

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

PREDITORES DO MEDO E VITIMAÇÃO *ONLINE*: UM ESTUDO EMPÍRICO

José Pedro Patrocínio Martins

M

2021

Dissertação apresentada à Faculdade de Direito
da Universidade do Porto para obtenção do
grau de Mestre em Criminologia, elaborada sob
orientação da Professora Doutora Inês Maria
Ermida de Sousa Guedes



RESUMO

A presente dissertação procurou, através de uma metodologia quantitativa, perceber que fatores influenciam os níveis de medo do cibercrime e da vitimação *online* (a partir de uma componente relativa à propriedade – fraude ao consumidor *online*, furto de identidade *online* –, e uma componente interpessoal – cyberbullying, *cyberstalking* –, assim como vitimação por *phishing* e descoberta de *software* malicioso). Para alcançar estes objetivos, foi aplicado um questionário *online* a uma amostra de 726 indivíduos, que mediu variáveis sociodemográficas, variáveis constituintes da Teoria das Atividades de Rotina (Cohen & Felson, 1979), a percepção do risco de vitimação *online*, a experiência de vitimação *online*, assim como o medo sentido no contexto *offline*. Dos 726 indivíduos, 440 reportaram ter sido vítimas de pelo menos um cibercrime. No que respeita ao medo do cibercrime, o estudo sugere uma forte influência do medo proveniente do contexto *offline*, na medida em que, quem reportou ter medo de crimes contra a propriedade, medo de crimes interpessoais e maior insegurança económica, reportou níveis mais elevados de medo *online*. Segundo a tese das vulnerabilidades, os indivíduos menos escolarizados reportaram maiores níveis de medo *online*. A Teoria das Atividades de Rotina (TAR) mostrou ter importância no medo do cibercrime: abrir ficheiros desconhecidos e adotar comportamentos e ferramentas de segurança (guardião) relacionaram-se positivamente com o medo *online*; quem possui menos conhecimentos informáticos reportou mais medo *online*. Por fim, o risco percebido de vitimação *online* influenciou o medo sentido *online*, contudo a experiência de vitimação *online* foi independente deste. Relativamente à segunda variável dependente, a vitimação *online*, a TAR também foi importante na sua explicação, já que, comunicar ou fornecer dados a desconhecidos aumentou, em mais do dobro, a chance de ocorrer vitimação por cibercrime. A percepção que os indivíduos têm de serem vitimados *online* relacionou-se positivamente com a chance efetiva de serem vítimas por cibercrime. Por fim, enquanto os anos de escolaridade aumentaram a chance de vitimação, rendimentos mais altos foram associados a uma menor probabilidade de ocorrer vitimação *online*. Os resultados do presente estudo, assim como as suas implicações, irão ser discutidos.

Palavras-chave: medo do cibercrime; cibercrime; vitimação online; sentimento de insegurança; risco percebido online; medo *offline*; atividades de rotina.

ABSTRACT

This study aims to explore, in one hand, the predictors of fear of cybercrime, and the predictors of cybervictimization (a composite measure of property – *online* consumer fraud, *online* identity theft – and interpersonal cybercrime – cyberbullying and cyberstalking –, as well as *phishing* and *malware* discovery). This quantitative study employs an *online* questionnaire applied to 726 individuals, measuring sociodemographic variables, routine activities variables, stemming from the Routine Activities Theory (Cohen & Felson, 1979), perception of *online* victimization risk, previous *online* victimization, as well as *offline* fear of crime. Of the total of 726 individuals, 440 were already victims of at least one cybercrime. Concerning the fear of cybercrime, it was observed that the predictors were *offline* interpersonal fear, *offline* property fear and economic insecurity, showing that *offline* fear of crime is positively related to the composite measure of fear of cybercrime. According to the vulnerability thesis, less educated individuals reported higher levels of fear *online*. Moreover, Routine Activities Theory (RAT) showed to have an importance in the fear of cybercrime since open unknown files and adopting security behaviors (guardianship) were positively related to fear of cybercrime; computer skills, where individuals with higher skills report to feel lower levels of fear of cybercrime. Finally, perceived risk of *online* victimization influenced fear *online*, however previous *online* victimization was independent. Regarding *online* victimization, this study suggests that RAT is also important to explain it since communicate or give personal information to unknown individuals increased twice the likelihood of being victimized *online*. The perception that individuals have of being victimized *online* was positively related to the actual chance of being victims of cybercrime. Lastly, while the years of education increased the likelihood of victimization, higher incomes were associated with lower likelihood of being *online* victimization. These results will be discussed in the line of the main theories used to explain both fear of cybercrime and *online* victimization.

Key-words: fear of cybercrime; cybercrime; *online* victimization; feelings of insecurity, online risk perception, *offline* fear; routine activities

AGRADECIMENTOS

Findo o último detalhe desta dissertação, torno a uma seção que me permite registrar, com todo o decoro e mais algum, todo o apoio dispensado nesta longa caminhada.

À Professora Doutora Inês Sousa Guedes, minha Orientadora, agradeço todo o apoio conferido desde o primeiro dia. Acima de tudo, venero a firmeza e motivação inculcada em procurar dar e encontrar sempre algo mais, e por toda a disponibilidade profissional e pessoal oferecida.

Aos meus amigos e colegas, um especial obrigado por todos os diálogos produtivos e de ajuda acadêmica, mas sobretudo pela alegria e bem-estar do corpo e da alma.

Não menos importante, felicito todos e todas as pessoas que superaram as adversidades dos últimos tempos...

Por fim, agradeço à minha família toda a fortuna presenteada. Mil vidas não chegariam para agradecer todo o amor, carinho e amizade.

Índice Geral

RESUMO	II
ABSTRACT	III
AGRADECIMENTOS	IV
ÍNDICE DE ANEXOS	VII
ÍNDICE DE TABELAS	VIII
ABREVIATURAS E SIGLAS	X
INTRODUÇÃO	1
CAPÍTULO I – Enquadramento Teórico	3
1. Evolução da cibercriminalidade	3
1.1. Definição e tipologias do cibercrime	4
2. Cibercrimes a estudar	7
2.1. Fraude <i>online</i> (financeira)	7
2.1.1. Fraude ao consumidor <i>online</i>	8
2.1.2. Furto de identidade <i>online</i>	10
2.2. <i>Phishing</i>	11
2.3. Descoberta de <i>software</i> malicioso	13
2.4. Crimes Interpessoais <i>online</i>	14
2.4.1. <i>Cyberstalking</i>	15
2.4.2. Ciberbullying	17
3. Teoria das Atividades de Rotina	18
3.1. Exposição a ofensores motivados	20
3.2. Alvo adequado	22
3.3. Guardião	25
4. Variáveis explicativas da vitimação <i>online</i>	27
5. Sentimento de Insegurança	28
5.1. Medo do crime	29
5.2. Perceção do risco de vitimação	29
5.3. Comportamentos de segurança	30
6. Variáveis explicativas do medo do cibercrime	31
6.1. Variáveis contextuais aplicadas ao medo do cibercrime	31
6.2. Variáveis individuais aplicadas ao medo do cibercrime	31
CAPÍTULO II – Estudo Empírico (Metodologia)	35

1. Objetivos	35
2. Hipóteses	36
2.1. Medo de vitimação <i>online</i> :	36
2.2. Vitimação <i>online</i> :	36
3. Caraterização do estudo	37
4. Forma de constituição da amostra	37
5. Instrumento e Variáveis	38
5.1. Secção I – Questões pessoais e sociodemográficas	38
5.2. Secção II – Questões relativas ao contexto e forma de aceder à <i>Internet</i>	38
5.3. Secção III – Teoria das Atividades de Rotina <i>online</i>	39
5.4. Secção IV – Medição do medo de vitimação <i>online</i> , insegurança geral, medo <i>offline</i> interpessoal e medo <i>offline</i> propriedade	42
5.5. Secção V – Perceção do risco de vitimação <i>online</i> e experiência de vitimação <i>online</i>	43
6. Procedimentos de recolha de dados	44
7. Procedimentos de análise estatística	45
7.1. Análise estatística descritiva	45
7.2. Análise estatística inferencial	46
CAPÍTULO III – Análise dos resultados	47
1. Caraterização descritiva das variáveis	47
1.1. Caraterização da amostra segundo os dados sociodemográficos	47
1.2. Caraterização da amostra segundo o tipo de dispositivo e o local de acesso à <i>Internet</i>	48
1.3. Caraterização da amostra segundo as variáveis da Teoria das Atividades de Rotina <i>online</i>	49
1.4. Caraterização da amostra segundo o medo <i>online</i> , perceção do risco de vitimação <i>online</i> , insegurança geral e medo <i>offline</i> interpessoal e propriedade	50
1.5. Caraterização da amostra segundo a vitimação <i>online</i>	51
2. A relação entre o medo do cibercrime e as variáveis independentes	52
2.1. Medo do cibercrime e variáveis sociodemográficas	52
2.2. Medo de cibercrime em função do tipo de dispositivo informático e local de acesso à <i>Internet</i>	53
2.3. Medo de cibercrime e Teoria das Atividades de Rotina	54
2.4. Medo de cibercrime e medo <i>offline</i> , insegurança geral e perceção do risco de vitimação <i>online</i>	55
2.5. Medo de cibercrime e experiência de vitimação <i>online</i>	56

3. A relação entre vitimação <i>online</i> e as variáveis independentes	56
3.1. Vitimação <i>online</i> e variáveis sociodemográficas	57
3.2. Vitimação <i>online</i> em função do tipo de dispositivo informático e local de acesso à Internet	58
3.3. Vitimação <i>online</i> e Teoria das Atividades de Rotina	58
3.4. Vitimação <i>online</i> em função do medo <i>offline</i>, insegurança geral e percepção do risco de vitimação <i>online</i>	59
4. Variáveis preditoras do medo do cibercrime e da vitimação <i>online</i>	60
4.1. Variáveis preditoras do medo do cibercrime	60
4.2. Variáveis preditoras da vitimação <i>online</i>	62
DISCUSSÃO DOS RESULTADOS	64
BIBLIOGRAFIA	77
ANEXOS	81

ÍNDICE DE ANEXOS

ANEXO 1 – Análise fatorial dos itens da exposição online	81
ANEXO 2 – Análise fatorial dos itens do alvo adequado	81
ANEXO 3 – Itens da exposição online em atividades e alvo adequado a partir da TAR e respetivos alfas de Cronbach que indicam a consistência interna	82
ANEXO 4 – Itens do medo, percepção do risco de vitimação e vitimação online, e respetivos alfas de Cronbach que indicam a consistência interna	82
ANEXO 5 – Testes-t: medo de cibercrime em função do tipo de dispositivo informático e local de acesso à Internet	83
ANEXO 6 – Qui-quadrado: prevalência da vitimação online em função do tipo de dispositivo informático e local de acesso à Internet	83
ANEXO 7 – MODELO 1 – Predição do medo do cibercrime segundo as variáveis sociodemográficas (variáveis independentes)	84
ANEXO 8 – MODELO 2 –Predição do medo do cibercrime segundo as variáveis referentes à TAR (variáveis independentes)	84
ANEXO 9 – MODELO 3 – Predição do medo do cibercrime segundo a insegurança económica, insegurança geral, medo offline interpessoal e propriedade, percepção do risco de vitimação online e vitimação online (variáveis independentes)	85

ANEXO 10 – Predição da chance de vitimação online segundo as variáveis sociodemográficas (variáveis independentes).	85
ANEXO 11 – Predição da chance de vitimação online segundo as variáveis constituintes da TAR e ao percepção do risco de vitimação online (variáveis independentes).	85
Anexo 12 – Itens do medo/vitimação online relativo às componentes propriedade e interpessoal, e respetivos alfas de Cronbach que indicam a consistência interna.	86
ANEXO 13 – Médias do medo online geral e respetivas componentes (propriedade e interpessoal).	86
ANEXO 18 – Medo de vitimação online e offline controlando para o género.	86

ÍNDICE DE TABELAS

Tabela 1 Caraterísticas sociodemográficas (género, estado civil, situação profissional, teletrabalho, percepção sobre os rendimentos do agregado familiar e zona de residência) dos participantes da amostra.	47
Tabela 2 Caraterísticas sociodemográficas (idade, insegurança económica e escolaridade) dos participantes da amostra.	48
Tabela 3 Percentagem dos indivíduos mediante o tipo de dispositivo informático utilizado e o local onde acedem à Internet.	83
Tabela 4 Médias e desvios-padrões da exposição online, alvo adequado, informação disponibilizada online e índice do guardião.	49
Tabela 5 Percentagem dos indivíduos em função da exposição online em horas e conhecimento informático.	50
Tabela 6 Médias e desvios-padrões do medo do cibercrime, percepção do risco de vitimação online, insegurança geral, medo offline interpessoal e medo offline propriedade.	50
Tabela 7 Percentagem dos indivíduos vítimas de furto de identidade online, fraude ao consumidor, cyberbullying, cyberstalking, descoberta de software malicioso e phishing.	51
Tabela 8 Testes-t: medo do crime em função das variáveis género, estado civil, teletrabalho e zona de residência.	52
Tabela 9 Correlações de Pearson: correlações entre ao medo de cibercrime e as variáveis idade, escolaridade e insegurança económica.	53

Tabela 10 Teste ANOVA: medo de cibercrime em função da variável percepção dos rendimentos auferidos pelo agregado familiar.	53
Tabela 11 Correlações Pearson: correlações entre a variável dependente medo do cibercrime e as variáveis constituintes da TAR (exposição online, alvo adequado, informação disponibilizada online e índice do guardião).....	54
Tabela 12 ANOVA: medo do cibercrime em função da exposição online em horas e do conhecimento informático.....	55
Tabela 13 Correlações Pearson: correlações entre a variável dependente medo do cibercrime as variáveis percepção do risco de vitimação online, insegurança geral, medo offline interpessoal e medo offline propriedade.	55
Tabela 14 Testes-t: medo de cibercrime em função da experiência de vitimação online.	56
Tabela 15 Qui-quadrado: prevalência da vitimação online em função das variáveis género, estado civil, teletrabalho e zona de residência.	57
Tabela 16 Testes-t: prevalência da vitimação online em função das variáveis idade, escolaridade, insegurança económica e percepção sobre os rendimentos do agregado familiar.	57
Tabela 17 Testes-t: prevalência de vitimação online em função da exposição online, alvo adequado, informação disponibilizada online e índice do guardião.	58
Tabela 18 Prevalência da vitimação online em função da exposição online em horas e do conhecimento informático.....	59
Tabela 19 Testes-t: prevalência da vitimação online em função das variáveis percepção do risco de vitimação online, insegurança geral, medo offline interpessoal e medo offline propriedade.....	59
Tabela 20 Predição do medo do crime a partir das variáveis que nos modelos anteriores tiveram significado estatístico (género, escolaridade, exposição entretenimento, abrir ficheiros desconhecidos, informação disponibilizada, índice do guardião, conhecimento informático, insegurança económica, medo offline interpessoal e propriedade, percepção do risco de vitimação online e vitimação online.....	62
Tabela 21 Predição da chance de vitimação online a partir das variáveis que nos modelos anteriores tiveram significado estatístico, nomeadamente a escolaridade, os rendimentos, a exposição entretenimento, o alvo adequado comunicar ou fornecer dados a desconhecidos e a percepção do risco de vitimação online.	64

ABREVIATURAS E SIGLAS

art./arts. – Artigo/artigos

APAV – Associação Portuguesa de Apoio à Vítima

C.P. – Código Penal

CERT.PT – Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT – *Computer Emergency Response Team*)

CNCS – Centro Nacional de Cibersegurança.

TIC – Tecnologias de Informação e Comunicação.

VPN – Rede Virtual Privada [Virtual Private Network].

p.e.p. – previsto e punido

INTRODUÇÃO

A presente dissertação procurou explorar um conjunto de fatores individuais e contextuais na relação com duas variáveis independente: o medo do cibercrime e a vitimação online. O enquadramento teórico é feito a partir da Teoria das Atividades de Rotina (TAR) e, em complemento, a partir do Sentimento de Insegurança.

A literatura sobre a vitimação online, nomeadamente quando aplicada à luz da TAR, tem evidenciado resultados mistos da influência da exposição e atratividade, medidas a partir das atividades de rotina online (Reyns & Henson, 2016; Virtanen, 2017). Por sua vez, existem poucos estudos empíricos que analisaram o medo online. Além das críticas às medições da componente emocional do sentimento de insegurança no contexto offline, as mesmas adversidades foram transportadas para o ciberespaço. A medição de ambos os fenómenos no ciberespaço tem encontrado diferentes vias de análise. Por um lado, há estudos que se focam numa medida agregada de vários tipos de cibercrime (e.g., Virtanen, 2017), e, por outro lado, há estudos que se focam particularmente num determinado tipo de cibercrime. Naturalmente, as medidas agregadas de medo/vitimação online perdem algum rigor, porque não permite associar fatores individualizados com a tipologia específica de crime. Outros estudos têm optado por estudar várias tipologias de crime, mas de certa forma congruentes, ou seja, a partir de uma componente financeira (e.g., Brands & Van Wilsem, 2019) e interpessoal (e.g., Henson et al., 2013) tanto para explicar o medo como a vitimação no contexto online.

Todavia, é de salientar que grande parte destes estudos são recentes. Por um lado, os estudos empíricos sobre a vitimação online são mais prevalentes, contribuindo para uma forte densificação da literatura. Por outro lado, os estudos empíricos sobre o medo online são escassos. Com o objetivo de contribuir para este problema, este estudo procurou estudar o medo e a vitimação online a partir de uma medida geral, e complementarmente, analisando os fatores que se relacionam com uma componente de cibercrimes contra a propriedade – furto de identidade online e fraude ao consumidor online -, e com uma componente interpessoal – cyberbullying e cyberstalking. A TAR foi aplicada na relação com ambas as variáveis dependentes, seguindo uma perspetiva da vítima. Para tal, foi aplicado um questionário online a uma amostra de 726 indivíduos.

A estrutura da dissertação é composta por três capítulos principais. O primeiro é relativo ao enquadramento teórico das características pessoais e contextuais, assim como as teorias de apoio, tanto ao medo do cibercrime como à vitimação online. A TAR será analisada de acordo

com a concepção original de Cohen & Felson (1979), nomeadamente quanto à exposição, alvo adequado e ausência de guardiões, nos pressupostos em que foi pensada, ou seja, no contexto físico. Posteriormente, analisar-se-á a sua transposição para o ciberespaço, com vista a explorar relações com a vitimação online, mas também para perceber se é um bom preditor do medo online. Relativamente ao Sentimento de Insegurança, será delineada a explicação das dimensões medo do crime, perceção do risco de vitimação e comportamentos de segurança. As dimensões vão, também elas, transpostas para o ciberespaço, permitindo explorar se os preditores para o contexto tradicional, podem ser aplicados nesse espaço. A dimensão emocional – medo do crime -, é tida como variável dependente e as restantes como independentes. Por sua vez, os comportamentos de segurança serão analisados paralelamente com os guardiões da TAR na passagem para o ciberespaço. No segundo capítulo, expor-se-á a metodologia que guia o estudo, nomeadamente quanto à definição dos objetivos e hipóteses. De seguida, apresentaremos a estrutura do questionário e a operacionalização das variáveis dependentes e independente a medir. Por fim, exporemos como foi aplicado o questionário, tendo em conta os princípios éticos de investigação, e os procedimentos de análise estatística descritiva e inferencial. No último capítulo, apresentaremos a caracterização da amostra quanto às variáveis do estudo, e as relações entre elas. De seguida, exporemos a predição das variáveis dependentes através de modelos de regressão linear e logística. Finalmente, iremos expor a discussão das hipóteses levantadas, e apresentar sugestões e limitações aos resultados encontrados, assim como indicações que futuras investigações poderão seguir.

CAPÍTULO I – Enquadramento Teórico

1. Evolução da cibercriminalidade

A Revolução da Tecnologia Eletrónica Digital mudou radicalmente a forma como se rege a vida em comunidade, contribuindo para o que Marshall McLuhan designa ser uma “aldeia global”. A informação da Era Digital (Webster, 2003 citado em Yar, 2006) e a forma como e onde ela é armazenada e transmitida nos diversos meios tecnológicos é acompanhada por comportamentos e serviços de segurança adequados a protegê-la. Ao mesmo tempo, a globalização, alcançada pela disseminação da *Internet*, repercutiu-se e tem acompanhado os vários domínios e atividades da vida quotidiana: desde a formação educacional até ao mercado de trabalho, à prestação dos serviços económico-financeiros mais básicos como pagar contas ou usufruir do homebanking, à propagação política, à difusão dos *media*, a atividades de lazer ou procura de satisfação de necessidades pessoais, aumentando a dependência da sociedade com a *Internet*. Alguns *websites* apontam para a presença de mais de quatro mil milhões e meio de utilizadores na *Internet* mundialmente¹. Contudo, enquanto evoluem os mecanismos de segurança, progridem também as formas e técnicas empregues no seio da cibercriminalidade. Efetivamente, as Tecnologias de Informação e Comunicação (TIC) fornecem recursos globais instantâneos a baixo custo, pelo que são acessíveis (e tendem a ser cada vez mais) a um número elevado de pessoas. Veja-se, por exemplo, a evolução da indústria dos *smartphones* a preços acessíveis durante a última década. Estas, inevitavelmente, ficam sujeitas a maiores níveis de exposição *online*, contribuindo para que eventuais vitimações *online* ocorram. Os crimes praticados no contexto *online* acarretam perigos inerentes da má utilização das TIC – a partir das ações do utilizador – assim como a partir das ações do potencial ofensor, e os seus custos são tanto incalculáveis como imprevisíveis. Devido ao seu carácter virtual, estendem-se a qualquer parte do mundo e contribuem para um vasto leque de novas oportunidades da atividade criminal, sem precedentes e limitada à legislação nacional de cada ordenamento jurídico (Wall, 2001; Roberts, 2008).

A cibercriminalidade acontece dentro de um sistema global de rede eletrónica digital com múltiplos dispositivos informáticos interconectados, isto é, na *Internet*. Neste espaço, existe um inestimável número de potenciais ofensores e potenciais vítimas. Uma conexão estabelecida na *Internet* entre um recetor e um remetente, ainda que de forma indireta, permite que eventuais vitimações *online* ocorram. Por exemplo, o contato estabelecido através das redes sociais

¹ (e.g., <https://www.internetlivestats.com/>, acesso a 25 de julho de 2021).

possibilita a ocorrência de episódios de cyberbullying, assim como o contato por email possibilita tentativas de *phishing*. As vantagens e acessibilidades que encontramos “à distância de um clique” existem também para o cometimento de atividades criminais. Com a extinção das limitações físicas e temporais, a cibercriminalidade é passível de ser exercida em larga escala com intervalos de tempo diminuídos. Por exemplo, a difusão de *software* malicioso pode ocorrer de forma automatizada para um número inestimável de destinos num curto intervalo de tempo, Furnell, 2002). Ao mesmo tempo, existem inúmeras vantagens para um agressor *online*, como por exemplo, o anonimato, o conforto, a facilidade, o carácter eficiente na execução das atividades, assim como as dificuldades de perseguição, investigação e deteção do cibercrime (Pereira *et al.*, 2016, Dias, 2010). Dias (2010) refere ainda que tanto os cibercrimes económicos como os interpessoais apresentam graves consequências lesivas e devastadoras, em comparação com a criminalidade *offline*. A questão do anonimato no ciberespaço é complexa de descrever, visto que a *Internet* possibilita a manipulação e reinvenção da identidade social, ou seja, um ofensor consegue manipular e criar a sua identidade virtual. Outro aspeto importante é relativo ao uso de VPN's – *Virtual Private Network* – que viabiliza a ocultação do endereço IP de um utilizador, oferecendo uma proteção extra assente na encriptação de todo o tráfego de dados e histórico de *Internet*² (Kaspersky, 2021). Efetivamente, estas questões podem ser utilizadas por qualquer utilizador de modo a acrescentarem nova camada de proteção às suas atividades *online*/para inviabilizar eventuais tentativas de devassa da vida privada. Do mesmo modo, Dias (2010) salienta a importância do direito à reserva da vida privada no ambiente *online*³, contudo, não pode deixar de existir a perseguição criminal de atividades ilícitas.

1.1. Definição e tipologias do cibercrime

De seguida, apresentamos uma delineação abrangente de cibercrime e as tipologias que têm sido empregues na sua classificação.

Num contexto cibernético e tecnológico em constante evolução, torna-se difícil encontrar uma definição apropriada de cibercrime e um sistema de categorização dos vários tipos de ofensas *online* (Tsakalidis *et al.*, 2019). Segundo alguns autores (e.g. Grabosky, 2001; Wall, 2001, 2007), o termo cibercrime envolve o uso do ciberespaço ou a tecnologia de um

² <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn> (acesso a 20 de maio de 2021).

³ O Código Penal elenca alguns crimes que podem ser enquadrados nesta temática, por exemplo, “Devassa da vida privada” – p.e.p. pelo art. 192.º – ou “Devassa por meio de informática” – p.e.p. pelo art. 193.º. (<https://www.direitosedeveres.pt/>, acesso a 28 de julho de 2021). Alguma literatura tem debatido questões de invasão de privacidade online

computador para facilitar atos criminais. Os cibercrimes são cometidos através do uso de redes de comunicação eletrônica e sistemas de informação (European Commission (2020). Relativamente à sua classificação, as distinções têm sido feitas da seguinte forma: por um lado, existem atividades criminais que foram extrapoladas do contexto físico para o contexto virtual, fazendo uso de novos mecanismos na prossecução dos seus objetivos – “crimes assistidos pelo computador”; por outro lado, existem atividades criminais *online* que vão surgindo com o ciberespaço e à medida que este evolui, ou seja, são “crimes focados no computador” (Furnell, 2002). Wall (2007, revisto em 2011), com algumas semelhanças, faz uma divisão tripartida dos objetivos e padrões das ofensas *online*: por um lado, atividades como *hacking*, *cracking* ou a difusão de *software* malicioso são considerados “crimes contra a integridade da máquina”; enquanto “crimes relacionados com computador” são cometidos através do uso da máquina ao facilitar a obtenção de informação da vítima e assim dar seguimento a outros crimes (e.g. *phishing* e outras técnicas de engenharia social); e, por último, “crimes relacionados com o conteúdo do computador” apelam à obscenidade da informação e material presente no computador (e.g. distribuição de pornografia). Em suma, a literatura foca-se, por um lado, nos crimes focados no computador ou crimes contra a integridade da máquina, que se enquadram dentro do que o Wall (2007, 2008) apelida de terceira geração de cibercrimes, isto é, são considerados “verdadeiros” cibercrimes e dependem em exclusivo da *Internet* ou tecnologia para existirem; e por outro lado os crimes assistidos pelo computador. Ao nível das tipologias de vítimas abrangidas, Yar (2005) defende que os cibercrimes são frequentemente classificados de acordo com indivíduos ou a propriedade.

Do ponto de vista de enquadramento legal, Wall (2001) divide o cibercrime em quatro categorias legais, sendo cada uma delas composta por várias atividades: *cyber-trespass*; *cyber-deceptions and thefts*; *cyber-pornography*; *cyber-violence*. A primeira categoria – *cyber-trespass* – alude a atividades que invadem o espaço e a propriedade de outras pessoas ou que causam dano (e.g. *hacking*). A categoria *cyber-deceptions and thefts* abrange crimes contra a propriedade (e.g. furto de identidade *online*). A terceira categoria, *cyber-violence*, inclui crimes contra a pessoa e têm como consequência danos psicológicos (e.g. *ciberbullying*, *cyberstalking*). Por último, a categoria *cyber-pornography* abarca crimes que ultrapassam os limites do obsceno e da decência (crimes contra a moralidade) e decorre da tipologia de “crimes relacionados com o conteúdo do computador” acima descrito⁴. Podemos referir também crimes

⁴ O Wall chama atenção para as diferenças de critérios ao nível moral e legal do que pode ser estabelecido como obsceno ou depravado (2001, p. 6).

contra o estado, cujas atividades violam as leis que protegem a integridade da nação e a sua infraestrutura (e.g. terrorismo, Yar, 2006).

O direito penal português intervém nesta matéria através da proteção do fim criminoso e dos bens-jurídicos visados: fá-lo, por um lado, através do Código Penal [C.P.], e por outro lado, através da proteção dos sistemas informáticos e dos dados informáticos (Lei n.º 109/2009, de 15 de setembro – Lei do Cibercrime). Coexistem também outros regimes jurídicos e disposições legais (e.g. Lei n.º 46/2018, de 13 de agosto que estabelece o regime jurídico da segurança do ciberespaço). Estas disposições sofrem ainda influência de diretivas e decisões-quadro no seio da Europa. Deste modo, existem inconsistências no vocabulário do cibercrime e no ciberespaço que se repercutem ao nível da cooperação transnacional, ou na falta dela (Tsakalidis *et al.*, 2019), e nas definições que académicos e legisladores utilizam para um determinado tipo de crime. Em alguns casos não se observa sequer uma referência explícita e específica plasmada na lei do termo cibercrime (Wall, 2001, p. 2). Por outro lado, existe uma propagação de informações e diretrizes que advêm de diferentes setores: disposições legais/legislativas como o Código Penal, agências de aplicação da lei, empresas de segurança cibernética como o centro nacional de cibersegurança e o setor académico (Tsakalidis *et al.*, 2019).

O atual panorama ciber-situacional agravado pela pandemia Covid-19 fez aumentar os casos de cibercriminalidade. Em Portugal, o *Relatório Riscos & Conflitos 2021* do CNCS – Centro Nacional de Cibersegurança – assinala incrementos de *phishing/smishing* e infeção por *malware*, nomeadamente a partir do primeiro confinamento social até ao fim do ano, como as os incidentes mais registados no CERT.PT – Equipa de Resposta a Incidentes de Segurança Informática Nacional⁵. Estes dados são auxiliados pela migração em massa para o ambiente *online* durante os meses de confinamento social e que se foi mantendo até aos dias de hoje, aumentando assim os alvos *online* e as oportunidades para o crime. Também as questões financeiras encontram avultados volumes de prejuízos. O relatório *Internet Crime Report 2020*⁶ do FBI assinala prejuízos de 4.2 mil milhões de USD causados por fraudes *online* (e.g. *phishing*, *smishing*, *pharming*, pagamento de bens ou serviços que não são entregues), infeção por *malware* (e.g. *ransomware*) e extorsão.

⁵ O CERT.PT é um serviço integrante da Rede Nacional de CSIRTs (Computer Security Incident Response Team e do CNCS (Centro Nacional de Cibersegurança).

⁶ O relatório teve em conta o público americano.

2. Cibercrimes a estudar

Ao longo deste capítulo, expomos um conjunto de vitimações *online* categorizadas a partir de uma componente financeira (fraude ao consumidor e furto de identidade) e uma componente interpessoal (ciberbullying e *cyberstalking*). De modo a garantir um maior nexo quanto ao conteúdo tipológico da cibercriminalidade, estudar-se-á também a vitimação por *phishing* e a descoberta de *software* malicioso – *malware*.

Além das dificuldades existentes em encontrar um consenso entre as definições que os académicos e não académicos usam, é de realçar que o enquadramento com a lei penal portuguesa também não é claro. Com exceção do *hacking* que tem como correspondente direto o artigo 6.º da Lei do Cibercrime – “Acesso ilegítimo” – para os restantes não há uma referência direta e explícita na lei penal. Por um lado, relativamente à componente financeira, a fraude ao consumidor *online* pode ser enquadrada como “Burla informática e nas comunicações” (p.e.p. pelo art. 221.º do C.P.). Por sua vez, o furto de identidade *online* pressupõe duas atividades criminais para a sua consumação: além da usurpação de informação pessoal ou financeira é necessário uma segunda atividade criminosa que pode ter várias finalidades e consequentemente diferentes formas de enquadrar com a lei (e.g. o prejuízo patrimonial pode ser enquadrado à luz da burla informática; o dano à reputação pode ser enquadrado à luz do crime de difamação, p.e.p. pelo art. 180.º e por força do art. 182.º “Equiparação” quando refere por qualquer outro meio de expressão). Relativamente à componente interpessoal, o ciberbullying e o *cyberstalking* provêm essencialmente das atividades tradicionais do mundo *offline*. Enquanto o *cyberstalking* pode ser enquadrado à luz do artigo 154.º -A “Perseguição”, o ciberbullying não está tipificado como crime em Portugal. No que toca à distribuição de *software* malicioso, devido às suas finalidades, pode ser enquadrado em vários artigos da Lei do Cibercrime – Lei n.º 109/2009 de 15 de setembro (e.g. art. 3.º “Falsidade informática”; art. 4.º “Dano relativo a programas”; art. 5.º “Sabotagem informática”; art. 6.º “Acesso ilegítimo”; art. 7.º “Interceção ilegítima”, Venâncio, 2011). Por último, o *phishing* acaba por ser negligenciado pela falta de qualificação penal, apesar de ser já uma atividade bastante dinamizada e conhecida no meio informático.

2.1.Fraude *online* (financeira)

A conexão à *Internet* tem evoluído favoravelmente em termos de acessibilidade e celeridade no contexto de transações *online* – e-commerce. Para este efeito, existem vários dispositivos informáticos, como por exemplo, um *smartphone*, computador, tablet, TV ou até uma consola

de jogar, que os consumidores podem utilizar para aceder a uma determinada loja *online* e efetuar os seus pedidos. Ao mesmo tempo, pode ser o consumidor a ser contactado, quando por exemplo, recebe ofertas de publicidade e marketing. Em ambas as interações podem suceder-se situações de vitimação. Por um lado, o consumidor pode efetuar a compra de um determinado bem que nunca lhe é entregue. Por outro lado, quando recebe emails, pode tratar-se de uma tentativa de *phishing* com vista a enganar e defraudar a vítima. Este conjunto de fraudes *online* (também conhecidas como *scams online*, Yar, 2006, p. 80) são perpetrados muitas vezes por sistemas automatizados, alargando a rede de potenciais vítimas.

A fraude *online* é um tipo generalizado de crime que engloba diferentes tipologias de vitimação no meio *online*. Pode ser definida como “*Fazer desonestamente uma representação falsa (inverídica ou enganosa) com o objetivo de ganho ou com a intenção de causar perda*” (de algo material) (Law, 2018). As motivações são maioritariamente financeiras (Yu, 2014) e assumem especial gravidade pelas somas avultadas de prejuízos financeiros que registam anualmente. Dois exemplos de cibercrimes cujo foco principal é a vertente patrimonial são a fraude ao consumidor e o furto de identidade. O primeiro centra-se em exclusivo nas transações do e-commerce e o segundo abrange vários domínios que veremos de seguida. Ambos são crimes pré-existentes no contexto *offline*, mas ganham novas formas de se reproduzirem no ciberespaço, ou seja, são crimes assistidos pelo computador (Furnell, 2002). “Computador” é aqui entendido como qualquer dispositivo informático passível de facilitar a atividade criminosa. Van Wilsem (2019, p. 3) refere que “*(...) as experiências de vitimação relacionadas com crimes financeiros online ou um estágio preparatório (hacking, infeção por malware) representam uma grande parte do número total de experiências de vitimação por cibercrime*”.

2.1.1. Fraude ao consumidor online

Um dos subdomínios da fraude *online* é a fraude cometida no campo do e-commerce. Este tipo de vitimação peca, de forma geral, pela baixa quantidade de estudos empíricos que o têm analisado. De acordo com o European Commission (2020), a fraude ao consumidor *online* acontece quando “*o consumidor 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*”. Estas situações são frequentemente vinculadas a fraudes de leilão *online* (Yar, 2006, p. 82; FBI⁷). De acordo com a primeira parte da definição – comprar produtos ou serviços – a

⁷ <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-auction-fraud> (acesso a 15 de maio de 2021).

problemática incide essencialmente sobre a forma de pagamento. Esta pode ser feita a partir de um site falso (*pharming*), pelo que a compra do produto que a vítima pretendia nunca se efetivou, ou seja, o produto não vai ser entregue. Pode também acontecer que no ato da transação *online*, a transmissão da informação pessoal não seja segura ou seja armazenada pelo fornecedor de serviços ou pela própria loja *online* (Brands & Van Wilsen, 2019). Relativamente aos produtos que são comprados e recebidos, estes podem ser diferentes da forma como foram previamente anunciados (e.g., podem ser falsificados, podem ser produtos em segunda mão ou não funcionarem plenamente ou podem ser produtos inflacionados, mas que estavam em promoção, Yar, 2006, p. 83).

Brands & Van Wilsen (2019) identificam outras formas de fraude ao consumidor, tais como esquemas de adiantamento de taxas, também conhecidos como fraude nigeriana ou scam 419 (i.e., o fraudador pede ajuda para que a vítima pague quantias adiantadas e em retorno receberia algo de valor superior como uma comissão ou um prémio (FBI⁸; Investopedia⁹) e esquemas em pirâmide.

O estudo de Van Wilsem (2013) elenca algumas medidas de prevenção situacional do crime que permitem maior segurança no ato de fazer compras *online*: por exemplo, os sites de leilões *online* podem receber feedback dos clientes de acordo com a atuação dos vendedores, permitindo monitorizar e até recusar vendedores com classificações negativas ou incutir a utilização de métodos de pagamento *online* mais seguros como o PayPal. Existem também agências e fóruns que podem ajudar e informar os consumidores sobre determinadas situações de perigo (e.g. DECO Proteste – Associação Portuguesa Para a Defesa do Consumidor). Outro exemplo advém da DSP2 (Diretiva dos Serviços de Pagamento revista), que “(...) *visa trazer mais comodidade aos pagamentos, centralizando e facilitando o acesso à informação, ao mesmo tempo que obriga a novos requisitos de segurança, proporcionando maior proteção aos utilizadores*”¹⁰, e que se podem materializar no uso de cartões encriptados e temporários para compras únicas como o *MB Way*. Todas estas questões permitem um uso mais seguro da *Internet*, nomeadamente em contexto de e-commerce. O medo resultante destas atividades pode ter como consequência a quebra da confiança e segurança do consumidor *online* (Lynch, 2005, citada em Roberts *et al.*, 2013).

⁸ <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/advance-fee-schemes> (acesso a 15 de maio de 2021).

⁹ <https://www.investopedia.com/terms/n/nigerianscam.asp> (acesso a 15 de maio de 2021).

¹⁰ <https://www.cgd.pt/Site/Saldo-Positivo/guias-e-infografias/Pages/DSP2-O-que-muda.aspx> (acesso a 10 de março de 2021).

2.1.2. Furto de identidade *online*

O furto de identidade *online* é também ele um subdomínio de fraude *online*. No ordenamento jurídico português é um fenómeno que outrora teve qualificação penal (art. 38.º da Lei nº 12/91, de 21 de maio – Lei da Identificação Civil e Criminal). Com a evolução das TIC, merece uma maior reflexão do ponto de vista jurídico-penal, nomeadamente no que toca às diferenças encontradas nas definições tanto do furto de identidade *online* como dos diferentes *modus operandi* e técnicas que têm em vista a usurpação de informação alheia (por exemplo, o *phishing* pode ser considerado um método de furto de identidade *online*, investopedia). Estes últimos, por sua vez, podem também ter dificuldade de enquadramento penal, assim como diferentes momentos de consumação.

Primeiramente, é necessário referir que “identidade *online*” pode ser entendida como o conjunto de informações pessoais e que, em certo grau, deveriam ser intransmissíveis (e.g. o email ou a combinação do nome de utilizador e a respetiva palavra-passe, Roberts *et al.*, 2013). Diz-se em certo grau, porque, sendo do domínio próprio, o expetável é que estas informações não sejam acessíveis ao coletivo. Contudo, casos como o email, o número de telemóvel ou o nome são frequentemente publicados nas redes sociais e, conseqüentemente, na *Internet* em geral¹¹. Depreende-se que, os utilizadores, são livres de publicar qualquer tipo de informação pessoal *online*.

A literatura tem apontado duas fases na prática do furto de identidade *online*, projetando, assim, dois possíveis momentos de quando se dá a consumação do crime. Primeiramente, relativo à obtenção de informação pessoal ou financeira, as práticas *online* mais recorrentes são através de técnicas de engenharia social como o *phishing* (e.g. alguém estabelecer contacto com a vítima e referir que pertence a um banco, fazendo com que as vítimas enviem as informações sem se aperceberem do engodo, Van Wilsen, 2019), o *pharming*, o *hacking* ou através de *software* malicioso. Estes exemplos, se automatizados, são ilustrativos das repercussões que podem ter para dezenas de milhões de utilizadores. Assim, a consumação dá-se com a obtenção de informação alheia, sem autorização ou consentimento e desde que feita através da *Internet*. Numa segunda fase, as informações digitais das identidades pessoais furtadas, podem ser usadas, ilicitamente, para a prática de novos crimes (Wall, 2008). Podem visar danos à reputação de outrem; prejuízo patrimonial, através do enriquecimento ilegítimo; assim como o

¹¹ Uma limitação da proliferação dos dados *online* pessoais na internet em geral, depende em muito das definições que cada utilizador aplica internamente em determinadas aplicações e redes sociais, como ter o perfil privado, mas estes fatores de segurança não são exclusivos.

uso da informação pessoal para encobrimento de outros crimes, entre outras finalidades¹². Do ponto de vista económico-financeiro, o furto de identidade *online* pode funcionar como um estágio preparatório à própria fraude ao consumidor. Ou seja, a fraude ao consumidor é um exemplo de atividade fraudulenta com fins económicos. Tsakalidis & Vergidis (2017) identificam uma fase intermediária a estas duas, onde o ofensor pode tirar proveito da informação furtada, por exemplo, ao vender registos do cartão de crédito a terceiros.

A literatura sobre o medo do furto de identidade *online* apresenta uma divisão tripartida entre o medo de perdas financeiras, medo de sofrer danos à reputação e medo de perder privacidade *online* (Hille *et al.*, 2011). O contributo destes autores é pensado a partir das consequências que o medo do furto de identidade *online* tem ao nível dos comportamentos em contexto de e-commerce. As questões de privacidade *online* assumem um carácter mais generalizado, nomeadamente a partir das preocupações que as pessoas têm com a privacidade e a segurança *online*. Por sua vez, as questões de reputação assumem maior relevância em contexto de interação entre dois elementos, como por exemplo nas redes sociais, mensagens instantâneas, sites de encontros, assim como no armazenamento de informação e documentação, inclusive nas *clouds* (Hille *et al.*, 2015). Segundo Li, Yazdanmehr, Wang & Rao (2019), não se sabe ao certo os efeitos que o furto de identidade *online* exerce sobre as vítimas ou que alterações estas têm ao nível das atividades *online*. Contudo, Hille *et al.* (2011) referem que as vítimas do furto de identidade *online* tendem a reduzir o uso de fazer compras *online* ou utilizar o homebanking.

2.2. Phishing

O *phishing* pode ser enquadrado dentro dos crimes relacionados com o computador, ou seja, aqueles que são assistidos pelo uso da máquina na execução da atividade ilícita (Wall, 2007, revisto em 2011). Ao nível da engenharia social, o *phishing* é uma técnica bastante dinamizada que faz uso da *Internet*, podendo ser definido como “(...) *tentativas de enganar os alvos a divulgar informações confidenciais, ao apresentarem-se como uma entidade legítima*” (Reyns, 2015). Existem diversas formas de estabelecer contacto com a vítima com vista à obtenção da

¹² Uma lacuna que parece não ter sido ainda atendida é o uso de tais informações para fins políticos. Um exemplo significativo remete para o caso *Facebook Cambridge*: a Cambridge Analytica coletou dados de mais de 80 milhões de utilizadores visando os eleitores com anúncios políticos nas eleições de 2016 nos EUA, violando assim os termos de serviço do Facebook. Até que ponto os termos e condições de determinadas aplicações e *websites* falham nas pretensões e âmbitos de aplicação de legislação internacional? E no quadro jurídico europeu? Estas situações podem remeter para a existência de problemas de regulação e policiamento transnacional – um aspeto que visa o contexto legislativo e criminal de um ordenamento jurídico (Yar, 2006, p. 91), mas também na coerência desses ordenamentos jurídicos com as empresas que criam estas aplicações.

sua informação pessoal. A principal forma é através do email, mas pode acontecer através das redes sociais, chamadas telefónicas¹³ ou *SMS's*¹⁴. O ofensor faz-se passar por uma entidade confiável que pareça relevante e com a exposição de uma questão que surta interesse em ser resolvido pela vítima, como um banco ou empresas como o Ebay (Brody *et al.*, 2007). Por exemplo, em Portugal, o email recebido pela vítima contém um link para que seja efetuado um pagamento relativo à entrega de uma encomenda por parte dos CTT¹⁵. Esta técnica consegue ser ainda mais eficaz se apresentar diretamente uma referência multibanco, à qual, a vítima, através de formas céleres e acessíveis como o *MB WAY*, realizar o pagamento. Outra tipologia de *phishing* mais sofisticada do ponto de vista tecnológico é o *pharming*. Esta técnica utiliza *malware* para efetuar o *phishing* (Direção Geral do Consumidor¹⁶). Por exemplo, ao clicar em *links* ou abrir ficheiros de emails recebidos, são instalados, sem a vítima saber, programas maliciosos no dispositivo em uso. Quando a vítima tenta aceder a um website fidedigno, o *software* malicioso redireciona para um website falso. Toda e qualquer informação que a vítima aqui colocar, como número de contas bancárias, palavras-passe, podem ser furtadas (Brody *et al.* (2007). Estas técnicas aludem ao carácter voluntário das ações das vítimas e podem funcionar como estágios preparatórios para outros tipos de vitimação. Por exemplo, ao nível da componente financeira, a vítima pode efetuar a compra de um produto que posteriormente não é recebido (fraude ao consumidor). Como suprarreferido, quando se trata de obtenção de informação pessoal, estas atividades permitem dar seguimento a outras atividades fraudulentas (e.g., furto de identidade *online*) ou atentar diretamente contra os indivíduos através do uso de chantagem, por exemplo.

As formas de prossecução do *phishing* são essencialmente automatizadas e realizadas em massa (e.g., através de *spam*) com o objetivo de alcançar o máximo de potenciais vítimas possíveis (Leukfeldt, 2014). Alguns organismos destacam-se nas respostas dadas a estes ilícitos. Por exemplo, a DSP2 (Diretiva dos Serviços de Pagamento) incide sobre formas mais seguras de transações digitais; os serviços de webmail como o Outlook ou o Gmail têm inteligência artificial para identificar potenciais tentativas de *phishing* (nomeadamente quando são reencaminhados muitas vezes) e permitem que o utilizador, manualmente, denuncie determinado email como *phishing*.

¹³ *Vishing* é uma forma de *phishing* que utiliza as chamadas de voz para contactar a vítima (Dias, 2010).

¹⁴ *Smishing* faz uso de mensagens escritas (*SMS's*) para contactar a vítima (Dias, 2010).

¹⁵ <https://www.noticiasao minuto.com/economia/1685498/recebeu-um-email-em-nome-dos-ctt-atencao-pode-ser-phishing> (acesso a 10 de abril de 2021).

¹⁶ <https://www.consumidor.gov.pt/perguntas-frequentes1/fraudes-na-net/pishing-pharming.aspx> (acesso a 10 de abril de 2021).

Recentemente, em consequência da pandemia Covid-19, há registo de incrementos das atividades de *phishing* (*Relatório Riscos & Conflitos 2021*, CNCS; relatório *Cybercrime: Covid-19 Impact*, INTERPOL, 2020). Em alguns casos, os ofensores utilizaram os temas relacionados com a pandemia.

2.3. Descoberta de *software* malicioso

O *software* malicioso é definido como um “*programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima*” (National Institute of Standards and Technology, 2013, citado no CNCS, p. 104). A vítima pode ser um indivíduo ou uma pessoa coletiva como entidades e organizações que têm informações pessoais e financeiras em servidores e computadores. Os propósitos da distribuição de *software* malicioso podem ser financeiros, mas também visar o furto de informação digital, nomeadamente através das práticas de *pharming*. Existem várias tipologias com diferentes e inovadoras formas de propagação do *software* malicioso, como o *ransomware*, cavalos de Troia, worms e vírus (Reyns, 2015). As principais vantagens para os ofensores deste tipo de cibercriminalidade atentam na massificação da distribuição feita de forma automatizada. Assim, um único indivíduo pode afetar milhares de alvos ao mesmo tempo (Yar, 2005).

No outro lado da esfera desta vitimação encontra-se a perspetiva da vítima, mais especificamente quando tem conhecimento da injeção de *software* malicioso nos seus dispositivos informáticos. A descoberta de *software* malicioso tem sido medida de acordo com a noção da sua mera presença nos dispositivos informáticos (e.g. Leukfeldt & Yar, 2016). Por exemplo, Reyns (2015) perguntou sobre eventuais problemas de segurança na *Internet* envolvendo vírus, *malware* ou *adware*. No entanto, as vítimas podem ter dificuldade em reconhecer a presença de *software* malicioso nos seus dispositivos (Bossler & Holt, 2009). Esse reconhecimento pode estar dependente dos conhecimentos e skills informáticas que o indivíduo tem ou de programas antivírus que analisem essa atividade (Holt & Bossler, 2013) e mesmo assim pode não ser eficaz.

Segundo dados do CERT.PT, as infeções por *malware*, nomeadamente por *ransomware*, foram dos tipos de incidentes mais registados em 2020, fruto da forte migração para o ambiente *online* que aumentou as oportunidades para o crime em contexto de pandemia Covid-19. Alguns setores primordiais sofreram avultados ataques de *software* malicioso com propósitos

financeiros, ações de desinformação digital, mas também de ciberespionagem (e.g. o setor da saúde como hospitais e outras entidades envolvidas na resposta à Covid-19 como empresas com vista à investigação e desenvolvimento de vacinas; setor dos transportes; setor da banca) (CNCS, p. 87).

2.4. Crimes Interpessoais online

A vitimação *online* de cariz interpessoal pode ser identificada como qualquer tipo de comportamento de agressão, ameaça ou intimidação realizado através da *Internet* e/ou das TIC com o propósito de ofender ou assustar outrem (APAV¹⁷). A literatura tem dirigido atenções para o assédio *online* como um tipo de crime mais geral que agrupa qualquer tipo de agressão feita através das TIC desde que seja de forma persistente, repetida e indesejada (Bocij, 2004; Pereira *et al.*, 2016). Vários estudos apontam para a existência de uma diversidade de comportamentos subsidiários do assédio *online*, nomeadamente o cyberbullying, o *cyberstalking*, o assédio sexual *online*, a intrusão relacional obsessiva, assim como outras formas de intimidação e ameaças de violência (Henson *et al.*, 2013; Pereira *et al.*, 2016).

Nos próximos subcapítulos iremos descrever de forma mais detalhada as ofensas de cyberbullying e *cyberstalking*. Em primeiro lugar, importa destacar que se tratam de dois cibercrimes pré-existentes no contexto físico, mas que na passagem para o contexto *online* apresentam algumas semelhanças comportamentais que consequentemente levantam dificuldades de interpretação. Ainda assim, cada uma destas ciber-tipologias tem as suas especificidades. Segundo Wall (2001) são considerados, do ponto de vista de enquadramento legal, crimes de ciber-violência, ou seja, cibercrimes contra a pessoa. Estes comportamentos podem ser considerados crimes assistidos pelo computador (Virtanen, 2017), que em concreto se caracterizam pelo uso da *Internet* através do email, mensagens instantâneas e redes sociais. A questão do anonimato e o facto de não existir contato físico e direto entre agressor e vítima no ciberespaço permite que agressores e vítimas manipulem e reinventem a sua identidade social. Henson *et al.* (2013) refere que no caso das vítimas, os níveis de anonimato podem reduzir o medo de vitimação *online* interpessoal.

A vitimação interpessoal *online* pode, em alguns casos, funcionar como um estágio preparatório para futuras experiências de vitimação interpessoal no ambiente *offline*. Por exemplo, o ofensor pode estabelecer formas de comunicação com a vítima por email e somente quando estiver em contato físico e direto com ela é que pratica atos de agressão (Yar, 2006).

¹⁷ <https://www.apavparajovens.pt/pt/go/o-que-e7~> (acesso a 28 de junho de 2021).

Ou, inversamente, pode suceder que se trate de uma variante *online*, ou seja, uma extensão da vitimação *offline*. Veremos nos próximos capítulos o que têm dito os autores quanto a este aspeto. Independentemente da vitimação ser *offline* ou *online* – ou na coexistência de ambas – há a possibilidade da violência praticada conduzir a um impacto psicológico na saúde mental e no bem-estar emocional da vítima, nomeadamente sentimentos de medo, mas também raiva, stress ou tristeza (Henson *et al.*, 2013).

Outro aspeto relevante prende-se com o facto de alguns estudos terem transposto para o ciberespaço a análise da relação entre ofensor-vítima, isto porque, tal como no contexto *offline*, é comum a vitimação interpessoal (*online*) ser cometida por alguém conhecido (e.g., Melander, 2010); estudo 2014), nomeadamente um ex-parceiro íntimo (e.g., Sheridan & Grant, 2007; Alexy, 2015). Englander & Muldowney (2007, citados em Tokunaga, 2010) retratam o cyberbullying como uma ofensa oportunista, assente na facilidade de execução da ação ainda que muitas vezes vítima e agressor se conheçam. Também Reyns *et al.* (2012) destaca as estruturas únicas de oportunidade de stalking por um lado, e *cyberstalking* por outro.

2.4.1. Cyberstalking

O *cyberstalking* é entendido como um conjunto de comportamentos de (tentativa) de contacto, de perseguição, de assédio, de intrusão ou de (re)aproximação de alguém, efetuado através do uso das TIC, nomeadamente a partir da *Internet* (APAV¹⁸; Spitzberg & Cupach, 2007; Pereira & Matos, 2015b). Enquadrado à luz da violência interpessoal *online*, o *cyberstalking* é uma subtipologia do assédio *online* dotada de algumas particularidades centrais, a saber: persistência, intenção, deliberação e indesejabilidade (Spitzberg & Cupach, 2007; Pereira & Matos, 2015a). Estes fatores são consensuais na literatura, sendo a natureza repetitiva do comportamento um critério imprescindível para a sua identificação. A forma de contato e/ou aproximação, realizada através das TIC, pode ser fruto do uso da *Internet* (e.g. email, mensagens instantâneas, salas de chat, blogs, redes sociais), mas também através de outros dispositivos eletrónicos que permitem enviar SMS's ou efetuar chamadas (Baum *et al.*, 2009; Reyns, 2010; Reyns *et al.*, 2012).

Alguns estudos (APAV¹⁹; Sheridan & Grant, 2007; Baum *et al.*, 2009) indicam que o *cyberstalking* é considerado uma extensão ou uma forma similar de stalking. Por exemplo, o estudo de Dreßing *et al.* (2014) respeitante à prevalência do *cyberstalking*, mostra que a relação mais frequente foi de ex-parceiros onde as mulheres foram maioritariamente vítimas e os

¹⁸ <https://www.apavparajovens.pt/pt/go/o-que-e7>

homens agressores. Por outro lado, outros estudos indicam que existem diferenças assinaláveis entre ambos, nomeadamente a partir das vantagens das TIC como o anonimato (Bocij, 2003). O estudo de Alexy, *et al.* (2005) refere que os homens foram o grupo mais vitimado de *cyberstalking*, pelo que as mulheres podem fazer uso dessas vantagens para cometer ilícitos *online*. Efetivamente, ao ser extrapolado para o ciberespaço, o *cyberstalking* é passível de ser cometido sem atender às limitações espaciais e temporais do stalking físico (Reyns *et al.*, 2012). Contudo, atendendo ao critério similar que define ambas as vitimações, retoma-se a ideia inicial em que pode ser considerado uma dimensão paralela. Existem também disparidades relativamente ao critério utilizado na definição do stalking e *cyberstalking*, pois existe alguma variabilidade no que às definições usadas pelos académicos diz respeito. Por exemplo, não existe unanimidade ou um critério quanto ao número de comportamentos que compõem a vitimação, nem à delimitação do espaço temporal para ser considerado comportamento prolongado no tempo (Bocij, 2003; Spitzberg & Cupach, 2007; Pereira & Matos, 2015a).

O stalking virtual pode ser cometido de forma direta (e.g. focado no próprio indivíduo) ou indireta (e.g. direccionar-se para as pessoas próximas da vítima), quer por conhecidos como por desconhecidos. Segundo Bocij (2004), no stalking físico existe quase sempre uma relação física ou emocional com a vítima (p.23). Esta pode chegar a ter um teor romântico quando o agressor é um ex-parceiro. Fazendo uma comparação direta com o conceito de ORI e as formas como este se manifesta, nomeadamente através da invasão da privacidade *online*, monitorização e controlo da vítima, podemos aferir que estes comportamentos iniciam-se, principalmente, depois de um relacionamento íntimo ter acabado (Bocij, 2004, p. 54).

Muitas destas ações podem dar a ideia de serem comportamentos de rotina inofensivos (APAV²⁰; Pereira & Matos, 2015b). A título de exemplo, “*receber chamadas sem uma aparente justificação*” (Spitzberg & Hoobler, 2002) ou o simples ato de ser notificado do recebimento de pedidos para seguir ou de adicionar amizade numa rede social, ainda que de forma repetida. Contudo, pode existir um escalar na seriedade e gravidade dos comportamentos do cyberstalker (e.g. “*exposição de informações privadas a outros*”, Spitzberg & Hoobler, 2002). Saber delimitar os comportamentos que passam ou não as barreiras do moralmente aceitável/barreiras de comportamentos normativos, é um procedimento difícil de avaliar e não é unânime. Talvez por isso, a legislação penal portuguesa tenha deixado em aberto os comportamentos integrantes do crime de stalking no artigo 154.º -A. Ao nível dos impactos

²⁰ <https://www.apavparajovens.pt/pt/go/o-que-e7>

psicológicos para a saúde das vítimas, estes comportamentos intimidatórios e intrusivos podem causar ansiedade, medo e insegurança (Bocij, 2003; Ybarra *et al.* 2006; Henson *et al.* 2013).

A tipificação do stalking dá entrada no ordenamento jurídico português (i.e., é aditada ao C.P.) com a lei n.º 83/2015, de 05 de agosto, criminalizando no artigo 154.º -A do C.P. a conduta como “Perseguição”. À luz da legislação penal, podemos considerar que o stalking praticado através das TIC está indiretamente referenciado quando a lei, na alínea 1, se refere “*por qualquer meio*”. É de notar que não existe uma referência taxativa aos comportamentos. Na mesma alínea, é de salientar que o medo é um dos fins visados pela conduta criminal: “*medo ou inquietação ou a prejudicar a sua liberdade de determinação*”.

2.4.2. Ciberbullying

O ciberbullying é enquadrado na mesma linha que o *cyberstalking* enquanto uma subtipologia comportamental do assédio *online*. A literatura tem apontado como elementos centrais destas ações o carácter agressivo e hostil, feito de forma deliberada e intencional, e repetida ao longo do tempo e que cause dano ou desconforto a outrem. Por sua vez, a ação pode ser cometida individualmente ou em grupo. A meta-síntese de Tokunaga (2010) corrobora estas informações com uma definição integrativa do ciberbullying: “*(...) qualquer comportamento realizado através da media eletrónica ou digital por indivíduos ou grupos que, de forma repetida, comunicam mensagens hostis ou agressivas com a intenção de infligir dano ou desconforto a outros indivíduos*” (p. 278). Esta definição surge perante inconsistências encontradas em vários estudos que visam o mesmo tema, mas utilizam medidas diferentes. Por consequência, não existe uma definição universalmente aceitável pelos académicos, algo que o autor pretende solucionar (Tokunaga, 2010; Randa, 2014). Veja-se, a título de exemplo, alguns dos elementos centrais utilizados nas definições de ciberbullying por outros autores: Hinduja & Patchin (2010) definem-no como “*dano intencional e repetido infligido através do uso de computadores, telemóveis e outros dispositivos eletrónicos*”, salientando o facto de ser uma definição simples e por capturar os principais elementos; enquanto Juvonen & Gross (2008) ou Slonje & Smith (2007) focam-se no carácter agressivo e hostil das ações intermediadas pelas TIC, mas não utilizaram o elemento repetição ou a intencionalidade nas suas definições.

Enquanto no *cyberstalking* parece existir alguma ambiguidade em considerá-lo como uma extensão do stalking, o ciberbullying apresenta maior consenso quanto às influências do bullying que é praticado no mundo *offline*. Por um lado, a principal (senão a única) diferença está na forma como o comportamento é infligido – através das TIC. Naturalmente, a forma

física do bullying tradicional (e.g. agressões, empurros) não pode ser realizada *online* de forma genuína, podendo, no entanto, ter comportamentos semelhantes como ameaças ou intimidações *online* (Hinduja, 2010). A literatura sobre o bullying centra-se quase exclusivamente no ambiente educacional, ou seja, em crianças e adolescentes e na diferença de estatuto e/ou poder entre ambos. Inclusive, o estudo de Roberts *et al.* (2013, por exemplo) mostra que ambos são comuns de suceder nas escolas. Contudo, o cyberbullying não se circunscreve ao estabelecimento de ensino. Ao nível da prevalência do fenómeno, Patchin & Hinduja (2006) indicam que mais de 29% dos jovens foram vítimas *online*, enquanto no estudo de Roberts *et al.* (2013) foram vítimas de cyberbullying 9% dos estudantes com idades entre os 12 e os 18. De forma geral, as percentagens determinam que aproximadamente 15 a 35% dos estudantes foram vítimas de cyberbullying enquanto 10 a 20% dos estudantes admitiram ser os agressores (Hinduja and Patchin (2010).

Após a explicação destes conceitos, cabe agora apresentar a abordagem teórica deste trabalho – a Teoria das Atividades de Rotina – assente no modelo oportunista que une as ações realizadas pela vítima e os objetivos do ofensor, e a probabilidade de ocorrência das vitimações *online* analisadas.

3. Teoria das Atividades de Rotina

Nesta secção, expomos, inicialmente, o modelo da Teoria das Atividades de Rotina (TAR), na conceção original de Cohen & Felson (1979), delineando as suas principais características, assim como as teorias que a precedem. De seguida, apresentamos como estas características têm sido aplicadas no ciberespaço e as eventuais dificuldades dessa aplicação. Por fim, analisamos a influência contextual desta teoria com a probabilidade de vitimação *online*.

A conceção original da Teoria das Atividades de Rotina defende que a atividade criminal exige a convergência no tempo e no espaço de três elementos: um potencial ofensor motivado, um alvo adequado e a ausência de um guardião capaz de prevenir que o crime ocorra (Cohen & Felson, 1979). Estes investigadores defendem que a falta de um dos elemento é suficiente para que o crime não aconteça, ou pelos menos, tenha a sua probabilidade de consumação diminuída. A teoria enfatiza uma natureza ecológica (que parte da teoria ecológica humana de Hawley, 1950) antecedente às oportunidades para o crime, que surgem mediante a análise da organização social e os estilos de vida dos indivíduos (e.g. Felson & Cohen, 1980). Assim, as oportunidades para o crime resultam das alterações na organização social da sociedade, do olhar

do potencial ofensor, das ações do alvo, da ausência de guardiões e mediante fatores situacionais ao nível do tempo e do espaço. Isto significa que podem existir aumentos da criminalidade – sem que existam mais ofensores para a praticar – desde que coexistam mais alvos, ou se os guardiões não estiverem presentes (Felson & Clarke, 1998).

Considerando o ponto de vista do ofensor, a teoria destaca o cálculo racional que este realiza ante a conduta, ou seja, o ofensor pondera os prós e contras do crime. Deste modo, é importante atender a categorias específicas do crime, visto que os propósitos atribuídos pelos ofensores, assim como os fatores situacionais, diferem na forma como as influenciam (Felson & Clarke, 1998). Outro fator importante que rege o seu comportamento é a motivação. Ao nível do alvo adequado, salienta-se a relação dependente entre as capacidades do potencial ofensor executar a atividade e as características da vítima. Por um lado, é o ofensor que avalia a situação e o nível de atratividade do alvo. Por outro, é o alvo que nas suas rotinas do dia a dia pode tornar-se mais acessível, visível e menos resistente. A atratividade do alvo é analisada a partir do acrónimo VIVA – Valor, Inércia, Visibilidade e Acessibilidade. Relativamente à figura do guardião, esta atenta na proteção conferida ao alvo. Através da sua presença, o guardião pode prevenir a ocorrência do crime, contudo quando ele está ausente a probabilidade de vitimação aumenta (Felson & Clarke, 1998).

Apesar de alguns autores reconhecerem a cibercriminalidade como “*old wine in new bottles*” (Grabosky, 2001), existem algumas lacunas na aplicação dos pressupostos da TAR no ciberespaço. A literatura que se foca nesta vertente, peca na operacionalização de alguns conceitos, e além disso, não há um consenso geral de qual critério utilizar, permitindo que existam diferentes concetualizações mediante diferentes autores. Segundo Yar (2005, p. 422):

“(...) divergências entre real e virtual resultam das características estruturais dos próprios ambientes; (...) características como a distância, a localização e o movimento diferem acentuadamente entre os dois domínios, e essas configurações vão afetar a natureza da visibilidade e acessibilidade dentro dos respetivos ambientes.”

Outro exemplo aplica-se ao conceito de proximidade. A natureza ecológica da teoria e as implicações que o crime como um evento acarreta – convergência no tempo e no espaço dos três elementos centrais da teoria – emergem relações de proximidade ou distanciamento entre ofensor e alvo que explicam a probabilidade da vitimação ocorrer (Yar, 2005). Por um lado, o contexto físico tem apontado relações significativas entre a proximidade física do alvo-ofensor e a probabilidade de vitimação. No contexto virtual, por sua vez, podemos estar perante uma

proximidade virtual, exequível pela dinamização das TIC que encurtaram e eliminaram distâncias físicas (e.g. redes sociais facilitam a copresença de conhecidos e desconhecidos num mesmo espaço virtual, independentemente do espaço físico em que o acesso é feito). Contudo, não basta saber da existência da presença virtual de algo ou alguém na *Internet*, pois a sua (tentativa de) descoberta pode exigir tempo e esforço (Yar, 2005, pág. 416). Com isto parece evidente um distanciamento virtual. O autor menciona também a influência dos algoritmos na questão de aproximar determinados sites e páginas em prol de outros. Esta questão é particularmente complexa. Atualmente, os algoritmos não tratam só de questões de otimização dos resultados nos motores de busca (i.e., o que é mais procurado ou comentado pela generalidade), mas apresentam resultados, ainda que previsíveis, cada vez mais personalizados ao nível individual de acordo com o histórico de pesquisa, local onde a pessoa se encontra, etc. Isto atinge repercussões de publicidade, enquadrado num âmbito maior de marketing digital. O problema repercute-se essencialmente em questões de segurança e privacidade dos dados *online*, algo que ultrapassa o âmbito deste trabalho.

Nos próximos subcapítulos atender-se-á à exposição dos três conceitos piramidais da TAR, com a respetiva transposição para o ciberespaço que vários autores têm realizado.

3.1.Exposição a ofensores motivados

A potencial exposição a ofensores motivados deve ser entendida com critérios específicos para cada tipologia de crime. O perfil de um ofensor motivado para executar crimes interpessoais como o *cyberstalking* ou o ciberbullying não será o mesmo que o perfil de um ofensor motivado que pretenda difundir *software* malicioso em larga escala. É necessário ter em conta as suas motivações e se este tem as capacidades necessárias para realizar a conduta criminal (Felson & Cohen, 1980). O ofensor realiza também um cálculo racional dos custos e benefícios antes da conduta, ainda que por breves momentos (Felson & Clarke, 1998). Todavia, a partir da análise situacional do crime como um evento, o foco passa para o contexto que pode facilitar ou reduzir as oportunidades para o crime, pelo que as características e motivações individuais do ofensor perdem força na explicação do crime (Felson e Clarke, 1998). Em todo o caso, a teoria original considera a figura do potencial ofensor como dada, isto é, com inclinação e motivos para a via criminosa.

A exposição a um potencial ofensor é usualmente conceitualizada a partir do ponto de vista e das ações da vítima ou do alvo. A operacionalização deste conceito tem-se medido pela exposição (e.g. tempo passado fora de casa) ou pela proximidade do alvo ao potencial ofensor

(Cohen, Kluegel, & Land, 1981; McNeeley, 2015 citados em Reyns & Henson, 2016). Segundo alguns autores (e.g., Felson & Clarke, 1998; Reyns & Henson, 2016), a exposição refere-se à acessibilidade ou visibilidade do alvo. Ou seja, o nível de exposição fica assim dependente das ações do alvo perante o potencial ofensor, patentes nas atividades de rotina que realiza *online*. Estas são, aliás, duas subcomponentes do acrónimo VIVA (explicado no subcapítulo 3.2.) que identificam um alvo como mais ou menos adequado. O acrónimo VIVA é um multiconceito tradicional da TAR e define, inclusive, o nível de risco da prática da atividade criminal por parte do potencial ofensor, logo implica também a coexistência de configurações do ponto de vista do ofensor. Segundo Leukfeldt (2014), para um ofensor, o grau de visibilidade está ligado ao grau em que uma pessoa é um alvo adequado.

A operacionalização da exposição *online* a ofensores motivados tem sido, maioritariamente, medida através da frequência, em horas, do uso da *Internet* e as respetivas atividades de rotina *online*, tanto de forma integrativa como separada, a partir do ponto de vista da vítima quanto à sua vitimação (e.g., Henson *et al.*, 2013; Reyns, 2015). É de salientar que, a par de um uso cada vez mais frequente da *Internet* por parte da população, os próprios itens de medição evoluíram também (e.g. Emmanouilides & Hammond em 2000, agruparam as respostas em baixo uso de *Internet* [1-3 vezes no espaço de um mês], moderado [4-19 vezes] e alto [mais de 20 vezes]). Mais recentemente, Roberts *et al.* (2013) utilizaram uma escala de 7 pontos com respostas a começarem em “várias vezes por dia”. Quanto à exposição *online* em atividades, Reyns (2013) chama a atenção para a falta do uso de medidas que incidam diretamente sobre as atividades de rotina *online*, já que, até então, os autores se limitavam a perguntar sobre o tempo passado na *Internet*. Nesse contexto, o autor elenca dez atividades que procuram medir diretamente as rotinas *online*, e que na falta de guardiões, torna os utilizadores *online* expostos a possíveis ofensores motivados e, conseqüentemente, adequados à vitimação.

Todavia, os resultados apresentados têm sido mistos (Reyns & Henson, 2016; Virtanen, 2017). Por um lado, alguns autores encontraram associações entre o uso da *Internet* e a vitimação *online*: Marcum *et al.* (2010) refere que participar em atividades *online* aumenta a probabilidade de receber conteúdo sexualmente explícito indesejado como pornografia, assédio não sexual indesejado e solicitações sexuais indesejadas, durante os períodos equivalentes ao último ano do ensino secundário e o primeiro ano do ensino superior); Ngo & Paternoster (2011) encontraram associações significativas entre a frequência do uso de mensagens instantâneas e assédio *online*; no estudo de Van Wilzen (2011), fazer compras *online* e participar em fóruns aumentou a probabilidade de ser vítima de fraude. Por outro lado, há

estudos que não encontraram associações entre a frequência do uso da *Internet* e a vitimação *online*: no estudo de Holt (2009), fazer compras *online*, conversar *online* e utilizar o *homebanking*, não influenciaram a perda de informação digital através da vitimação por *malware*; Leukfeldt (2014) não encontrou correlações entre as atividades *online* e a probabilidade de vitimação *online*.

Por outro lado, o estudo de Pratt *et al.* (2010), alude à ideia que a exposição *online* varia em função do género, idade e raça, sendo os homens e os mais velhos a estarem mais expostos *online*. Em suma, alguns estudos têm analisado a hipótese que, quanto maior a frequência do uso de *Internet*, maior será o nível de exposição *online*, e consequentemente, maior será também a probabilidade de vitimação *online*.

3.2. Alvo adequado

O alvo adequado é representado pela atratividade que uma pessoa, lugar ou objeto tem para um potencial ofensor (Cohen *et al.*, 1981; McNeeley, 2015 citados em Reyns & Henson, 2016). Como vimos, o conceito está intimamente ligado à forma como a exposição a ofensores motivados é operacionalizada, ou seja, mediante as atividades de rotina da vítima. No ciberespaço, a generalidade dos cibercrimes atenta na natureza informativa do conteúdo digital (Yar, 2005). A literatura tem apontado como possíveis alvos *online*: a informação pessoal e/ou financeira (e.g. palavras-passe; números de acesso ao cartão de crédito²¹), o computador em si mesmo (nomeadamente ao nível do *software*), assim como o próprio indivíduo (e.g., honra) ou a propriedade (por exemplo, a vítima vende determinada propriedade a um preço reduzido proposto por outro, mediante a comparação incorreta de preços com outros produtos similares) (e.g. Ngo & Paternoster, 2011; Holt & Bossler, 2013).

Segundo Felson e Clarke (1998), o acrónimo VIVA determina a ideia geral de adequação de um determinado alvo à atividade criminal perpetrada por um ofensor motivado, influenciando o nível de risco do alvo ser atacado. Por outras palavras, a atratividade do alvo baseia-se em quatro elementos: o valor, a inércia, a visibilidade e a acessibilidade. Assim, um determinado alvo será mais ou menos adequado de acordo com essas características. Quanto maior a visibilidade, a acessibilidade, o valor e a inércia, maior será também a adequação do alvo. Estas dimensões são apreciadas do ponto de vista do ofensor, atendendo ao nível de risco das suas ações (Cohen & Felson, 1979; Felson & Clarke, 1998). alvos mais fáceis podem ser mais adequados ou atrativos (Clarke & Cornish, 2000 citados em Reyns & Henson, 2016)

²¹ Nomeadamente, um código de 16 dígitos e um código de 3 dígitos aleatórios (CVV – *Card Verification Value*; ou CVC – *Card Verification Code*).

Estes conceitos receberam reformulações ao longo dos anos como por exemplo o acrónimo CRAVED²² em 1999 por Clarke. Também Newman e Clarke (2003) descrevem as características do ambiente cibernético, nomeadamente ao nível do *hardware* e *software* dos sistemas de informação, assim como da própria rede através do acrónimo SCAREM²³. Estes sistemas *online* – *websites* – são ambientes criminogénicos caracterizados pelas qualidades SCAREM. Por exemplo, as redes sociais permitem a ocorrência de *cyberstalking*, assim como *websites* de compras permitem a ocorrência de fraude ao consumidor *online*. O objetivo passa por atuar sobre estas qualidades para prevenir e reduzir as oportunidades para o crime (Reyns, 2010, 2013).

Partindo da conceção do VIVA – Valor, Inércia, Visibilidade e Acessibilidade – aprofunda-se de seguida, a descrição das suas dimensões, assim como a respetiva operacionalização que alguns autores têm realizado na transposição para o ciberespaço (Cohen & Felson, 1979; Felson e Clarke, 1998).

Primeiramente, quanto ao valor, pode constatar-se que um mesmo alvo (e.g. informação pessoal) pode ter diferentes avaliações e objetivos traçados pelo ofensor. O valor atribuído está dependente, ainda que não exclusivamente, do ponto de vista do ofensor e esta avaliação – juntamente com as capacidades de conduzir o ato – pode afetar o seu nível de adequação (Yar, 2005). Partindo do princípio de que o ofensor tem a motivação e as ferramentas tecnológicas necessárias para executar o cibercrime, ele pode, por exemplo, atribuir um valor ou objetivo económico a determinadas informações financeiras que pretende aceder – alguns estudos (e.g., Leukfeldt, 2014) vinculam os ativos e os rendimentos financeiros para identificar alguém com possibilidades económicas, fator que pode ser determinante para a probabilidade de vitimação. Pode também atribuir um valor pessoal, quando por exemplo, o objetivo é o alvo enquanto indivíduo ou as suas informações pessoais, ou atribuir um valor simbólico, isto é, o ofensor fá-lo por razões de entretenimento e/ou prazer próprio). Em suma, podemos considerar valores específicos de acordo com tipologias específicas de cibercrime.

Em segundo lugar, na literatura tradicional, a inércia refere-se a características físicas (como peso, tamanho e forma) da pessoa ou objeto e que funcionam como uma barreira, limitação ou obstáculo à prática da atividade criminal conduzida pelo ofensor (Cohen & Felson, 1979). Níveis maiores de resistência oferecidos por este elemento diminuem as chances do alvo

²² Concealable, Removable, Available, Valuable, Enjoyable e Disposable.

²³ Stealth, Challenge, Anonymity, Reconnaissance, Escape e Multiplicity

ser visto como adequado pelo ofensor, como por exemplo, a facilidade de transporte de um objeto pesado (Yar, 2005, p. 420). No contexto *online*, este autor considera como alvo a informação digital, e mesmo esta tem propriedades inerciais como o volume ou o tamanho dos ficheiros, a velocidade com que estes podem ser transferidos e ainda a capacidade dos dispositivos em armazenar os ficheiros. De acordo com estes critérios, a transposição da inércia para o ciberespaço é um processo difícil de operacionalizar, não existindo estudos empíricos que (ao nível da resistência objetiva ao ato criminal), tenham medido estas propriedades (Yar, 2005; Leukfeldt & Yar, 2016). Existem ainda limitações objetivas quanto ao tipo de alvo em análise, visto que, considerando outros alvos – que não a informação digital – as propriedades suprarreferidas têm menos rigor na sua aplicação.

Por fim, no que toca às dimensões visibilidade e acessibilidade, veremos como tem sido feita a sua adaptação ao ciberespaço. Enquanto a visibilidade tem mostrado relativa facilidade de aplicação nos estudos que se focam na vitimação *online*, a acessibilidade tem sido operacionalizada com menor frequência e com evidentes diferenças entre estudos.

A visibilidade como o próprio nome indica, apresenta-se como uma dimensão omnipresente no meio cibernético, na medida em que existe uma efetiva presença virtual na *Internet* do alvo ou da vítima. Uma larga fatia dos estudos empíricos refere que a visibilidade é a variável que mais suporte empírico encontra para as várias tipologias de vitimação *online* (Stalans, 2018). A sua medição tem sido feita através das atividades *online* realizadas pela vítima que são tidas como fatores de risco para a vitimação *online*, tendo em conta que podem expor os indivíduos a ofensores *online*. As atividades que predizem maior risco de vitimação diferem de acordo com a tipologia em análise (Leukfeldt, 2014). Assim, dependendo do contexto, determinadas atividades económicas *online* podem ter maior influência no nível de risco de cibercrimes da componente propriedade, enquanto atividades de cariz social e interativo podem influenciar mais os cibercrimes da componente interpessoal.

Quanto à acessibilidade, tradicionalmente, refere-se ao desenho do espaço e à acessível localização do objeto que aumenta o risco de ataque ou facilita a sua execução (Miró, 2014). Assim, relaciona-se com a facilidade de acesso ao alvo e de entrar em contato com o mesmo, isto é, a acessibilidade no tempo e no espaço é importante na determinação da eventual vitimação (Yar, 2016). No ciberespaço, alguns estudos focaram-se no tipo de informação publicada e acessível *online* (e.g. Marcum, 2010; Reyns, 2016) e no tipo de atividades de rotina

que realizam *online*²⁴ e que por sua vez indicam atratividade para um potencial ofensor. Por outro lado, alguns estudos focaram-se somente no tipo de informação que indica atratividade do alvo (e.g. Reyns, 2011). Segundo este autor, se determinadas informações sobre o perfil de alguém estiverem disponíveis na *Internet*, tal acaba por aumentar o nível de atratividade do alvo e, assim, facilitar a probabilidade da sua vitimação (o estudo incorporou também o género, estado civil, orientação sexual para medir a atratividade do alvo). Ou seja, os autores (e.g. Reyns, 2011) acabam por fazer referência direta à componente alvo adequado como um todo, a partir do tipo de informação acessível *online*. Não obstante a importância do valor, inércia e acessibilidade como fatores para a considerar na atratividade do alvo, o autor não faz uma referência a estes critérios. Em todo o caso, partindo da análise que outros estudos fizeram, podemos supor que a acessibilidade está subentendida no tipo de informação, contudo continua a faltar uma referência explícita tanto à acessibilidade como às restantes subcomponentes do alvo adequado. Mais recentemente, Leukfeldt (2014) e Leukfeldt & Yar (2016) associam a acessibilidade do alvo ao tipo de *software* que este utiliza. Para estes autores, eventuais falhas de segurança no sistema operativo ou nos browsers de *Internet* facilitavam o acesso do ofensor motivado ao alvo. Contudo, isto delimita o campo de potenciais ofensores e pressupõe que estes têm as *skills* tecnológicas necessárias para hackear ou difundir *software* malicioso e, assim, desencadear e aceder a falhas nos diferentes tipos de *software* que o alvo utiliza. Ou seja, esta subcomponente, nos traços que foi identificada pelos autores, parece ter sentido se for utilizada para crimes focados no computador (e.g. *hacking* e *software* malicioso). Este estudo mostra resultados positivos da influência destas variáveis para a vitimação por *malware*, mas o mesmo não acontece para a vitimação por *hacking*. Outros estudos utilizaram também características sociodemográficas como o género para medir a atratividade do alvo *online* (e.g. Reyns *et al.* 2011).

Os estudos têm encontrado resultados distintos quanto à influência das atividades que visam a atratividade do alvo. Marcum *et al* 2010.

3.3. Guardião

Tendo em conta os trabalhos originais de Cohen e Felson (1979), a figura do guardião é representada por alguém capaz de impedir que um determinado crime ocorra através de determinadas ações voluntárias, mas também pela sua mera presença. Ou seja, acaba por nem

²⁴ Note-se que estas atividades de rotina *online* não devem ser confundidas com as atividades perguntadas na subcomponente visibilidade, ou seja, aqui as atividades de rotina têm inerente um nível de risco mais direto (e.g. “comunicou com desconhecidos *online*”).

ser necessário tomar qualquer ação voluntária já que o crime por si só é menos provável de acontecer desde que o guardião esteja presente. O exemplo mais claro da assunção desta figura é o da polícia, contudo, não se circunscrevem somente a pessoas com autoridade ou poder, mas sim a qualquer pessoa que de forma indireta e involuntária, pela sua presença, e na realização das suas atividades de rotina, previne a atividade criminal (Miró, 2014). Em suma, o guardião tradicional pode ser social formal (e.g. polícia) e social informal (e.g. qualquer pessoa), existindo também medidas físicas (e.g. barreiras, alarmes). Ressalta-se algumas reformulações desta figura, que originaram tipologias com características distintas.

Um dos primeiros autores que procurou transpor os guardiões tradicionais para o ciberespaço foi Yar (2005). Quanto aos guardiões sociais formais (e.g. polícia), apesar de existirem formas de presença policial em determinados contextos virtuais, a sua proteção peca pela mesma razão que no contexto *offline* – “*é improvável que a polícia esteja no local onde ocorre o crime*” (Yar, 2005, pág 423). Relativamente aos guardiões sociais informais, o autor refere que já não basta a mera presença do guardião *online* (e.g. a presença pode ser notada virtualmente em salas de chat), pois o seu efeito não é tão preventivo.

Alguns estudos (e.g. Holt & Bossler, 2008; Bossler & Holt, 2009) operacionalizaram o guardião social tendo em conta se o indivíduo tinha pares desviantes que realizassem atividades ilícitas *online* como *hacking*. Por outro lado, as medidas “físicas” de segurança tratam-se de medidas tecnológicas (e.g. *software* antivírus) e têm sido comumente operacionalizadas e aplicadas em estudos empíricos. Por exemplo, Choi (2010) identifica os programas antivírus, *antispyware* e *firewall* como três tipos de guardiões digitais. Por sua vez, Ngo & Paternoster (2011) distinguem o guardião físico, atente na segurança do *software* dos mesmos tipos de programas, do guardião pessoal – composto por um item baseado na escala de Rogers (2001) sobre o conhecimento e skills tecnológicas, assim como a participação em workshops ou *websites* destinados à educação sobre o cibercrime. Leukfeldt & Yar (2016) remetem o guardião técnico para o *software* de segurança e um guardião pessoal atente no conhecimento técnico e na preocupação com os riscos *online*. O estudo de Williams (2016) introduziu uma nova tipologia de guardiões *online* ao nível individual: o guardião físico passivo (“*using only one computer, email spam filtering, installing antivirus and secure browsing*”); o guardião pessoal ativo e o guardião pessoal de evitamento para desencorajar comportamentos *online*.

Alguns estudos que analisaram os efeitos dos guardiões na probabilidade de ocorrer vitimação *online*, apresentam resultados mistos. O estudo de Williams (2016) refere não existir evidência empírica que a presença de guardiões reduz a probabilidade do furto de identidade

online. Mais especificamente, a presença de guardiões físicos (*software* de segurança) não reduziu o risco de assédio *online* (Holt & Bossler, 2008). Por outro lado, o estudo de Ngo & Paternoster (2011) teve uma correlação positiva entre o *software* de proteção e a injeção de *malware* e assédio por estranhos. Relativamente aos conhecimentos e *skills* informáticas, Bossler & Holt (2009) e Ngo & Paternoster (2011) não encontraram relações significativas com a injeção de *malware*, ao passo que Holt & Bossler (2013) encontraram correlações positivas.

4. Variáveis explicativas da vitimação online

Além da influência que as variáveis provenientes da Teoria das Atividades de Rotina exercem sobre a vitimação *online*, a literatura tem apontado, também, resultados importantes quanto à influência de variáveis individuais como explicativas da vitimação tradicional. De seguida, apresentamos essas relações para a vitimação *online*.

A análise de determinadas características pessoais pode aumentar a probabilidade de vitimação *online* (Reyns, 2013). Reyns (2015) refere que a literatura sobre a vitimação encontra consistentemente influência das características pessoais no risco de vitimação, maiores até, que os efeitos da oportunidade e outras variáveis teoricamente relevantes.

Relativamente às características individuais, tanto o género como a idade não são preditores consistente de vitimação *online*. No que toca à primeira, Tokunaga (2010) refere que a variável não prediz o cyberbullying. Também no estudo de Ngo & Paternoster (2011), o género não foi preditor para nenhum dos diferentes tipos de vitimação (e.g. vírus informático; receber solicitações sexuais). Reyns (2015) refere que as mulheres têm menor probabilidade de serem vítimas de *phishing* e de reportarem infeção de *malware*. No estudo de Bossler & Holt (2013) as mulheres reportaram maiores níveis de medo de injeção de *software* malicioso. Quanto à idade, o estudo de Ngo & Paternoster (2011) refere que quanto mais velho se é, menor a probabilidade de vitimação *online*. Reyns (2015) refere que os mais velhos têm maior probabilidade de sofrerem vitimação por *phishing*, enquanto os mais novos têm menor probabilidade de reportarem injeção por *malware*. Em sentido contrário, Tokunaga (2010) refere que a idade não tem efeito na vitimação por cyberbullying. O estudo de Pratt *et al.* (2010) refere que os mais novos têm maior probabilidade de serem vítimas de fraude ao consumidor *online*.

Quanto às características individuais económico-financeiras como os rendimentos auferidos, e o nível de escolaridade, estes têm apresentado resultados mistos. Reyns (2015) observou que ter maiores rendimentos estava associado a maiores chances de ser vítima de

phishing e de contrair vírus informático. Mais recentemente, o estudo de Burnes *et al.* (2020) refere que os indivíduos com estatuto socioeconómico mais alto têm mais probabilidade de sofrer vitimação de uma tipologia do furto de identidade *online* – uso não autorizado de cartão de crédito/conta bancária existentes. Todavia, Leukfeldt (2014) não encontrou associações entre as características financeiras como o rendimento e a vitimação por *phishing*. Também para o nível de educação, este autor refere que a probabilidade de vitimação por *phishing* é igual para todos os níveis de escolaridade analisados. Prat *et al.* (2010) encontraram resultados significativos entre maiores níveis de educação e maior probabilidade de fraude ao consumidor *online*.

Relativamente à perceção do risco de vitimação *online*, Reyns (2013) encontrou correlações positivas entre o risco percebido de furto de identidade e o furto de identidade *online*. Isto é, quanto maior é a perceção do risco de vitimação *online* para este tipo de crime, maior é também, a probabilidade da sua ocorrência.

5. Sentimento de Insegurança

O presente capítulo incide sobre o sentimento de insegurança enquanto fenómeno tripartido e multidimensional perspectivado pela potencial vítima de um crime ao nível das suas dimensões afetivas, cognitivas e comportamentais (Madriz, 1997; Gabriel & Greeve, 2003, citados em Guedes, 2012). A dimensão afetiva corresponde ao medo que alguém sente de ser vítima de um crime. Por sua vez, a dimensão cognitiva corresponde à perceção do risco de ser-se vítima, enquanto a dimensão comportamental tem sido estudada a partir de comportamentos de proteção e comportamentos de evitamento. Apesar deste construto não ser isento de críticas, o mesmo usufruiu de um crescimento notável do ponto de vista académico e permitiu densificar a literatura sobre os conceitos de medo do crime e perceção do risco de vitimação, os seus precedentes, as consequências psicológicas e comportamentais inerentes, assim como as características dos grupos sociais que mais medo sentem de acordo com as particularidades de cada crime. Todavia, a literatura sobre o sentimento de insegurança aplicada às TIC não acompanhou as vagas de crime *online*, encontrando-se, para o efeito, ainda numa fase de crescimento. Nos próximos subcapítulos, apresentamos uma breve descrição das dimensões afetiva, cognitiva e comportamental do sentimento de insegurança e a sua relação com a vitimação *online*.

5.1. Medo do crime

O medo do crime é, desde os anos 60, uma das principais áreas de conhecimento e evolução académica (Hale, 1996). Pode ser definido como uma resposta emocional de terror ou ansiedade ao crime ou a símbolos associados a ele (Ferraro & LaGrange 1987, 1992 citados em Ferraro 1995). Esta definição é comumente usada, mas não existe um consenso universalmente aceite. As principais limitações à medição deste fenómeno prendem-se com o facto de, por norma, a questão utilizada poder retratar preocupações mais gerais. Por exemplo, a questão “*Quão seguro se sente quando está sozinho no seu bairro depois de escurecer?*” – usada nos principais inquéritos de vitimação desde a década de 70, como o *General Social Survey* [GSS], o *National Crime Survey* [NCS] ou o *International Crime Victims Survey* [ICVS] – não permite distinguir as diferentes especificidades dos crimes, nem a sua real mensuração ao nível da intensidade e frequência (Jackson, 2004; Gray *et al.*, 2008). Para aumentar a validade deste item, alguns autores recomendam, ainda, ser específico aos diferentes cibercrimes; delimitar o tempo abrangido na resposta até aos últimos 12 meses, de modo a evitar eventuais *efeitos de telescoping* ou perda de memória e utilizar a palavra “medo” para refletir diretamente a componente emocional do sentimento de insegurança, e assim, distingui-la do risco percebido de vitimação (Hale, 1996; Ferraro & LaGrange, 1987; Jackson, 2004; Gray *et al.*, 2008). Efetivamente, existe uma conexão com o risco percebido de vitimação, na medida em que, para o medo – enquanto reação emocional – subsista, é necessária uma situação possuidora de potencial perigo para o indivíduo, mas ambas devem ser separadamente medidas.

A crescente expansão das atividades criminais *online* a que assistimos a partir da metade da primeira década deste século possibilitou alargar o olhar dos académicos sobre um novo derivado de medo de vitimação. Apesar de serem poucos os estudos empíricos sobre o medo de vitimação *online* (Henson & Reynolds, 2015), caminhamos para uma maior densificação do conhecimento sobre esta temática auxiliada pelos preditores pensados para o medo tradicional. Esta transposição parece, contudo, uma tarefa árdua tendo em conta que a relação entre duas variáveis pode estar dependente de outros fatores, e no ciberespaço (constantemente em evolução), essa exatidão parece ainda mais difícil de identificar.

5.2. Perceção do risco de vitimação

A dimensão cognitiva do sentimento de insegurança é uma antecipação à probabilidade de se ser vítima (Amerio & Roccato, 2007; Machado & Agra, 2002, citados em Guedes, 2012). Segundo o modelo de interpretação do risco, o indivíduo na associação com os outros faz uma

avaliação cognitiva da realidade (Ferraro, 1995). Esta avaliação incide sobre a probabilidade de se ser vítima e é influenciada pelas características pessoais e sociais do ator (e.g. género, idade, posição social), ou seja, por vulnerabilidades físicas ou sociais. Por sua vez, determinadas características pessoais do ator social podem aumentar o risco percebido de vitimação e, conseqüentemente, aumentam também o medo do crime. Em suma, este modelo enfatiza a importância que a percepção do risco tem sobre o medo do crime: quanto mais provável for o risco de vitimação, maior será o medo sentido (Ferraro, 1995).

5.3.Comportamentos de segurança

Em 1972, Furstenberg refere que “*a relação entre crime e as suas consequências não é óbvia nem simples*” (cit. in. Garofalo, 1981). É a partir desta altura que a literatura sobre o medo do crime começa a estudar quais consequências comportamentais lhe são relacionáveis (e.g. Liska *et al.*, 1988; Rader, 2004; Rader *et al.*, 2007). Por sua vez, estes comportamentos restritivos têm sido categorizados em comportamentos de evitamento e comportamentos de proteção (Garofalo, 1981; Liska *et al.*, 1988). Os comportamentos de evitamento atuam na medida em que as pessoas com medo do crime evitam determinadas zonas e situações potenciadoras de perigo ou insegurança. Os comportamentos de proteção referem-se ao uso de instrumentos ou técnicas de segurança, tanto no sentido material da segurança (e.g. instalar um alarme em casa) como no sentido pessoal (e.g. aprender a defender-se). Em suma, são uma resposta comportamental ou atitudinal, muitas vezes impulsionadas pelo medo do crime, ao restringir o comportamento das pessoas, que, por consequência, mudam ou adotam novas condutas às suas rotinas. Esta dimensão atende também à percepção do risco de vitimação. Aponta-se ainda a possibilidade do medo do crime e os comportamentos resultantes, apresentarem efeitos recíprocos: ter medo provoca um comportamento posterior restrito e um comportamento restrito pode provocar mais medo (Liska *et al.* 1988; Rader, 2004).

Os comportamentos de evitamento e de proteção podem também ser aplicados no ciberespaço. Por um lado, as pessoas podem evitar aceder a determinados “locais” na *Internet* (e.g. evitar aceder ao homebanking). Todavia, ao restringirem-se a ambientes seguros (e.g.), estamos a supor que o indivíduo abdica da acessibilidade e celeridade das TIC, que podem ser importantes para o seu dia-a-dia. Por outro lado, os comportamentos de proteção referem-se ao uso de programas de segurança como antivírus, *antispyware* e *firewall*.

6. Variáveis explicativas do medo do cibercrime

Nesta seção, expomos um conjunto de variáveis de índole contextual (i.e., atividades de rotina) e individual (i.e., características individuais) na relação com o medo do cibercrime. Ao nível contextual, aplicamos a Teoria das Atividades de Rotina ao medo do cibercrime, nos mesmos moldes em que foi operacionalizada para a vitimação *online*, ou seja, tendo em conta os efeitos da exposição a ofensores, a atratividade do alvo e os guardiões. Em segundo, apresentamos a influência das variáveis individuais no medo do cibercrime, a partir da tese das vulnerabilidades.

6.1. Variáveis contextuais aplicadas ao medo do cibercrime

Relativamente à exposição a ofensores motivados, a variável tem sido medida através das atividades *online* realizadas pela vítima e que influenciam o medo de vitimação *online* sentido. Alguns autores encontraram associações entre o uso da *Internet* e o medo *online* (e.g. Roberts *et al.*, 2013 aludem à frequência do uso da *Internet* como fator para maiores níveis de medo de furto de identidade *online* e atividade fraudulenta; Yu, 2014 utilizou medidas específicas do uso de *Internet* e encontrou correlações positivas com diferentes tipos de medo do cibercrime. Por outro lado, há estudos que não encontraram associações entre a frequência do uso da *Internet* e o medo de vitimação *online* (e.g. Alshalan (2006) não encontrou associações para o medo do cibercrime de vírus e hacking; Henson *et al.*, 2013 não encontraram associações entre a frequência do uso de *Internet* e o medo de vitimação interpessoal *online*). Em suma, os estudos apresentam resultados mistos quanto à importância que o tempo passado *online* ou as atividades rotineiras que realizam nesse ambiente têm ao nível de exporem os alvos ao ponto de estes sentirem medo de vitimação *online*.

6.2. Variáveis individuais aplicadas ao medo do cibercrime

Os preditores do medo do crime têm sido estudados ao nível comunitário (e.g. influência dos níveis de criminalidade na zona próxima do indivíduo e influência dos *media*) (Ferraro, 1995; 1996; Wall, 2008; Henson & Reyns, 2015) e ao nível individual (e.g. características individuais como o género) (Hale, 1996). Também a experiência de vitimação ou o risco percebido de vitimação têm sido estudados na relação com o medo do crime (*idem*). Algumas destas características individuais como o género, a idade, a escolaridade e a perceção sobre o rendimento familiar são usuais nos estudos que medem o medo do crime tradicional. Nos últimos anos, a sua aplicabilidade tem-se estendido ao contexto *online*. No caso do género e da idade, é a partir da tese das vulnerabilidades (física) que se têm delineado resultados: Hale

(1996) refere existir um paradoxo para estas variáveis, na medida em que são as mulheres e os mais velhos que reportam maiores níveis de medo do crime, contudo, ambos têm menor risco objetivo de sofrerem vitimação (e.g., Garofalo, 1981; Warr, 1984; Ferraro, 1995; 1996; Rader, 2004; Rader *et al.*, 2007). Em complemento, a tese das vulnerabilidades sociais, como por exemplo, o rendimento e o nível de escolaridade também têm sido estudados na relação com o medo. Hale (1996) defende que, não obstante as vulnerabilidades objetivas, as vulnerabilidades percebidas também surtem efeitos nos níveis de medo apresentados.

No caso do género, como vimos, trata-se de um bom preditor para o medo *offline*, contudo existem resultados mistos quando analisado o medo de diferentes tipos de cibercrime: no estudo de Virtanen (2017), as mulheres reportaram maiores níveis de medo do cibercrime. Também no estudo de Brands & Van Wilsem (2019), as mulheres reportaram níveis mais elevados de medo *online* para uma componente financeira. Noutros estudos, o género foi fraco preditor para o medo do furto de identidade *online* e vírus no computador (Roberts *et al.* 2013; Yu, 2014). Relativamente às atividades contra as pessoas, como o cyberbullying ou o assédio *online*, as mulheres reportaram maiores níveis de medo nos estudos de Henson (2013), Yu (2014) e Pereira (2016 ingles). Mais recentemente, também o estudo de Virtanen (2017) obteve como resultados as mulheres reportarem maiores níveis de medo de cibercrime. Em suma, as mulheres parecem ter maior medo de crimes interpessoais *online* (idem). Esta questão pode ter como explicação a hipótese *shadow of sexual assault* (Warr, 1984; Ferraro 1995, 1996; Fisher & Sloan, 2003; Henson & Reyns, 2015), cuja premissa parte do medo que as mulheres sentem de crimes de natureza sexual, e que se generaliza a outros tipos de medo, ou seja, questionadas sobre o medo do crime, as mulheres associam-no ao medo de crimes de violação ou abuso sexual, por exemplo, e este medo aumenta igualmente o medo de outros tipos de crime, nomeadamente os que envolvam a interação pessoal.

Quanto à idade, os estudos sobre o medo do crime tradicional têm apontado os mais velhos como o grupo que reporta sentir mais medo (e.g., Ferraro, 1995), todavia, mais recentemente, os estudos não têm encontrado diferenças entre os grupos, salientando a importância de outros fatores – como o risco percebido de vitimação ou a maior vulnerabilidade física dos idosos – como justificação de altos níveis de medo sentidos, pelo que os resultados são mistos (Warr, 1984; Hale, 1996). No ciberespaço, ser mais novo foi um preditor do medo de vitimação *online* (Virtanen, 2017). Também Henson *et al.* (2013) observaram que são os mais novos que reportam maiores níveis de medo para a componente interpessoal do medo *online*, por um parceiro íntimo ou um amigo/conhecido. Ao mesmo tempo, Randa (2013)

encontrou correlações negativas entre a idade e o medo, isto é, os mais novos reportam mais medo de cyberbullying num dos modelos gerais do estudo. No estudo de Roberts (2013), a idade foi um preditor no medo do furto de identidade *online* e atividades fraudulentas, mas contou com menos de 1% de variância única no medo de furto de identidade *online* e atividade fraudulenta. Contrariamente, Yu (2014) refere que a idade não foi preditor do medo de quatro tipos de vitimação *online* (*scam online*, cyberbullying, vírus informático e pirataria digital). No estudo de Brands & Van Wilsem (2019), foram os mais velhos a reportar maiores níveis de medo *online* para uma componente financeira.

No que toca às vulnerabilidades sociais, em relação à perceção dos rendimentos auferidos, a maioria dos estudos mostra que são os que têm níveis mais baixos de rendimentos ou de posição social que reportam maiores níveis de medo (Hale, 1996). No ciberespaço, estes resultados estão em conformidade com o estudo de Virtanen (2017) que encontrou associações entre estatutos sociais mais baixos (numa escala de 1-10) – mas não o mais baixo – e maiores níveis de medo do cibercrime. A posição social mais baixa só foi preditor significativo do medo quando analisada em conformidade com o facto de ter sido vítima (*idem*). Roberts (2013) analisou três níveis de rendimento familiar anual (baixo, médio e alto) e nenhum deles se relacionou de forma estatisticamente significativa com o medo do furto de identidade *online* e atividades fraudulentas. Brands & Van Wilsem (2019) encontraram níveis baixos de medo para membros de agregados familiares com altos níveis de rendimentos. Também o nível de escolaridade tem mostrado relações negativas: são os que têm menores índices escolares que reportam maior medo do crime (Guedes, 2012). No mundo *online*, Roberts (2013) mostra que a educação é um fraco preditor do medo de furto de identidade *online* e atividade fraudulenta. Brands & Van Wilsem (2019) referem que quem reportou maiores níveis de escolaridade, tinham menos níveis de medo.

A influência do medo tradicional *offline* no medo que é sentido *online* foi medido no estudo de Roberts *et al.* (2013). Os autores defendem a existência de uma componente generalizada de medo que alberga o medo tradicional e o medo *online*. Assim, o medo do crime é um fator disposicional geral (pág. 324). Concretamente, esta componente geral de medo advém da correlação positiva entre o medo *offline* (medido a partir da preocupação em ser fisicamente atacado em casa, fisicamente atacado na rua ou outros espaços públicos, ser abusado sexualmente e ter a casa arrombada) como preditor do medo do furto de identidade *online* e atividades fraudulentas. Em suma, este medo *online*, específico desta tipologia de

cibercrime, é influenciado por uma componente de medo generalizada já existente a todos os tipos de crime. Ou seja, o medo do crime é um fator disposicional generalizado.

Quanto à percepção do risco de vitimação no contexto *online*, a literatura tem também apontado relações positivas entre a dimensão cognitiva e afetiva. Maiores níveis de percepção de risco *online* são reportados em linha com maiores níveis de medo do crime (e.g. Jonathan, 2009; Truman, 2005 citados em Pereira & Matos, 2015b). Henson (2013) identificou relações entre o risco percebido de vitimação interpessoal *online* e o medo de cibercrime interpessoal. Yu (2014) encontrou correlações positivas entre o risco percebido de vitimação e o medo de *online scams* e medo de cyberbullying. Também Higgins *et al.* (2008) verificaram correlações positivas entre a percepção do risco e medo de vitimação *online* atendendo ao uso do Facebook por estudantes universitários.

Relativamente à experiência de vitimação no contexto tradicional, os resultados são mistos, havendo estudos que obtiveram relações positivas entre a vitimação anterior e o medo do crime (e.g. Liska *et al.*, 1988) e outros que obtiveram relações fracas (e.g. Hale, 1996 citado em Guedes, 2012). A mesma linha repercute-se no ciberespaço (e.g. Henson *et al.* 2013 refere que a vitimação direta (composta por *hacking* e furto de identidade *online*) entre parceiros íntimos foi preditor do medo de vitimação interpessoal *online*. Contudo, ao ser específico ao crime, a vitimação interpessoal *online* (composta pelos comportamentos *online* contato indesejado, assédio, avanços sexuais indesejados e ameaças de violência) não foi preditor do medo de vitimação interpessoal *online*. Randa (2013) encontrou relações positivas entre a vitimação por cyberbullying e medo de cyberbullying; em contrapartida com estes resultados para a componente interpessoal, Yu (2014) registou uma correlação negativa entre a vitimação *online* anterior e o medo de cyberbullying, mas quando analisado o medo de vírus informático, a vitimação anterior foi influente. Pereira *et al.* (2016 inglês) referem que os adolescentes reportaram mais medo quando o assédio *online* era mais persistente. No estudo de Brands & Van Wilsem (2019), *all victimization experiences have higher levels of fear of online financial crime*.

CAPÍTULO II – Estudo Empírico (Metodologia)

1. Objetivos

A presente dissertação visa aprofundar o conhecimento sobre os preditores de duas variáveis dependentes: o medo do cibercrime e a vitimação *online*. Concretamente, procura-se, por um lado, analisar a relação entre o medo do cibercrime e as seguintes variáveis: vulnerabilidades físicas e sociais (e.g., género, nível de escolaridade), o medo *offline*, a experiência de vitimação *online* e atividades de rotina no contexto *online*, derivadas da Teoria das Atividades de Rotina. Por outro lado, este trabalho procura analisar a relação entre a vitimação *online*, as características pessoais (e.g., género) e as atividades de rotina. Complementarmente, e a título exploratório, analisar-se-á também quais são as variáveis predictoras do medo *online*/vitimação *online* contra as pessoas (incluindo o cyberbullying e *cyberstalking*) e do medo *online*/vitimação *online* contra a propriedade (englobando as ofensas de furto de identidade *online* e fraude ao consumidor *online*).

Em concreto, procura-se com este estudo ir de encontro aos seguintes objetivos específicos:

- a) Perceber qual a relação entre as vulnerabilidades físicas (e.g., idade, género) e socioeconómicas e o medo *online*.
- b) Analisar a relação entre exposição *online* a ofensores motivados, a adequação do alvo e a falta de guardiões e o medo de vitimação *online*;
- c) Analisar a influência que a insegurança geral e o medo *offline* surtem no medo do cibercrime;
- d) Analisar a influência da percepção do risco de vitimação *online* no medo do cibercrime;
- e) Analisar a relação entre a experiência de vitimação *online* e medo de vitimação *online*.
- f) Examinar como as características pessoais se relacionam com a vitimação *online*;
- g) Analisar a relação entre exposição *online* a ofensores motivados, a adequação do alvo e a falta de guardiões com a probabilidade de ocorrer vitimação *online*;
- h) Analisar a influência da percepção do risco de vitimação *online* na probabilidade de vitimação *online*.

2. Hipóteses

2.1. Medo de vitimação *online*:

H1: o género, a idade, os níveis de escolaridade e a perceção sobre os rendimentos auferidos influenciam os níveis de medo de cibercrime;

H2: quanto mais uma pessoa se expõe *online*, maior o medo do cibercrime;

- a. a exposição económica influencia os níveis de medo *online* para a componente propriedade;
- b. a exposição interativa influencia os níveis de medo *online* para a componente interpessoal;

H3: quanto maior a frequência de atividades de risco e o tipo de informação publicada *online*, maior o medo do cibercrime;

H4: quanto maior o conhecimento informático e os comportamentos e ferramentas de segurança (guardião), menor o medo do cibercrime;

H5: quanto maior forem os níveis de insegurança geral, o medo interpessoal *offline* e o medo relativo à propriedade *offline*, maior serão também os níveis de medo do cibercrime;

- a. o medo *offline* interpessoal correlaciona-se positivamente com o medo *online* interpessoal;
- b. o medo *offline* propriedade correlaciona-se positivamente com o medo *online* propriedade;

H6: o risco percebido de vitimação *online* está positivamente correlacionado com o medo do cibercrime;

H7: a experiência de vitimação *online* relaciona-se com o medo de vitimação *online*; NAO

- a. a experiência de vitimação *online* propriedade relaciona-se com o medo de vitimação *online* propriedade;
- b. a experiência de vitimação *online* interpessoal relaciona-se com o medo de vitimação *online* interpessoal.

2.2. Vitimação *online*:

H8: o género, o nível de escolaridade e a perceção sobre os rendimentos auferidos influenciam a probabilidade de ocorrer vitimação *online*;

H9: quanto mais uma pessoa se expõe *online*, maior a probabilidade de vitimação *online*;

- a. a exposição económica influencia os níveis de vitimação *online* para a componente propriedade;
 - b. a exposição interativa influencia os níveis de vitimação *online* para a componente interpessoal.
- H10: quanto maior a frequência de atividades de risco e o tipo de informação publicada *online*, maior a probabilidade de vitimação *online*;
- H11: quanto maior o conhecimento informático e os comportamentos e ferramentas de segurança (guardião), menor a probabilidade de vitimação *online*;
- H12: o risco percebido de vitimação *online* relaciona-se com a vitimação *online*;

3. Caraterização do estudo

O presente estudo adota uma metodologia quantitativa para explorar relações entre variáveis sociodemográficas, variáveis que derivam da Teoria das Atividades de Rotina, assim como outras variáveis (e.g., medo *offline*, risco percebido de vitimação *online*) e as variáveis dependentes medo do cibercrime e vitimação *online*. O tipo de investigação apresenta-se como correlacional, na medida em que o investigador não intervém sobre as variáveis, limitando-se a observá-las (Mâroco, 2014). De acordo com as relações analisadas, o estudo poderá, também, apresentar-se como explicativo do medo do cibercrime e da vitimação *online*, ainda que de forma parcial.

4. Forma de constituição da amostra

A amostra total deste estudo é constituída por 726 indivíduos. Para a recolha de dados procedeu-se à aplicação de um questionário *online* em dois espaços e momentos diferentes. Primeiramente, o questionário foi publicado e partilhado nas redes sociais. Seguidamente, foi disseminado pelo email institucional da Faculdade de Direito da Universidade do Porto com as devidas autorizações por parte da Reitoria da UP. A utilização do questionário *online* permite realizar uma delimitação inicial de uma caraterística dos participantes e que é decisiva para o estudo – o uso da *Internet* (e.g. atividades que realiza *online*). Além disso, sendo disseminado via *online*, permite aceder a uma larga dimensão amostral com reduzidos custos financeiros e com celeridade no processo de recolha de dados. Assim, o método de amostragem foi não probabilístico, pois não se conhece a probabilidade de cada elemento vir a integrar a amostra e, ainda, por conveniência, ou seja, a adesão ao estudo parte da disponibilidade e vontade de cada indivíduo.

5. Instrumento e Variáveis

Nos próximos subcapítulos será descrita a estrutura que compõe o questionário *online*, nomeadamente as questões utilizadas e as formas de dicotomização e codificação das variáveis, componentes e índices para futura análise. Além disso, no subcapítulo 5.5., encontram-se as definições dos cibercrimes, utilizados nas medidas do medo *online* e risco percebido *online*.

5.1. Secção I – Questões pessoais e sociodemográficas

Esta primeira secção incide sobre as características sociodemográficas dos intervenientes.

No que respeita ao género, somente 3 indivíduos registaram a opção “outro”, pelo que essa opção foi excluída da análise, e assim dicotomizou-se a variável (0=Feminino; 1=Masculino). A situação profissional foi questionada, mas excluída da análise metodológica. Por sua vez, a idade foi medida em anos. O nível de escolaridade foi medido através de 18 opções (entre 1=1º ano e 18=pós-doutoramento). Como também foi medido a opção “curso profissional”, recodificou-se a variável para ficar equivalente com o 12º ano. O estado civil foi questionado com as seguintes categorias de resposta: Solteiro; Casado/em União de facto; Divorciado ou Separado e Viúvo. Posteriormente, foi recodificado para uma variável dicotómica (0=Solteiro, composto pelos grupos solteiro e divorciado ou separado; 1=Casado, composto pelo grupo casado/em união de facto). Relativamente à perceção dos rendimentos auferidos pelo agregado familiar, as 5 categorias de resposta variam entre: Baixo; Médio-baixo; Médio; Médio-alto e Alto. Ademais, questionou-se a quem tinha respondido ser trabalhador por conta de outrem ou por conta própria, se estavam em regime de teletrabalho. Devido à forte adesão à questão do grupo profissional “estudante-trabalhador”, esta foi também incluída. A zona de residência foi também dicotomizada em 0=Zona rural; 1=Zona urbana. Questionou-se também sobre a insegurança económica que os indivíduos têm a partir de 3 situações, medidas numa escala de insegurança de 1 a 10 valores: “Com a possibilidade de perder ou não arranjar emprego devido à atual situação económica”; “Com a possibilidade de não ascender na sua carreira devido à atual situação económica” e “Em confrontar-se com uma despesa considerável e imprevista”. Esta variável latente foi adaptada do estudo de Couto (2019). O α de Cronbach foi de 0.858.

5.2. Secção II – Questões relativas ao contexto e forma de aceder à Internet

Para efeitos de estatística descritiva, esta seção perguntou sobre o contexto em que se efetua a ligação à Internet. Por um lado, questionou-se sobre o tipo de dispositivo informático mais utilizado: *smartphone*; computador; tablet; TV; consola de jogar e/ou outra opção, e por outro lado, sobre o local onde mais frequentemente se conectam à Internet: casa; trabalho/escola;

locais públicos, mas sem utilizar a rede WI-FI pública (e.g. utiliza dados móveis ou um dispositivo de *Internet* móvel pessoal) e locais públicos com rede WI-FI pública (e.g. centros comerciais, estabelecimentos de restauração, transportes públicos).

5.3. Seção III – Teoria das Atividades de Rotina *online*

Nesta seção procura-se reaplicar as variáveis da TAR no ciberespaço, nomeadamente a exposição *online*, o alvo adequado e o guardião.

a) Exposição *online*

A exposição a ofensores motivados vai incidir sobre a frequência diária, em horas, do uso de *Internet* e as respetivas atividades de rotina *online*. Relativamente à exposição *online* em horas, trata-se de uma medida que tem sido aplicada em vários estudos (e.g. Henson *et al.*, 2013; Virtanen, 2017). Neste estudo questionou-se aos participantes “Em média, quantas horas por dia passa na *Internet*?”. As opções de resposta foram: menos de 1 hora; entre 1 a 2 horas; entre 3 a 5 horas; entre 6 a 9 horas e 10 ou mais horas. Quanto à exposição *online* em atividades – visibilidade –, questionaram-se os indivíduos sobre as seguintes atividades de rotina *online*: 1) uso do banco *online* ou gestão de finanças; 2) comprar bens ou serviços na *Internet*; 3) uso do e-mail ou mensagens instantâneas; 4) utilização de redes sociais (e.g. Facebook, Instagram, LinkedIn); 5) atualização diária das suas redes sociais; 6) ler notícias, blogs ou fóruns; 7) participar ativamente em salas de chat ou outros fóruns; 8) interação em *websites* de encontros/fazer amizades (e.g. Tinder, Omegle); 9) fazer downloads de músicas, filmes, jogos ou podcasts; 10) visualização de conteúdo de entretenimento (e.g. Youtube, Twitch, Netflix, Spotify); 11) utiliza como suporte de trabalho ou estudo. Os itens 1), 2), 3), 4), 6), 7), 9) e 11) foram baseados nos estudos de Reyns (2013), os itens 1) e 2) foram baseados em Virtanen (2017), os itens 3) e 6) foram baseados no European Commission (2020), o item 5) foi baseado em Reyns, *et al.* (2011) e o item 8) em Henson *et al.* (2013). O item 10) foi baseado no European Commission (2020) com exemplos nossos. As opções de resposta variavam numa escala de 1 (nada frequentemente) a 4 (muito frequentemente). Certas atividades *online* realizadas pelos indivíduos podem ajudar a explicar variações específicas nos índices de medo e vitimação *online* à luz da exposição que se sujeitam a ofensores motivados. Por forma a agrupar estas atividades em categorias foi realizada uma análise fatorial (ver Anexo 1). Verificou-se, assim, que as atividades se aglomeravam em três grandes grupos, os quais foram designados por exposição económica, exposição interativa e exposição de entretenimento (ver Anexo 3).

b) Alvo adequado

No que toca à operacionalização do alvo adequado, este foi medido através de duas medidas que podem aumentar a sua atratividade. Numa primeira questão, a atratividade resulta de determinadas atividades *online* com um certo nível de risco inerente. Assim, perguntou-se aos participantes se nos últimos 12 meses: 1) Comunicou com desconhecidos *online*; 2) Abriu anexos ou *links* desconhecidos recebidos por e-mail; 3) Abriu anexos ou ficheiros recebidos através de mensagens instantâneas de alguém desconhecido; 4) Forneceu voluntariamente os seus dados pessoais a alguém desconhecido; 5) Clicou em mensagens pop-up e 6) Visitou *websites* duvidosos. Os itens 1) e 4) são baseados nos estudos de Ngo & Paternoster (2011) e Marcum (2010), os itens 2), 3) e 5) são baseados em Choi (2008) e Ngo & Paternoster (2011), e o item 6) é baseado em Reyns (2015). Enquanto Martins (2018) utilizou respostas dicotómicas, no presente estudo perguntou-se sobre a frequência numa escala de 1 (nada frequentemente) a 4 (muito frequentemente).

Por forma a organizar as atividades de risco em grupos optou-se, igualmente, pela realização de uma análise fatorial (ver Anexo 2). Assim, obtiveram-se três grupos que contemplam a abertura de ficheiros, *links* ou anexos desconhecidos, a comunicação ou fornecimento de dados a desconhecidos e o uso de risco de páginas de *Internet* (ver Anexo 3).

Numa segunda questão, questionou-se sobre a quantidade de informação publicada nas redes sociais e na *Internet* em geral. Os itens em 1) são baseados nos estudos de Marcum *et al.* (2010), que se restringe às redes sociais, e de Reyns *et al.*, (2011). Ademais, os itens em 2) foram desenvolvidos por nós. Deste modo, criou-se um índice da quantidade de informação disponibilizada *online* (que variava entre 0 e 12, sendo 12 a resposta “sim” a todas as opções) dos seguintes tipos de informação que indicam atratividade: 1) Nome completo, idade, género, orientação sexual, estado de relacionamento, número de contacto, endereço de email, fotos ou vídeos de si próprio, interesses e metas pessoais, atividades/passatempos, endereços para outras redes sociais/blogs, angústias emocionais ou conflitos familiares; 2) Local de residência, local onde se encontra no momento da partilha de informação.

Por sua vez, a medição objetiva da inércia e do valor atribuído por um potencial ofensor, não foram perguntados.

c) Guardião online

Quanto ao guardião *online*, adotou-se duas tipologias: um guardião físico/tecnológico e um guardião pessoal. O primeiro refere-se a todo o tipo de *software* de segurança que funcione de forma automatizada e que se enquadre nos limites do funcionamento da máquina (e.g.

programas antivírus, *antispyware*, *firewall*). Esta figura do guardião *online* que funciona com ações automáticas e programadas pelo computador, necessita, contudo, que exista ação humana no momento de instalação desses programas de *software*, assim como a sua manutenção (e.g. além de ser necessário o estabelecimento de ligação à *Internet*, pode também ser necessário fazer atualizações manuais no caso de *softwares* gratuitos). Todavia, nos limites que temos pensados para a presente dissertação, esta manifestação humana funcionaria em todo o caso como guardião pessoal – mais concretamente como comportamento de proteção – e sem essa operação o *software* de segurança não funcionaria. Assim, o tipo de *software* de segurança é medido como guardião físico/tecnológico (e.g. Ngo & Paternoster, 2011; Williams, 2016), mas de forma excecional incorporará também as ações necessárias para o seu pleno funcionamento. Em segundo lugar, no que respeita ao guardião pessoal, atendeu-se à divisão entre: 1) comportamentos de proteção; 2) comportamentos de evitamento e 3) conhecimento informático. Os comportamentos de proteção e de evitamento são incorporados como guardiões pessoais seguindo os moldes da TAR (i.e., a sua presença pode ajudar a evitar a probabilidade de vitimação), mas vão também de encontro com a literatura sobre o medo do (ciber)crime (i.e., eles existem, usualmente, por consequência da insegurança sentida, Liska *et al.*, 1988). Em suma, a ausência de guardiões capazes de proteger o utilizador *online* aumentará a probabilidade de determinados alvos sofrerem vitimação *online* por parte de ofensores motivados, assim como os níveis de medo de ser-se vítima de cibercrime.

A par dos estudos de Guedes (2012) e Martins (2018), questionou-se os respondentes, se “por razões de segurança” realizam algum dos seguintes comportamentos. Ao nível do guardião físico/tecnológico questionou-se, se: 1) Utiliza filtro de spam no email; 2) Utiliza *software* de segurança do navegador de *Internet* (e.g. Avast Secure Browser, Google Safe Browsing, Tor Browsing); 3) Tem instalado e atualizado *software* antivírus, *software* *antispyware* ou *software/hardware* firewall pago e 4) Tem instalado e atualizado *software* antivírus, *software* *antispyware* ou *software/hardware* firewall gratuito. Por outro lado, ao nível do guardião pessoal, quanto aos comportamentos de proteção perguntou-se, se: 5) Muda regularmente as palavras-passe; 6) Utiliza palavras-passe fortes em tamanho e caracteres; 7) Utiliza a verificação de segurança de 2 passos; 8) Utiliza características biométricas (e.g. reconhecimento facial, impressão digital); 9) Utiliza apenas os seus dispositivos informáticos e 10) Apenas acede a *websites* fidedignos. No que toca aos comportamentos de evitamento: 11) Evita aceder ao banco *online*; 12) Evita fazer compras *online*; 13) Evita abrir e-mails de pessoas que não conhece; 14) Evita conectar-se à *Internet* por redes WI-FI públicas; 15) Evita utilizar

websites de encontros/fazer amizades (e.g. Tinder, Omegle) e 16) Evita partilhar informação pessoal nas redes sociais ou na *Internet* em geral. Os itens 1), 10), 11), 12), 13) são baseados nos estudos de Williams (2016), o item 3) é baseado no estudo de Ngo & Paternoster (2011) e os itens 5), 6), 8), 9), 10), 13), 14) e 16) são baseados no European Commission (2020). Por último, os itens 2), 7) e 15) foram desenvolvidos por nós. Além disso, optou-se por dividir o item 3) relativo ao *software* de segurança em entre *software* pago, por um lado e gratuito, por outro. De salientar que, o European Commission (2020) utilizou “usa passwords mais complexas” para o item 6), pelo que modificou-se para se perceber mais facilmente. As opções de resposta são dicotómicas (0=não; 1=sim).

Finalmente, o conhecimento informático foi baseado no estudo de Holt & Bossler (2013) através da questão “Qual considera ser o seu nível de conhecimento informático?”. As respostas variavam entre “Básico; Médio e Avançado”.

No presente estudo optou-se por utilizar um índice geral do guardião (composto pelo guardião físico/tecnológico e pelos guardiões pessoais comportamentos de proteção e comportamentos de evitamento) em que pontuações mais altas indicam presença e maior capacidade de proteção pelos guardiões.

5.4. Seção IV – Medição do medo de vitimação *online*, insegurança geral, medo *offline* interpessoal e medo *offline* propriedade

Na presente dissertação mediu-se o medo do crime em dois contextos (*online* e *offline*, sendo o medo do crime *online* uma das variáveis dependentes). De acordo com as recomendações da literatura (e.g., Ferraro & LaGrange, 1987; Jackson, 2004; Gray *et al.*, 2008), e dada a extensão do questionário, decidiu-se medir diretamente a intensidade do medo sentido com os diferentes cibercrimes em análise neste estudo, através da pergunta “Numa escala de 1 (nenhum medo) a 4 (muito medo), quanto medo tem que as seguintes situações lhe aconteçam”. A consistência interna foi .816 de alfa de Cronbach (Anexo 4).

Relativamente às variáveis alusivas ao contexto tradicional, procurou-se medir a insegurança geral e duas medidas do medo *offline* (interpessoal e relativo à propriedade). Para a insegurança geral, questionou-se, numa escala de 1 (Muito Inseguro) a 5 (Muito Seguro), “Como é que se sente quando caminha sozinho(a) na sua zona de residência, depois de escurecer?”. Posteriormente, a escala foi recodificada de forma inversa, para que pontuações mais altas refletissem níveis mais elevados de insegurança geral. No âmbito do estudo de Rodrigues (2017), para as restantes variáveis do medo *offline*, perguntou-se “Quanto medo

sente que o seguinte lhe aconteça?”. As opções foram: ser agredido, ser agredido sexualmente, ser roubado, ter a casa assaltada, ter a propriedade vandalizada e ter o carro roubado. A partir destas questões criou-se um índice do medo *offline* interpessoal composto pelos medos de agressão e agressão sexual e um índice do medo *offline* propriedade composto pelos medos de ser roubado, ter a casa assaltada, ter a propriedade vandalizada e do carro ser roubado. A consistência interna foi de 0.827 e 0.900 de alfa de *Cronbach* respetivamente.

5.5. Seção V – Perceção do risco de vitimação *online* e experiência de vitimação *online*

Para medir a perceção do risco de vitimação *online*/risco percebido *online*, perguntou-se “Numa escala de 1 (nada provável) a 4 (muito provável), quão provável acha que as seguintes situações lhe possam acontecer, nos próximos 12 meses.” As opções de resposta abrangiam a vitimações *online* deste estudo. O alfa de *Cronbach* foi de 0,792 (Anexo 4).

Por fim, foi medida a experiência pessoal de vitimação *online* e a respetiva frequência. Além dos cibercrime abordados nas medição do medo *online* e risco percebido *online* – fraude ao consumidor; furto de identidade *online*; *cyberstalking*; ciberbullying e a descoberta de *software* malicioso –, foi também incorporado o *phishing*. Assim, mediu-se a prevalência corrente (vitimação nos últimos 12 meses) com respostas dicotómicas (0=não; 1=sim). Como já foi referido, a redação das definições dos cibercrimes foi igualmente utilizada para a medição do medo de vitimação *online* e para a perceção do risco de vitimação *online*:

- a) O furto de identidade *online* foi baseado na definição de Saunders & Zucker (1999) “*apropriação e uso não consentido dos seus dados pessoais ou financeiros para fins criminosos*” (cit. in. Hille et al. 2015) sendo redigido como “Alguém se apropriar e usar, de forma não consentida, os seus dados pessoais ou financeiros para fins criminosos”.
- b) A fraude ao consumidor *online* foi descrita como “Comprar produtos ou serviços via *Internet* e estes não chegarem a sua casa, serem falsificados ou não serem iguais à forma como lhe foram anunciados?”, cuja definição é retirada do European Commission (2020).
- c) Ciberbullying foi descrito como “Receber mensagens hostis ou agressivas que lhe causem dano ou desconforto, através da *Internet* ou outro dispositivo eletrónico?”, baseado na definição integrativa do estudo de Tokunaga (2010, p. 278). Como vimos no capítulo 2.4.2, as definições de ciberbullying utilizadas nos estudos empíricos não são diferenciadoras o suficiente de outras formas de vitimação pessoal *online* como o assédio ou o *cyberstalking* (Randa & Reyns, 2014). Assim, a definição de ciberbullying

adotada, visa sobretudo afastar-se da definição de *cyberstalking* e simplificar a visão que os respondentes teriam desse fenómeno (e.g. não utilizar o elemento “repetição”). Ao mesmo tempo, a literatura – nomeadamente a hipótese *shadow of sexual assault* (e.g., Warr, 1984) – defende que o medo de agressão sexual que as mulheres sentem, aumenta o medo de outros tipos de crime, nomeadamente os crimes que envolvam o confronto interpessoal, pelo que a distinção entre ambos os comportamentos, que são subsidiários do assédio *online*, deve ser efetiva (Henson & Reynolds, 2015).

- d) *Cyberstalking* foi definido como “Alguém, de forma repetida e intencional, lhe imponha formas indesejadas de comunicação, aproximação ou perseguição, através da *Internet* ou outro dispositivo eletrónico”, e é baseado na definição do estudo de Pereira & Matos (2015b).
- e) A descoberta de *software* malicioso foi descrita como “Descobrir *software* malicioso no seu dispositivo (e.g., vírus, cavalos de Troia, *spywares*)”, retirada do European Commission (2020).
- f) Por último, o *phishing* foi descrito como “Receber emails fraudulentos a pedir informação pessoal (e.g. um link de um site falso a pedir informação para fazer um pagamento)” e é retirado no item do European Commission (2020).

Em caso afirmativo à questão filtro, perguntou-se a frequência dessa vitimação para o mesmo espaço de tempo. Dada a extensão do questionário, esta questão não foi obrigatória.

6. Procedimentos de recolha de dados

Após a construção do instrumento supradesenvolvido, procedeu-se, antes da divulgação efetiva do questionário *online*, à realização de um pré-teste. Para tal, obteve-se uma amostra de 5 pessoas, questionando-se a amigos próximos se estariam disponíveis para realizarem o pré-teste do presente estudo. Esta fase preliminar permitiu receber feedback dos respondentes quanto à compreensão e coerência das questões e dos conceitos utilizados que podiam atentar contra a validade e fiabilidade do instrumento, assim como o tempo médio de autopreenchimento do questionário e outras questões de formatação gráfica (e.g. quem utilizou um *smartphone* reportou alguma dificuldade em responder a questões com escalas muito grandes). Após a realização do pré-teste e as alterações mencionadas, passou-se para a aplicação do questionário *online* tendo em conta as fases já descritas na secção 4. deste capítulo. Assim, primeiramente este foi publicado e partilhado nas redes sociais a 28 de fevereiro, seguido da sua publicação no email institucional da Faculdade de Direito da Universidade do Porto a 16

de março com as devidas autorizações da Reitoria da Universidade do Porto. O questionário *online* esteve disponível um total de 18 dias, atingindo-se a amostra de 726 indivíduos. Note-se que os participantes foram devidamente informados, na folha de rosto, das questões éticas da investigação científica, nomeadamente quanto à confidencialidade e ao anonimato dos seus dados, assim como dos objetivos do estudo e a voluntariedade da sua participação no mesmo.

7. Procedimentos de análise estatística

Esta secção descreve os procedimentos estatísticos adotados quanto à análise estatística descritiva e à análise estatística inferencial dos dados. O tratamento dos dados foi feito a partir do *software* IBM SPSS Statistics 26.

7.1. Análise estatística descritiva

Para a descrição das características pessoais utilizaram-se medidas de tendência central e medidas de dispersão. As primeiras permitem representar a tendência das variáveis (e.g., média). As segundas permitem verificar a dispersão face a uma medida de tendência central (e.g., desvio-padrão face à média). No que toca às variáveis quantitativas como a idade ou os anos de escolaridade, utilizou-se a média amostral ($\bar{X}$) e o desvio-padrão (S.D), além dos mínimos e máximos. Para as variáveis qualitativas como o género ou a vitimação *online* utilizaram-se frequências e percentagens. No presente estudo, dado o elevado tamanho amostral ($n=726$) e tendo em conta o Teorema do Limite Central – que defende que à medida que o tamanho da amostra aumenta, a distribuição das médias amostrais tende a uma distribuição normal –, optou-se pela utilização de testes paramétricos. Desta forma, de acordo com a tipologia das variáveis, utilizaram-se *testes-t* para analisar as diferenças de médias entre dois grupos (e.g., vítimas e não vítimas); testes *ANOVA* quando uma das variáveis tivesse mais de dois grupos independentes (e.g., exposição *online* em horas em função do medo *online*) e testes Qui-quadrado (χ^2) para analisar as diferenças entre dois ou mais grupos independentes perante uma variável categórica e as respetivas tabelas de contingências (e.g., conhecimento informático em função da vitimação *online*).

A análise fatorial permitiu o agrupamento de vários itens em fatores, criando assim índices (e.g., exposição económica). A redução de várias variáveis observadas agregadas num único fator comum latente foi realizada através do método de rotação *Varimax*, e possibilita que a análise da variância desse fator descreva os dados de forma mais simples e estruturada. Por último, para medir a consistência interna dos índices criados utilizou-se o alfa (α) de *Cronbach*.

7.2. Análise estatística inferencial

Para a análise de correlações entre variáveis utilizou-se o coeficiente de correlação de Pearson. Esta medida de associação permite estabelecer a intensidade e a direção entre duas variáveis quantitativas. Os valores do coeficiente de correlação variam de -1 a 1. Quanto mais este valor se distanciar do zero, mais forte será a relação entre as duas variáveis. Segundo Cohen (1988), as correlações que obtenham um valor entre -1 e -0.5 ou 0.5 e 1 apresentam uma relação elevada. As correlações cujos valores se situem entre -0.5 e -0.3 ou 0.3 e 0.5 apresentam uma relação moderada e as que apresentem valores entre -0.3 e 0 ou 0 e 0.3 apresentam uma relação fraca. As correlações são tidas como estatisticamente significativas, se $p < 0,05$, atendendo a um intervalo de confiança de 95%.

Por último, realizaram-se regressões lineares e regressões logísticas de forma a saber quais são as variáveis independentes que melhor prediziam as variáveis dependentes medo do cibercrime e vitimação *online*, respetivamente. Para o medo do cibercrime realizaram-se diferentes modelos de regressão linear com variáveis sociodemográficas; variáveis provenientes da TAR; variáveis do medo *offline*, perceção do risco de vitimação *online* e vitimação *online*. No fim, realizou-se um modelo final com as variáveis que foram estatisticamente significativas nos modelos anteriores. Note-se que, foram tidos em conta os valores do coeficiente de correlação (r), e, do coeficiente de determinação (r^2 e r^2 ajustado), caso o r fosse estatisticamente significativo ($p < 0,05$). Para a vitimação *online* fizeram-se modelos de regressão logística com variáveis sociodemográficas e as variáveis constituintes da TAR, juntamente com o risco percebido *online*. Novamente, realizou-se um modelo final com as variáveis que atingiram significância estatística nos modelos precedentes. Tiveram-se em conta os valores do -2 (Log likelihood) e do pseudo R ao quadrado de Nagelkerke.

Além disso, salienta-se o facto de não existirem indícios fortes de multicolinearidade que pudessem alterar as estimativas das variáveis independentes com as variáveis dependentes nos vários modelos de regressão linear e logística, ou seja, as variáveis não estavam altamente correlacionadas entre si. Segundo o diagnóstico de colinearidade do SPSS, os valores de VIF foram todos inferiores a pelo menos 3, enquanto os valores de tolerância foram todos > 0.1 , ou seja, as variáveis preditoras podem estar moderadamente correlacionadas.

CAPÍTULO III – Análise dos resultados

1. Caraterização descritiva das variáveis

1.1. Caraterização da amostra segundo os dados sociodemográficos

A tabela 1 apresenta a frequência e respetiva percentagem dos dados sociodemográficos da amostra, nomeadamente do género, estado civil, situação profissional, regime de teletrabalho, perceção dos rendimentos auferidos e zona de residência. Por sua vez, na tabela 2, podem ser observadas as médias e desvios-padrões da idade, escolaridade e insegurança económica. Nas próximas linhas, iremos, a partir das tabelas, descrever a amostra do presente estudo (n=726) que é constituída, na sua maioria, por indivíduos do sexo feminino (70,4%).

Tabela 1 Caraterísticas sociodemográficas (género, estado civil, situação profissional, teletrabalho, perceção sobre os rendimentos do agregado familiar e zona de residência) dos participantes da amostra.

Variáveis	N	%
Género		
Feminino	511	70.4
Masculino	212	29,2
Estado civil		
Solteiro	575	79.2
Casado/em União de facto	151	20.8
Situação Profissional		
Empregado(a) por conta de outrem	161	22.2
Empregado(a) por conta própria	19	2.6
Estudante	448	61.7
Estudante – Trabalhador	69	9.5
Reformado(a)/pensionista	7	1
Desempregado(a)	15	2.1
Outro	7	1
Teletrabalho	233	32.1
Não	119	16.4
Sim	114	15.7
Rendimentos		
Baixo	61	8.4
Médio-Baixo	182	25.1
Médio	344	47.4
Médio-Alto	131	18
Alto	8	1.1
Zona de Residência		
Rural	234	32.2
Urbana	492	67.8

Relativamente ao estado civil, a análise é feita através da divisão entre solteiro e casado/em união de facto com 70,2% e 20,8% respetivamente. Quanto à situação profissional, 61,7% da amostra respondeu ser estudante, seguindo-se empregado por conta de outrem com 22,2% da amostra. Por sua vez, uma minoria respondeu trabalhar por conta própria (2,6%), estarem sem emprego (2,1%) e estar reformado ou ser pensionista (1%). No que toca ao regime de teletrabalho, de um universo de 233 respostas, verificou-se que 15,7% se encontravam em teletrabalho na altura da realização do questionário, enquanto 16,4% reportaram não estar em teletrabalho. Já relativamente à perceção sobre os rendimentos do agregado familiar, verificou-se que 47,4% dos inquiridos reportaram ter um nível médio, 25,1% consideraram estar no patamar “médio-baixo” e 18% como médio-alto. Por fim, 8,4% responderam ter baixos rendimentos e somente 1,1% consideraram ter rendimentos altos. Por último, respeitante à zona de residência, percebe-se que 67,8% dos respondentes afirmam viver numa zona urbana enquanto 32,2% reportam viver numa zona rural.

Tabela 2 Caraterísticas sociodemográficas (idade, insegurança económica e escolaridade) dos participantes da amostra.

Variáveis	N	X	SD	Min	Max
Idade	725	27.47	11.78	16	72
Insegurança económica	726	5.82	2.52	1	10
Escolaridade	726	12.7	1.78	1	17

Os participantes do estudo têm idades compreendidas entre os 16 e os 72 anos. A média amostral é de 27,47 anos com um desvio-padrão de 11,78. A variável latente insegurança económica registou, numa escala de 1 a 10, uma média amostral de 5,82 (SD=2,52). Relativamente à escolaridade, a média amostral fixou-se nos 12,7, ou seja, entre “12º ano/Curso profissional” e “Licenciatura”, com um desvio-padrão de 1,78.

1.2. Caraterização da amostra segundo o tipo de dispositivo e o local de acesso à Internet

A próxima tabela incide sobre o contexto em que é efetuado o acesso *online*, nomeadamente quanto ao tipo de dispositivo informático utilizado e o local onde o acesso à Internet é realizado. O *smartphone* e o computador são os dois dispositivos mais utilizados para aceder à Internet com 90,6% e 88,8% respetivamente. Usar um tablet ou uma TV são utilizados por 12,3%, enquanto 3,2% dos inquiridos referiram utilizar uma consola de jogos. Relativamente ao local de acesso à Internet, a maioria (97,9%) referiu aceder em casa, enquanto 42,1% referiu utilizar a Internet no local de trabalho ou na escola. A utilização de Internet em locais públicos, mas sem fazerem uso da ligação a hotspots públicos foi reportada por 15,6% da amostra, enquanto 5,8% referiu fazê-lo com ligação a hotspots públicos.

1.3. Caracterização da amostra segundo as variáveis da Teoria das Atividades de Rotina *online*

Na tabela 4 podem ser observadas as médias e desvios-padrões das variáveis referentes à TAR. Em concreto, analisaremos os resultados quanto à exposição *online*, o alvo adequado e informação disponibilizada *online*, e os guardiões.

Tabela 3 Médias e desvios-padrões da exposição *online*, alvo adequado, informação disponibilizada online e índice do guardião.

Componente	Descrição	N	X	SD	Min	Max
Exposição económica	Uso do banco <i>online</i> ou gestão de finanças + Compra de bens ou serviços na <i>Internet</i>	726	2.42	0.84	1	4
Exposição interativa	Participar ativamente em fóruns + Interação em <i>websites</i> de encontros/fazer amizades (e.g. Tinder, Omegle)	726	1.33	0.51	1	4
Exposição de entretenimento	Utilização de redes sociais (e.g. Facebook, Instagram, LinkedIn) + Fazer download de músicas, filmes, jogos ou podcasts + Visualização de conteúdo de entretenimento (e.g. Youtube, Twitch, Netflix, Spotify)	726	3.01	0.67	1	4
Alvo adequado (abrir ficheiros desconhecidos)	Abriu anexos ou <i>links</i> desconhecidos recebidos por email + Abriu anexos ou ficheiros, recebidos através de mensagens instantâneas de alguém desconhecido	726	1.13	0.36	1	4
Alvo adequado (comunicar ou fornecer dados a desconhecidos)	Comunicou com desconhecidos <i>online</i> + Forneceu voluntariamente os seus dados pessoais a alguém desconhecido	726	1.34	0.50	1	4
Alvo adequado (uso de risco da <i>Internet</i>)	Clicou em mensagens pop-up + Visitou <i>websites</i> duvidosos	726	1.26	0.43	1	4
Alvo adequado (subcomponente)	Informação disponibilizada <i>online</i>	726	4.10	2.36	0	12
Guardião	Índice do guardião	726	10.54	2.24	2	16

Segundo a tabela 4, as atividades de exposição *online* entretenimento são, em média, as mais realizadas pela amostra ($X=3,01$, $SD = .67$). De seguida, as atividades de exposição *online* económica registaram uma média de 2,42 ($SD = .84$) enquanto as atividades de exposição interativa tiveram uma média de 1,33 ($SD = .51$). Relativamente ao alvo adequado, o alvo adequado comunicar ou fornecer dados a desconhecidos registou uma média de 1,34 ($SD = .50$). O alvo adequado uso de risco da *Internet* registou 1,26 de média ($SD = .43$), enquanto o índice abrir ficheiros desconhecidos registou uma média de 1,13 ($SD = .36$). A informação disponibilizada *online* registou em média 4,10 tipos diferentes de informação ($SD = 2.36$).

Quanto ao guardião, os indivíduos da amostra adotaram, em média, 10,54 comportamentos de segurança (SD =2.24).

Na tabela 5 é possível verificar a descrição da exposição *online* em horas diárias de uso de *Internet* e o conhecimento informático.

Tabela 4 Percentagem dos indivíduos em função da exposição *online* em horas e conhecimento informático.

Variáveis	N	%
Exposição <i>online</i> em horas		
Menos de 1 hora	8	1.1
Entre 1 a 2 horas	73	10.1
Entre 3 a 5 horas	216	29.8
Entre 6 a 9 horas	286	39.4
10 ou mais horas	143	19.7
Conhecimento informático		
Básico	180	24.8
Médio	448	61.7
Alto	98	13.5

Relativamente ao tempo médio passado na *Internet*, mais de dois terços dos inquiridos responderam passar no mínimo 3 horas por dia na *Internet*: 39,4% responderam entre 6 a 9 horas e 29,8 responderam entre 3 a 5 horas. Uma percentagem significativa dos respondentes afirma passar 10 ou mais horas por dia na *Internet*. Somente 1.1% responderam passar menos de 1 hora por dia.

De acordo com o nível percecionado das competências informáticas, mais de metade da amostra (61,7%) reportou ter um nível médio de conhecimento informático. Por sua vez, 24,8% da amostra reportou ter um nível básico de conhecimento informático, enquanto 13,5% reportaram ter alto saber informático.

1.4. Caraterização da amostra segundo o medo *online*, perceção do risco de vitimação *online*, insegurança geral e medo *offline* interpessoal e propriedade

A Tabela 6 apresenta a caraterização da amostra relativamente ao medo do cibercrime e da perceção do risco de vitimação (componente emocional e cognitiva do sentimento de insegurança, respetivamente). A tabela apresenta, ainda, as médias e desvios-padrões da insegurança geral e do medo *offline* interpessoal e relativo à propriedade.

Tabela 5 Médias e desvios-padrões do medo do cibercrime, perceção do risco de vitimação *online*, insegurança geral, medo *offline* interpessoal e medo *offline* propriedade.

Índices	N	X	SD	Min	Max
---------	---	---	----	-----	-----

Medo do cibercrime	726	2.93	0.68	1	4
Risco percebido online	726	2.01	0.53	1	4
Insegurança geral	726	3.20	1.18	1	5
Medo Offline					
Interpessoal	726	3.35	1.29	1	5
Propriedade	726	3.37	1.14	1	5

Em primeiro lugar, verifica-se que, de 1 a 4, a média da amostra do medo do cibercrime em geral é de 2,93 (SD = .68). Por sua vez, a amostra reporta uma média de percepção do risco de vitimação *online* de 2.01 (SD =.53).

Relativamente ao espaço *offline*, a média da insegurança geral é de 3,20 (SD =1.18), enquanto os medos *offline* interpessoal e propriedade apresentam médias semelhantes (X=3,35 e X=3,37, respetivamente).

1.5. Caraterização da amostra segundo a vitimação *online*

Na tabela 7 expõem-se os resultados quanto à vitimação *online*. As questões incidem sobre a experiência de vitimação nos últimos 12 meses (prevalência corrente).

Tabela 6 Percentagem dos indivíduos vítimas de furto de identidade *online*, fraude ao consumidor, cyberbullying, *cyberstalking*, descoberta de *software* malicioso e *phishing*.

Variáveis	N	%
Vitimação online		
Furto de identidade	31	4.3
Fraude ao consumidor	110	15.2
Cyberbullying	78	10.7
<i>Cyberstalking</i>	68	9.4
Descobrir <i>software</i> malicioso	90	12.4
<i>Phishing</i>	354	48.8

A amostra apresenta baixas taxas de incidência no que à vitimação *online* diz respeito, à exceção do *phishing* que foi reportado por quase metade da amostra (48,8%). Especificamente aos cibercrimes da componente financeira, 4,3% reportaram ter sido vítimas de furto de identidade *online*, enquanto 15,2% reportaram ter sido vítimas de fraude ao consumidor *online*. No total, reportaram ser vítimas para a componente relativa à propriedade 19.5%. A componente interpessoal obteve menores diferenças entre cyberbullying e *cyberstalking* (10.7% e 9.4% respetivamente), totalizando 20.1% de vítimas. Por sua vez, 12.4% da amostra reportaram ter descoberto *software* malicioso.

2. A relação entre o medo do cibercrime e as variáveis independentes

Nesta secção, expõem-se os resultados do medo de vitimação *online* em função das variáveis independentes. Primeiro, analisaremos a sua relação com as variáveis sociodemográficas. Posteriormente, analisaremos a influência das variáveis da TAR, nomeadamente a exposição *online*, alvo adequado e guardiões. Veremos também a relação com a perceção do risco de vitimação *online* e a influência que as medidas de medo *offline* possam ter com o medo *online*. Por último, verificaremos a relação com a segunda variável dependente do estudo – a vitimação *online*.

2.1. Medo do cibercrime e variáveis sociodemográficas

As tabelas 8, 9 e 10 caracterizam os resultados da amostra relativamente à variável dependente medo do cibercrime em função das variáveis sociodemográficas. A partir da tabela 8, pode observar-se um conjunto de diferenças nas médias do medo do cibercrime em função de algumas variáveis sociodemográficas.

Tabela 7 Testes-t: medo do crime em função das variáveis género, estado civil, teletrabalho e zona de residência.

Variáveis	Medo de Cibercrime		
	N	(X±S.D)	p
Género			
Feminino	511	3.08±0.63	.000
Masculino	212	2.59±0.68	
Estado civil			
Solteiro	575	2.99±0.68	.000
Casado/em União de facto	151	2.73±0.67	
Teletrabalho			
Não	119	2.87±0.67	.028
Sim	114	2.67±0.69	
Zona de residência			
Zona rural	234	3.04±0.71	.003
Zona urbana	492	2.89±0.67	

Relativamente ao género, observa-se que as mulheres apresentam maiores níveis de medo de cibercrime (X=3,08) do que os homens (X=2,59), sendo esta diferença estatisticamente significativa (p-value=.000). Por sua vez, verifica-se que os indivíduos solteiros apresentam níveis mais elevados de medo (X=2,99) em comparação com os casados/em união de facto (X=2,73, p-value=.000). Relativamente ao regime de teletrabalho, quem respondeu não estar em teletrabalho reportou maiores níveis de medo de cibercrime (X=2,87) do que os que estão em teletrabalho (X=2,67), atingindo esta diferença significância estatística (p-value=.028).

Quanto à zona de residência, verifica-se que quem vive em zonas rurais reporta, em média, mais medo do cibercrime ($X=3,04$) do que quem vive em zonas urbanas ($X=2,89$, $p\text{-value}=.003$).

Tabela 8 Correlações de Pearson: correlações entre ao medo de cibercrime e as variáveis idade, escolaridade e insegurança económica.

Variáveis	Medo cibercrime
Idade	-.17**
Escolaridade	-.16**
Insegurança Económica	.38**

**A correlação é significativa ao nível 0.01 (2-tailed)

No caso das variáveis idade e escolaridade, observa-se que a relação com o medo de cibercrime é negativa, ou seja, os indivíduos mais novos e com menor nível de escolaridade apresentam maiores índices de medo de cibercrime. Mais se adianta que a magnitude da associação de ambas as variáveis é fraca ($r=-.17$, $p\text{-value} <.001$; $r=-.16$, $p\text{-value}<.001$, respetivamente). Por outro lado, constata-se uma correlação positiva entre a insegurança económica e o medo do cibercrime ($r=.38$, $p\text{-value}<.001$). Isto é, quanto maior a insegurança económica reportada pela amostra, maiores os níveis de medo do cibercrime.

Tabela 9 Teste ANOVA: medo de cibercrime em função da variável perceção dos rendimentos auferidos pelo agregado familiar.

Variável	Medo Cibercrime	
	($\bar{X} \pm S.D$)	<i>p</i>
Rendimentos		
Baixo	3.03±0.69	.223
Médio-Baixo	2.99±0.70	
Médio	2.93±0.66	
Médio-Alto	2.83±0.68	
Alto	2.80±1.03	

Quanto à perceção dos rendimentos auferidos pelo agregado familiar, verifica-se que níveis mais baixos de rendimentos estão em linha com maiores níveis de medo de cibercrime. A relação não atinge, ainda assim, significância estatística ($p\text{-value}=.223$).

2.2. Medo de cibercrime em função do tipo de dispositivo informático e local de acesso à Internet

O Anexo 5 apresenta a relação entre o medo de cibercrime e o dispositivo informático utilizado para aceder à *Internet*, assim como o local onde o acesso foi feito. Relativamente ao

dispositivo informático utilizado para aceder à *Internet*, verifica-se que quem faz uso de um *smartphone* apresenta maiores níveis de medo de cibercrime ($X=2,96$) do que quem não utiliza um *smartphone* ($X=2,71$, $p\text{-value}=.004$), sendo esta diferença estatisticamente significativa. Por outro lado, quem referiu utilizar uma consola de jogos para navegar na *Internet* apresenta menos índices de medo de cibercrime ($X=2,60$) em comparação com quem a utiliza ($X=2,94$, $p\text{-value}=.020$), atingindo-se significância estatística. Relativamente ao ambiente físico em que o acesso à *Internet* é realizado, não existem diferenças que atinjam significado estatístico.

2.3. Medo de cibercrime e Teoria das Atividades de Rotina

As tabelas 11 e 12 apresentam a relação entre o medo do cibercrime e as componentes da TAR (exposição em atividades e horas *online*, alvo adequado e informação disponibilizada *online*, e o guardião e os conhecimentos informáticos.

Tabela 10 Correlações Pearson: correlações entre a variável dependente medo do cibercrime e as variáveis constituintes da TAR (exposição *online*, alvo adequado, informação disponibilizada *online* e índice do guardião).

Componente	Descrição	Medo de cibercrime
Exposição <i>online</i>	Económica	-.07
	Interativa	-.04
	Entretenimento	.17**
Alvo adequado	Abrir ficheiros desconhecidos	.10*
	Comunicar ou fornecer dados a desconhecidos	-.02
	Uso de risco da <i>Internet</i>	-.01
	Informação disponibilizada <i>online</i>	.10**
Guardião <i>online</i>	Índice do guardião	.09*

*A correlação é significativa ao nível 0.05 (2-tailed)

**A correlação é significativa ao nível 0.01 (2-tailed)

A tabela 11 apresenta um conjunto de correlações estatisticamente significativas que importa, desde já, analisar. Em primeiro lugar, no que respeita à exposição *online*, verifica-se que a variável específica de entretenimento se correlaciona positivamente com o medo do cibercrime ($r=.17$, $p\text{-value} < .001$), ou seja, quanto maiores os níveis de exposição de entretenimento *online*, maiores os níveis de medo de cibercrime. No que respeita ao alvo adequado, constata-se que abrir ficheiros desconhecidos está positivamente correlacionado com o medo do cibercrime ($r=.10$). Isto é, os indivíduos que reportam abrir ficheiros desconhecidos apresentam níveis mais elevados de medo do cibercrime ($r=.10$, $p < .005$). Quanto ao total de informação disponibilizada *online*, verifica-se uma correlação positiva com o medo do cibercrime ($r=.10$, $p\text{-value} < .001$), ou seja, quanto mais informação é publicada *online*, maiores são os níveis de medo de cibercrime. Por fim, quanto ao guardião, a relação com o medo do

cibercrime é fraca e positiva ($r=.09$, $p<.005$). Neste caso, os resultados referem níveis mais elevados de medo do cibercrime estão associados a uma maior adoção de comportamentos de segurança.

Tabela 11 ANOVA: medo do cibercrime em função da exposição *online* em horas e do conhecimento informático.

Variáveis	Medo Cibercrime	
	(X±S.D)	<i>p</i>
Exposição <i>online</i> em horas		
Menos de 1 hora	3.18±0.72	.217
Entre 1 a 2 horas	2.85±0.73	
Entre 3 a 5 horas	2.93±0.67	
Entre 6 a 9 horas	2.90±0.69	
10 ou mais horas	3.04±0.66	
Conhecimento informático		
Básico	3.09±0.67	.000
Médio	2.92±0.66	
Alto	2.72±0.77	

Na tabela 12, observa-se a relação entre a exposição *online* em horas e o medo do cibercrime. Adicionalmente, pode observar-se a relação entre o conhecimento informático e o medo do cibercrime. Quanto à primeira, verifica-se que não existem diferenças nos níveis de medo de cibercrime em função do número de horas que os indivíduos passam na *Internet* ($p\text{-value}=.217$). Quanto à segunda variável, os níveis de medo do cibercrime variam de acordo com as competências informáticas reportadas ($p=.000$). O teste *post-hoc* revela diferenças entre o medo do cibercrime em função das três categorias de conhecimento informático. Mais se adianta, que quem reportou ter um nível básico de conhecimento informático reporta maiores níveis de medo de vitimação *online* ($X=3,09$), enquanto quem reportou ter um nível alto de conhecimentos informáticos registou menores índices de medo de vitimação *online* ($X=2,72$).

2.4. Medo de cibercrime e medo *offline*, insegurança geral e percepção do risco de vitimação *online*

A tabela 13 apresenta a relação entre medo de cibercrime, percepção do risco de vitimação, insegurança geral e dois tipos de medo *offline* – interpessoal e propriedade.

Tabela 12 Correlações Pearson: correlações entre a variável dependente medo do cibercrime as variáveis percepção do risco de vitimação *online*, insegurança geral, medo *offline* interpessoal e medo *offline* propriedade.

Índices	Medo de cibercrime
Risco percebido <i>online</i>	.30**
Insegurança geral	.29**

Medo <i>offline</i> interpessoal	.57**
Medo <i>offline</i> propriedade	.57**

*A correlação é significativa ao nível 0.05 (2-tailed)

**A correlação é significativa ao nível 0.01 (2-tailed)

Em primeiro lugar, verifica-se que existe uma correlação positiva e moderada entre a percepção do risco de vitimação *online* e o medo do cibercrime ($r=.30$, $p\text{-value} < .001$). Assim, à medida que aumenta o risco percebido *online*, incrementam também os níveis de medo de vitimação *online*. Por sua vez, constata-se que a insegurança geral se correlaciona positivamente com o medo de cibercrime ($r=.29$), ou seja, maiores níveis de insegurança em andar sozinho(a) na zona de residência depois de escurecer, estão em linha com maiores níveis de medo de cibercrime. Também o medo *offline* interpessoal e o medo *offline* propriedade apresentam uma correlação positiva e elevada com o medo de cibercrime ($r=.57$, $p\text{-value} < .001$). Quer isto dizer que quanto mais medo *offline* para cada uma das duas componentes, mais medo os indivíduos da amostra sentem *online*.

2.5. Medo de cibercrime e experiência de vitimação *online*

A tabela 14 apresenta os resultados referentes à relação entre o medo do cibercrime e a experiência de vitimação *online*.

Tabela 13 Testes-t: medo de cibercrime em função da experiência de vitimação *online*.

Variável	Medo de Cibercrime		
	N	($\bar{X} \pm S.D$)	p
Experiência de Vitimação Online			
Não	286	2.98 $\pm$ 0.70	.117
Sim	440	2.90 $\pm$ 0.67	

Como é possível observar na tabela, não se verificam diferenças estatisticamente significativas nos níveis de medo do crime de acordo com a experiência de vitimação *online* ($p\text{-value}=.117$). Efetivamente, os níveis médios de medo de cibercrime são semelhantes entre vítimas ($\bar{X}=2,90$, $SD= .67$) e não vítimas por cibercrime ($\bar{X}=2,98$, $SD =.70$).

3. A relação entre vitimação *online* e as variáveis independentes

Seguem-se, agora, os resultados referentes à segunda variável dependente do estudo – a vitimação *online*. Numa primeira fase analisaremos a prevalência da vitimação de acordo com as variáveis sociodemográficas. Em seguida, analisaremos a influência das variáveis da TAR, nomeadamente a exposição *online*, alvo adequado e guardiões. Por fim, verificaremos como é que a vitimação *online* se relaciona com a percepção do risco de vitimação *online*.

3.1. Vitimação *online* e variáveis sociodemográficas

Nas tabelas 15 e 16 podem ser observados os resultados referentes à análise da vitimação e a sua relação com as variáveis sociodemográficas.

Tabela 14 Qui-quadrado: prevalência da vitimação *online* em função das variáveis género, estado civil, teletrabalho e zona de residência.

Variáveis	NV	V	X ²	p
Género				
Feminino	28.9%	41.8%	1.31	.252
Masculino	10.7%	18.7%		
Estado civil				
Solteiro	32.2%	47%	1.96	.161
Casado/em União de facto	7.2%	13.6%		
Teletrabalho				
Não	19.7%	31.3%	3.46	.063
Sim	13.3%	35.6%		
Zona de residência				
Rural	12.9%	19.3%	0.87	.768
Urbana	26.4%	41.3%		

Nota: os testes qui-quadrado apresentados são analisados à luz do modelo qui-quadrado de Pearson. NV=Não vítima; V=Vítima. A percentagem para a variável género foram realizadas para um total amostral de 723 (99.6% da amostra) e a variável teletrabalho para 233 (32.1% da amostra).

De acordo com a tabela 15, não se observam diferenças estatisticamente significativas para as variáveis na relação com a vitimação *online*. Constata-se, contudo, que existe um *p-value borderline* ($p=.063$) na associação entre teletrabalho e vitimação – sendo que, tendencialmente, os indivíduos que estão em teletrabalho são mais vítimas, embora não atinja a significância estatística.

Tabela 15 Testes-t: prevalência da vitimação *online* em função das variáveis idade, escolaridade, insegurança económica e perceção sobre os rendimentos do agregado familiar.

Variáveis	Amostra total	NV	V	t	p
	(X±S.D)	(X±S.D)	(X±S.D)		
Idade	27.47±11.78	26.29±11.20	28.23±12.09	-2.174	.030
Escolaridade	12.7±1.78	12.37±1.64	12.92±1.84	-4.233	.000
Insegurança económica	5.82±2.52	5.67±2.44	5.91±2.58	-1.290	.197
Rendimentos	2.78±0.875	2.86±0.84	2.73±0.90	2.016	.044

Focando agora a atenção para a tabela 16, pode observar-se um conjunto de diferenças estatisticamente significativas. Em primeiro lugar, a variável idade permite-nos aferir que as vítimas de cibercrime ($X=28,23$) são, em média, mais velhas do que as não vítimas ($X=26,29$,

p=.030). Quanto à escolaridade, constata-se que os indivíduos que já foram vítimas de cibercrime ($X=12,92$) reportam uma média de estudos maior do que as não vítimas ($X=12,37$, $p=.000$). Relativamente à percepção dos rendimentos do agregado familiar, verifica-se que no grupo dos vitimados ($X=2,73$) existe um nível mais baixo de rendimentos em comparação com o grupo dos não vitimados ($X=2,86$). Por fim, a insegurança económica não obteve diferenças estatisticamente significativas comparando vítimas e não vítimas.

3.2. Vitimação *online* em função do tipo de dispositivo informático e local de acesso à *Internet*

O anexo 6, agrupa as proporções das vítimas e não vítimas segundo o tipo de dispositivo informático utilizado e o local de acesso à *Internet*. Estas questões não apresentam diferenças estatisticamente significativas com a vitimação *online*.

3.3. Vitimação *online* e Teoria das Atividades de Rotina

As tabelas 17 e 18, apresentam as médias e desvios-padrões das vítimas e não vítimas segundo os pressupostos da TAR, nomeadamente a exposição *online*, o alvo adequado, a informação disponibilizada *online*, o guardião e os conhecimentos informáticos.

Tabela 16 Testes-t: prevalência de vitimação *online* em função da exposição *online*, alvo adequado, informação disponibilizada *online* e índice do guardião.

Componente	Descrição	Amostra	NV	V	t	p
		($X \pm S.D$)	($X \pm S.D$)	($X \pm S.D$)		
Exposição <i>online</i>	Económica	2.42±0.84	2.37±0.86	2.46±0.83	-1.538	.124
	Interativa	1.33±0.51	1.30±0.48	1.36±0.52	-1.701	.089
	Entretenimento	3.01±0.67	3.04±0.62	2.98±0.70	1.171	.242
Alvo adequado	Abrir ficheiros desconhecidos	1.13±0.36	1.11±0.30	1.15±0.39	-1.393	.164
	Comunicar ou fornecer dados a desconhecidos	1.34±0.50	1.23±0.38	1.40±0.56	-5.194	.000
	Uso de risco da <i>Internet</i>	1.26±0.43	1.21±0.38	1.29±0.45	-2.826	.005
	Informação disponibilizada <i>online</i>	4.10±2.36	3.95±2.30	4.19±2.39	-1.372	.171
Guardião	Índice do guardião	10.54±2.24	10.48±2.36	10.58±2.15	-0.571	.568

No que toca às variáveis advindas da TAR, observam-se apenas diferenças estatisticamente significativas nas variáveis referentes ao alvo adequado, nomeadamente ao índice comunicar ou fornecer dados a desconhecidos e uso de risco da *Internet*. Concretamente, os indivíduos que comunicam e/ou fornecem voluntariamente dados pessoais a desconhecidos reportam, em média ($X=1,40$), ser mais vezes vítimas do que não vítimas ($X=1,23$, $p=.000$).

Quanto aos indivíduos que clicam em mensagens pop-up e/ou acedem a *websites* duvidosos, estes são, em média ($X=1,29$) mais vezes vítimas do que não vítimas ($X=1,21$, $p=.005$).

Tabela 17 Prevalência da vitimação *online* em função da exposição *online* em horas e do conhecimento informático.

Variáveis	Descrição	NV	V	X ²	p
Exposição <i>online</i> em horas	Menos de 1 hora	0.8%	0.3%	9.547	.049
	Entre 1 a 2 horas	4%	6.1%		
	Entre 3 a 5 horas	12.5%	17.2%		
	Entre 6 a 9 horas	16%	23.4%		
	10 ou mais horas	6.1%	13.6%		
Conhecimento informático	Básico	11.2%	13.6%	5.555	.062
	Médio	24.1%	37.6%		
	Alto	4.1%	9.4%		

Nota: os testes qui-quadrado apresentados são analisados à luz do modelo qui-quadrado de Pearson.

A partir da tabela 18 verifica-se que o grupo que referiu utilizar a *Internet* entre 6 a 9 horas (23.4%) reportou ser mais vitimado do que o grupo que se expõe menos de 1 hora por dia *online*. A variável atinge significância estatística com a vitimação *online*, apesar da relação ser fraca (V de Cramer = .115, p -value = .049).

3.4. Vitimação *online* em função do medo *offline*, insegurança geral e percepção do risco de vitimação *online*

A Tabela 19 apresenta, por um lado, a relação entre a experiência de vitimação *online* e a percepção do risco de vitimação *online*, e por outro lado, a relação com a insegurança geral, o medo *offline* interpessoal e o medo *offline* propriedade.

Tabela 18 Testes-t: prevalência da vitimação *online* em função das variáveis percepção do risco de vitimação *online*, insegurança geral, medo *offline* interpessoal e medo *offline* propriedade.

	Amostra	NV	V	t	p
Risco percebido <i>online</i>	2.01±0.53	1.93±0.53	2.06±0.53	-3.138	.002
Insegurança geral	3.20±1.18	3.22±1.17	3.18±1.18	.391	.696
Medo <i>offline</i> interpessoal	3.35±1.29	3.42±1.26	3.30±1.30	1.302	.193
Medo <i>offline</i> propriedade	3.37±1.14	3.44±1.17	3.33±1.12	1.225	.221

De acordo com a tabela 19, constata-se que a percepção do risco de vitimação *online* apresenta diferenças estatisticamente significativas ($p=.002$) quando se compara vítimas e não vítimas. Efetivamente, as vítimas reportam em média maiores níveis da dimensão cognitiva do sentimento de insegurança ($X=2,06$, $SD = .53$) do que as não vítimas ($X=1,93$, $SD = .53$). No campo *offline*, a variável insegurança geral e os dois índices de medo *offline* (interpessoal e

propriedade) não tiveram diferenças estatisticamente significativas em função da vitimação *online*.

4. Variáveis preditoras do medo do cibercrime e da vitimação *online*

De forma a saber quais as variáveis independentes que melhor predizem as variáveis dependentes (medo do cibercrime e vitimação *online*) efetuar-se-ão 4 modelos de regressão linear para o medo do cibercrime e 3 modelos de regressão logística para a vitimação *online*. Atendendo à variável medo do cibercrime, far-se-ão regressões lineares cujos modelos subdividem-se em: Modelo 1) variáveis sociodemográficas, Modelo 2) Teoria das Atividades de Rotina, Modelo 3) insegurança económica, insegurança geral, medo *offline* interpessoal e propriedade, perceção do risco de vitimação *online*, vitimação *online* e em Modelo 4), um modelo que agrupa todas as variáveis independentes com poder preditivo, ou seja, com significado estatístico ($p < 0.05$). Relativamente à variável vitimação *online*, irão realizar-se modelos de regressão logística divididos em: Modelo 1) variáveis sociodemográficas, Modelo 2) Teoria das Atividades de Rotina e perceção do risco de vitimação *online*, e no Modelo 3) as variáveis que, nos modelos anteriores, atingiram significado estatístico com a vitimação *online*.

4.1. Variáveis preditoras do medo do cibercrime

Modelo 1 – Variáveis sociodemográficas e medo do cibercrime

Segundo o anexo 7, verifica-se que 18% da variância total no medo do cibercrime é explicada pelas variáveis independentes. O presente modelo é estatisticamente significativo ($p = .000$). Do conjunto das variáveis sociodemográficas presentes no modelo, apenas o género ($p = .000$) e a escolaridade ($p = .000$) afetam significativamente o medo do cibercrime.

Assim, as variáveis sociodemográficas género e o nível de escolaridade são as que mais contribuem para a explicação do medo do cibercrime. Ambas as variáveis entram negativamente na explicação desta variável dependente. Mais especificamente, quanto ao género, o valor de β foi de $-.515$, enquanto o nível de escolaridade o valor de β foi de $-.109$. Ou seja, as mulheres e os indivíduos com menor escolaridade, têm níveis mais altos de medo.

Modelo 2 – Teoria das Atividades de rotina e medo do cibercrime

A partir do segundo modelo das regressões lineares (Anexo 8), observa-se que 8.9% da variância total do medo do cibercrime é explicada pelas variáveis independentes relativas à TAR. Além disso, este modelo possui significado estatístico ($p = .000$). Existem cinco variáveis independentes que afetam significativamente na predição do medo do cibercrime: exposição entretenimento, índice do guardião, conhecimento informático (todas com $p\text{-value} = .000$), o

alvo adequado (abrir anexos desconhecidos, com $p\text{-value}=0.001$) e o total de informação disponibilizada *online* ($p=0.022$).

Assim, as variáveis relativas à TAR que mais contribuíram para a explicação do medo do cibercrime foram: a exposição entretenimento ($\beta=0.176$), o índice do guardião ($\beta=0.139$), o alvo adequado (abrir anexos desconhecidos, $\beta=0.123$) e a informação disponibilizada *online* ($\beta=0.092$). Todas elas entram de forma positiva na explicação do medo do cibercrime, ou seja, quanto maior a exposição de entretenimento, os guardiões adotados e a informação disponibilizada *online* pelos indivíduos, assim como quanto mais abrem anexos desconhecidos, maiores os níveis de medo do cibercrime. Por outro lado, o conhecimento informático ($\beta=-0.179$) entra de forma negativa na explicação da variável dependente, indivíduos com níveis mais elevados de conhecimento têm menos medo online.

Modelo 3 – Insegurança económica, insegurança geral, medo *offline* interpessoal e propriedade, risco percebido *online*, vitimação *online* e medo do cibercrime

A partir do Anexo 9, observa-se que 44.3% da variância total do medo do cibercrime é explicada pelas variáveis independentes. Além disso, este modelo tem significado estatístico ($p=0.000$). Das variáveis independentes a analisar, todas atingiram significância estatística à exceção da insegurança geral ($p=0.950$). Mais especificamente, observa-se que a insegurança económica ($\beta=0.146$), o medo *offline* interpessoal ($\beta=0.302$), o medo *offline* propriedade ($\beta=0.274$) e o risco percebido *online* ($\beta=0.201$) entram positivamente para a explicação do medo do cibercrime, enquanto a vitimação *online* ($\beta=-0.061$) entra de forma negativa para a explicação do medo do cibercrime. Assim, indivíduos que têm maiores níveis de insegurança económica, medo *offline* interpessoal e relativo à propriedade, e têm maior risco percebido *online*, têm maiores níveis de medo do cibercrime. Por outro lado, ser vítima de um cibercrime, tendencialmente, tem menos medo *online*.

Modelo 4 – Modelo final de explicação do medo do cibercrime

No último modelo, estima-se o efeito das variáveis independentes que atingiram significância estatística nos modelos anteriores no medo do cibercrime, nomeadamente o género, a escolaridade, a exposição *online* entretenimento, o alvo adequado abrir ficheiros desconhecidos, o total de informação disponibilizada *online*, o índice do guardião, o conhecimento informático, a insegurança económica, o medo *offline* interpessoal e propriedade, a perceção do risco *online* e a vitimação *online*. Na tabela 20, observa-se que o conjunto das variáveis explica 45.9% da variância total do medo do cibercrime ($p=0.000$). Verifica-se, ainda,

que as variáveis independentes género, exposição *online* entretenimento, informação disponibilizada *online* e vitimação *online* não têm significado estatístico ($p > .05$), pelo que deixam de ter poder preditivo no medo do cibercrime. Constata-se, contudo, que existe um *p-value borderline* na variável vitimação *online* ($p = .056$). Por outro lado, as variáveis independentes que atingiram significância estatística na predição do medo do cibercrime foram a escolaridade ($p = .045$), o alvo adequado (abrir ficheiros desconhecidos, $p = .020$), o índice do guardião ($p = .001$), o conhecimento informático ($p = .025$), a insegurança económica ($p = .000$), o medo *offline* interpessoal ($p = .000$), o medo *offline* propriedade ($p = .000$) e a perceção do risco de vitimação *online* ($p = .000$).

Tabela 19 Predição do medo do crime a partir das variáveis que nos modelos anteriores tiveram significado estatístico (género, escolaridade, exposição entretenimento, abrir ficheiros desconhecidos, informação disponibilizada, índice do guardião, conhecimento informático, insegurança económica, medo *offline* interpessoal e propriedade, perceção do risco de vitimação *online* e vitimação *online*).

Variável	B	SE B	β	t	P
Género	-.059	.051	-.039	-1.136	.256
Escolaridade	-.022	.011	-.058	-2.012	.045
Exposição entretenimento	.025	.032	.025	.802	.423
Alvo adequado (abrir ficheiros desconhecidos)	.125	.053	.065	2.336	.020
Informação disponibilizada online	.014	.009	.048	1.564	.118
Índice do guardião	.028	.009	.092	3.211	.001
Conhecimento informático	-.073	.032	-.064	-2.241	.025
Insegurança económica	.037	.008	.136	4.434	.000
Medo offline interpessoal	.130	.025	.244	5.277	.000
Medo offline propriedade	.170	.023	.282	7.230	.000
Risco percebido online	.244	.037	.190	6.644	.000
Vitimação online	-.075	.039	-.054	-1.915	.056

Nota. $r = .684$; $r^2 = .468$; r^2 ajustado = .459 ($p = .000$);

Efetivamente, a variável que mais contribui para a explicação do medo do cibercrime é o medo *offline* propriedade ($\beta = .282$), seguido do medo *offline* interpessoal ($\beta = .244$), perceção do risco *online* ($\beta = .190$), insegurança económica ($\beta = .136$), índice do guardião ($\beta = .092$), alvo adequado (abrir ficheiros desconhecidos, $\beta = .065$), conhecimento informático ($\beta = -.064$) e nível de escolaridade ($\beta = -.058$).

4.2. Variáveis preditoras da vitimação *online*

MODELO 1 – Variáveis sociodemográficas e vitimação *online*

Segundo o Anexo 10, verifica-se que 4.5% da variância total na vitimação *online* é explicada pelas variáveis independentes. O presente modelo é estatisticamente significativo

($p=.000$). Do conjunto das variáveis sociodemográficas presentes no modelo, apenas a escolaridade ($p=.000$) e a percepção sobre os rendimentos auferidos ($p=.011$) afetam significativamente a vitimação *online*.

Ao nível das variáveis sociodemográficas, a escolaridade e a percepção sobre os rendimentos são as variáveis que contribuem para a chance de ocorrer vitimação *online*. Relativamente à variável escolaridade, os resultados indicam que quanto maior o nível de escolaridade, maior a chance de vitimação *online* ($OR=1.212$; $p\text{-value}=.000$). Por outro lado, é possível verificar que os rendimentos predizem negativamente a vitimação. Ou seja, os indivíduos que têm maiores rendimentos são menos propensos a serem vítimas de cibercrime ($OR=.793$, $p\text{-value}=.011$).

Modelo 2 – Teoria das Atividades de Rotina, risco percebido *online* e vitimação *online*

A partir do Anexo 11, verifica-se que 9.7% da variância total da vitimação *online* ocorrer é explicada pelas variáveis independentes, sendo este modelo estatisticamente significativo ($p=.000$). Do conjunto das variáveis independentes analisadas, somente três predizem significativamente a chance de vitimação *online*: exposição entretenimento ($p=.003$), comunicar ou fornecer dados a desconhecidos, $p=.000$) e o risco percebido *online* ($p=.003$).

Quanto ao alvo adequado, verifica-se que comunicar ou fornecer dados a desconhecidos mais vezes, aumenta a chance de ocorrer vitimação *online* ($OR= 2.356$, $p\text{-value}=.000$). Ao mesmo tempo, os indivíduos que percebem maiores níveis de risco de vitimação *online* têm 1.6 vezes maiores chances de serem vítimas *online*. Por outro lado, verifica-se que quanto maior é a exposição entretenimento, menor é a chance de ocorrer vitimação *online* ($OR=.675$, $p\text{-value}=.003$).

Modelo 3 – Modelo final de explicação do vitimação *online*

No último modelo agrupam-se as variáveis independentes que atingiram significância estatística nos modelos anteriores, nomeadamente o nível de escolaridade, a percepção sobre os rendimentos auferidos pelo agregado familiar, a exposição entretenimento, o alvo adequado comunicar ou fornecer dados a desconhecidos e a percepção do risco de vitimação *online*. Estas variáveis explicam 10.6% da variância na variável dependente vitimação *online*. Além disso, verifica-se que este modelo final alcançou significância estatística ($p=.000$). Analisando os valores apresentados na tabela 21, observa-se que as variáveis independentes escolaridade ($p=.000$), rendimentos ($p=.036$), comunicar ou fornecer dados a desconhecidos ($p=.000$) e risco

percebido *online* ($p=.007$) atingem significado estatístico na predição da vitimação *online*. Por outro lado, a exposição *online* entretenimento não atingiu significância estatística ($p>.05$).

Tabela 20 Predição da chance de vitimação *online* a partir das variáveis que nos modelos anteriores tiveram significado estatístico, nomeadamente a escolaridade, os rendimentos, a exposição entretenimento, o alvo adequado comunicar ou fornecer dados a desconhecidos e a percepção do risco de vitimação *online*.

Variáveis	B	SE B	Wald	OR	P
Escolaridade	.193	.051	14.471	1.212	.000
Rendimentos	-.195	.093	4.391	.823	.036
Exposição entretenimento	-.215	.126	2.906	.807	.088
Alvo adequado (comunicar ou fornecer dados a desconhecidos)	.920	.189	23.709	2.510	.000
Risco percebido online	.419	.154	7.388	1.520	.007

Nota. -2 Log likelihood=914.283; Nagelkerke R²=.106 ($p=.000$)

Assim, verifica-se que os indivíduos que comunicam ou fornecem dados a desconhecidos têm uma chance 2,510 superior de sofrerem vitimação *online*. O mesmo se sucede para maiores níveis do risco percebido *online*, aumentando em 1,520 vezes a chance de ocorrer vitimação *online*. Ao mesmo tempo, quem possui níveis superiores de escolaridade apresenta uma chance de 1,212 de sofrer vitimação *online*. Relativamente à percepção sobre os rendimentos auferidos, verifica-se que indivíduos com níveis mais elevados de rendimentos têm uma chance menor de sofrerem vitimação ($OR=.823$, $p\text{-value}=.036$).

DISCUSSÃO DOS RESULTADOS

A presente dissertação procurou relacionar um conjunto de fatores sociodemográficos e contextuais com duas variáveis dependentes: por um lado, o medo do cibercrime, e, por outro, a vitimação por cibercrime. A partir da Teoria das Atividades de Rotina (Cohen & Felson, 1979), mediu-se a exposição *online*, a atratividade do alvo e se estes adotam comportamentos de segurança (guardiões). Paralelamente, analisou-se as dimensões do sentimento de insegurança no ciberespaço: medo do crime, percepção do risco de vitimação e comportamentos de segurança. Complementarmente, e a título exploratório, procurou-se perceber a importância de atividades *online* específicas com as componentes propriedade e interpessoal do medo/vitimação *online*, assim como relações com as medidas de medo *offline* específicas. Com estes objetivos em consideração, foi aplicado um questionário *online* a uma amostra de 726 indivíduos. Apresentam-se, de seguida, a discussão das hipóteses levantadas, e em que medida estão em conformidade ou não com a literatura, indicando-se algumas sugestões

para os resultados inesperados encontrados. Por fim, apontamos as limitações do estudo e sugestões para futuras investigações.

a) Medo do cibercrime

Aquando da análise dos resultados, confirmou-se, em parte, a primeira hipótese: “o gênero, a idade, os níveis de escolaridade e a percepção sobre os rendimentos auferidos influenciam os níveis de medo do cibercrime”. Primeiramente, no que toca ao gênero, verificou-se que as mulheres apresentam maiores níveis de medo de cibercrime do que os homens. Este resultado vai de encontro com a literatura sobre o medo tradicional, identificando o gênero como o preditor mais forte do medo do crime (Ferraro, 1996; Hale, 1996) e também quando aplicado ao medo do crime no ciberespaço, de acordo com o estudo de Virtanen (2017). Outros estudos empíricos (e.g., Warr, 1984; Ferraro 1996), têm mostrado que, apesar de as mulheres reportarem maiores níveis de medo do crime, o seu risco objetivo de vitimação é menor que nos homens – o chamado paradoxo medo-vitimação. Neste estudo, o gênero não foi estatisticamente significativo na relação com a vitimação *online*, pelo que não podemos concluir a existência deste paradoxo. Por sua vez, verificou-se que a variável idade tem uma relação negativa com o medo do cibercrime, ou seja, os indivíduos mais novos reportam maiores níveis de medo do cibercrime. Este resultado corrobora os resultados do estudo de Virtanen (2017), mas não os de Yu (2014) para diferentes tipos de vitimação *online*. No que respeita aos anos de escolaridade, a relação encontrada foi também ela negativa com o medo do cibercrime, isto é, os indivíduos que reportaram níveis mais baixos de escolaridade, reportaram maiores índices de medo *online*. Contrariamente, o estudo de Alshalan (2006) não encontrou associações entre a educação e o medo do cibercrime. Finalmente, quanto à percepção sobre os rendimentos do agregado familiar, a sua relação com o medo do cibercrime não atingiu significância estatística. O estudo de Alshalan (2006) também não encontrou associações entre os rendimentos e o medo do cibercrime. Porventura, no contexto *online* fará mais sentido analisar os rendimentos que uma pessoa possui e o eventual medo de cibercrimes financeiros (e.g., Brands & Van Wilsem, 2019). Deste conjunto de variáveis atrás enumeradas, somente os anos de escolaridade foram significativos no modelo final de regressão linear para o medo do cibercrime.

Relativamente à segunda hipótese – “quanto mais uma pessoa se expõe *online*, maior o medo do cibercrime”, verificaram-se os seguintes resultados. Quanto à variável exposição *online* em horas, refuta-se a hipótese descrita, visto que não se encontraram diferenças

estatisticamente significativas. No que respeita à exposição *online* em atividades, a exposição entretenimento apresentou uma correlação positiva com o medo do cibercrime, ou seja, quanto mais um utilizador utiliza as redes sociais, faz *download* de músicas, filmes, jogos ou *podcasts* e visualiza conteúdo de entretenimento, maiores os níveis de medo de vitimação *online*, contudo, a relação é fraca ($r=.17$). O estudo de Virtanen (2017) encontrou associações significativas entre a frequência do uso de *Internet* e o medo do cibercrime, nos modelos com interações entre a vitimação e baixa confiança em usar a *Internet*. Curiosamente, tanto a exposição económica, como a exposição interativa, apesar de não influenciarem o medo do cibercrime, apresentam uma tendência negativa com o mesmo. Possivelmente, os indivíduos ao não anteciparem medo no contexto *online*, expõem-se com maior facilidade. No modelo final de regressão linear do medo do cibercrime, a exposição entretenimento não foi significativa.

Como vimos, parece que atividades específicas online podem-nos tornar mais receosos. Efetivamente, os estudos têm demonstrado a importância de utilizar as atividades de rotina *online* de forma especificada (e.g., Yu, 2014). Contudo, esta abordagem particularizada das atividades deve ser analisada, igualmente, com tipologias específicas de medo de crimes, isto porque, sem elas, os resultados podem sugerir efeitos de sombreamento – “*shadowing effects*” –, não permitindo saber quais crimes realmente são temidos (Ferraro, 1996). Segundo Yu (2014), resultados positivos que atendam a estes critérios de especificidade sugerem que o medo de determinados cibercrimes pode ter a ver com diferentes hábitos *online*. Assim, para delimitar melhores resultados, torna-se essencial ser também específico aos tipos de medo de cibercrimes, dando seguimento às recomendações que a literatura tem vindo a impor nesta temática. Conforme o Anexo 14, para a componente propriedade do medo de vitimação *online*, a única variável de exposição *online* que teve influência foi a exposição entretenimento, apontando uma relação positiva, ainda que fraca ($r=.127$). Contrariamente ao que seria de esperar para este tipo de medo, a exposição económica não obteve resultados estatisticamente significativos. Por sua vez, relativamente à componente interpessoal do medo de vitimação *online*, verificou-se que a exposição económica ($r= -.073$) e a exposição entretenimento ($r= .160$) influenciam a resposta emotiva ao cibercrime interpessoal, de formas opostas: maiores níveis de exposição económica estão associados com menores índices de medo desta tipologia, enquanto maiores níveis de exposição entretenimento apresentam relação com maiores níveis de medo interpessoal. Em suma, verifica-se que a exposição entretenimento foi influente no medo do cibercrime geral e nas componentes propriedade e interpessoal.

A terceira hipótese supôs o seguinte: “quanto maior a frequência de atividades de risco e o tipo de informação publicada *online*, maior o medo do cibercrime”. Os resultados evidenciaram uma correlação positiva entre “abrir ficheiros desconhecidos” e o medo do cibercrime ($r=.10$), ou seja, os indivíduos que reportam abrir ficheiros desconhecidos exibem níveis mais elevados de medo do cibercrime. Comunicar ou fornecer dados a desconhecidos e o uso de risco na *Internet* não atingiram resultados estatisticamente significativos. Porventura, os respondentes podem ter procurado respostas socialmente aceitáveis quanto ao facto de não comunicar ou fornecer dados a desconhecidos *online*. Por outro lado, podem não ter entendido o significado de páginas *pop-up*. Quanto à variável total de informação disponibilizada *online*, os resultados apresentam uma correlação positiva com o medo do cibercrime, ou seja, quanto mais informação é publicada *online*, maiores são os níveis de medo de cibercrime sentidos, porém a relação é fraca ($r=.10$). Quanto a este resultado, uma vez que são pessoas que arriscam mais, será que elas têm mais medo porque, ao colocarem mais informação *online* se sentem um alvo? Em estudos transversais (*Cross-sectional*) torna-se difícil ver a direção, contudo estudos longitudinais podem permitir confirmar este resultado. Relativamente ao modelo final de regressão linear do medo do cibercrime, somente abrir ficheiros desconhecidos foi significativo.

A quarta questão que este estudo procurou responder foi, se, “quanto maior o conhecimento informático e os comportamentos e ferramentas de segurança (guardiões), menor o medo do cibercrime”. No que respeita à variável “conhecimentos informáticos”, verificou-se que os indivíduos que reportaram ter um nível básico de conhecimento informático, reportaram maiores níveis de medo de vitimação *online*, em comparação com os indivíduos que reportaram ter um nível médio ou alto de conhecimentos informáticos. O estudo de Virtanen (2017) também encontrou relações negativas. O facto de as pessoas se sentirem mais capazes por terem competências técnicas faz com que sintam um maior controlo em possíveis situações de perigo. Por outro lado, quanto aos comportamentos e ferramentas de segurança (guardiões), os resultados sugerem que níveis mais elevados de medo do cibercrime, estão associados a uma maior adoção de comportamentos de segurança, apesar da relação ser fraca ($r=.09$). Este segundo resultado, apesar de refutar a segunda parte da hipótese levantada, vai de encontro com estudos do medo tradicional. Com efeito, a literatura defende que os comportamentos restritivos são usualmente realizados devido ao medo do crime (e.g. Liska *et al.*, 1988), ou seja, os indivíduos ao antecipar o medo ou a senti-lo, usualmente, adotam comportamentos de segurança. Ou seja, a relação positiva encontrada pode sugerir que os indivíduos adotam aqueles comportamentos de segurança porque, precisamente, têm geralmente mais medo.

Novamente, como referido atrás, as correlações não permitem estabelecer uma direção ou causalidade entre variáveis. No modelo final de regressão linear do medo do cibercrime, ambas as variáveis foram estatisticamente significativas.

Quando analisada a relação entre o medo sentido no contexto *offline* e o medo no ciberespaço, este estudo procurou responder à hipótese: “quanto maior forem os níveis de insegurança geral, o medo interpessoal *offline* e o medo relativo à propriedade *offline*, maior serão também os níveis de medo do cibercrime”. Esta hipótese foi confirmada na integridade. Tanto a insegurança geral, como as componentes específicas do medo *offline* correlacionaram-se positivamente com o medo do cibercrime. Estes resultados vão de encontro com a componente generalizada de medo do estudo de Roberts *et al.*, (2013), que aborda medidas interpessoais e financeiras *offline*. Em suma, estes resultados podem ser explicados pelo facto dos indivíduos que responderam ter medo *offline*, transporem a emoção para o ambiente *online* e a possibilidade de este ser um fator disposicional generalizado e não um fator dependente do risco (Roberts *et al.*, 2013). Resultados idênticos podem ser retirados deste estudo, visto que, no modelo final de regressão linear, o medo *offline* interpessoal e o medo *offline* relativo à propriedade foram as variáveis que mais contribuíram para a explicação do medo do cibercrime, enquanto nenhum tipo de exposição *online* foi significativo. O estudo de Guedes *et al.* (2018) observaram relações entre o medo disposicional de várias situações e medo do crime específico, o que demonstra que ter medo do crime em geral *offline* pode também transpor-se para o ciberespaço.

Não obstante os resultados apresentados, parece-nos importante analisar as especificidades do medo *offline* com as especificidades do medo *online*. Para a componente de medo de crimes contra a propriedade verifica-se que ter medo *offline* relativo à propriedade, apresenta uma correlação positiva com o medo relativo à propriedade *online* ($r=.483$). Para o medo interpessoal *online*, verifica-se a mesma tendência perante a influência do medo *offline* respetivo. A falta de interação física e outros fatores como o anonimato no contexto *online*, resulta em níveis mais baixos de medo interpessoal e propriedade *online* em comparação com os medos respetivos *offline*. No caso da componente interpessoal, como suprarreferido, as relações foram mais fortes. Controlando para variável género (ver Anexo 18), o medo *offline* interpessoal reportado pelas mulheres registou os valores mais altos de todas as componentes de medo do estudo, indo de encontro com a hipótese *shadow of sexual assault* (Warr, 1984; Ferraro 1995, 1996). Contudo, extrapolar esta justificação para o ciberespaço deve ser realizada

de forma cuidada. Até que ponto o medo de crimes interpessoais, nomeadamente de natureza sexual, afeta o medo de crimes *online* onde não existe uma interação física direta? Será que as mulheres ao imaginarem serem vítimas desta criminalidade, antecipam a probabilidade de o crime *online* atingir repercussões mais graves que possam depois ser transportadas para o contexto físico?

Por sua vez, a hipótese: “o risco percebido de vitimação *online* está positivamente correlacionado com o medo do cibercrime” foi confirmada. Efetivamente, observa-se que a dimensão cognitiva (*online*) do sentimento de insegurança tem influência no medo de vitimação *online* ($r=.30$). Este resultado vai ao encontro da literatura tradicional quanto à dependência de ambas as variáveis (e.g., Ferraro, 1995; Jackson, 2004; Mesch, 2000; Smith & Torstensson, 1997). Contudo, a literatura também tem avançado que as duas dimensões são podem ser confundidas, até porque são explicadas por diferentes preditores (e.g., Guedes *et al.*, 2018; Farrall *et al.*, 2009).

Relativamente à hipótese “a experiência de vitimação *online* relaciona-se com o medo de vitimação *online*”, a literatura tem apresentado resultados mistos (e.g., Yu, 2014; Brands & Van Wilsen, 2019). Este estudo não encontrou resultados estatisticamente significativos que permitam dizer qual grupo – vitimados ou não vitimados – reporta mais ou menos medo do cibercrime. Já na literatura tradicional relativa ao medo *offline* se têm observado resultados mistos quando aquele é relacionado com a vitimação (Hale, 1996). Contudo, cabe ressaltar que os resultados encontrados na presente dissertação podem ser explicados pelo uso de medidas agregadas do medo do cibercrime, na medida em que, os indivíduos podem ter medo de um crime específico, mas a medida agregada não permite identificá-lo (Ferraro, 1996). Outros estudos verificam que a medição da vitimação *online* deve também ser específica (Yu, 2014). A título exploratório, utilizámos medidas específicas – uma componente propriedade e uma componente interpessoal – ainda que agregadas por dois tipos de cibercrimes, de vitimação/medo *online* (Anexo 12). Os resultados obtidos não encontraram influência entre a vitimação propriedade *online* e o medo propriedade *online*, apesar da tendência de serem as vítimas dessa tipologia a reportarem mais medo relativo à propriedade *online*. Por sua vez, também a vitimação interpessoal não foi significativa com o medo interpessoal *online*. Curiosamente, estes resultados foram também encontrados no estudo de Henson *et al.* (2013): a vitimação interpessoal *online* ao longo da vida não foi preditor do medo de vitimação interpessoal *online*. Segundo o autor, uma possível explicação advém do facto dos indivíduos não levarem a vitimação *online* de forma séria. Relativamente à componente financeira, no

estudo de Brands & Van Wilsem (2019), todas as vitimações analisadas tiveram maiores níveis de medo de cibercrimes financeiros *online*. Apesar de, neste estudo, não terem sido encontrados resultados estatisticamente significativos para a componente propriedade, algumas semelhanças podem ser paralelamente confirmadas: analisando vitimações específicas, verificou-se que as vítimas de crimes relativos à propriedade *online* (furto de identidade; fraude ao consumidor) reportaram mais medo propriedade *online* do que medo interpessoal *online* ou medo geral *online*. O mesmo verificou-se para as vítimas interpessoal (ciberbullying; *cyberstalking*). Porventura, as componente propriedade e interpessoal da vitimação/medo *online*, apesar de específicas, continuam a encobrir qual a tipologia de cibercrime que as vítimas efetivamente receiam. Além disso, à exceção do medo interpessoal *online*, a consistência interna foi baixa para o medo relativo à propriedade *online* e ambas as componentes de vitimações *online*.

b) Vitimação *online*

A primeira hipótese relacionada com a vitimação procurou saber, se “o gênero, a idade, o nível de escolaridade e a percepção sobre os rendimentos auferidos influenciam a probabilidade de ocorrer vitimação *online*”, tendo-se observando que a hipótese não se confirma na integridade. Em primeiro lugar, como já tinha sido referido, a variável gênero não foi significativa na relação com a vitimação *online*. A relação entre gênero e vitimação tem sido mista: em alguns estudos, os homens foram mais vítimas (e.g. Alshalan, 2006, Holt & Turner, 2012); Reyns, 2013). Quanto à idade, os mais velhos reportaram ser mais vítimas que os mais novos. Este resultado vai contra o estudo de Ngo & Paternoster (2011), onde ser os indivíduos mais velhos tinham menor probabilidade de ser vítimas de cibercrime. Perante o nível de escolaridade, este estudo mostra uma associação entre níveis mais altos de escolaridade e vitimação *online*. Bunes et al. 2020 também encontrou isto para furto de identidade. Por fim, também a variável rendimentos influencia a vitimação *online*, na medida em que os vitimados percecionam ter rendimentos mais baixos. Os indivíduos com menores rendimentos podem ter menos possibilidades de se equiparem melhor para evitarem ser vítimas. No modelo final de regressão logística, os anos de escolaridade e os rendimentos foram significativos na explicação da vitimação *online*.

Relativamente à exposição *online*, colocou-se a seguinte hipótese: “quanto mais uma pessoa se expõe *online*, maior a probabilidade de ocorrer vitimação *online*”. Os resultados mostram que a exposição *online* em horas exerce influência na probabilidade de ocorrer vitimação *online*,

ou seja, os indivíduos passam mais tempo *online* por dia, reportaram ser mais vezes vítimas de cibercrime. Contudo, no modelo final de explicação da vitimação *online*, a exposição *online* em horas deixou de ser influente. No que toca à exposição *online* em atividades, e em contraste com o que seria de esperar, não se encontraram resultados estatisticamente significativos com a vitimação *online*. Como tem vindo a ser referido, o facto de se incluir uma medida agregada de vitimação *online*, pode encobrir determinados resultados, não permitindo saber, mediante as diferentes tipologias de cibercrime, quais atividades *online* realmente as afetam (Bossler & Holt (2010). Além disso, os índices de exposição *online* e a vitimação *online* apresentam baixos valores de consistência interna, surgindo necessidade de utilizar medidas ainda mais específicas. Uma vez mais, torna-se pertinente estudar as atividades de rotina *online* com tipos mais específicos de cibercrime, ainda que agregados. Nesta análise secundária, a exposição económica teve influência na vitimação *online* propriedade. Por sua vez, a exposição interativa e a exposição entretenimento também se relacionam com a vitimação interpessoal *online*, assim como a exposição *online* em horas. Em suma, estes resultados permitem aferir que participar em atividades específicas é importante para perceber a vitimação *online* (Ngo & Paternoster, 2011).

A hipótese: “quanto maior a frequência de atividades de risco e o tipo de informação publicada *online*, maior a probabilidade de vitimação *online*”, foi parcialmente corroborada. Confirmou-se que “comunicar ou fornecer dados a desconhecidos” e o “uso de risco da *Internet*” influenciam a probabilidade de ocorrer vitimação *online*. Por um lado, quem comunica e/ou fornece voluntariamente os seus dados pessoais a desconhecidos tem maior probabilidade de vitimação, foi alcançado também no estudo de Alshalan (2006) e Marcum *et al.* (2010). Relativamente a quem clica em mensagens pop-up e/ou acede a *websites* duvidosos, existe também maior probabilidade de vitimação por cibercrime. No modelo final de regressão logística, somente comunicar ou fornecer dados a desconhecidos foi significativo na estimação da vitimação *online*. Por outro lado, apesar de as vítimas terem referido que disponibilizavam mais informação *online*, não se encontraram diferenças estatisticamente significativas que permitam concluir que esta variável é importante na probabilidade de ocorrer vitimação *online*. Resultados idênticos também se verificaram no estudo de Reyns *et al.* (2011) perante cinco comportamentos de perseguição (contacto indesejado, assédio, avanços sexuais, ameaças de violência e uma medida geral de *cyberstalking*). Uma possível explicação para este resultado pode atender à operacionalização da medida: por ser extensa, os inquiridos podem não ter respondido em conformidade com a realidade ou não ter levado a sério a pergunta. Outra

possível explicação deve-se à ordem com que foi apresentada “nas redes sociais ou na *Internet* em geral”. Quiçá, as respostas foram pensadas e enquadradas com as informações postadas nas redes sociais e neste ambiente as vitimações analisadas neste estudo podem não ser tão frequentes. Além disso, as informações perguntadas incidem mais sobre questões pessoais e não tanto económicas (efetivamente, os estudos de Marcum *et al.*, 2010 e Reyns *et al.*, 2011 visaram a vitimação *online*, contudo, os cibercrimes analisados tinham uma componente mais interpessoal), e a medida de vitimação *online* engloba ambos os tipos de vitimação. Pode ser que os cibercrimes interpessoais sejam mais facilmente enquadrados nas redes sociais do que os outros.

Relativamente à hipótese “quanto maior o conhecimento informático e os comportamentos e ferramentas de segurança, menor a probabilidade de vitimação *online*”, não se confirma a afirmação. Quem respondeu ter um nível de conhecimento informático elevado reportou ser menos vítima, contudo não se encontram diferenças estatisticamente significativas entre os três níveis de conhecimento informático. Também os estudos de Bossler & Holt (2009) e Ngo & Paternoster (2011) não encontraram relações para esta variável. Uma possível explicação deste resultado deve-se ao uso de uma medida de perceção sobre os conhecimentos informáticos. Porventura, o nível de conhecimento que uma pessoa perceciona ter é mais baixo do que pensa quando comparado com o conhecimento geral dos indivíduos, ou através de determinados critérios: por exemplo, Rogers (2001) utiliza uma medida que aborda quatro afirmações mais exemplificativas e específicas das realidades tecnológicas, contudo, não só é esta medida desatualizada, como se torna difícil saber delimitar quais questões podem medir realmente o que se pretende medir no ciberespaço, de modo a agregar os resultados ao conhecimento que uma pessoa possui sobre ele. Outro aspeto importante concerne ao tipo de vitimação em causa. A título de exemplo, entender os contornos de determinadas vitimações *online*, como por exemplo, encontrar *malware* no dispositivo informático pessoal e tomar as ações necessárias para a sua eliminação, exige conhecimentos informáticos mais elevados do que outros tipos de vitimação *online*. Por outro lado, adotar mais comportamentos de segurança também não tem influência na probabilidade de ocorrer vitimação.

Finalmente, a hipótese: “o risco percebido de vitimação *online* relaciona-se com a vitimação *online*”, é confirmada pelos resultados. Assim, verifica-se que a vitimação *online* é influenciada por maiores níveis de risco percebido *online*. Esta variável está também incluída no modelo final que explica a vitimação *online*. Estudos futuros devem estudar melhor esta relação.

Limitações e sugestões para investigações futuras:

Não obstante os contributos do presente trabalho, e em complemento aos estudos empíricos que aplicaram a TAR ao ciberespaço, este estudo é mais um exemplo dos proveitos académicos que podem ser colhidos da sua transposição, contudo é necessário debruçar melhor sobre a operacionalização de alguns conceitos. Por exemplo, alguns dos guardiões utilizados, nomeadamente os comportamentos de evitamento, retratavam realidades já medidas na exposição *online* em atividades, pelo que poderá ser adequado, procurar utilizar medidas divergentes para cada uma das dimensões da TAR. Ainda assim, não se deixa de salientar resultados positivos da sua mutualidade. Por exemplo, nas questões sobre os tipos de informação publicada *online*, não é possível identificar, nos casos em que não se assinala uma resposta, se se trata de um comportamento de segurança de evitamento, ou simplesmente o utilizador não publica porque não tem interesse. Questionando, precisamente, se evita publicar determinada informação *online*, já o permite.

Por outro lado, outros conceitos, como o acrónimo VIVA, também limitam a utilidade da teoria (Yar, 2005). Relativamente ao “valor”, Leukfeldt & Yar (2016) referem, por exemplo, que é possível atribuir valor financeiro ao alvo mediante algumas características deste (e.g., rendimentos). Investigações futuras devem analisar determinados valores específicos com vitimações específicas semelhantes. Será que as características económico-financeiras de um indivíduo aumentam a probabilidade de vitimação financeira? Não obstante as sugestões, estudar o valor atribuído pelo ofensor visa, fundamentalmente, o seu ponto de vista, algo que ultrapassa os objetivos do presente estudo. Em segundo lugar, quanto à “inércia”, o conceito tem difícil aplicabilidade *online*. Não obstante as propriedades inerciais (e.g., tamanho dos ficheiros) que foram identificadas para o alvo “informação digital” no estudo de Yar (2005), que propriedades podemos assumir quando o alvo é o próprio indivíduo, e está em causa um crime de difamação na *Internet*? De que modo se aplicam as propriedades inerciais tecnológicas que o estudo de Yar aborda?

Outro problema que evidenciamos, surge mediante algumas medidas da exposição *online* utilizadas, serem datadas de estudos com 10 anos. Por exemplo, não há um critério definido que invalide a possibilidade de, ao invés de medir o índice “comunicar ou fornecer dados a desconhecidos” para a atratividade do alvo, não o fazer enquanto comportamento de segurança (i.e., “evita comunicar/fornecer dados pessoais a desconhecidos *online*”).

Outro aspeto prende-se com as medidas de medo/vitimação *online* agregadas utilizadas. Ferraro & La Grange (1987) sugerem examinar tipos de crime específicos. Contudo, tendo em conta os procedimentos de recolha de dados e a sua análise, não se trata de uma prática ideal

(idem). Leukfeldt & Yar (2016) expõem o mesmo problema: formular hipóteses por cada tipo de ofensa é um processo difícil. Apesar disso, de forma exploratória, juntámos os dois tipos de fraude *online* (a fraude ao consumidor *online* e o furto de identidade *online*) para criar uma componente propriedade, e dois cibercrimes interpessoais (*cyberstalking* e *ciberbullying*) para criar uma componente interpessoal. O mesmo foi feito para o medo *online*, com os mesmos crimes. A partir daqui, levantaram-se algumas hipóteses exploratórias, nomeadamente: a associação entre os medos *online* individualizados e a exposição *online* em atividades, o medo *offline* relativo à propriedade e o interpessoal, assim como a relação com as duas componentes da vitimação *online*. Por sua vez, procurou-se, também, analisar a relação entre as vitimações *online* individualizadas e a exposição *online* em atividades. O objetivo foi analisar relações congruentes entre as componentes: medidas relativas à propriedade com propriedade e medidas interpessoais com interpessoal. Positivamente, os índices de medo *offline* influenciaram as medidas de medo *online* idênticas. O mesmo aconteceu com as componentes da exposição *online* e as vitimações *online* análogas. Uma possível explicação para os fracos resultados encontrados pode surgir do facto de estas medidas não cumprirem os requisitos de fiabilidade, ou seja, os itens nela incluídos podem não refletir exatamente o construto que visam medir (ver Anexo 12). Por exemplo, a vitimação interpessoal obteve taxas de vitimação relativamente próximas entre *ciberbullying* e *cyberstalking* (10,7% e 9,4% respetivamente), situação que pode ser explicada pelo facto dos crimes não serem diferenciadores o suficiente (Pereira & Matos, 2015). Estudos futuros devem fazer uma melhor delimitação das tipologias de medo/vitimação *online* que pretendem estudar, e utilizar as variáveis constituintes da TAR no mesmo sentido.

Mais atenção deve ser facultada quanto às respostas que envolvem a perceção sobre certas características individuais. Por exemplo, quando se pergunta sobre a perceção dos rendimentos auferidos, não é possível identificar se no momento em que responderam ao questionário, a perceção era igual à do momento da vitimação *online*. Outro exemplo advém da perceção sobre o nível de conhecimento informático, discutido anteriormente. Por outro lado, outras características individuais, como a idade, devem ser cuidadosamente analisadas na associação com determinadas atividades, como o *ciberbullying*. As amostras analisadas nos estudos que envolvem este tipo de atividades têm, frequentemente, uma idade máxima de 18 anos, enquanto as restantes tipologias de vitimação não têm esse limite, impossibilitando generalizar resultados de um índice geral de medo/vitimação.

Relativamente aos comportamentos de segurança e o medo *online*, será possível que existam, previamente ao medo, comportamentos de segurança *online*, através de aprendizagens

em cursos ou formações sobre o conhecimento e correto uso das TIC? Ou seja, tratar-se-ia de um meio de proteção, e não uma consequência direta do medo. Esta questão permitiria saber se existem efeitos recíprocos entre os comportamentos adotados e o medo. O estudo de Ngo & Paternoster (2011) mediu a participação em *workshops* e se visitavam *websites* com vista à educação sobre os perigos *online*, contudo, os resultados foram contra o esperado, pelo que sugeriram utilizá-la como atividade de rotina. No presente estudo, não é possível analisar efeitos de reciprocidade entre os comportamentos adotados e o medo sentido, nem saber se estes comportamentos existem previamente a algum tipo de vitimação, porém, pesquisas futuras podem procurar analisar estas relações. Todavia, tal procedimento não se afigura fácil. Porventura, o medo está sempre presente e é sempre antecipado.

Este estudo permitiu também analisar o tipo de dispositivo informático mais utilizado, e o local de acesso à *Internet*. Relativamente ao tipo de dispositivo, 90.6% da amostra referiu utilizar um *smartphone* para aceder à *Internet*. Com a expansão e acessibilidade de *smartphones* no mercado, serão estes dispositivos mais ou menos seguros para navegar na *Internet*? Quão seguros se sentem os utilizadores de *smartphones* comparativamente com utilizadores de computadores? Por exemplo, 12.4% da amostra reportou ter descoberto *software* malicioso num dispositivo. Será que todos os dispositivos informáticos capazes de aceder à *Internet* efetuam análises de segurança frequentes? Ou, o facto de não existir *software* de segurança nesses dispositivos, ou ele ser gratuito, impede esta proteção extra. Por outro lado, no que toca ao local de acesso à *Internet*, 5.8% dos indivíduos responderam conectar-se à *Internet* através de uma rede WI-FI pública. Isto pode implicar que determinadas atividades *online* (e.g. aceder ao homebanking através de uma rede WI-FI pública, utilizar passwords ou associar cartões de crédito) não sejam seguras, expondo a informação e a vítima a ofensores motivados que se conectem à mesma rede (Reyns, 2013). Com outro sentido, Marcum *et al.* (2010) referem que o local onde os adolescentes acedem à *Internet* pode, em conjunto com a presença e os conhecimentos tecnológicos dos pais, ser considerado um guardião. Devem ser realizadas análises mais aprofundadas para saber se estes fatores contextuais incrementam a exposição ao risco. Estas sugestões podem ser analisadas ao nível do medo, mas também da vitimação *online*, todavia, deve-se ter em conta a tipologia da vitimação incorporada. Por exemplo, no caso de atividades ilícitas dentro da mesma rede pública, é provável que estas surtam mais efeito para tipologias específicas de crime, como o *hacking* ou a difusão de *malware*, e não tanto para crimes interpessoais.

Outro aspeto prende-se com o tipo de informação publicada nas redes sociais e na *Internet* em geral. Esta é, essencialmente, informação pessoal. Será que os indivíduos que mais informação publicam têm um risco percebido de vitimação menor? Esta baixa percepção do risco influenciará a falta de vontade em adotar comportamentos de segurança? Ou, por outro lado, eventuais vitimações prendem-se com falhas de segurança do *software* e não por mão humana?

Futuras investigações devem, também, procurar medir os conhecimentos informáticos de acordo com determinados critérios, e não de acordo com a percepção. Será que ter elevados conhecimentos informáticos é suficiente para que um indivíduo sinta menos medo *online*? Ou, será que, com um real conhecimento informático, o utilizador patenteia melhor os reais perigos das TIC? Por outro lado, será que um melhor conhecimento informático predispõe o utilizar com maiores probabilidades de evitar vitimações *online*? Vários estudos empíricos têm referido a importância de educar e sensibilizar as pessoas quanto ao uso dos dispositivos informáticos e da *Internet* para melhor se protegerem (e.g., Curso Geral de Cibersegurança, do CNCS). Contudo, a divulgação dessas campanhas passa muitas vezes despercebidas ao olhar público, seja por falta de vontade ou porque têm uma falsa proteção percebida das suas capacidades e conhecimentos informáticos.

BIBLIOGRAFIA

- Bocij, P. (2003). *Victims of cyberstalking: An exploratory study of harassment perpetrated via the internet*. First Monday, 8,10. doi:org/10.5210/fm.v8i10.1086
- Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. USA: Praeger Publishers.
- 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).
- Brody, R. G., Mulig, E., & Kimball, V. (2007). *PHISHING, PHARMING AND IDENTITY THEFT*. *Academy of Accounting & Financial Studies Journal*, 11(3).
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.), Lawrence Erlbaum Editors.
- Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, 16, 41-96.
- Dias, V. (2010). *A Problemática da Investigação do Cibercrime*. IDPCC, Faculdade de Direito.
- Emmanouilides, C., & Hammond, K. (2000). *Internet usage: Predictors of active users and frequency of use*. *Journal of Interactive Marketing*, 14(2), 17–32. doi:10.1002/(sici)1520-6653(200021)14:2<17::aid-dir2>3.0.co;2-e
- 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.
- Garofalo, J. (1981). The Fear of Crime: Causes and Consequences. *Journal of Criminal Law and Criminology* 72(2), p. 839–857.
- Ferraro, K. F., & Grange, R. L. (1987). *The Measurement of Fear of Crime*. *Sociological Inquiry*, 57(1), 70–97. doi:10.1111/j.1475-682x.1987.tb01181.x
- Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. SUNY [State University of New York] Press, Albany.
- OU Ferraro, K. (1995). *Fear of crime: interpreting the victimization risk*. New York: State University of New York Press.
- Ferraro, K. F. (1996). *Women's fear of victimization: Shadow of sexual assault?*. *Social forces*, 75(2), 667-690.
- Furnell, S. (2002). *Cybercrime: Vandalizing the information society* (p. 3-540). London: Addison-Wesley.
- Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies* 10(2), p. 243–249.
- Gray, E., Jackson, J. & Farral, S. (2008). *Reassessing the fear of crime*. *European Journal of Criminology*, 5(3), 363–380.

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.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25.

Jackson, J. (2004). *Experience and expression: social and cultural significance in the fear of crime*. *The British Journal of Criminology*, 44(6), 946-966.

Marchesini, S. (2015). O stalking nos acórdãos da Relação de Portugal: a compreensão do fenómeno antes da tipificação. *Revista Configurações*, 16, 55-74. <https://doi.org/10.4000/configuracoes.2847>

Melander, L. A. (2010). *College Students' Perceptions of Intimate Partner Cyber Harassment*. *Cyberpsychology, Behavior, and Social Networking*, 13(3), 263–268. doi:10.1089/cyber.2009.0221

Miró, F. (2014). Routine Activity Theory. *The Encyclopedia of Theoretical Criminology*, p. 1–7. doi:10.1002/9781118517390.wbetc198

Miró, F. (2014). Routine Activity Theory. In Miller, J. M. (Ed.), *The Encyclopedia of Theoretical Criminology*, (nº do volume, nºs das páginas). Local de publicação: Editor
Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148–169.

Pereira, F., & Matos, M. (2015a). *Cyberstalking entre adolescentes: Uma nova forma de assédio e perseguição? [Cyber-stalking among adolescents: A new form of harassment and persecution?]* *Psicologia, Saúde & Doenças [Psychology, Health & Diseases]*, 16. <http://dx.doi.org/10.15309/15psd160207>.

Pereira, F., & Matos, M. (2015b). *Cyber-stalking victimization: What predicts fear among Portuguese adolescents?* *European Journal on Criminal Policy and Research*, 1e18. <http://dx.doi.org/10.1007/s10610-015-9285-7>.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267-296.

Rader, N. E. (2004). *The threat of victimization: A theoretical reconceptualization of fear of crime*. *Sociological Spectrum*, 24(6), 689-704.

Reyns, W. (2010). *A Situational Crime Prevention Approach to Cyberstalking Victimization: Preventive Tactics for Internet Users and Online Place Managers*. *Crime Prevention and Community Safety* 12:99–118.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). *Being Pursued Online*. *Criminal Justice and Behavior*, 38(11), 1149–1169. doi:10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). *Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students*. *Deviant Behavior*, 33(1), 1–25. doi:10.1080/01639625.2010.538364

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.

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.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, 4(1), 66–78. doi:10.1177/14614440222226271.

Spitzberg, B. H., & Cupach, W. R. (2007). *The state of the art of stalking: taking stock of the emerging literature*. *Aggression and Violent Behavior: A Review Journal*, 12, 64–86. doi:10.1016/j.avb.2006.05.001.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A Cybercrime Incident Architecture with Adaptive Response Policy. *Computers & Security*. doi:10.1016/j.cose.2019.01.011

Venâncio, P. D. (2011). *Lei do Cibercrime: anotada e comentada*. Coimbra Editora.

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, 24(3), 323–338.

Wall, D. S. (2001). *Cybercrimes and the internet*. In D. S. Wall (Ed.), *Crime and the internet* (pp. 1-17). New York: Routledge.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, 22(1–2), 45–63.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime. *Information, Communication & Society*, 11(6), 861-884.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. POLITY.

Wall, David S. (2007). *Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace* (Revised Feb 2011) (May 2, 2007). *Police Practice and Research: An International Journal*, Vol. 8, No. 2, pp. 183-205, May 2007, Available at SSRN: <https://ssrn.com/abstract=853225>

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.

Law, J. (2018). *A Dictionary of Law*. Oxford Reference. <https://www.oxfordreference.com/view/10.1093/acref/9780198802525.001.0001/acref-9780198802525>

Saldo Positivo, Caixa Geral de Depósitos. (2019, dezembro, 06). *A DSP2 veio mudar a forma como são feitas as transações eletrónicas, simplificando os pagamentos e aumentando o grau de segurança*. <https://www.cgd.pt/Site/Saldo-Positivo/guias-e-infografias/Pages/DSP2-O-que-muda.aspx>

Observatório de Cibersegurança, Centro Nacional de Cibersegurança. (2021). *Cibersegurança em Portugal: Riscos & Conflitos*. CNCS.

International Criminal Police Organization. (2020, agosto, 4). *Cybercrime: Covid-19 Impact*. INTERPOL.

European Commission, © European Union. (2020, janeiro). *Special Eurobarometer 499, Europeans' attitudes towards cyber security*, Cybersecurity. <https://europa.eu/eurobarometer/surveys/detail/2249>

ANEXOS

ANEXO 1 – Análise fatorial dos itens da exposição *online*

Itens exposição <i>online</i>	Fator		
	1	2	3
Uso do banco <i>online</i> ou gestão de finanças		.79	
Comprar bens ou serviços na <i>Internet</i>		.75	
Uso do e-mail ou mensagens instantâneas		.55	
Utilização de redes sociais (e.g. Facebook, Instagram, LinkedIn)	.67		
Atualização diária das suas redes sociais			.53
Ler notícias, blogs ou fóruns			
Participar ativamente em salas de chat ou outros fóruns			.71
Interação em <i>websites</i> de encontros/fazer amizades (e.g. Tinder, Omegle)			.60
Fazer downloads de músicas, filmes, jogos ou podcasts	.57		
Visualização de conteúdo de entretenimento (e.g. Youtube, Twitch, Netflix, Spotify)	.78		

Nota: O método de extração foi “Principal Component Analysis” com rotação (Varimax com Normalização Kaiser) ortogonal. Coeficientes dos fatores >0.50.

ANEXO 2 – Análise fatorial dos itens do alvo adequado

Itens do alvo adequado	Fator		
	1	2	3
Comunicou com desconhecidos <i>online</i>			.80
Abriu anexos ou <i>links</i> desconhecidos recebidos por e-mail	.75		
Abriu anexos ou ficheiros recebidos através de mensagens instantâneas de alguém desconhecido	.85		
Forneceu voluntariamente os seus dados pessoais a alguém desconhecido			.66
Clicou em mensagens pop-up		.81	
Visitou <i>websites</i> duvidosos		.76	

Nota: O método de extração foi “Principal Component Analysis” com rotação (Varimax com Normalização Kaiser) ortogonal. Coeficientes dos fatores >0.50.

ANEXO 3 – Itens da exposição *online* em atividades e alvo adequado a partir da TAR e respectivos alfas de *Cronbach* que indicam a consistência interna.

Fator	alfa	Descrição dos itens: Exposição <i>online</i> em atividades
Exposição económica	.647	Uso do banco <i>online</i> ou gestão de finanças Compra de bens ou serviços na <i>Internet</i>
Exposição interativa	.414	Participar ativamente em fóruns Interação em <i>websites</i> de encontros/fazer amizades (e.g. Tinder, Omegle)
Exposição de entretenimento	.571	Utilização de redes sociais (e.g. Facebook, Instagram, LinkedIn) Fazer download de músicas, filmes, jogos ou podcasts Visualização de conteúdo de entretenimento (e.g. Youtube, Twitch, Netflix, Spotify)
Descrição dos itens: Alvo adequado		
Abrir ficheiros desconhecidos	.584	Abriu anexos ou <i>links</i> desconhecidos recebidos por email Abriu anexos ou ficheiros, recebidos através de mensagens instantâneas de alguém desconhecido
Comunicar ou fornecer dados a desconhecidos	.300	Comunicou com desconhecidos <i>online</i> Forneceu voluntariamente os seus dados pessoais a alguém desconhecido
Uso de risco da <i>Internet</i>	.493	Clicou em mensagens pop-up Visitou <i>websites</i> duvidosos

ANEXO 4 – Itens do medo, percepção do risco de vitimação e vitimação *online*, e respectivos alfas de *Cronbach* que indicam a consistência interna.

Fator	alfa	Descrição dos itens: Medo, percepção do risco de vitimação e vitimação <i>online</i>
Medo vitimação <i>online</i>	.816	Medo de fraude ao consumidor <i>online</i> Medo de furto de identidade <i>online</i> Medo de cyberbullying Medo de <i>cyberstalking</i> Medo de descobrir <i>software</i> malicioso
Percepção do risco de vitimação <i>online</i>	.792	Percepção do risco da fraude ao consumidor <i>online</i> Percepção do risco do furto de identidade <i>online</i> Percepção do risco do cyberbullying Percepção do risco do <i>cyberstalking</i> Percepção do risco de descobrir <i>software</i> malicioso
Vitimação <i>online</i>	.493	Fraude ao consumidor <i>online</i> Furto de identidade <i>online</i> Cyberbullying <i>Cyberstalking</i> Descobrir <i>software</i> malicioso <i>Phishing</i>

Tabela 21 Percentagem dos indivíduos mediante o tipo de dispositivo informático utilizado e o local onde acedem à *Internet*.

Variáveis	N	%
Tipo de dispositivo informático		
<i>Smartphone</i>	658	90.6
Computador	645	88.8
Tablet	89	12.3
TV	89	12.3
Consola de jogos	23	3.2
Local de acesso		
Casa	711	97.9
Trabalho/Escola	306	42.1
Local público sem WiFi	113	15.6
Local publico com WiFi	42	5.8

ANEXO 5 – *Testes-t*: medo de cibercrime em função do tipo de dispositivo informático e local de acesso à *Internet*.

Variáveis	Descrição	Medo de Cibercrime		
		N	(X±S.D)	p
Dispositivo informático	<i>Smartphone</i>	Não	68 2.71±0.71	.004
		Sim	658 2.96±0.68	
	Computador	Não	81 3.01±0.61	.258
		Sim	645 2.92±0.69	
	Tablet	Não	637 2.93±0.69	.499
		Sim	89 2.98±0.67	
	TV	Não	637 2.92±0.68	.330
		Sim	89 3±0.70	
	Consola de jogos	Não	703 2.94±0.68	.020
		Sim	23 2.60±0.58	
Local de acesso à Internet	Casa	Não	15 3.11±0.75	.323
		Sim	711 2.93±0.68	
	Trabalho/Escola	Não	420 2.90±0.69	.152
		Sim	306 2.98±0.68	
	Local público sem WIFI	Não	613 2.92±0.69	.396
		Sim	113 2.98±0.67	
	Local público com WIFI	Não	684 2.93±0.68	.646
		Sim	42 2.98±0.75	

ANEXO 6 – Qui-quadrado: prevalência da vitimação *online* em função do tipo de dispositivo informático e local de acesso à *Internet*.

Variáveis	Descrição		NV	V	X ²	p
Dispositivo informático	<i>Smartphone</i>	Não	3.3%	6.1%	.528	.467

Local de acesso à Internet	Computador	Sim	36.1%	54.5%	.556	.456
		Não	4.8%	6.3%		
	Tablet	Sim	34.6%	54.3%	.228	.633
		Não	34.8%	52.9%		
	TV	Sim	4.5%	7.7%	3.381	.066
		Não	33.5%	54.3%		
	Consola de jogos	Sim	5.9%	6.3%	3.101	.078
		Não	38.7%	58.1%		
	Casa	Sim	0.7%	2.5%	.002	.961
		Não	0.8%	1.2%		
	Trabalho/Escola	Sim	38.6%	59.4%	.297	.586
		Não	23.3%	34.6%		
	Local público sem WIFI	Sim	16.1%	26%	.012	.914
		Não	33.3%	51.1%		
	Local público com WIFI	Sim	6.1%	9.5%	.022	.882
		Não	37.1%	57.2%		
		Sim	2.3%	3.4%		
		Não				

Nota: os testes qui-quadrado apresentados são analisados à luz do modelo qui-quadrado de Pearson

Modelo 1 – Variáveis sociodemográficas e medo do cibercrime

ANEXO 7 – MODELO 1 – Predição do medo do cibercrime segundo as variáveis sociodemográficas (variáveis independentes).

Variável	B	SE B	β	t	p
Género	-.515	.088	-.362	-5.833	.000
Idade	.003	.004	.048	.687	.492
Escolaridade	-.109	.024	-.321	-4.468	.000
Estado civil	-.072	.096	-.053	-.756	.450
Teletrabalho	-.079	.090	-.058	-.876	.382
Zona de residência	.043	.097	.028	.445	.657

Nota: $r = .448$; $r^2 = .201$; r^2 ajustado = .180 ($p = .000$);

Modelo 2 – Teoria das Atividades de rotina e medo do cibercrime

ANEXO 8 – MODELO 2 – Predição do medo do cibercrime segundo as variáveis referentes à TAR (variáveis independentes).

Componente	Variável	B	SE B	β	t	p
Exposição online	Horas por dia	.043	.027	.059	1.576	.115
	Económica	-.043	.030	-.053	-1.450	.148
	Interativa	-.041	.052	-.030	-.794	.428
	Entretenimento	.180	.040	.176	4.514	.000

Alvo adequado	Abrir ficheiros desconhecidos	.235	.074	.123	3.189	.001
	Comunicar ou fornecer dados a desconhecidos	-.085	.056	-.063	-1.520	.129
	Uso de risco da <i>Internet</i>	-.080	.063	-.050	-1.280	.201
Guardião	Informação disponibilizada <i>online</i>	.027	.012	.092	2.303	.022
	Índice do guardião	.042	.011	.139	3.691	.000
	Conhecimento informático	-.201	.041	-.179	-4.841	.000

Nota. $r = .319$; $r^2 = .102$; r^2 ajustado = .089 ($p = .000$);

Modelo 3 – Insegurança económica, insegurança geral, medo *offline* interpessoal e propriedade, risco percebido *online*, vitimação *online* e medo do cibercrime.

ANEXO 9 – MODELO 3 – Predição do medo do cibercrime segundo a insegurança económica, insegurança geral, medo *offline* interpessoal e propriedade, percepção do risco de vitimação *online* e vitimação *online* (variáveis independentes).

Variável	B	SE B	β	t	p
Insegurança económica	.039	.008	.146	4.790	.000
Insegurança geral	-.001	.019	-.002	-.063	.950
Medo <i>offline</i> interpessoal	.160	.023	.302	7.059	.000
Medo <i>offline</i> propriedade	.164	.023	.274	7.150	.000
Risco percebido <i>online</i>	.258	.037	.201	7.053	.000
Vitimação <i>online</i>	-.086	.039	-.061	-2.190	.029

Nota. $r = .669$; $r^2 = .447$; r^2 ajustado = .443 ($p = .000$);

Modelo 1 – Variáveis sociodemográficas e vitimação *online*

ANEXO 10 – Predição da chance de vitimação *online* segundo as variáveis sociodemográficas (variáveis independentes).

Variável	B	SE B	Wald	OR	P
Idade	.005	.007	.526	1.005	.468
Escolaridade	.192	.052	13.845	1.212	.000
Rendimentos	-.232	.091	6.526	.793	.011

Nota. -2 Log likelihood = 947.006; Nagelkerke $R^2 = .045$ ($p = .000$).

Modelo 2 – Teoria das Atividades de Rotina, percepção do risco de vitimação *online* e vitimação *online*

ANEXO 11 – Predição da chance de vitimação *online* segundo as variáveis constituintes da TAR e ao percepção do risco de vitimação *online* (variáveis independentes).

Componente	Variável	B	SE B	Wald	OR	P
Exposição <i>online</i>	Horas por dia	.133	.089	2.248	1.142	.134
	Económica	.115	.098	1.380	1.122	.240
	Interativa	.023	.174	.017	1.023	.897

	Entretenimento	-.394	.132	8.885	.675	.003
	Abrir ficheiros desconhecidos	-.144	.258	.311	.866	.577
Alvo adequado	Comunicar ou fornecer dados a desconhecidos	.857	.210	16.660	2.356	.000
	Uso de risco da <i>Internet</i>	.335	.219	2.334	1.398	.127
	Informação disponibilizada <i>online</i>	.029	.038	.595	1.030	.440
Guardião	Índice do guardião	.064	.038	2.856	1.066	.091
	Conhecimento informático	.212	.137	2.398	1.236	.121
	Risco percebido <i>online</i>	.470	.157	9.019	1.600	.003

Nota. -2 Log likelihood=919.771; Nagelkerke R²=.097 (p=.000).

ANEXOS DA ANÁLISE EXPLORATÓRIA

Anexo 12 – Itens do medo/vitimação *online* relativo às componentes propriedade e interpessoal, e respetivos alfas de *Cronbach* que indicam a consistência interna.

Fator	alfa	Descrição dos itens: Vitimação/medo <i>online</i> propriedade e interpessoal
Medo propriedade <i>online</i>	.520	Medo de fraude ao consumidor <i>online</i> Medo de furto de identidade <i>online</i>
Medo interpessoal <i>online</i>	.877	Medo de <i>cyberstalking</i> Medo de cyberbullying
Vitimação propriedade <i>online</i>	.159	Fraude ao consumidor <i>online</i> Furto de identidade <i>online</i>
Vitimação interpessoal <i>online</i>	.594	<i>Cyberstalking</i> Ciberbullying

ANEXO 13 – Médias do medo *online* geral e respetivas componentes (propriedade e interpessoal).

Índices	N	X	SD	Min	Max
Medo do cibercrime	726	2.93	0.68	1	4
Medo do cibercrime propriedade	726	3.09	0.64	1	4
Medo do cibercrime interpessoal	726	2.66	0.99	1	4

ANEXO 14 – Medo de vitimação *online* e *offline* controlando para o género.

Variáveis	Mulheres (X±S.D)	Homens	p
Medo de vitimação <i>online</i>	3.08±0.63	2.59±0.68	.000
Medo de vitimação <i>online</i> propriedade	3.20±0.60	2.87±0.67	.000
Medo de vitimação <i>online</i> interpessoal	2.88±0.92	2.14±0.94	.000
Insegurança geral	3.10±1.12	2.07±0.95	.000
Medo <i>offline</i> interpessoal	3.80±1.07	2.22±1.05	.000
Medo <i>offline</i> propriedade	3.60±1.07	2.86±1.13	.000