamento Mbway não foi uma opção de resposta, logo não é possível estabelecer comparações.

média, cada indivíduo foi vítima de 1.45 cibercrimes durante a pandemia, sendo que, variava de 0 a 9 (ver anexo 7).

1.5. Atividades de rotina online durante a pandemia

Tendo em conta a última parte do questionário, sobre as atividades de rotina *online* durante a pandemia, ao nível do alvo adequado e do guardião eficaz, verifica-se que, em geral, os indivíduos mantiveram a frequência da realização dessas atividades. Por exemplo, relativamente ao alvo adequado, 87.8% dos indivíduos não alteraram a atividade de abertura de anexos de e-mails desconhecidos, 87.6% mantiveram a frequência com que abrem links desconhecidos a partir de e-mails e 86.3% registaram a mesma frequência no que concerne ao fornecimento de dados pessoais a desconhecidos (consultar anexo 8). Relativamente ao guardião eficaz, 90.4% dos indivíduos indicam que não alteraram a visita de websites destinados à educação pública sobre o cibercrime, 90.3% continuaram a participar em *workshops* destinados à educação pública sobre o cibercrime e, por fim, 88.9% dos indivíduos da amostra não alteraram os seus comportamentos relativos à instalação e atualização do *software* ou *hardware firewall* (ver anexo 9). Por outro lado, quanto à exposição *online*, a frequência com que realizaram a maior parte das atividades *online* manteve-se, com exceção da realização de determinadas rotinas *online* que registaram um aumento. Assim sendo, 67.5% dos indivíduos da amostra indicam que a realização do trabalho ou estudo *online* aumentou, 62.7% utilizaram com mais frequências as redes sociais e, por fim, 60.1% dos indivíduos desta amostra compraram mais bens e serviços *online* durante o período pandémico (consultar anexo 10).

2. Vitimação por furto de identidade online

2.1. Vitimação por furto de identidade online de acordo com as variáveis individuais

Depois de realizados os testes do Qui-quadrado, e quando analisados os valores do mesmo (ver anexo 11), verifica-se que existe uma relação entre as habilitações literárias e a probabilidade de vitimação por furto de identidade *online* (p=.029). Em concreto, os indivíduos que possuem níveis mais elevados de educação são mais vítimas daquela ofensa. Quanto à relação entre a vitimação e as restantes variáveis – género e estatuto socioeconómico – não se verificam resultados estatisticamente significativos dado o valor do *p.value* ser superior a .05. Por outro lado, realizado o Teste t para estudar a relação entre idade, medo geral e vitimação por furto de identidade *online* (ver anexo 12), constata-se que não foram obtidos resultados estatisticamente significativos, visto que, *p.value* > .05.

2.2. Vitimação por furto de identidade online de acordo com o medo e do risco percebido

De seguida, foi realizado um Teste t (consultar anexo 13) com o objetivo de perceber se existem diferenças estatisticamente significativas entre vítimas e não vítimas quanto ao medo e risco percebido de furto de identidade *online*. Relativamente ao medo de furto de identidade concluir-se que não existem diferenças estatisticamente significativas, pois o *p.value* > .05. Quanto à perceção do risco de vitimação por furto de identidade, perante os dados apresentados, conclui-se que não há diferenças estatisticamente significativas entre vítimas e não vítimas no que toca ao risco percebido (*p.value* > .05). No entanto, considera-se que o *p.value* está próximo da linha de rejeição, sendo que existe uma tendência de uma média superior de risco percebido de furto de identidade *online* em indivíduos que foram vítimas daquela ofensa.

2.3. Vitimação por furto de identidade online de acordo com as variáveis contextuais

Na tabela 3, é possível observarem-se os resultados obtidos na realização do Teste t, que teve como objetivo caracterizar as diferenças de médias das diferentes atividades de rotina entre vítimas e não vítimas. Perante estes resultados, pode concluir-se que as vítimas de furto de identidade *online* reportam abrir mais links duvidosos (*p*=.015), não tendo as restantes atividades de rotina obtido significância estatística (*p.value* > .05).

Tabela 3: Caracterização das atividades de rotina tendo por base diferenças de média entre vítimas e não vítimas

	Vítimas			**Não vítimas**			***p***
	n	**M**	**SD**	**n**	**M**	**SD**	
Exposição a ofensores motivados							
Rotinas financeiras	62	6.31	2.30	668	6.08	2.07	.414
Rotinas de trabalho/ estudo	62	8.65	1.44	668	8.69	1.39	.456
Rotinas de lazer	62	9.37	2.50	668	9.42	2.71	.886
Horas na Internet	62	5.69	2.83	668	5.83	3.17	.737
Alvo adequado							
Interação com estranhos	62	.58	.59	668	.45	.60	.101
Abrir links duvidosos	62	.31	.84	668	.14	.46	**.015**
Visitar conteúdos de risco	62	.45	.72	668	.45	.62	.933
Guardião eficaz							
Proteção do software/ hardware	62	2.02	1.11	668	1.94	1.16	.635

Comportamentos de evitamento	62	.68	.74	668	.58	.77	.343
Informação	62	.37	.71	668	.23	.56	.067
Comportamentos de proteção	62	2.29	.88	668	2.17	.90	.303

2.4. Vitimação por furto de identidade online de acordo com os locais de acesso à Internet

Por forma a perceber se existe relação entre a vitimação por furto de identidade *online* e os locais a partir dos quais se acede à *Internet* foi realizado um Teste de Qui-quadrado (ver anexo 14). Assim, observando os resultados, pode concluir-se que somente o acesso à *Internet* em locais públicos apresenta uma relação com a vitimação. Os restantes locais de acesso, como a casa, o local em que estuda/ trabalha e os estabelecimentos comerciais, não apresentam relações estatisticamente significativas ($p > .05$).

3. Medo de furto de identidade online

3.1. Medo de furto de identidade online de acordo com as variáveis individuais

Para estudar a relação entre medo do furto de identidade *online* e o género foi realizado um Teste t. Já para a relação entre medo de furto de identidade e as variáveis habilitações literárias e estatuto socioeconómico foram realizados testes *ANOVA* (tabela 4). Por fim, no que toca à idade e ao medo geral do crime, foi realizada uma correlação de Pearson (tabela 5).

Tabela 4: Medo de furto de identidade *online* de acordo com as variáveis individuais (género, habilitações literárias e estatuto socioeconómico)

	N	**M ± SD**	***p***
Género			
Masculino (0)	203	2.94±.81	**.001**
Feminino (1)	521	3.21±.71	
Habilitações literárias			
Até ao 12º ano (1)	321	3.16±.77	.304
Licenciatura (2)	246	3.17±.73	
Mestrado, Pós-Graduação ou Doutoramento (3)	161	3.01±.73	
Estatuto socioeconómico			
Baixo (1)	99	3.21±.76	.955
Médio (2)	594	3.12±.74	
Alto (3)	37	3.05±.79	

Tendo em conta os resultados apresentados na tabela 4, é possível concluir que as mulheres (M= 3.21) apresentam mais medo de furto de identidade *online* do que os homens (M= 2.94; *p*=.001). Quanto às restantes variáveis sociodemográficas – habilitações literárias, situação profissional e estatuto socioeconómico (tabela 4) e idade (tabela 5) – não se encontram resultados estatisticamente significativos ($p > .05$). Finalmente, no que fiz respeito à relação entre medo de furto de identidade *online* e o medo geral do crime, constata-se uma correlação positiva fraca (*p*=.001), ou seja, indivíduos que reportam sentir mais medo geral do crime, também reportam sentir mais medo de furto de identidade *online*.

Tabela 5: Correlação entre medo de furto de identidade *online*, idade e medo geral do crime

	Medo de furto de identidade online
Idade	-.008
Medo geral do crime	**.123****

* A correlação é significativa ao nível .05 (2-tailed)
** A correlação é significativa ao nível .01 (2-tailed)

3.2. Medo de furto de identidade online e de acordo com as variáveis contextuais

Na tabela 6 são apresentados os resultados das correlações realizadas entre as variáveis contextuais – derivadas da TAR – e o medo de furto de identidade *online*.

Tabela 6: Correlações entre o medo de furto de identidade *online* e a exposição, alvo adequado e guardião eficaz

	Medo de furto de identidade online
Exposição online	
Rotinas financeiras	.001
Rotinas de trabalho/ estudo	.020
Rotinas de lazer	.061
Número de horas online	-.049
Alvo adequado	
Interação com estranhos	**-.101****
Abrir links duvidosos	-.013
Visitar conteúdos de risco	-.009
Guardião eficaz	
Proteção do software/ hardware	-.049
Comportamentos de evitamento	**.145****
Informação	**.104****
Comportamentos de proteção	.0

* A correlação é significativa ao nível .05 (2-tailed)
** A correlação é significativa ao nível .01 (2-tailed)

Primeiramente, no que respeita à exposição *online*, não foram encontradas correlações estatisticamente significativas ($p > .05$ em todas as correlações). Por outro lado, quanto ao alvo adequado, pode concluir-se que a interação com estranhos se correlaciona negativamente com

o medo de furto de identidade *online*, ou seja, quanto menos uma pessoa interage com estranhos *online*, mais medo reporta (r=-.101, p=.006). No que concerne ao guardião eficaz, os comportamentos de evitamento correlacionam-se positivamente com o medo de furto de identidade, o que significa que, quem adota mais comportamentos de evitamento, apresenta mais medo (r=.145; p=.001). Ainda sobre o guardião eficaz, e mais especificamente no que toca à procura de informação sobre o cibercrime, este encontra-se correlacionado de forma positiva com o medo, logo quem procura educar-se sobre o cibercrime reporta mais medo de furto de identidade (r=.104, p= 005). Por fim, realça-se que todas as correlações descritas são fracas.

3.3. Medo de furto de identidade online de acordo com os locais de acesso à Internet

Por forma a perceber-se se existem diferenças de médias entre vítimas e não vítimas no que respeita aos locais de acesso à *Internet* (casa, local onde estuda/trabalha, locais públicos e estabelecimentos comerciais), foi realizado um Teste t (ver anexo 15). Tendo em conta os dados apresentados, conclui-se que não existem diferenças de médias estatisticamente significativas.

3.4. Medo de furto de identidade online durante a pandemia

Durante a pandemia, o medo que os indivíduos desta amostra sentiram face à possibilidade de os seus dados pessoais e financeiros i) serem furtados, manteve-se (70.5%); ii) serem furtados para obtenção de ganhos financeiros, manteve-se (70.8%); iii) serem furtados para danificar a sua reputação, manteve-se (75.1%) (consultar anexo 16).

4. Perceção do risco de vitimação por furto de identidade online

4.1. Perceção do risco de vitimação por furto de identidade online de acordo com as variáveis individuais

De seguida, analisam-se os resultados da perceção do risco de vitimação por furto de identidade *online* de acordo com as variáveis individuais. Enquanto que para o género foi realizado um Teste t, para o estatuto socioeconómico e habilitações literárias efetuou-se um teste *ANOVA* (ver anexo 17). Perante os dados apresentados, verifica-se que não existem diferenças estatisticamente significativas (p> .05).

Já na tabela 7, encontra-se a correlação realizada entre a idade e o risco percebido de vitimação por furto de identidade, constatando-se que não existem uma correlação entre ambas as variáveis (p > .05). A mesma conclusão é aplicada à relação entre o risco percebido e o medo geral do crime (p >.05). Contrariamente, existe uma correlação positiva entre o medo e o risco

percebido de furto de identidade *online* (*p*=.001), ou seja, quanto mais medo de furto de identidade os indivíduos reportam, mais elevado é também o risco percebido de vitimação.

Tabela 7: Correlação entre o risco percebido de furto de identidade *online*, a idade e o medo geral do crime

	Risco percebido de furto de identidade online
Idade	.070
Medo de furto de identidade online	**.263****
Medo geral do crime	.056

* A correlação é significativa ao nível .05 (2-tailed)
** A correlação é significativa ao nível .01 (2-tailed)

4.2. Perceção do risco de vitimação por furto de identidade online de acordo com as variáveis contextuais

Na tabela 8, encontram-se os resultados das correlações realizadas entre a perceção do risco de vitimação por furto de identidade e as variáveis da TAR. Relativamente à exposição *online*, as rotinas financeiras correlacionam-se positivamente com a perceção do risco de vitimação (r= .108; *p*=.004), isto é, quanto mais os indivíduos da amostra se expõem a rotinas financeiras, maior a perceção do risco. Já em relação ao alvo adequado, constata-se a inexistência de resultados estatisticamente significativos (*p.value* > .05). Por fim, quanto ao guardião eficaz, a procura de informação sobre o cibercrime encontra-se positivamente relacionada com a perceção do risco de vitimação (r=.087; *p*=.018), ou seja, quanto mais informação procuram, maior perceção do risco têm, enquanto a proteção do *software* se correlaciona negativamente com a perceção (r=-.084; *p*=-024), o que significa que quanto mais protegem o *software*, menor perceção do risco de furto de identidade reportam.

Tabela 8: Correlações entre o risco percebido de furto de identidade *online* e as variáveis contextuais (exposição online, alvo adequado e guardião eficaz)

	Risco percebido de furto de identidade online
Exposição online	
Rotinas financeiras	**.108****
Rotinas de trabalho/ estudo	.045
Rotinas de lazer	-.058
Número de horas online	-.050
Alvo adequado	
Interação com estranhos	.029
Abrir links duvidosos	.059
Visitar conteúdos de risco	.029
Guardião eficaz	

Proteção do software/ hardware	**-.084***
Comportamentos de evitamento	-.038
Informação	**.087***
Comportamentos de proteção	-.022

* A correlação é significativa ao nível .05 (2-tailed)
** A correlação é significativa ao nível .01 (2-tailed)

5. Fatores explicativos do medo de furto de identidade online

Modelo 1: Variáveis individuais e medo de furto de identidade online

Perante o modelo 1 (ver anexo 18), verifica-se que 3% da variância total do medo de furto de identidade *online* é explicada pelas variáveis individuais, sendo este modelo significativo (*p*=.001). Perante o conjunto de variáveis individuais incluídas no modelo, apenas o género (*p*=.001) e as habilitações literárias (*p*=.047) apresentam poder preditivo. No que concerne ao género, a relação é positiva (β=.148) logo, pode concluir-se que as mulheres apresentam níveis mais elevados de medo. Por outro lado, a relação apresentada com as habilitações literárias é negativa (β=-.084), ou seja, quanto menor a escolaridade, mais medo de furto de identidade *online* os indivíduos reportam.

Modelo 2: Variáveis contextuais e medo de furto de identidade online

No modelo 2 (ver anexo 19), é possível observar que as variáveis contextuais explicam 6.7% da variância do medo de furto de identidade *online*, sendo este modelo significativo (*p*=.001). Perante os dados apresentados, pode concluir-se que, em termos de exposição *online*, as rotinas de lazer são preditoras do medo de furto de identidade *online* (β=.088, *p*=.025), ou seja, quanto mais as pessoas se expõem ao risco, mais medo de furto de identidade apresentam. Quanto ao alvo adequado, a interação com estranhos (β=-.083; *p*=.026) é o único fator a contribuir para a explicação do medo de furto de identidade *online*, apresentando uma relação negativa, logo, quem interage mais com estranhos, apresenta menores níveis de medo. Por fim, em termos de guardião eficaz, os comportamentos de evitamento, a procura de informação sobre o cibercrime e o conhecimento informático contribuem para a explicação do medo. Quanto aos comportamentos de evitamento (β=.170; *p*=.001) e à informação (β=.111; *p*=.003), sendo ambas as relações positivas, significa que quanto mais comportamentos de evitamento os indivíduos adotam e quanto mais informação procuram sobre o cibercrime, mais medo de furto de identidade *online* reportam. Contrariamente, o conhecimento informático apresenta uma relação negativa (β=-.177; *p*=.001), e, neste sentido, indivíduos com maior conhecimento informático reportam menos níveis de medo de furto de identidade *online*.

Modelo 3: Modelo final de explicação do medo de furto de identidade online

No último modelo, foram incluídas as variáveis, quer individuais, quer contextuais, que obtiveram significância estatística no primeiro e segundo modelo, respetivamente. Observando-se a tabela 9, verifica-se que este é um modelo significativo (*p*=.001) e 6.5% da variância total do medo pode ser explicada pelas variáveis independentes em análise. Observa-se, ainda, que todas as variáveis mantiveram o seu poder preditivo, à exceção das habilitações literárias (*p. value* >.05).

Tabela 9: Predição do medo de furto de identidade *online* a partir das variáveis que nos dois modelos anteriores obtiveram significância estatística (género, habilitações literárias, rotinas de lazer, interação com estranhos, comportamentos de evitamento e informação)

Variável	B	SE B	β	t	*p*
Género	.251	.060	.151	4.172	**.001**
Habilitações literárias	-.042	.034	-.046	-1.235	.217
Rotinas de lazer	.022	.010	.080	2.159	**.031**
Interação com estranhos	-.107	.045	-.087	-2.365	**.018**
Comportamentos de evitamento	.137	.036	.141	3.833	**.001**
Informação	.141	.047	.109	3.012	**.003**

Nota: r= .271; r^2 =.073; r^2 ajustado= .065 (*p*=.001)

Perante os dados apresentados, pode concluir-se que a variável que mais contribui para a explicação do medo de furto de identidade *online* é o género (β=.151; *p*=.001), sendo que, são as mulheres que reportam mais medo. De seguida, encontra-se a adoção de comportamentos de evitamento (β=.141; *p*=.001), a procura de informação (β=.109; *p*=.003) e as rotinas de lazer (β=.080; *p*=.031), ou seja, quem adota mais comportamentos de evitamento, procura mais informação sobre cibercrime e se expõe a rotinas de lazer, reporta mais medo de furto de identidade *online*. Por fim, indivíduos que interagem mais com estranhos (β=-.087; *p*=.018), reportam menos medo.

6. Fatores explicativos da perceção do risco de furto de identidade online

Modelo 1: Variáveis individuais e perceção do risco de furto de identidade online

O presente modelo (ver anexo 20), sobre o poder predito das variáveis individuais na perceção do risco de furto de identidade *online*, apresenta significância estatística (*p*=.007) e explica 1.6% da variância. Observando a referida tabela constata-se que apenas o estatuto socioeconómico (β=-.076; *p*=.043) e a vitimação por furto de identidade *online* (β=.083; *p*= .027) têm poder preditivo. Em relação à vitimação, a sua maior probabilidade está relacionada positivamente com a maior perceção do risco de furto de identidade. Por outro lado, quanto ao

estatuto socioeconómico, uma vez que a relação é negativa, constata-se que quanto mais elevado o estatuto socioeconómico, menor a perceção do risco de furto de identidade *online*.

Modelo 2: Variáveis contextuais e perceção do risco de furto de identidade online

O modelo 2 (consultar anexo 21), sobre a predição do risco de vitimação por furto de identidade *online* tendo em conta as variáveis contextuais, é significativo (*p*=.001) e este conjunto de variáveis explica 5.2% da variância. Em termos de exposição *online*, constata-se que as rotinas financeiras possuem poder preditivo (β=.141; *p*=.004) e, sendo este valor positivo, tal indica que quanto mais as pessoas se expõem nestas rotinas, maior a perceção do risco. No que toca ao guardião eficaz, a procura de informação sobre o cibercrime (β=.044; *p*=.010) e o conhecimento informático (β=-.187; p=.001) também têm poder preditivo. Em relação à procura de informação, este resultado sugere que quanto mais os indivíduos procuram educar-se sobre o cibercrime, maior a sua perceção do risco de vitimação. Por outro lado, quanto ao conhecimento informático, quanto mais conhecimento informático o indivíduo reporta, menor a sua perceção do risco de vitimação por furto de identidade *online*. Por fim, neste modelo sobre as variáveis contextuais, verifica-se que o alvo adequado não obteve significância estatística em nenhuma das variáveis.

Modelo 3: Modelo final de explicação da perceção de risco de furto de identidade online

No modelo final da explicação da perceção do risco de furto de identidade *online* (tabela 10) foram incluídas as variáveis que obtiveram significância estatística no modelo 1 (estatuto socioeconómico e vitimação por furto de identidade *online*) e no modelo 2 (rotinas financeiras, informação e conhecimento informático). Este é um modelo significativo (*p*=.001) e as variáveis independentes em análise explicam 5.5% da variância na variável perceção de risco de furto de identidade *online*.

Tabela 10: Predição da perceção do risco de furto de identidade *online* a partir das variáveis que nos dois modelos anteriores obtiveram significância estatística (estatuto socioeconómico, vitimação por furto de identidade *online*, rotinas financeiras, informação e conhecimento informático)

Variável	B	SE B	β	t	*p*
Estatuto socioeconómico	-.069	.057	-.043	-1.197	.232
Vitimação por FIO	.197	.087	.082	2.266	**.024**
Rotinas financeiras	.043	.012	.133	3.618	**.001**
Informação	.108	.043	.092	2.522	**.012**
Conhecimento informático	-.188	.038	-.187	-5.016	**.001**

Nota: r= .248; r^2 =.061; r^2 ajustado= .055 (*p*=.001)

No modelo final da explicação da perceção do risco de furto de identidade *online* apenas o estatuto socioeconómico perdeu o poder preditivo. Tendo em conta os resultados apresentados, conclui-se que a variável que mais contribui para a explicação da perceção do risco de furto de identidade *online* é o conhecimento informático (β=-.187; *p*=.001) significando que quanto mais conhecimento informático, menor a perceção do risco de vitimação, pois a relação é negativa. Seguidamente, são as rotinas financeiras (β=.133; *p*=.001) o que significa que quem se expõe mais ao nível das rotinas financeiras, apresenta maior perceção do risco. Após as rotinas financeiras, encontra-se a procura de informação sobre o cibercrime (β=.092; *p*= .012), ou seja, quem procura mais educação sobre o cibercrime apresenta maior perceção do risco. Por fim, encontra-se a vitimação por furto de identidade *online* (β= .082; *p*=.024), o que significa que quem é vítima tem maior perceção do risco de vitimação por furto de identidade.

7. Fatores explicativos da vitimação por furto de identidade online

Modelo 1: Variáveis individuais e furto de identidade online

Neste primeiro modelo (consultar anexo 22), encontram-se os resultados obtidos na regressão logística realizada com o objetivo de perceber quais as variáveis individuais que explicam a vitimação por furto de identidade *online*. Este modelo não é significativo (*p*> .05), explica 1.6% da variância total da vitimação e nenhuma das variáveis incluídas no modelo (género, idade, habilitações literárias e estatuto socioeconómico) tem poder preditivo.

Modelo 2: Variáveis contextuais e furto de identidade online

No segundo modelo (ver anexo 23) são incluídas as variáveis contextuais, sendo que este modelo não é significativo (*p*> .05) e explica 6% da variância total da vitimação. Quanto à exposição *online*, nenhuma das variáveis independentes tem poder preditivo sobre a vitimação. Por outro lado, no que concerne ao alvo adequado, o facto de abrir links duvidosos tem poder preditivo sobre a vitimação, ou seja, os indivíduos que abrem links duvidosos têm uma chance 1.624 maior de serem alvos de furto de identidade *online* do que os indivíduos que não abrem links duvidosos. Por fim, quanto ao guardião eficaz, apenas a procura de informação sobre o cibercrime tem poder preditivo, no fundo, quem procura informação sobre o cibercrime tem uma chance 1.593 maior de ser vítima de furto de identidade *online* do que as pessoas que não procuram qualquer tipo de informação sobre este fenómeno.

Modelo 3: Modelo final de explicação da vitimação por furto de identidade online

Quanto ao modelo final (tabela 11) da vitimação por furto de identidade *online* verifica-se que é um modelo significativo e que explica 3.3% da variância total da vitimação. Posto isto, verifica-se que somente a abertura de links duvidosos é um preditor da vitimação por furto de identidade *online* e, em contrapartida, a procura de informação sobre o cibercrime perdeu a significância estática. Assim sendo, verifica-se que os indivíduos que abrem mais links duvidosos apresentam uma chance 1.735 maior de serem vítimas de furto de identidade *online* do que os indivíduos que não adotam este comportamento de risco.

Tabela 11: Predição da vitimação por furto de identidade online a partir das variáveis que obtiveram significância estatística no modelo anteriores (abrir links duvidosos e procurar informação sobre o cibercrime)

Variável	B	SE	OR	*p*
Abrir links duvidosos	.551	.121	1.735	**.001**
Informação	.305	.174	1.357	.079
X^2 + *p*		.013; *p*= 001		
-2. Log Likelihood		775.191		
Nagelkerke R^2		.033		

Capítulo IV: Discussão dos resultados e limitações

1. Discussão dos resultados

A presente dissertação teve dois grandes objetivos. Primeiramente, procurou comparar a vitimação e o sentimento de insegurança de furto de identidade *online* antes e depois da pandemia de Covid-19. Para além disso, procurou explorar a relação entre variáveis individuais (e.g., dados sociodemográficos) e contextuais (e.g., atividades de rotina *online*) com as duas variáveis dependentes em estudo, a vitimação e o sentimento de insegurança de furto de identidade *online*. Por forma a alcançar os dois objetivos principais desta investigação foi aplicado um questionário *online* ao qual responderam 730 indivíduos.

No presente capítulo, da discussão dos resultados, a estrutura será a seguinte: *i*) discussão dos resultados relacionados com a vitimação por furto de identidade *online, ii*) discussão dos resultados relacionados com o sentimento de insegurança e, por fim, *iii*) apresentação das limitações da presente investigação e orientações para estudos futuros que possam, eventualmente, vir a ser realizados sobre o furto de identidade *online*.

Vitimação

No que concerne à vitimação, na presente investigação, 8.5% dos indivíduos (n= 730) reportaram terem sido vítimas de furto de identidade *online* nos últimos 12 meses. Para além disso, mais indivíduos (47.5%) indicam que conhecem algum familiar, amigo e/ou conhecido

que foi vítima, confirmando-se a hipótese de que, tanto a vitimação direta como indireta, serem mais elevadas na amostra pós-pandemia. Para além disso, também se verifica que a vitimação por furto de identidade ao longo da vida aumentou. Estes resultados estão em consonância com os relatórios nacionais e internacionais, assim como como as investigações que têm sido feitas em relação ao impacto da pandemia de Covid-19 no cibercrime. Resultados esses que apontam para uma tendência do aumento de vitimações por cibercrime (e.g., Buil-Gil *et al*., 2021; Lallie *et al*., 2021; Observatório de Cibersegurança, 2022), devido ao facto de as rotinas se terem alterado e do nível de exposição ao risco ter aumento como consequência da pandemia.

Comparando as rotinas de ambas as amostras, como seria expectável, os indivíduos da amostra pós-pandemia despenderam mais tempo *online* para realizar as suas rotinas de lazer, trabalho/estudo e, também, para desenvolver as rotinas financeiras. Em termos de comportamentos de segurança *online*, verifica-se um aumento da procura de informação e educação sobre o cibercrime, o que pode ser explicado pelo facto de muitas pessoas terem passado, por força das medidas de confinamento, a desempenhar o seu trabalho e/ou estudo e demais rotinas no contexto cibernético, podendo estas terem sentido necessidade de se informarem sobre dispositivos e redes que, até então, lhes eram desconhecidos. Por fim, em termos de atividade de risco, na amostra pós-Covid verifica-se uma diminuição da abertura de links duvidosos o que se pode dever à maior educação e informação sobre cibercrime que, como foi visto anteriormente, aumentou neste grupo amostral.

Relativamente à análise da relação entre as variáveis individuais (e.g., variáveis sociodemográficas) e a vitimação por furto de identidade, verificou-se, através da análise dos resultados que as variáveis sociodemográficas incluídas neste estudo não possuem poder preditivo, logo, há outras variáveis que não foram consideradas neste estudo que explicam melhor a vitimação. Esta fraca relação encontrada entre as características sociodemográficas e a vitimação por furto de identidade *online* pode dever-se ao facto de, atualmente, a *Internet* ser transversal a toda a sociedade, motivo que pode tornar mais complexa a tarefa de traçar o perfil das vítimas no ciberespaço. Tendo em conta os testes realizados previamente à regressão logística, o Teste Qui-quadrado (género, estatuto socioeconómico e habilitações literárias) e o Teste t (idade), só foram encontradas diferenças estatisticamente significativas entre vítimas e não vítimas para a variável habilitações literárias, indicando que quem tem níveis de educação superiores é mais vítima de furto de identidade. Este resultado é semelhante ao encontrado por Bunes e colaboradores (2020) que, na sua investigação, observaram que níveis mais elevados de educação estão relacionados com níveis mais altos de vitimação por furto de identidade

online relacionada com o cartão de crédito ou cartão bancário. Na perspetiva dos autores, tal acontece porque estes indivíduos têm mais poder aquisitivo e utilizam mais equipamentos nos quais armazenam e transferem informações, o que faz com que tenham mais informação disponível e, ao mesmo tempo, exposta (Bunes *et al*., 2020).

Quanto ao estudo da relação entre a vitimação por furto de identidade e as variáveis contextuais (derivadas da TAR), foi possível notar que, no que concerne à exposição *online*, têm sido vários os estudos que encontram relação entre a exposição e o furto de identidade *online*. É de forma consistente e sistemática que a literatura indica que determinadas atividades realizadas *online* aumentam a probabilidade de vitimação. Por exemplo, Reyns (2013) descobriu que o uso do banco *online* e de mensagens instantâneas aumentam em 50% a probabilidade de vitimação por furto de identidade. Também Reyns e Henson (2016) e Bunes e colaboradores (2020), indicam que as operações bancárias e a compra de bens e serviços *online* contribuem de forma positiva e significativa para a vitimação por furto de identidade. Por fim, no estudo de Milani e colaboradores (2020), existia uma hipótese que afirmava que a frequência das atividades realizadas na *Internet* representaria o nível de exposição ao risco. Os autores confirmaram que, independentemente do cibercrime em questão, os indivíduos que usam de forma mais frequente a *Internet* ou os serviços de *networking*, apresentam maior probabilidade de vitimação *online*. Contrariamente, nesta investigação, nenhuma das atividades incluídas na operacionalização da exposição *online* prediz o furto de identidade. Tal pode dever-se ao facto de, quer seja para cibercrimes interpessoais (e.g., *cyberstalking*), quer seja para cibercrimes de natureza financeira (e.g., furto de identidade *online*), como é o caso desta investigação, se utilizarem os mesmos itens para medir a exposição *online*. Isto é, os cibercrimes de natureza interpessoal podem exigir a medição de determinadas variáveis contextuais que, no caso dos cibercrimes financeiros, podem não fazer sentido. Para além disso, outra explicação, pode dever-se ao facto de os índices da exposição *online* apresentarem baixos valores de consistência interna (ver anexo 1).

Por sua vez, quanto ao alvo adequado, alguns estudos têm demonstrado que determinadas atividades realizadas *online*, por serem consideradas comportamentos de risco, aumentam a probabilidade de vitimação por cibercrime. Na investigação realizada por Reyns (2013) atividades como compras *online* e *downloads* aumentavam a probabilidade de vitimação em 30%. Também nas investigações de Choi (2008) e Marcum (2008), atividades como o *download* de jogos e músicas de *websites* desconhecidos, abrir e-mails desconhecidos e clicar em mensagens *pop-up*, aumentaram a probabilidade de vitimação. Para além disso, no estudo

de Alshalan (2006) e Marcum e colaboradores (2010), quem fornecia os seus dados pessoais a desconhecidos apresentava maior probabilidade de vitimação. Já na investigação realizada por Reyns e Randa (2020), os indivíduos que visitam *websites* inseguros ou de risco e aqueles que tornam a sua informação pessoal disponível são considerados alvos adequados. Posto isto, os resultados da presente investigação corroboram os que são sugeridos pelos anteriores, na medida em que, a abertura de links duvidosos foi significativa na estimação da vitimação por furto de identidade *online*. Assim sendo, os indivíduos que abrem mais links duvidosos apresentam maior probabilidade de vitimação de furto de identidade *online*. Por fim, pode concluir-se que a ausência de significância estatística nos restantes itens desta dimensão se pode dever ao facto de os indivíduos não responderem de forma sincera já que são questionados acerca dos comportamentos de risco que adotam *online* e, por esse motivo, podem ter respondido de forma socialmente desejável[27].

O guardião eficaz *online* foi, também, um dos elementos testados na presente dissertação, sendo que, dos três fundamentais, é o que tem sido menos estudado da TAR (Choi *et al*., 2021). No estudo de Williams (2016) o guardião pessoal (e.g., alteração de palavras-passes com regularidade) e o guardião físico passivo (e.g., utilizar apenas um computador) reduziram significativamente a vitimação por furto de identidade. Neste estudo, aquando da realização do modelo de regressão entre vitimação e variáveis contextuais, verificou-se que a procura de informação sobre o cibercrime, ou seja, participar em *workshops* destinados à educação sobre o cibercrime e visitar *websites* destinados à educação pública sobre essa temática, estava relacionada com a vitimação por furto de identidade *online* de forma positiva, ou seja, quem foi vítima de furto de identidade procura mais informação para se proteger futuramente. Contudo, no modelo final esta variável perdeu o seu poder preditivo. Por outro lado, quanto ao nível de conhecimento informático, é comumente estabelecido que os utilizadores da *Internet* com mais conhecimento informático e/ou com mais consciência dos riscos que existem *online* são mais capazes de antecipar os ataques e, assim, apresentam menor probabilidade de vitimação *online* (Leukfeldt & Yar, 2016). Nesta investigação, tal como nas investigações realizadas por Bossler e Holt (2009) e Ngo e Paternoster (2011), não foi encontrada qualquer relação entre o conhecimento informático e a vitimação por furto de identidade *online*, não se confirmando a hipótese que estabelecia que quem se perceciona como tendo mais conhecimento informático, seria menos vítima de furto. Uma possível explicação para este resultado pode dever-se à

[27] A desejabilidade social corresponde à tendência de responder às questões apresentadas com respostas que o indivíduo considera que são socialmente aceites, em vez de responder de forma sincera/ verdadeira (Grimm, 2010).

operacionalização do conhecimento informático, visto que a resposta corresponde à perceção que a pessoa tem acerca do seu conhecimento informático, contudo, a perceção que a pessoa tem sobre as suas capacidades informáticas pode não corresponder à realidade e, nesse sentido, esta questão deveria ter sido mais objetiva. Em investigações futuras, deve procurar-se utilizar medidas concretas sobre os conhecimentos informáticos e não medidas generalistas.

Em suma, apesar de serem muitos os estudos que investigam a aplicabilidade da TAR à vitimação no ciberespaço, os resultados encontrados têm sido mistos, especialmente no que concerne ao guardião eficaz e à exposição *online* (Park & Vieraitis, 2021). Esta fraca aplicabilidade e inconsistência desta teoria ao mundo digital pode dever-se a diferentes fatores (Leukfeldt & Yar, 2016; Smith, 2022) como por exemplo a operacionalização das componentes centrais da teoria diferir de estudo para estudo (Leukfeldt & Yar, 2016). Por outro lado, pode ocorrer pelo facto de os estudos serem essencialmente desenvolvidos com amostras constituídas por jovens e, apesar de o uso da *Internet* ser prevalente junto desta faixa etária, atualmente, o uso desta rede é transversal a toda a população, motivo pelo qual, as investigações deveriam selecionar amostras mais representativas das sociedades atuais (Park & Vieraitis, 2021). Pelos motivos enunciados, os investigadores têm-se questionado sobre a possibilidade da presente teoria explicar melhor a vitimação por cibercrimes considerados como *high tech* (e.g., infeção por *malware*) do que os cibercrimes que envolvem uma vertente financeira (e.g., fraudes e furto de identidade *online*) (Leukfeldt & Yar, 2016).

Sentimento de Insegurança

Não obstante se verifique uma crescente tomada de atenção e interesse pelo estudo dos determinantes da vitimação por furto de identidade *online* (e.g., Reyns, 2013), continuam a ser escassas as investigações realizadas sobre o estudo dos preditores do medo de furto de identidade *online* (e.g., Henson *et al*., 2013; Roberts *et al*., 2013). O estudo destes preditores é importante na medida em que, por um lado, pode auxiliar a desenvolver estratégias de combate ao fenómeno e, por outro, porque o medo tem consequências negativas na vida das pessoas (Doran & Burgees, 2012) e é importante que estas se sintam seguras e confiantes e, acima de tudo, livres quando navegam na *Internet* (Brands & Wilsem, 2021).

A propósito do estudo dos determinantes do medo de furto de identidade *online* começou-se por analisar a relação entre esta variável e as variáveis sociodemográficas. Assim, em primeiro lugar, partiu-se da hipótese de que as mulheres iriam apresentar níveis mais elevados de medo de furto de identidade *online* do que os homens, o que se confirmou. Tal resultado está

em conformidade com os dados encontrados para o medo de crime tradicional, segundo os quais são as mulheres que sentem mais medo do crime, adotam mais comportamentos de segurança e percebem mais o risco de vitimação (e.g., Hale, 1996). Na literatura sobre o medo do crime é apresentado o já explicado paradoxo medo-vitimação, isto é, embora as mulheres sintam mais medo, são os homens os mais vitimados (e.g., War, 1984), contudo neste estudo não é possível observar este paradoxo, uma vez que, ao nível da vitimação, não foram encontradas diferenças estatisticamente significativas entre homens e mulheres. Posto isto, este resultado – de que as mulheres reportam mais medo de furto de identidade *online* – está em conformidade com as investigações realizadas sobre o medo de cibercrime (e.g., Virtanen, 2017). Contrariamente, nas investigações de Roberts e colaboradores (2013) e de Yu (2014), o género não foi um preditor do medo de furto de identidade *online*. Já para o risco percebido de furto de identidade *online* colocou-se como hipótese que as mulheres apresentariam maior perceção do risco, tal como sucede com a perceção do risco tradicional (e.g., LaGrange & Ferraro, 1989), contudo, não foram encontrados resultados estatisticamente significativos.

Relativamente à idade, tradicionalmente os resultados encontrados são mistos. Por um lado, há estudos que indicam que são os indivíduos mais velhos que reportam mais medo do crime (e.g., Ziegler & Mitchell, 2003) e, por outro, há investigações em que são os indivíduos mais novos (e.g., LaGrange & Ferraro, 1989). Esta mesma situação é verificada no ciberespaço. Por exemplo, enquanto Alshalan (2006) e Lee e colaboradores (2019) verificaram que os indivíduos mais velhos que apresentavam mais medo do cibercrime, outros sugeriram que são os mais jovens (e.g., Henson *et al*., 2013; Virtanen, 2017). No que concerne ao furto de identidade, na investigação desenvolvida por Roberts e colaboradores (2013) a idade foi um preditor do medo de furto, ou seja, indivíduos mais velhos apresentavam mais medo de furto de identidade. Contrariamente, nesta investigação, não se obtiveram resultados com significância estatística. Quanto à perceção do risco, há estudos que indicam que a idade influencia a perceção do risco de furto de cartão de crédito (e.g., Reisig *et al*., 2009), contudo, na presente investigação, não foram encontrados resultados estatisticamente significativos para a relação entre estas variáveis.

Quanto ao medo de furto de identidade *online* e estatuto socioeconómico, não foi encontrada nenhuma relação estatisticamente significativa entre ambos, contrariamente ao que sucede nas investigações de Virtanen (2017), Brands e Wilsem (2019) e Reisig e colaboradores (2009), nas quais se observou que indivíduos de estatuto socioeconómico mais baixo, reportavam níveis mais elevados de medo. No que concerne à relação entre o estatuto socioeconómico e a perceção do risco de furto de identidade *online*, inicialmente, no modelo parcelar com as variáveis

individuais, o estatuto socioeconómico era um dos preditores, isto é, quanto mais alto o estatuto, menor a perceção do risco. Segundo Henson e colaboradores (2013), a perceção do risco de vitimação *online* pode ser afetada pela vulnerabilidade e, assim sendo, faz sentido que pessoas com vulnerabilidade financeira se percecionem como estando em maior risco porque podem ter dificuldades em repor as perdas que podem advir do cibercrime. Este resultado – quanto mais alto o estatuto, menor a perceção do risco – possivelmente pode ser explicado pelo facto de estes indivíduos não serem afetados pela vulnerabilidade financeira. Por fim, apesar de o estatuto socioeconómico se ter revelado como um preditor no modelo individual, perdeu a significância estatística quanto testado juntamente com as restantes variáveis no modelo final.

No que diz respeito às habilitações literárias e medo de furto de identidade *online*, os resultados encontrados têm sido mistos. Por um lado, enquanto Alshalan (2006) e Roberts e colaboradores (2013) não encontraram nenhuma relação entre ambas as variáveis, Brands e Wilsem (2019) verificaram que os indivíduos com níveis mais elevados de educação apresentam menos medo e, por fim, Akdemir (2020) observou que indivíduos com níveis mais elevados de educação reportam mais medo. Segundo este autor, os indivíduos com níveis mais elevados de educação tendem a adotar mais medidas de segurança *online* o que reduz a probabilidade de vitimação no ciberespaço (Akdemir, 2020). Na presente investigação, as habilitações literárias apresentaram poder preditivo no modelo parcelar das variáveis individuais, no sentido em que, indivíduos com menos níveis de escolaridade, reportam níveis mais elevados de medo de furto de identidade *online*. Tendo em conta a explicação de Akdemir (2020), pode acontecer que indivíduos com menos níveis de escolaridade adotem menos medidas de segurança *online* e, como não se sentem protegidos, acabam por reportar níveis mais elevados de medo de furto de identidade *online*. Contudo, importa ressalvar que, no modelo final, esta variável perdeu o seu poder preditivo. Por fim, quanto à relação entre as habilitações literárias e a perceção do risco de furto de identidade *online* não foram encontrados resultados estatisticamente significativos.

Tendo em conta a TAR, mais especificamente a relação entre a exposição e o medo de furto de identidade *online,* observa-se que a exposição ao nível das rotinas de lazer[28] são preditoras do medo, ou seja, quem se expõe mais nas rotinas de lazer, reporta mais medo de furto de identidade. Este resultado corrobora as conclusões dos estudos de Roberts e colaboradores (2013) e de Choi e colaboradores (2021), visto que, nestas investigações, os indivíduos que se

[28] Ver televisão ou ouvir rádio *online*; participar em salas de chat ou fóruns; ler ou escreve blogs; fazer *downloads* de músicas, filmes, jogos ou podcasts.

expõem mais ao risco são os que reportam mais medo de furto de identidade. Contrariamente, tanto na investigação de Alshalan (2006), como na de Henson e colaboradores (2013), a exposição não teve influência nos níveis de medo de cibercrime. Por outro lado, quanto à exposição *online* e perceção do risco de furto de identidade *online* é possível observar-se que quem se expõe mais nas rotinas financeiras (uso do banco *online*/ gestão de finanças e compras de bens e serviços *online*.), apresenta maior perceção do risco. Segundo Roberts e colaboradores (2013) os indivíduos que se expõem mais na *Internet* podem ter a consciência de que, os comportamentos que adotam *online* os expõem mais ao risco e, consequentemente, reportam níveis mais elevados de medo porque têm consciência dos riscos a que estão expostos. Assim sendo, na presente investigação, pode acontecer que os indivíduos que se expõem mais nas rotinas de lazer apresentem mais medo de furto de identidade e os indivíduos que se expõem mais nas rotinas financeiras apresentem maior perceção do risco, porque podem estar cientes de que, ao realizar tais comportamentos, aumentam a probabilidade de serem vítimas de furto de identidade, nomeadamente, ao exporem dados sensíveis *online*.

No que concerne às atividades de risco *online* foi colocada a hipótese de que quanto mais atividades de risco *online* são desempenhadas, maior é o medo e a perceção do risco de furto de identidade *online*. Quanto ao medo, nesta investigação, verifica-se o contrário, os indivíduos que comunicam mais com desconhecidos *online* e que fornecem os seus dados pessoais a pessoas desconhecidas, apresentam menos medo de furto de identidade *online*. Este resultado pode ser explicado pelo facto de os indivíduos não estarem conscientes das consequências que tais comportamentos podem ter e, por esse motivo, não têm medo de furto de identidade *online*, pois não percecionam esse cenário como possível. Outra explicação possível para este resultado, relaciona-se com o facto de que, determinados indivíduos, se predisporem de forma natural a atividades de risco, logo, são indivíduos que, por si só, reportam menos medo. Este resultado seria um tópico de pesquisa interessante para futuras investigações. Por outro lado, quanto à perceção do risco não foram encontrados resultados estatisticamente significativos, o que demonstra que, efetivamente, o medo e a perceção do risco são dimensões do sentimento de insegurança realmente distintas, na medida em que, são explicados por diferentes preditores. Por fim, em relação ao alvo adequado, ressalva-se, mais uma vez, a ideia de que os itens incluídos na sua operacionalização constituem comportamentos de risco, motivo pelo qual, os indivíduos podem ter respondido de forma socialmente desejável.

A propósito da relação entre o medo de furto de identidade *online* e a dimensão dos guardiões eficazes da TAR, verifica-se que quem adota mais comportamentos de evitamento,

nomeadamente quem evita o uso de banco e compras *online*, assim como, quem procura mais informação sobre o cibercrime, através da participação em workshops ou visita a *websites* de educação sobre o cibercrime, apresenta mais medo de furto de identidade. Este resultado é consistente com a literatura relativa ao medo do crime tradicional, isto porque, alguns estudos indicam que, por norma, os comportamentos restritivos são adotados em virtude do medo que é sentido, isto é, os indivíduos antecipam o medo e, por esse motivo, adotam comportamentos de segurança (e.g., Liska *et al*., 1988). Já em relação à perceção do risco, os indivíduos que procuram mais informação sobre o cibercrime apresentam maior perceção do risco, o que pode ser explicado pelo facto de estarem mais informados sobre os riscos e perigos da *Internet*. Tal como indica Virtanen (2017), é extremamente importante que, cada vez mais, as sociedades sejam informadas e educadas de forma que se possa navegar de forma segura e confiante, ciente dos riscos e perigos que existem no ciberespaço.

Não obstante do estudo das variáveis individuais e contextuais, outra variável analisada na presente investigação foi o medo geral do crime e a sua relação com o medo e perceção do risco de furto de identidade *online*. Pese embora não tenha sido encontrada nenhuma correlação entre o medo geral do crime e o risco percebido de furto de identidade *online*, o mesmo não se verifica com o medo de furto de identidade *online* e o medo geral do crime, visto que, foi encontrada uma correlação positiva entre ambas as variáveis. Nesse sentido, quanto mais medo geral do crime os indivíduos reportam, mais medo de furto de identidade *online* sentem. Este resultado corrobora os resultados encontrados na investigação de Roberts e colaboradores (2013) e de Guedes *et al*., (2022), nas quais o medo geral do crime foi um preditor do medo de furto de identidade *online*. Para estes autores, este resultado apoia a perspetiva que entende que o medo do crime é um fator disposicional e não um fator dependente do risco percecionado pelos sujeitos. Assim sendo, os autores entendem que, quando se estuda o medo do crime, o foco deve voltar-se mais para características individuais, psicológicas ou disposicionais e focar-se menos no objeto do medo. No mesmo sentido, uma investigação realizada por Guedes e colaboradores (2018), observou que existia uma correlação positiva entre o medo disposicional e medo do crime específico, mas não com o risco percebido de vitimação, o que demonstra que ter medo do crime geral pode, também, transpor-se para o contexto digital. Por fim, no estudo de Choi e colaboradores (2021), os resultados demonstram que as pessoas reportam mais medo de furto de identidade *online* do que medo geral do crime o que, segundo os investigadores, se pode dever às consequências do furto.

Por fim, a vitimação por furto de identidade *online* explica a perceção do risco, isto é, quem já foi vítima de furto de identidade *online*, apresenta maior perceção do risco. Contudo, o mesmo não se verifica para o medo de furto de identidade *online*, visto que a vitimação não foi preditora do medo, tal como sucede no estudo de Henson e colaboradores (2013), no qual a vitimação interpessoal *online* – ao longo da vida – não foi um preditor do medo de vitimação interpessoal *online*. Contrariamente, na investigação realizada por Choi e colaboradores (2021), a vitimação prévia foi o preditor mais forte do medo de furto de identidade *online*. Conclui-se, perante estes resultados, que é importante e necessário distinguir as componentes do sentimento de segurança, nomeadamente através da sua operacionalização tripartida (medo do crime, perceção do risco e adoção de comportamentos de segurança).

2. Limitações e investigações futuras

Apesar dos contributos desta investigação para o crescimento científico acerca da vitimação e sentimento de insegurança de furto de identidade *online*, existem algumas limitações a apontar. Primeiramente, a amostra deveria ser mais diversificada de forma a aumentar a validade externa, visto que, esta é considerada uma amostra por conveniência não probabilística. Tal resulta do facto de o questionário ter sido essencialmente divulgado e respondido por estudantes, professores e *staff* da Universidade do Porto. Para além disso, ainda no que concerne à amostra, há a possibilidade de enviesamento dos dados devido à divulgação do questionário em redes sociais pessoais, pois, por norma, o questionário é difundido junto de amigos, conhecidos e familiares que partilham, à partida, os mesmos interesses, gostos e perspetivas (Ball, 2019). Assim sendo, seria benéfico replicar este estudo junto de uma amostra mais representativa da população.

Quanto ao questionário, poderiam ter sido incluídas definições de termos específicos do ciberespaço que podem ser desconhecidos e complexos (e.g, *firewall* e *antispyware*) para alguns dos elementos da amostra, assim, alguns termos poderiam ser clarificados. Para além disso, tanto o estatuto socioeconómico como o nível de conhecimento informático são medidos em termos de perceção e, como tal, podem não traduzir a realidade já que são questões subjetivas. Em investigações futuras, o nível de conhecimento informático poderá ser medido através de critérios previamente definidos para que a resposta seja o mais objetiva possível. Mais concretamente, para cada nível de conhecimento – baixo, médio e avançado – poderia apresentar-se um conjunto de ações/ técnicas para que os indivíduos pudessem avaliar de forma mais objetiva o seu conhecimento informático. Assim sendo, e a título de exemplo, ao nível

baixo poderiam corresponder competências de copiar e colar ficheiros e, ao nível avançado, poderiam corresponder competências de programação. Igual solução deve ser adotada para a operacionalização do estatuto socioeconómico.

No decorrer desta investigação, constatou-se que a TAR, mais especificamente as medidas que foram criadas, não foram fortes preditores do furto de identidade *online*. Uma explicação pode dever-se aos baixos valores de fiabilidade das escalas utilizadas, verifica-se que estes são alfas considerados fracos (consultar anexos 1, 2 e 3), ou seja, há baixa consistência interna, o que pode afetar a validade das conclusões estatísticas. Outra explicação para a fraca aplicabilidade desta teoria, pode dever-se ao facto de que, determinados comportamentos incluídos na operacionalização da exposição *online* serem, também, operacionalizados ao nível do guardião eficaz, mais especificamente, no que toca aos comportamentos de evitamento. Futuramente, deveriam utilizar-se medidas diferentes para cada uma das dimensões da teoria e, ainda, devem ser criadas escalas para cada cibercrime em específico. Por fim, dada a constante evolução da tecnologia e da *Internet*, futuras investigações devem dedicar-se à criação de medidas com itens atualizados, na medida em que, os itens utilizados nesta, e na maioria das investigações, serem adaptados de investigações realizadas há 10 anos, constatando-se que é urgente a atualização e adequação à realidade cibernética atual.

Enumeradas as limitações desta investigação, segue-se a apresentação de possíveis orientações para estudos a realizar futuramente. Primeiramente, uma vez que muitas das variáveis incluídas neste estudo não têm poder preditivo sobre a vitimação por furto de identidade *online*, devem ser realizadas novas investigações que incluam outras variáveis que possam contribuir para uma melhor explicação deste fenómeno (e.g., desviância *online*; Reyns, 2013). Por outro lado, poderá analisar-se o potencial de outras teorias criminológicas explicativas da vitimação no ciberespaço, já que a TAR apresenta resultados mistos e inconsistentes. No que toca ao sentimento de insegurança, alguns investigadores (e.g., Yu, 2014) têm realçado a importância de se investigar o impacto que a gravidade percebida de determinado cibercrime pode ter no medo, assim sendo, investigações futuras poderão debruçar-se no impacto que a gravidade do furto de identidade tem ao nível do medo deste mesmo fenómeno.

Por fim, de forma a complementar as investigações de cariz quantitativos, poderiam realizar-se investigações de natureza qualitativa com o objetivo de explorar as experiências de insegurança dos indivíduos, as rotinas adotadas *online* e, ainda, a perceção do risco. Desta forma, aprofundar-se-ia o conhecimento acerca do furto de identidade *online*, mais

especificamente nas dimensões mencionadas, e identificar-se-iam novas dimensões a incluir em futuros questionários.

3. Conclusão: importância da prevenção

A problemática do cibercrime advém das suas características (e.g., transnacionalidade, atemporalidade, deslocalização e anonimato), isoladas ou em conjunto, pois são estas que dificultam a sua prevenção, investigação, repressão e punição. Para além disso, são estas características que fazem com que este seja um dos fenómenos mais estudados e temidos da atualidade (Dias, 2012). Segundo Dias (2012) a prevenção do cibercrime deve ser feita através da sensibilização, mais concretamente através de seminários, campanhas públicas ou privadas, quer sejam dedicados à generalidade da população, quer sejam destinados a um pequeno grupo de pessoas e contextos. Nestas dinâmicas de sensibilização deve alertar-se para os riscos e perigos da *Internet* e devem ensinar-se técnicas de proteção *online*. No fundo, é fundamental dar ênfase ao problema e à imprescindibilidade das medidas de segurança.

Concretamente sobre o furto de identidade *online*, segundo Wang e Yuan (2006), há poucas medidas que são implementadas para prevenir este fenómeno (Shah *et al*., 2022). Contudo, alguns autores têm procurado enumerar estratégias de prevenção a adotar na *Internet*. Tal como Dias (2012) realça a importância da sensibilização, também Wang e Yuan (2006) destacam o papel da educação. Para estes investigadores, educar a população é uma forma eficaz de prevenir a exposição *online* dos dados pessoais e financeiros e, consequentemente, prevenir o furto de identidade *online*. Nesta perspetiva, quanto mais as pessoas estiverem consciencializadas sobre as ameaças deste fenómeno e das consequências danosas que deste podem advir, mais motivadas estarão para proteger os seus dados. Assim, urge a educação sobre medidas concretas a adotar, como por exemplo, não fornecer informações pessoais a estranhos; caso faça muitas compras *online* pode utilizar uma conta bancária com menos dinheiro para realizar essas transferências monetárias; e, caso seja vítima, deve informar de imediato as autoridades e, também, as instituições bancárias de forma a minimizar as perdas (e.g., cancelamento dos cartões) (Wang & Yuan, 2006). Park e Vieraitis (2021) sugerem que quem foi vítima de furto de identidade *online* deve receber aconselhamento gratuito e, ainda, deve receber aulas educacionais que fomentem a navegação segura. Nestas aulas, deve realçar-se a quantidade de dados pessoais que são disponibilizados assim que criam contas *online* pois, segundo os autores, a população em geral não está ciente da quantidade de informação pessoal que está disponível *online* que, combinada com outras informações sobre os seus hábitos e

rotinas online (e.g. os conteúdos que os indivíduos gostam ou leem *online)*, permite descobrir ainda mais informações sobre os mesmos e que depois pode ser usada para fins ilícitos.

Há, também, um conjunto de medidas de proteção que podem ser conferidas pela própria tecnologia (software/hardware). Segundo Wang e Yuan (2006) a própria tecnologia oferece recursos que dificultam o acesso às informações pessoais e financeiras, nomeadamente através do uso de medidas biométricas para autenticação. A biometria pode reduzir o risco de vitimação por furto de identidade *online* ao identificar o proprietário através de característica únicas como as impressões digitais, a voz ou o olhar. Estas medidas biométricas tornam difícil, senão impossível, personificar a identidade do outro. Na investigação realizada por Carmel e Akila (2020), com o objetivo de perceber se as medidas biométricas previnem eficazmente o furto de identidade *online*, concluiu-se que, mediante a utilização de medidas biométricas apropriadas, o furto de identidade *online* pode ser efetivamente prevenido.

Ao nível internacional, a Europol (2021b) recomenda que os indivíduos estejam alerta, isto é, que percecionem os e-mails ou *websites* que peçam informações pessoais como suspeitas, particularmente as que peçam informações bancárias, no fundo, deve fazer-se uma pesquisa no sentido de perceber se aquele e-mail foi realmente enviado pela instituição bancária ou se, pelo contrário, é uma tentativa de furto de identidade *online*. Para além disso, recomenda que se façam atualizações regulares do *software* de segurança e do antivírus e, por fim, recomendam que, sempre que alguém seja vítima, reporte de imediato às autoridades policiais e às instituições bancárias (Europol, 2021b).

Tendo em conta os custos associados ao cibercrime e a crescente importância que a *Internet* assume em todas as esferas do quotidiano, torna-se imprescindível a identificação de fatores de risco e proteção, tanto da vitimação, como do medo de cibercrime. Esta identificação será uma mais-valia para o desenho de estratégias de prevenção adequadas (Guedes *et al*., 2022). Para além disso, é importante que a Criminologia continue a produzir conhecimento científico sobre o impacto da pandemia de Covid-19 no cibercrime, visto que, como demonstram as investigações e os relatórios supramencionados, parece existir uma tendência de aumento do cibercrime e, como se verificou nesta investigação, efetivamente a vitimação por furto de identidade *online* aumentou após a pandemia.

Bibliografia

Acoca, B. (2007). *Scoping Paper on Online Identity Theft*. Ministerial Background Report. OECD. Retrieved from: http://www.oecd.org/dataoecd/35/24/40644196.pdf

Agra, C. (2007). Podemos medir a criminalidade e a segurança? *Sep. De Inovação, poder e desenvolvimento: Congresso de Cidadania*, 227-234.

Agra, C., e Kuhn, A. (2010). *Somos todos criminosos*? Porto: Casa das Letras.

Akdemir, N. (2020). Examining the impact of fear of cybercrime on internet users' behavioral adaptations, privacy calculus and security intentions. *International Journal of Eurasia Social Sciences*, *11*(40), 606-648.

Alshalan, A. (2006). *Cyber-crime fear and victimization: an analysis of a national survey*. Mississippi: Mississippi State University.

Amerio, P., & Roccato, M. (2007). Psychological reactions to crime in Italy: 2002-2004. *Journal of community psychology*, *32*(1), 91-102.

Antunes, M., & Rodrigues, B. (2018). Introdução à Cibersegurança: a internet, os aspetos legais e a análise digital forense. Lisboa: *FCA*.

Ball, H. L. (2019). Conducting online surveys. *Journal of human lactation*, *35*(3), 413-417.

Beck, U. (2015). *Sociedade de Risco Mundial: em busca da segurança perdida*. Edições 70: Lisboa.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and *malware* infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Brands, J., & Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology 18*(2), 213-234.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, Pharming and Identity Theft. *Academy of Accounting & Financial Studies Journal*, *11*(3).

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.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Bunes, D., DeLiema, M. & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 1-8.

Cahill, M. T. (2014). Extortion and blackmail. *The Encyclopedia of Criminology and Criminal Justice*, 1-5.

Capeller, W. (2001). Not such a neat net: some comments on virtual criminality. *Social and Legal Studies*, *10*(2), 229–242.

Carmel, V. V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. *J Crit Rev*, *7*(3), 540-547.

Choi, J., Kruis, N. E., & Choo, K. S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice*, *37*(3), 406-426.

Choi, K. (2008). An Empirical Assessment of an Integrated Theory of Computer Crime Victimisation. *International Journal of Cyber Criminology*, *2*(1), 308–33.

Choi, K.-S., Lee, C. S., & Louderback, E. R. (2019). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. *In The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–17). Springer International Publishing.

Clarke, R. V. (1999). Hot products: understanding, anticipating, and reducing demand for stolen goods. Police Research Series, Paper 112, Policing and Reducing Crime Unit. *Research Development and Statistics Directorate. Home Office*.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.), Lawrence Erlbaum Editors.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American sociological review*, 505-524.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44*, 588- 608.

Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations. *Scottish Institute for Policing Research*.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), pp. 933-948.

Correia, A., (2021). Velhos crimes, novas ferramentas; novos crimes, novas ferramentas. In Guedes, I., e Gomes, A. (Eds.), Cibercriminalidade: novos desafios, ofensas e soluções (pp. 53-71). Pactor.

Covington, J., & Taylor, R. B. (1991). Fear of crime in urban residential neighborhoods. The Sociological Quarterly, 32(2), 231-249.

Creswell, J. (2009). *Research design: qualitative, quantitative, and mixed methods approaches* (3ª ed.). Los Angeles: Sage.

Dias, V. M. (2012). A problemática da investigação do cibercrime. *Data Venia Revista Jurídica Digital, 1*(1), 63-87.

Doran, B. J., & Burgess, M. B. (2012). Why is fear of crime a serious social problem?. In *Putting fear of crime on the map* (pp. 9-23). Springer, New York, NY.

Duque, R. (2015). *Singularidades da coexistência da liberdade e da segurança em democracia*. In E. P. Correia, (coord.), Liberdade e Segurança (pp. 55-69). Lisboa. ISCPSI-ICPOL.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime prevention studies*, *16*, 7-40.

Emler, N. (1990). A social psychology of reputation. *European review of social psychology, 1*(1), 171-193.

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and measuring cybercrime.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police research series, paper, 98*(1-36), 10

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology, 8*(4), 389-406.

Fernandes, L., & Rêgo, X. (2011). *Por onde anda o sentimento de insegurança? Problematizações sociais e científicas do medo à cidade.* etnográfica, 15(1), 167- 181.

Ferraro, K. (1995). *Fear of crime: interpreting the victimization risk*. New York: State University of New York Press.

Ferraro, K. F., & Grange, R. L. (1987). *The Measurement of Fear of Crime. Sociological Inquiry, 57(1), 70–97.*

Fonseca, E. (1998). *Representação social da insegurança: crime e crise.* Tese de Mestrado. Faculdade de Psicologia e Ciências da Educação. Universidade do Porto.

Fox, S. (2001). *Fear of online crime.* Washington, DC: Pew Internet & American Life Project.

Furnell, S. (2002). Cybercrime: Vandalizing the information society. Boston: Addison Wesley.
Gabriel, U., & Greve, W. (2003). The psychology of fear of crime: conceptual and methodological perspectives. *British Journal of Criminology, 43*, 600-614.
Garofalo, J. (1981). The Fear of Crime: Causes and Consequences. *Journal of Criminal Law and Criminology 72*(2), p. 839–857.
Gercke, M. (2011). Understanding cybercrime: a guide for developing countries. International Telecommunication Union (Draft).
Gottfredson, M., & Hirschi, T. (1990). *A general theory of crime.* Stanford University Press.
Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243–9.
Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime*, *6*(1), 146-157.
Guedes, I., Cardoso, C., e Agra, C. (2012). Medo do crime: revisão conceptual e metodológica. In Agra, C. (Ed.), A Criminologia: um arquipélago interdisciplinar (pp. 213-248). Porto: Universidade do Porto.
Guedes, I., Domingos, S., & Cardoso, C. (2018). Fear of crime, personality and trait emotions: An empirical study. *european Journal of criminology*, *15*(6), 658-679.
Guedes, I., Martins, M. & Cardoso, C.S (2022). Exploring the determinants of victimization and fear of online identity theft: an empirical study. *Security Journal*.
Guedes, I., Moreira, S., e Cardoso, C. (2021). Cibercrime: conceptualização, desafios e perceções públicas. In Guedes, I., e Gomes, A. (Eds.), Cibercriminalidade: novos desafios, ofensas e soluções (pp. 3-23). Pactor.
Hale, C. (1996). Fear of Crime: A review of the literature. *International Review of Victimology, 4*, 79-150.
Harrell, E. 2015. *Victims of identity theft*, 2014, Bureau of Justice Statistics, NCJ 248991.
Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.
Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of Crime *Online*? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of *Online* Interpersonal Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 475–497.
Higgins, G., Ricketts, M., & Vegh, D. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice, 33*, 223–233.
Hill, M. M., & Hill, A. (1998). *Investigação empírica em ciências sociais: Um guia introdutório.* Lisboa: Dinâmica.
Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: scale development and validation. *Journal of Interactive Markting, 30*, 1-19.
Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.
Hirtenlehner, H. (2008). Vulnerability—mediating the perceived risk—fear of victimization—linkage? Testing a transactional theory of fear of crime using data from Austria. *Fear of crime—Punitivity new developments in theory and research,(Crime and crime policy, volume 3)*, 107-126.
Holt, T. J., & Bossler, A. M. (Eds.). (2020). *The palgrave handbook of international cybercrime and cyberdeviance*. London: palgrave macmillan.
Holt, T., & Bossler, A. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25.
Holt, T., & Bossler, A. (2013). Examining the relationship between routine activities and malware infection. *Journal of Contemporary Criminal Justice, 29*(4), 420–436.

Holt, T., & Turner, M. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, 308-323.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications, 40*, 307-324.

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing, *Journal of Criminal Psychology.*

Jackson, J. (2006). Introducing fear of crime to risk research. *Risk analysis, 26* (1), 253- 264.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501.

LaGrange, R., e Ferraro, K. (1989). Assessing age and gender differences in perceived risk and fear of crime. *Criminology*, *27*(4), 697-720.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lee, S. S., Choi, K. S., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 5-22.

Leukfeldt, E. (2014). Phishing for suitable targets in the netherlands: routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behavior*, 1-18.

Liska, A., Sanchirico, A., & Reed, M. (1988). Fear of crime and constrained behavior specifying and estimating a reciprocal effects model. *Social Forces*, *66*(3), 827-837.

Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological bulletin*, *127*(2), 267.

Machado, C. & Agra, C. d. (2002). *Insegurança e medo do crime: da rutura da sociabilidade à reprodução da ordem social.* Revista Portuguesa da Ciência Criminal, 12, 79-101.

Machado, C. (2004). *Crime e insegurança. Discursos do medo, imagens do Outro.* Lisboa: Editorial Notícias.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, *2*(2), 346.

Marcum, C., Higgins, G., & Ricketts, M., (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior, 31*(5), 381–410.

Marôco, J. (2014). *Análise estatística com o SPSS Statistics* (6ª ed.). Pêro Pinheiro, Portugal: Report Number.

Martins, M. (2018). *Sentimento de insegurança e vitimação no ciberespaço: a relação entre variáveis individuais e contextuais.* Dissertação de Mestrado. Faculdade de Direito. Universidade do Porto.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52.

Mesch, G. S. (2000). Perceptions of risk, lifestyle activities, and fear of crime. *Deviant, 21*(1), 47-62.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H. J. (2021). Situational and Individual Risk Factors for Cybercrime Victimization

in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*.
Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, *43*(2), 228-240.
Miri-Lavassani, K., Kumar, V., Movahedi, B., & Kumar, U. (2009). Developing an identity fraud measurement model: a factor analysis approach. *Journal of Financial crime*.
Miró, F. (2014). Routine Activity Theory. The Encyclopedia of Theoretical Criminology, p. 1–7.
Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321.
Newman, G., & Clarke, R. V. (2003). Superhighway robbery: Crime prevention and e-commerce. *Cullompton, Devon: Willan Publishing*.
Newman, G., & McNally, M. (2005). *Identity theft literature review.* Washington, DC: National Criminal Justice Reference Service.
Ngo, F., & Paternoster, R. (2011). Cybercrime victimization: an examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.
Paek, S., & Nalla, M. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and justice*, 1-17.
Pain, R. (1995). Elderly women and fear of violent crime: the least likely victims? A reconsideration of the extent and nature of risk. *British Journal of Criminology, 35(4),* 584-598.
Park, Y., & Vieraitis, L. M. (2021). Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experiences. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(2), 38-52.
Payne, J. L., Morgan, A., & Piquero, A. R. (2020). COVID-19 and social distancing measures in Queensland, Australia, are associated with short-term decreases in recorded violent crime. *Journal of experimental criminology*, 1-25.
Pereira, F., & Matos, M. (2015). Cyber-stalking victimization: What predicts fear among Portuguese adolescents? European Journal on Criminal Policy and Research, 1e18.
Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine online activity and Internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.
Rader, N., May, D., e Goodrum, S. (2007). An empirical assessment of the 'threat of victimization': considering fear of crime, perceived risk, avoidance, and defensive behaviors. Sociological Spectrum: Mid-Shouth Sociological Association, 27(5), 475-505.
Randa, R. (2013). The influence of the cyber-social environment on fear of victimization: Cyberbullying and school. *Security Journal*, *26*(4), 331-348.
Reid, L. W., & Konrad, M. (2004). The gender gap in fear: Assessing the interactive effects of gender and perceived risk on fear of crime. *Sociological Spectrum*, *24*(4), 399-425.
Reisig, M., Pratt, T., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: examining the effects of social vulnerability and financial impulsivity. *Criminal justice and behavior, 36*(4), 369-384.
Reyns, B. W. (2013). *Online* Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Reyns, B. W., & Randa, R. (2020). No honor among thieves: personal and peer deviance as explanations of online identity fraud victimization. *Security Journal*, *33*(2), 228-243.

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, *20*(3), 315–328.

Russo, S., e Roccato, M. (2010). How long does victimization foster fear of crime? A longitudinal study. *Journal of Community Psychology*, *38*(8), 960-974.

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13*(2), 183-192.

Shah, M. H., Ahmed, J., & Soomro, Z. A. (2016). Investigating the Identity Theft Prevention Strategies in M-Commerce. *International Association for Development of the Information Society*.

Silva, F. (2014). *A usurpação da ciberidentidade.* Dissertação de Mestrado. Escola de Direito. Universidade Católica do Porto.

Singh, P. (2007). *Laws on Cyber Crimes.* Jaipur: Book Enclave.

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime*. Beverly Hills, California: SAGE.

Smith, L., & Hill, G. (1991). Victimization and fear of crime. *Criminal Justice and Behavior*, *18*(2), 217-239.

Smith, R. G. (2011). Identity theft and fraud. In Jewkes, Y., & Yar, M. (Eds.), *Handbook of Internet Crime* (pp. 273-301). Londres: Routledge.

Smith, R., & Hutchings, A. (2014). *Identity crime and misuse in Australia: Results of the 2013 online survey.* Retrieved from: Australian Institute of Criminology: https://www.aic.gov.au/publications/rpp/rpp128

Smith, T. (2022). Assessing the Effects of COVID-19 on Online Routine Activities and Cybercrime: A Snapshot of the Effect of Sheltering in Place. *Caribbean Journal of Multidisciplinary Studies*, *1*(1), 36-60.

Solove, D. J. (2002). Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal*, *54*, 1227-1276.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in human behavior*, *26*(3), 277-287.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A Cybercrime Incident Architecture with Adaptive Response Policy. *Computers & Security.*

Vakhitova, Z. I., & Reynald, D. M. (2014). Australian internet users and guardianship against cyber abuse: An empirical analysis. *International Journal of Cyber Criminology*, *8*(2), 156.

Valente, M. M. G. (2013). Segurança um tópico Jurídico em reconstrução. *Lisboa: Âncora Editora*.

van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, *17*(4), 480-497.
Van Wilsem, J. (2013). "Bought it, but never got it." Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178.
Vandeviver, C. (2011). Fear of crime in the EU-15 and Hungary: assessing the impact of vulnerability, victimization and incivilities model on the fear of crime in a European cross-national context. Master Thesis, Hogeschool-Universiteit Brussel.
Venâncio, P. D. (2011). *Lei do Cibercrime: anotada e comentada*. Coimbra Editora.
Virtanen, S. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. Psychiatry, Psychology and Law, 24(3), 323-338.
Wall, D. (2001). *Cybercrime and the Internet.* Londres: Routledge.
Wall, D. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.
Wall, D. (2008). Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22*(1-2), 45–63.
Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. *Policing and Society*, *23*(4), 409-412.
Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. *IEEE Security & Privacy*, *4*(2), 30-38.
Warr, M. (1984). Fear of victimization: why are women and the elderly more afraid?. *Social Science Quarterly*, *65*(6), 81-702.
Warr, M. (2000). Fear of crime in the United States: avenues for research and policy. *Criminal Justice, 4*(4), 451-489.
Williams, M. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. The British Journal of Criminology, 56(1), 21–48.
Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political science quarterly*, *67*(4), 481-502.
Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.
Yar, M. (2006). *Cybercrime and Society.* London: Sage Publications.
Yar, M. (2010). Public perceptions and public opinion about Internet crime. In Jewels, I., & Yar, M. (Eds.), *Handbook of Internet crime* (pp. 104-119). Cullompton: Willian Publishing.
Yu, S. (2014). Fear of cyber crime among college students in the United States: an exploratory study. *International Journal of Cyber Criminology*, *8*(1), 36–46.
Zedner, L. (2009). *Security, Key Ideas in Criminology*, Abingdon - Oxon, Routledge.
Ziegler, R., & Mitchell, D. (2003). Aging and fear of crime: an experimental approach to an apparent paradox. *Experimental Aging Research, 29*(2), 173- 187.

Relatórios consultados

Comissão Europeia (2019). European's attitudes towards cyber security (cybercrime). Disponível em: https://europa.eu/eurobarometer/surveys/detail/2249 (acedido em maio de 2022).
Comissão Europeia (2020). Special Eurobarometer 499: Europeans' attitudes towards cyber security. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1 (acedido em dezembro de 2021).

Europol (2020a). Pandemic profiteering how criminals exploit the Covid-19. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf (acedido em maio de 2022).
Europol (2020b). Internet Organised Crime Threat Assessment – 2020. Disponível em: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (acedido em maio de 2022).
Europol (2021a). Internet Organised Crime Threat Assessment – 2020. Disponível em: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 (acedido em maio de 2022).
Europol (2021b). Tips and advice to prevent Identity Theft happening to you. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/infographic_-_id_theft.pdf (acedido em junho de 2022).
Gabinete do Cibercrime (2020). Covid-19: Cibercrime em tempo de pandemia. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2020_06_01_cibercrime_em_tempo_de_pandemia.pdf (acedido em maio de 2022).
Gabinete do Cibercrime (2021). Cibercrime: denúncias recebidas 2021. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf (acedido em maio de 2022).
Observatório de Cibersegurança (2021). Relatório Cibersegurança em Portugal: Riscos e Conflitos 2021. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf (acedido em maio de 2022).
Observatório de Cibersegurança (2022). Relatório de Cibersegurança em Portugal: Riscos e Conflitos. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf (acedido em maio de 2022).
Relatório Anual de Segurança Interna (2021). Disponível em: https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2021 (acedido em maio de 2022).

Leis consultadas

Código Penal;
Decreto-Lei n.º 81/ 2016, de 28 de novembro: Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica;
Despacho do Procurador-Geral da República de 7 de dezembro de 2011: cria o Gabinete de Cibercrime da Procuradoria-Geral da República;
Lei n.º 109/2009, de 15 de setembro: Lei do Cibercrime;
Lei n.º 33/99, de 18 de maio: Regula a identificação civil e a emissão do bilhete de identidade de cidadão nacional;
Lei n.º 46/2018 de 13 de agosto: Regime Jurídico da Segurança no Ciberespaço;
Lei n.º 12/91, de 21 de maio: Lei da Identificação Civil e Criminal;
Decreto-Lei n.º 3/2012, de 16 de janeiro: Altera a orgânica do Gabinete Nacional de Segurança.

Anexos

Anexo 1: Análise fatorial dos itens da exposição *online*

Fator	α	Itens
Rotinas financeiras	.612	Banco *online* e gestão de finanças
		Compra de bens e serviços *online*
Rotinas de trabalho	.537	E-mail ou mensagens instantâneas
		Trabalho ou estudo
Rotinas de lazer	.529	Ver televisão ou ouvir rádio
		Participar em salas de chats ou fóruns
		Ler ou escrever blogs
		Fazer download de músicas, filmes, jogos ou podcasts

Anexo 2: Análise fatorial dos itens do alvo adequado

Fator	α	Itens
Interação com estranhos	.323	Comunicou com desconhecidos *online*
		Forneceu os seus dados pessoais a alguém desconhecido
Abrir links duvidosos	.639	Abrir anexos desconhecidos de e-mails que recebeu
		Abrir algum link desconhecido de e-mails que recebeu
		Abriu algum ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido
Visitar conteúdo de risco	.368	Clicar em mensagens pop-up
		Visitar websites duvidosos

Anexo 3: Análise fatorial dos itens do guardião eficaz

Fator	α	Itens
Comportamentos de evitamento	.585	Evita utilizar o banco *online*
		Evita comprar *online*
Proteção do software	.777	Tem instalado e atualizado o software antivírus
		Tem instalado e atualizado o software anti-spyware
		Tem instalado e atualizado o software ou hardware firewall
Comportamentos de proteção	.420	Utiliza o filtro de spam no e-mail
		Altera as definições de segurança
		Utiliza diferentes palavras-passes para diferentes sites
Educação sobre cibercrime	.691	Participa em workshops destinados à educação sobre o cibercrime
		Visita websites destinados à educação pública sobre o cibercrime

Anexo 4: Itens do medo e perceção do risco de furto de identidade *online*

Fator	α	Itens
Medo de furto de identidade *online*	.882	Alguém furtar os seus dados pessoais e financeiros via online Alguém utilizar os seus dados pessoais e financeiros online para obter ganhos financeiros Alguém danificar a sua reputação com base na utilização ilegítima dos seus dados pessoais e financeiros online
Perceção do risco de furto de identidade *online*	.822	Alguém utilizar os seus dados pessoais e financeiros online, para obter ganhos financeiros, nos próximos 12 meses Alguém danificar a sua reputação devido à utilização ilegítima dos seus dados pessoais e financeiros online, nos próximos 12 meses

Anexo 5: Índice do medo geral do crime

Fator	α	Itens
Medo geral do crime	.389	Como se sente quando caminha sozinho(a) nas suas zonas de residência, depois de escurecer Como é que se sente quando está sozinho(a) na sua casa, depois de escurecer

Anexo 6: Atividades de rotina online antes e após a pandemia de Covid-19

	COVID				
	Antes		**Depois**		
	N (%)	**M±SD**	**N (%)**	**M±SD**	***p***
TAR					
Exposição online					
Horas despendidas online		5.31±3.27		5.82±3.14	**.002**
Rotinas financeiras		4.83±2.12		6.10±2.09	**.001**
Rotinas de trabalho		8.53±1.40		8.68±1.39	**.029**
Rotinas de lazer		8.55±2.60		9.42±2.69	**.001**
Formas de pagamento online					
Homebanking	25% (205)		34.9% (234)		**.001**
Paypal	28.3% (231)		32.6% (219)		.067
Cartão de crédito	34.5% (286)		56.5% (380)		**.001**
Paysafecard	3.2% (27)		2.1% (14)		.169
Mbnet	32.9% (269)		16.1% (108)		**.001**
Mbway	-		65.1% (437)		-

Outro	-	4.2% (28)	-
Alvo adequado			
Interação com estranhos	.41±.57	.46±.60	.067
Abrir links duvidosos	.23±.62	.16±.51	**.006**
Visitar conteúdos de risco	.50±.67	.45±.63	.106
Guardião eficaz			
Proteção do software/ hardware	2.41±.92	1.95±1.06	**.001**
Comportamentos de evitamento	.94±.88	.58±.77	**.001**
Informação	.12±.39	.24±.57	**.001**
Comportamentos de proteção	2.35±.84	2.18±.87	**.001**
Conhecimento informático	1.92±.67	1.83±.66	**.011**

Anexo 7: Vitimação online durante a pandemia de Covid-19

	Vitimação online	
Cibercrimes	**N**	**%**
Phishing	447	61.5
Hacking	142	19.8
Cyberstalking	112	15.4
Software malicioso	100	13.8
Cyberbullying	96	13.2
Fraude online	77	10.6
Extorsão	25	3.4
Furto de identidade online para cometimento de crimes	23	3.2
Furto de identidade online para criação de perfis falsos	21	2.9
Fraude Mbway	17	2.3
Variabilidade (de 0 a 9)	**X**	**SD**
	1.45	1.34

Anexo 8: Alvo adequando durante a pandemia

		Alvo adequado
		N (%)
Comunicou com desconhecidos online.	Aumentou	117 (16%)
	Diminuiu	57 (7.8%)
	Manteve-se	556 (76.2%)
Forneceu os seus dados pessoais a alguém desconhecido.	Aumentou	21 (2.9%)
	Diminuiu	79 (10.8%)
	Manteve-se	630 (86.3%)
Abriu anexos desconhecidos dos e-mails que recebeu.	Aumentou	14 (1.9%)
	Diminuiu	75 (10.3%)
	Manteve-se	641 (87.8%)
Abriu um link desconhecido dos e-mails que recebeu.	Aumentou	12 (1.6%)
	Diminuiu	77 (10.5%)
	Manteve-se	641 (87.6%)
Abriu algum ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido.	Aumentou	14 (1.9%)
	Diminuiu	77 (10.5%)
	Manteve-se	639 (87.5%)
Clicou em mensagens pop-up.	Aumentou	20 (2.7%)
	Diminuiu	75 (10.3%)
	Manteve-se	635 (87%)
Visitou websites duvidosos.	Aumentou	66 (9%)
	Diminuiu	85 (11.6%)
	Manteve-se	579 (79.3%)

Anexo 9: Guardião eficaz durante a pandemia

		Guardião eficaz
		N (%)
Evita utilizar o banco online.	Aumentou	37 (5.1%)
	Diminuiu	168 (23%)
	Manteve-se	525 (71.9%)
Evita fazer compras online.	Aumentou	48 (6.6%)
	Diminuiu	297 (40.7%)
	Manteve-se	385 (52.7%)

Utiliza apenas um computador.	Aumentou	83 (11.4%)
	Diminuiu	87 (11.9%)
	Manteve-se	560 (76.7%)
Utiliza filtro de spam no e-mail.	Aumentou	67 (9.2%)
	Diminuiu	22 (3%)
	Manteve-se	641 (87.8%)
Altera as definições de segurança.	Aumentou	100 (13.7%)
	Diminuiu	20 (2.7%)
	Manteve-se	610 (83.6%)
Utiliza diferentes palavras-passes para diferentes sites.	Aumentou	111 (15.2%)
	Diminuiu	19 (2.6%)
	Manteve-se	600 (82.2%)
Evita abrir e-mails de pessoas que não conhece.	Aumentou	61 (8.4%)
	Diminuiu	29 (4%)
	Manteve-se	640 (87.7%)
Visita apenas websites fidedignos.	Aumentou	66 (9%)
	Diminuiu	49 (6.7%)
	Manteve-se	615 (84.2%)
Tem instalado e atualizado o software antivírus	Aumentou	68 (9.3%)
	Diminuiu	20 (9.3%)
	Manteve-se	642 (87.9%)
Tem instalado e atualizado o software ou hardware firewall.	Aumentou	61 (8.4%)
	Diminuiu	20 (2.7%)
	Manteve-se	649 (88.9%)
Participa em workshops destinados à prevenção do cibercrime.	Aumentou	37 (5.1%)
	Diminuiu	34 (4.7%)
	Manteve-se	659 (90.3%)
Visita websites destinados à educação pública sobre o cibercrime.	Aumentou	39 (5.3%)
	Diminuiu	31 (4.2%)
	Manteve-se	660 (90.4%)

Anexo 10: Exposição online durante a pandemia

		Exposição online
		N (%)
Banco online e gestão de finanças	Aumentou	274 (37.5%)
	Diminuiu	21 (2.9%)
	Manteve-se	435 (59.6%)
E-mail ou mensagens instantâneas	Aumentou	390 (53.4%)
	Diminuiu	18 (2.5%)
	Manteve-se	322 (44.1%)
Ver televisão ou ouvir rádio	Aumentou	261 (35.8%)
	Diminuiu	53 (7.3%)
	Manteve-se	416 (57%)
Ler jornais online ou websites de notícias	Aumentou	282 (38.6%)
	Diminuiu	25 (3.4%)
	Manteve-se	423 (57.9%)
Participar em salas chat ou outros fóruns	Aumentou	250 (34.2%)
	Diminuiu	50 (6.8%)
	Manteve-se	430 (58.9%)
Ler ou escrever blogs	Aumentou	98 (13.4%)
	Diminuiu	42 (5.8%)
	Manteve-se	590 (80%)
Fazer downloads de músicas, filmes, jogos ou podcasts	Aumentou	228 (31.2%)
	Diminuiu	50 (6.8%)
	Manteve-se	452 (61.9%)
Redes sociais (Facebook, LinkedIn, Instagram, Twitter, etc.)	Aumentou	458 (62.7%)
	Diminuiu	32 (4.4%)
	Manteve-se	240 (32.9%)
Trabalho ou estudo	Aumentou	493 (67.5%)
	Diminuiu	46 (6.3%)
	Manteve-se	191 (26.2%)
Comprar bens ou serviços online	Aumentou	439 (60.1%)
	Diminuiu	28 (3.8%)
	Manteve-se	263 (36%)

Anexo 11: Vitimação por furto de identidade *online* de acordo com as variáveis individuais (género, habilitações literárias e estatuto socioeconómico)

	Vítima	Não Vítima	X2	*p*
Género				
Masculino (0)	13	190	1.68	.20
Feminino (1)	49	472		
Habilitações literárias				
Até ao 12º ano (1)	22	299	7.07	**.029**
Licenciatura (2)	18	228		
Mestrado, Pós-Graduação ou Doutoramento (3)	22	139		
Estatuto socioeconómico				
Baixo (1)	9	90	.51	.78
Médio (2)	51	543		
Alto (3)	2	35		

Anexo 12: Furto de identidade *online* de acordo com a idade e medo geral do crime

	N (%)	M±SD	*p*
Idade			
Não vítima	664	26.23±11.80	.68
Vítima	61	26.89±11.46	
Medo geral do crime			
Não vítima	668	2.39±.71	.23
Vítima	62	2.51±.78	

Anexo 13: Vitimação por furto de identidade *online* de acordo com o medo e risco percebido de furto de identidade online

		Medo de furto de identidade online	
Vitimação por furto de identidade online	**N (%)**	**M±SD**	***p***
Não (0)	668	3.14±.74	.54
Sim (1)	62	3.08±.78	
		Risco percebido de furto de identidade online	
Vitimação por furto de identidade online	**N (%)**	**M±SD**	***p***
Não (0)	668	2.09±.64	.06
Sim (1)	62	2.32±.90	

Anexo 14: Locais de acesso à *Internet* e vitimação por furto de identidade online

	Furto de identidade online			
Locais de acesso à Internet	**V**	**NV**	**X2**	***p***
Casa				
Não (0)	0	2	.186	.666
Sim (1)	62	666		
Local onde estuda/trabalha				
Não (0)	3	57	1.026	.311
Sim (1)	59	611		
Locais públicos				
Não (0)	8	165	4.367	**.037**
Sim (1)	54	503		
Estabelecimentos comerciais				
Não (0)	17	260	3.188	.074
Sim (1)	45	408		

Anexo 15: Locais de acesso à *Internet* e medo do furto de identidade *online*

	Medo de furto de identidade online		
	N (%)	**M±SD**	***p***
Casa			
Não (0)	2	3.17±.71	.95
Sim (1)	728	3.31±.75	
Local onde estuda/trabalha			
Não (0)	60	3.27±.76	.14
Sim (1)	670	3.12±.75	
Locais públicos			
Não (0)	173	3.11±.77	.72
Sim (1)	557	3.13±.74	
Estabelecimentos comerciais			
Não (0)	277	3.10±.80	.71
Sim (1)	453	3.15±.71	

Anexo 16: Medo de furto de identidade online durante a pandemia

		Medo de furto de identidade online
		N (%)
Alguém furtar os seus dados pessoais e financeiros via online.	Aumentou	208 (28.5%)
	Diminuiu	7 (1%)
	Manteve-se	515 (70.5%)
Alguém utilizar os seus dados pessoais e financeiros online para obter ganhos financeiros.	Aumentou	201 (27.5%)
	Diminuiu	12 (1.6%)
	Manteve-se	517 (70.8%)
Alguém danificar a sua reputação com base na utilização ilegítima dos seus dados pessoais e financeiros online.	Aumentou	172 (23.6%)
	Diminuiu	10 (1.4%)
	Manteve-se	548 (75.1%)

Anexo 17: Perceção do risco de vitimação por furto de identidade *online* de acordo com as variáveis individuais (género, habilitações literárias, situação profissional e estatuto socioeconómico)

		Perceção do risco de furto de identidade *online*	
	N (%)	**M±SD**	***p***
Género			
Masculino (0)	203	2.09±.67	.53
Feminino (1)	521	2.13±.67	
Habilitações literárias			
Até ao 12º ano (1)	321	2.08±-65	.66
Licenciatura (2)	246	2.10±.69	
Mestrado, Pós-Graduação ou Doutoramento (3)	161	2.20±.68	
Estatuto socioeconómico			
Baixo (1)	99	2.17±.75	.36
Médio (2)	594	2.12±.66	
Alto (3)	37	1.91±.65	

Anexo 18: Predição do medo de furto de identidade *online* a partir das variáveis individuais (género, idade, estatuto socioeconómico, habilitações literárias, medo geral do crime e vitimação por furto de identidade)

Variável	B	SE B	β	t	*p*
Género	.246	.064	.148	3.832	**.001**
Idade	.004	.003	.067	1.582	.114
Estatuto socioeconómico	-.086	.066	-.049	-1.317	.188
Habilitações literárias	-.076	.038	-.084	-1.99	**.047**
Medo geral	.073	.040	.071	1.815	.070
Vitimação por furto de identidade online	-.080	.099	-.030	-.813	.417

Nota: r= .203; r^2 =.041; r^2 ajustado= .033 (*p*=.001)

Anexo 19: Predição do medo de furto de identidade *online* a partir das variáveis contextuais (exposição *online*, alvo adequado e guardião eficaz)

Componente	Variável	B	SE B	β	t	*p*
Exposição online	Rotinas financeiras	.030	.017	.085	1.769	.077
	Rotinas de trabalho/ estudo	.013	.023	.024	.583	.560
	Rotinas de lazer	.024	.011	.088	2.247	**.025**
	Horas online	-.005	.009	-.023	-.063	.546
Alvo adequado	Interação com estranhos	-.103	.046	-.083	-2.227	**.026**
	Abrir links duvidosos	-.010	.054	-.007	-.181	.857
	Visitar conteúdos de risco	.005	.045	.004	.111	.912
Guardião eficaz	Proteção do software/ hardware	-.021	.024	-.032	-.851	.395
	Comportamentos de evitamento	.166	.041	.170	4.040	**.001**
	Informação	.145	.048	.111	3.014	**.003**
	Comportamentos de proteção	.020	.032	.024	.629	.530
	Conhecimento informático	-.199	.044	-.177	-4.571	**.001**

Nota: r= .290; r^2 = .084; r^2 ajustado= .067 (*p*=.001)

Anexo 20: Predição da perceção do risco de vitimação por furto de identidade *online* a partir das variáveis individuais (género, idade, estatuto socioeconómico, habilitações literárias, medo geral do crime e vitimação)

Variável	B	SE B	β	t	*p*
Género	.011	.058	.007	.184	.854
Idade	.004	.002	.065	1.541	.124
Estatuto socioeconómico	-.121	.059	-.076	-2.032	**.043**
Habilitações literárias	.037	.035	.045	1.055	.292
Medo Geral	.066	.037	.071	1.798	.073
Vitimação por furto de identidade online	.198	.089	.083	2.219	**.027**

Nota: r= .157; r^2 =.025; r^2 ajustado= .016 (*p*=.007)

Anexo 21: Predição da perceção do risco de vitimação por furto de identidade *online* a partir das variáveis contextuais (exposição *online*, alvo adequado e guardião eficaz)

Componente	Variável	B	SE B	β	t	*p*
Exposição online	Rotinas financeiras	.045	.015	.141	2.926	**.004**
	Rotinas de trabalho/ estudo	.014	.020	.030	.699	.485
	Rotinas de lazer	-.010	.010	-.074	-1.872	-062
	Horas online	-.007	.008	-.034	-.915	.361
Alvo adequado	Interação com estranhos	.067	.042	.060	1.604	.109
	Abrir links duvidosos	.054	.049	.041	1.096	.274
	Visitar conteúdos de risco	.019	.041	.018	.465	.642
Guardião eficaz	Proteção do software/ hardware	-.037	.022	-.063	-1.659	.097
	Comportamentos de evitamento	.001	.037	.002	.037	.970
	Informação	.113	.044	.096	2.593	**.010**
	Comportamentos de proteção	.007	.029	.009	.239	.811
	Conhecimento informático	-.189	.040	-.187	-4.783	**.001**

Nota: r= .262; r^2 = .069; r^2 ajustado= .052 (*p*=.001)

Anexo 22: Predição da vitimação de furto de identidade *online* de acordo com as variáveis individuais (género, idade, habilitações literárias e estatuto socioeconómico)

Variável	B	SE	OR	*p*
Género	.503	.338	1.653	.137
Idade	.004	.012	1.004	.772
Habilitações literárias	.334	.295	1.397	.258
Estatuto socioeconómico	-.306	.312	.736	.326
X^2 + *p*		5.068; *p*= .280		
-2. Log Likelihood		412.577		
Nagelkerke R^2		.016		

Anexo 23: Predição da vitimação de furto de identidade *online* de acordo com as variáveis contextuais

	Variável	B	SE	OR	*p*
Exposição online	Rotinas financeiras	.122	.096	1.130	.201
	Rotinas de trabalho/ estudo	-.079	.119	.924	.503
	Rotinas de lazer	-.029	.058	.971	.615
	Tempo na *internet*	.006	.049	1.006	.905
Formas de pagamento	Paypal	-.280	.332	.756	.400
	Cartão de crédito	.195	.305	1.215	.523
	Mbnet	-.279	.438	.757	.525
	Paysafecard	-.367	1.139	.693	.747
	Homebanking	-.106	.311	.899	.733
	Mbway	.047	.313	1.048	.881
Alvo adequado	Interação com estranhos	.375	.227	1.455	.099
	Abrir links duvidosos	.485	.215	1.624	**.024**
	Visitar conteúdos de risco	-.104	.242	.901	.668
Guardião eficaz	Proteção do *software/ hardware*	.056	.130	1.058	.664
	Comportamentos de evitamento	.324	.218	1.382	.139
	Informação	.465	.215	1.593	**.031**
	Comportamentos de proteção	.131	.177	1.140	.459
	Conhecimento informático	-.212	.226	.809	.348
X^2 + *p*		15.675; *p*= .267			
-2. Log Likelihood		376.801			
Nagelkerke R^2		.060			

Anexo 24: Consentimento Informado

Consentimento Informado

O presente questionário visa recolher dados para a realização de uma dissertação de Mestrado em Criminologia pela Faculdade de Direito da Universidade do Porto. A presente dissertação tem como grande finalidade estudar a Vitimação e o Sentimento de Insegurança no Furto de Identidade Online, fazendo uma comparação entre o momento pré e pós Pandemia de Covid-19.

Ao preencher o questionário, garantimos que todas as informações prestadas serão anónimas, confidenciais e que os dados que fornecer serão utilizados apenas no âmbito da presente investigação. Pedimos-lhe, assim, que não coloque o seu nome ou qualquer outro elemento identificativo ao longo das suas respostas. A sua participação é totalmente voluntária e o preenchimento do questionário não demorará mais do que 15 minutos.

Caso surja alguma dúvida pode contactar-nos através do e-mail: up201606389@up.pt.

Obrigada pela sua colaboração!

FACULDADE DE **DIREITO**